

Sella

Web3: la banca nel mondo dei Digital Assets

Manuale multidisciplinare sui digital assets, sulla nascita del “web3”
e sulla finanza costruita sui distruted ledger technologies (DLTs)

Come leggere il manuale

Questo manuale è composto da **8 capitoli divisi in macro-blocchi formativi** qui elencati:

Capitolo 1. Introduzione

1.	DLT e panoramica sui Digital Assets	12
2.	Analisi generale fintech e legaltech	14
3.	Elenco di soft skills fornite dal manuale	15

Capitolo 2. Trust Machine

1.	Il valore	22
2.	Internet	27
3.	Reti Peer to Peer	36
4.	Il nodo nella rete Peer to Peer	46
5.	Root of Trust e crittografia	60
6.	Le regole, la governance e il consenso distribuito	68
7.	The Protocol Money	81

Capitolo 3. Web3

1.	L'economia nel Web3	94
2.	La programmabilità e gli Smart Contract	102
3.	Applicazioni Decentralizzate (dApps)	113
4.	dApps e Tokenomics	123
5.	NFT	130
6.	Decentralized Autonomous Organization (DAO)	138
7.	Approfondimenti su Token e Smart Contract	144

Capitolo 4. Costruire sul web3

1.	Da dove parto a costruire nel Web3?	158
2.	Chi gestisce il nodo e le informazioni?	164
3.	Scalabilità	174
4.	Privacy	183
5.	Interoperabilità	188
6.	Cosa posso salvare sulla blockchain?	196
7.	Metaverso	202
8.	Identità Digitale	210

Capitolo 5. Banca e pagamenti nel Web3

1.	I sistemi monetari	222
2.	I sistemi di clearing e settlement	234
3.	I pagamenti nel Web3	247
4.	CBCD	266

Capitolo 6. Banca e investimenti nel Web3

1.	L'uomo e il processo di misurazione del valore	280
2.	Il modello di maturità del mercato Web3	287
3.	I servizi del mondo banking nel mercato Web3	296
4.	Prodotti derivati sul mercato Web3	308
5.	Bitcoin come digital asset	314

Capitolo 7. La gestione del rischio nel Web3

1.	Introduzione al rischio	342
2.	Analisi rischio tecnologico per area pagamenti	346
3.	Analisi rischio tecnologico per area investimenti (CEX)	354
4.	Analisi rischio tecnologico per area investimenti (DEX)	361
5.	Analisi rischio legal e compliance per area investimenti e pagamenti	369
6.	Overview normativa sull'identità digitale	384

Conclusioni

Considerazioni Finali	388
Ringraziamenti	389

Questi 8 capitoli hanno al loro interno 37 macro-blocchi formativi, i quali descrivono le **macroaree concettuali** riferite al web3, ai digital assets e alle distributed ledger technologies.

Ogni **macro-blocco** formativo a sua volta ha dei **micro-blocchi che lo compongono** con argomenti specifici, per approfondire il singolo argomento in tutti suoi aspetti.

Come leggere il manuale

Questo manuale è pensato con una logica che ti permette sia di leggerlo nella sua integralità, sia di farti concentrare solo sulle nozioni chiave da te ricercate o per te necessarie. Per agevolare questo processo di scoperta, abbiamo disegnato dei **percorsi formativi** interni ai capitoli così da leggere solamente i blocchi per te più interessanti.

Partiamo da una semplice domanda: sei un neofita o conosci già l'argomento? **Se è la prima volta in assoluto che affronti questo argomento, ti consigliamo di seguire il percorso principale, per poi deviare, qualora fosse per te di interesse, verso gli altri 4 percorsi tematici.** Il manuale è composto da oltre 200 blocchi formativi ed il lettore potrà comporre **la sua catena di blocchi, creando il suo personale percorso formativo.**

Ogni blocco formativo proposto nel libro avrà un titolo, **una legenda laterale** per posizionare il blocco all'interno di uno o più percorsi, **un parametro di difficoltà** rispetto all'approfondimento e **la descrizione dell'area disciplinare** che si andrà ad esaminare.

Difficoltà	Dove ti trovi?
Basic	Per chi è alle prime armi
Medium	Per chi vuole approfondire
Hard	Per chi ha una conoscenza approfondita

Se invece parti da un livello più alto e pensi di conoscere già i concetti chiave del funzionamento del web3, della blockchain e dei digital assets, puoi partire direttamente da alcuni percorsi formativi più verticali e specifici, o leggere direttamente il capitolo che interessa di più.

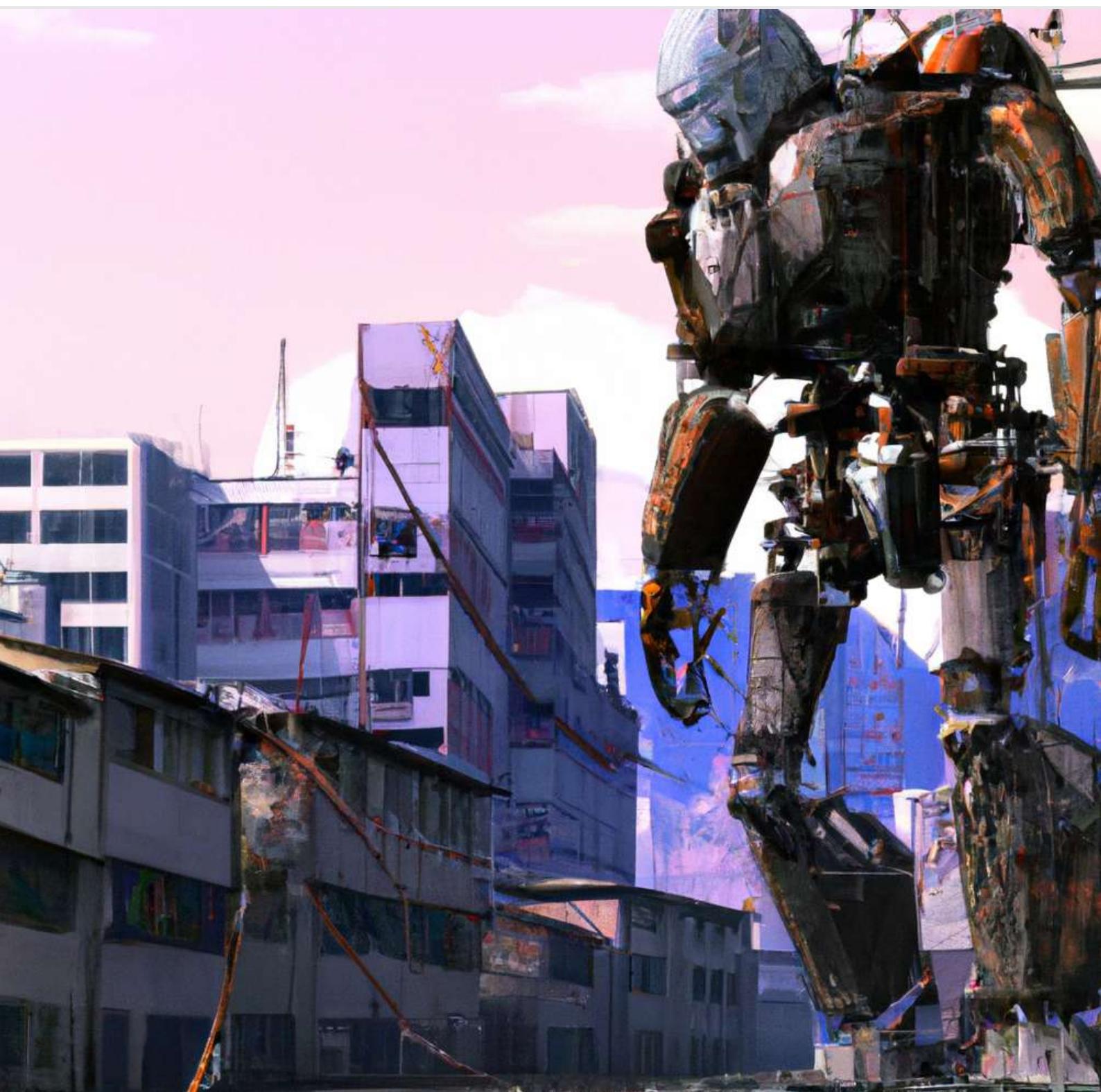
Percorsi	Descrizione	Capitolo di riferimento
PRINCIPALE	Percorso pensato per tutti coloro che per la prima volta si affacciano al mondo del web3 , volto a dare le informazioni base per affrontare gli altri percorsi	2, 3, 4, 5, 6, 7
PAGAMENTI	Percorso pensato per tutti coloro che lavorano nel settore dei pagamenti e approfondisce i temi del web3 e digital assets come strumenti per i pagamenti programmabili	2, 3, 4, 5
WEALTH	Percorso pensato per tutti coloro che lavorano nell'area degli investimenti, del trading e del wealth management, approfondendo i digital assets come strumento di investimento e nuova asset class	3, 4, 5, 6
RISCHIO	Percorso pensato per coloro che occupano posizioni in aree di business, per il settore di pagamenti ed investimenti, nel quale vengono descritti quali possono essere i rischi di cybersecurity, legali e di conformità per i servizi relativi al web3 e ai digital asset	2, 3, 4, 5, 6, 7
INNOVAZIONE	Percorso pensato per coloro che conoscono già l'argomento e vogliono approfondire la tecnologia in tutti suoi aspetti e i possibili campi di applicazione per innovare	2, 3, 4, 5, 6, 7

Per agevolare il lettore nel comprendere quale percorso seguire, abbiamo creato una tabella con una lista di possibili famiglie professionali e percorsi professionali a cuiabbiamo indirizzato i 4 percorsi tematici

Label	Percorso Formativo	Famiglia Professionale Suggerita	Profilo professionale Suggerito
	INNOVATION	<i>Transformation & Innovation</i> <i>IT</i> <i>Prodotti e servizi aziende</i> <i>Prodotti e servizi di Wealth e Asset Management</i> <i>Privacy</i>	<i>IT Project Manager</i> <i>Digital Product Manager</i> <i>Product Manager</i> <i>Analista Tecnico Funzionale</i> <i>Application Software Developer</i> <i>Full Stack Developer</i> <i>Front-end Developer</i> <i>Back-End Developer</i> <i>Business Development Specialist</i> <i>Database Administration</i>
	PAGAMENTI	<i>Privacy</i> <i>Risk Management e Antiriciclaggio</i> <i>Transformation & Innovation</i> <i>Prodotti e servizi banking e sistemi di pagamento</i> <i>Amministrazione e BPO</i> <i>Treasury & Financial Markets</i>	<i>Anti Fraud Specialist</i> <i>It Project Manager</i> <i>Business Owner</i> <i>Product Owner</i> <i>Product Manager</i> <i>Open Innovation Specialist</i> <i>Specialista Amministrazione sistemi di pagamento</i> <i>Tesoriere</i>
	WEALTH	<i>Treasury & Financial Markets</i> <i>Gestioni Patrimoniali</i> <i>Corporate & Investment Banking</i> <i>Consulenza Wealth & Business Advisory</i> <i>Consulenza Investment / Private Banking</i> <i>Gestione Fondi</i>	<i>Analista finanziario</i> <i>Analista Macroeconomico</i> <i>Addetto Succursale Private Banking</i> <i>Business Analyst</i> <i>CIB Analyst</i> <i>Cib Executive Director</i> <i>Consulente Finanziario</i> <i>Direttore Investimenti</i> <i>Portfolio Manager</i> <i>Private Banker</i>
	RISK	<i>Risk Management</i> <i>E Antiriciclaggio</i> <i>Privacy</i> <i>IT</i> <i>Prodotti e servizi banking e sistemi di pagamento</i> <i>Prodotti e servizi wealth e asset management</i>	<i>AML risk Specialist</i> <i>Product Owner</i> <i>Business Owner</i> <i>IT Team Leader</i> <i>IT Project Manager</i> <i>IT Delivery Manager</i> <i>Business Analyst</i> <i>Product owner</i> <i>Capital Risk Specialist</i> <i>Credit Risk Specialist</i>

Capitolo 1

INTRODUZIONE



Introduzione

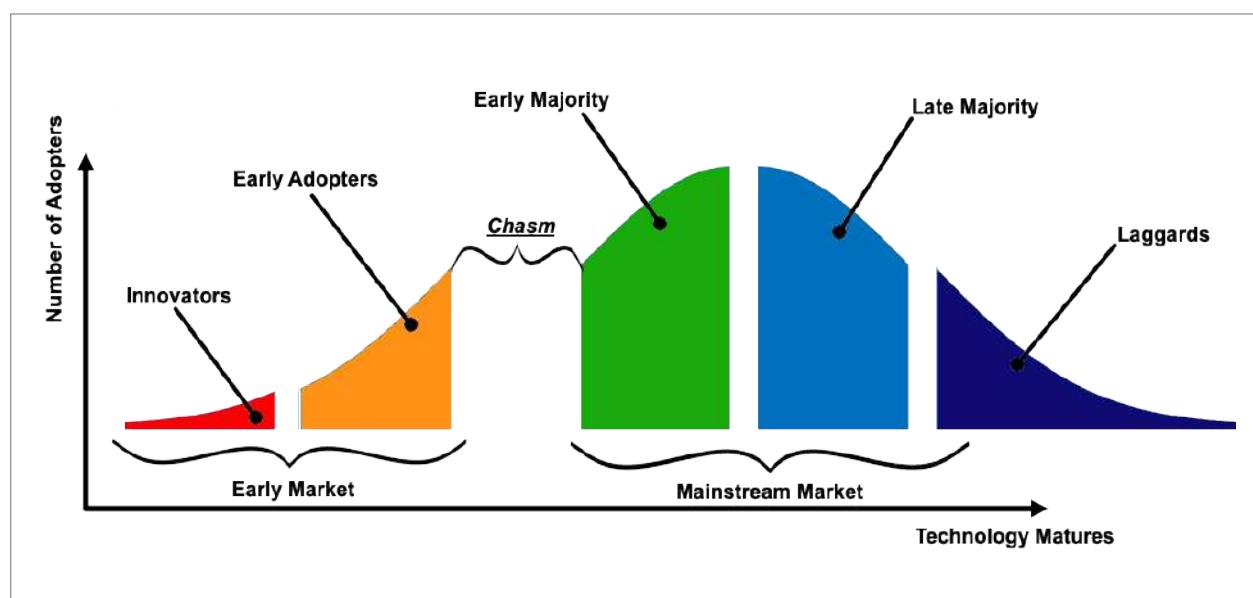
- DLT e Panoramica sui Digital Assets
- Analisi generale fintech e legaltech
- Elenco soft skills fornite dal libro per un team cross function

DLT e Panoramica sui Digital Assets

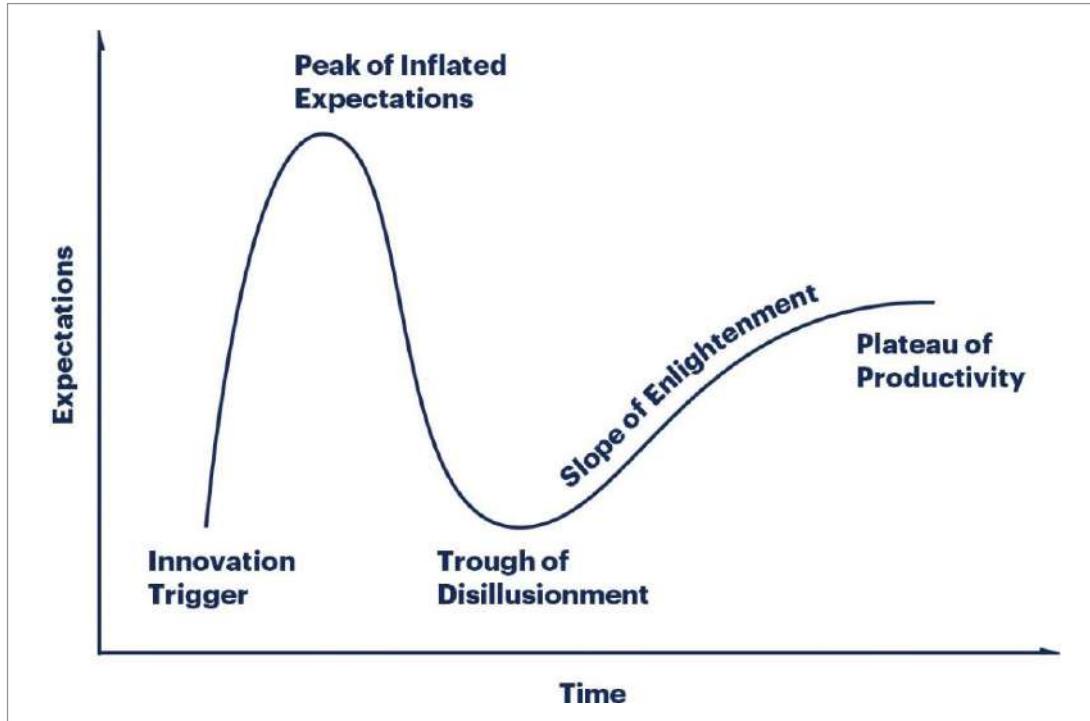
Il mondo dei digital assets e dei registri distribuiti sta vivendo un'espansione senza precedenti. Questo **manuale interdisciplinare** esplora la tecnologia alla base degli stessi, nonché le implicazioni normative e le opportunità per il futuro, affrontando tematiche quali blockchain, crittografia, quadro normativo globale e tanto altro. A titolo di esempio, vedremo come la tecnologia blockchain sta cambiando il modo in cui le aziende gestiscono i contratti e i pagamenti, e come i regolatori stanno cercando di affrontare le sfide poste dalla decentralizzazione delle valute digitali. Questi includono non solo l'aspetto tecnologico della blockchain e del web3, ma anche i fattori di mercato, l'adozione da parte del pubblico e la regolamentazione.

Ogni tecnologia *disruptive* ha i suoi tempi per l'adozione, per la sostituzione, e per la sua accettazione da parte del pubblico, processo che avviene, usualmente, solo dopo averne compreso i benefici, a causa di una necessità, o sulla base di requisiti e orientamenti normativi. Al fine di meglio comprendere l'evoluzione delle tecnologie, vi sono alcuni modelli che possono aiutare a comprendere meglio l'innovazione e le sue fasi attraverso gli occhi dell'utente.

Tra le varie, le due più interessanti sono la teoria del baratro di Moore e la Curva di Gartner (Hype Cycle), due **modelli di analisi dell'adozione di nuove tecnologie o prodotti**. Entrambi i modelli si basano su una curva di adozione dell'innovazione che descrive il percorso di adozione da parte di diversi gruppi di utenti, ma differiscono nella loro suddivisione dei gruppi e nella loro applicazione.



La **teoria del baratro di Moore** suddivide i gruppi di utenti in cinque fasi: innovatori, early adopters, early majority, late majority e ritardatari, e si concentra sulla discontinuità tra early adopters e early majority, rappresentata dal “baratro”. La teoria suggerisce che per superare il baratro, le aziende e tutti gli stakeholders all'interno di una industria come il web devono adottare una strategia di marketing in grado di aiutare l'utente a comprendere i reali vantaggi della tecnologia, creando una base utente abbastanza estesa che consenta una successiva crescita organica.



La **Curva di Gartner**, d'altra parte, suddivide le cinque fasi emotive, di un utente e della massa, quando entra nel mercato una nuova tecnologia disruptive come segue: Innesco dell'Innovazione, Picco di aspettative gonfiate, Gola della Disillusione, Crescita ed illuminazione e Plateau della Produttività. Questa curva descrive l'andamento del mercato delle nuove tecnologie in termini di hype, aspettative e disillusioni, e suggerisce che le tecnologie passano attraverso una fase di hype eccessivo prima di raggiungere la maturità. Spesso, inoltre, questa curva è anche rappresentativa dell'umore dei mercati, e delle conseguenti “bolle” o “speculazioni” attorno ad argomenti innovativi e complessi come i digital assets-asset e la DLT.

Mentre la teoria del baratro di Moore si concentra sulla sfida di superare il baratro tra **early adopters e early majority**, la Curva di Gartner si concentra sull'andamento del mercato delle nuove tecnologie nel suo insieme e sulla necessità di **superare la fase di hype eccessivo**.

Entrambi i modelli hanno vantaggi e limitazioni nell'analisi dell'adozione di nuove tecnologie o prodotti. La teoria del baratro di Moore fornisce una visione più dettagliata delle fasi di adozione dell'innovazione e offre una guida pratica per la definizione delle strategie di marketing, mentre la Curva di Gartner fornisce una visione più ampia del mercato delle nuove tecnologie e aiuta a prevedere le tendenze future. Inoltre, entrambi i modelli evidenziano l'importanza della comprensione dei comportamenti degli utenti e della definizione di strategie di marketing efficaci per raggiungere il pubblico di massa.

Ecco una lista di considerazioni rispetto all'adozione del web3 e di bitcoin utilizzando la Chasm Theory e la Curva di Gartner.

Teoria del Chiasmo:

- Il successo dell'adozione del web3 e dei digital assets dipenderà dal superamento della fase del “chasm”, ovvero il divario tra gli innovatori iniziali e la maggioranza degli utenti.
- Per superare il chiasmo, è necessario che ci sia una forte attenzione sulla creazione di una esperienza utente semplice, intuitiva ed accessibile per l'utente medio, così come la comunicazione efficace dei vantaggi dell'utilizzo di tecnologie.

- La strategia di marketing relative all'**awareness consapevole** e la capacità di raggiungere la massa critica di adozione saranno fattori chiave per superare il chasm.
- Una volta superato il chasm, l'adozione potrebbe accelerare rapidamente, con l'entrata nella fase di crescita.

Curva di Gartner:

- L'adozione del web3 sta passando attraverso la fase dell'"innovazione precoce" in cui gli innovatori e gli early adopters sono i primi ad adottare la tecnologia, seguiti dalla fase di "adozione precoce" in cui la tecnologia inizia a diffondersi tra gli early majority.
- La fase di "maturità" vedrà l'adozione raggiungere la maggioranza degli utenti, mentre la fase di "declino" vedrà l'adozione diminuire gradualmente. L'alternarsi di tecnologie e di nuovi standard seguono queste tendenze cicliche.
- Durante la fase di "picco di aspettativa", l'attenzione sulle tecnologie sarà al massimo, ma potrebbe essere seguita da una fase di "gola della disillusione", in cui l'entusiasmo iniziale viene mitigato da difficoltà pratiche e ritardi nell'adozione di massa.
- L'adozione di massa potrebbe essere raggiunta solo dopo la fase di "Crescita ed Illuminazione", in cui la tecnologia viene adottata su larga scala e integrata nella vita quotidiana.

In sintesi, entrambi i modelli di analisi sottolineano **l'importanza della comunicazione efficace dei vantaggi dell'adozione del web3 e dei digital assets, nonché la necessità di superare sfide pratiche e di marketing per raggiungere la massa critica di adozione.**

Analisi generale fintech e legaltech

Questa rivoluzione informatica possiamo visualizzarla all'interno di tutto il trend relativo alla digitalizzazione di servizi finanziari e legali, noto come fintech e legaltech.

Per il settore Fintech, tra le prime riflessioni rispetto all'utilizzo dei digital assets e della blockchain, possiamo trovare spazi ed opportunità di mercato nei seguenti settori:

1. Pagamenti cross border utilizzando le c.d. *stablecoin*;
2. Gestione di nuovi asset digitali;
3. Tokenizzazione di prodotti finanziari;
4. Programmabilità della moneta e nuovi servizi di pagamento.

Per il settore del Legaltech, possiamo trovare spazi ed opportunità di mercato nei seguenti settori:

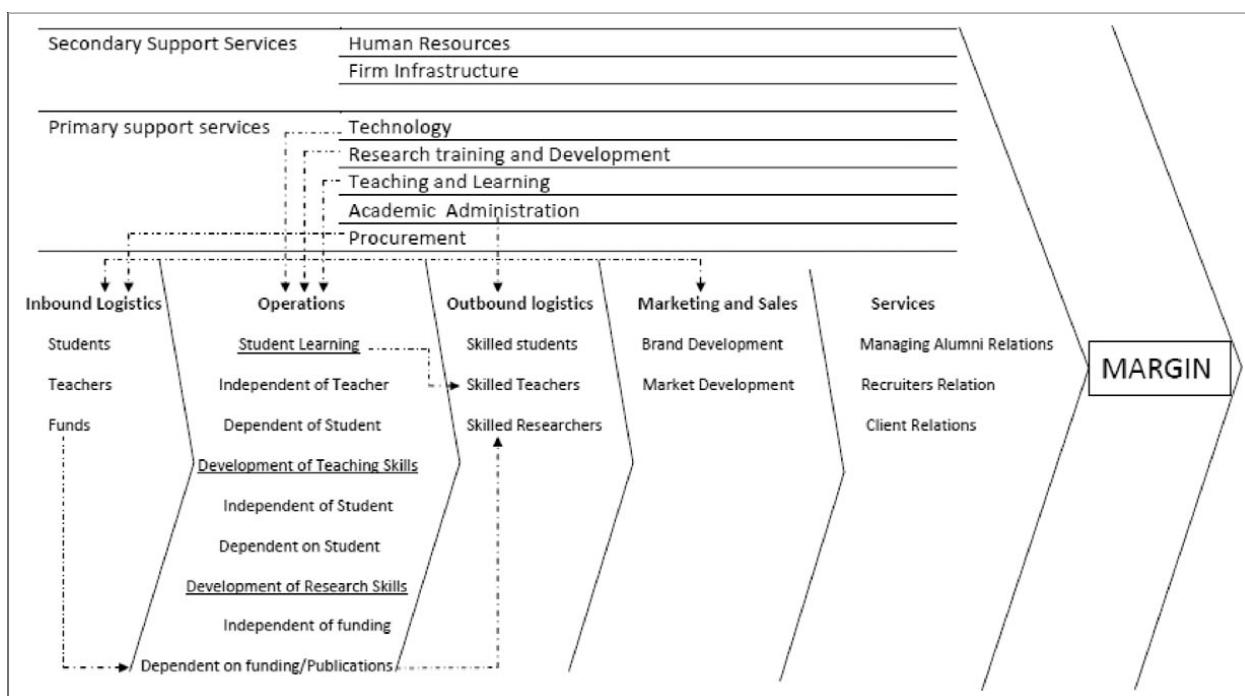
5. Creazione di Smart Legal Contracts;
6. Archiviazione di documenti su DLT;
7. Nuovi modelli di identità digitali;
8. Prodotti assicurativi innovativi e programmabili.

Speriamo che la condivisione di questo manuale possa accrescere il valore per tutti i lettori del Gruppo. Le contaminazioni di competenze all'interno di un network, come quello aziendale, sono il motore per una innovazione competitiva e robusta.

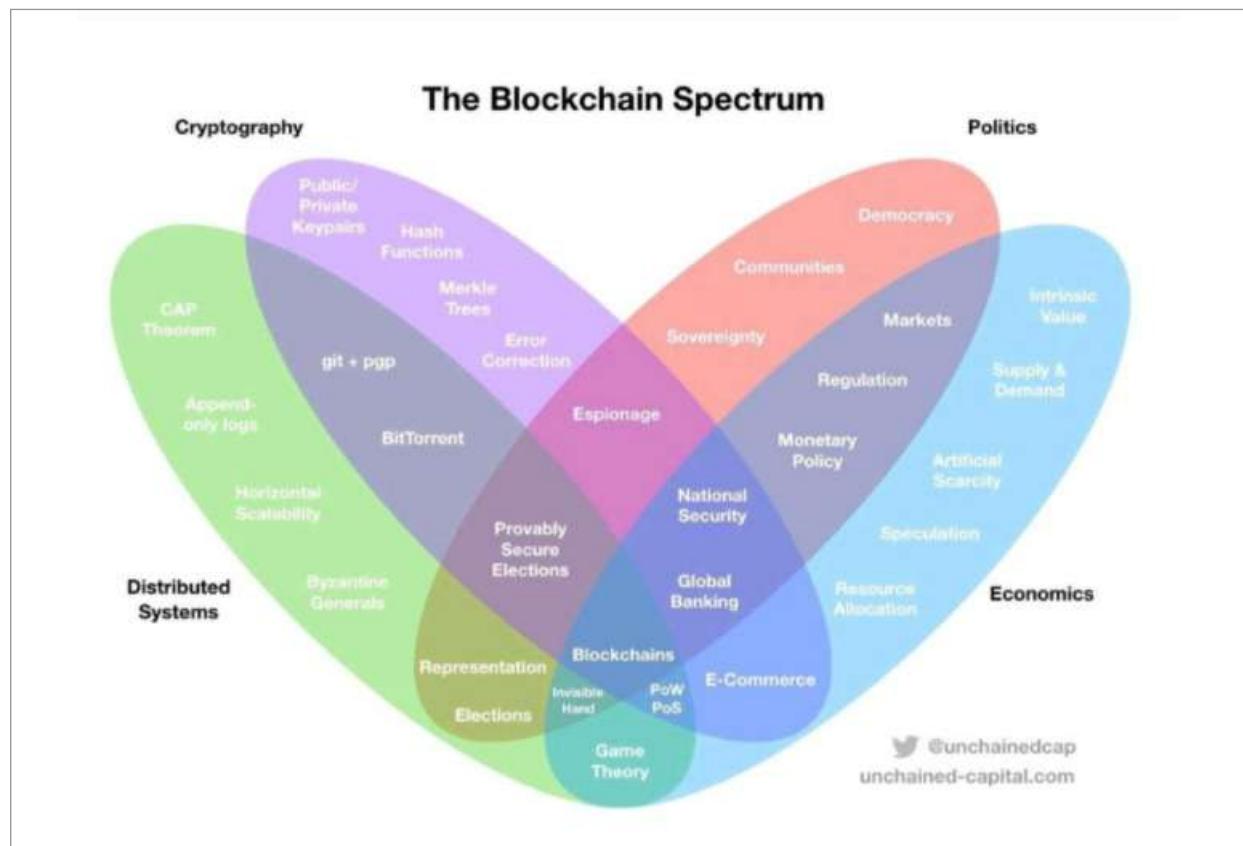
Elenco di soft skills fornite dal manuale

Secondo la teoria della Catena del Valore di Porter, la creazione di valore all'interno di un'azienda avviene attraverso una serie di attività interconnesse che vanno dalla produzione, alla distribuzione, alla commercializzazione e alla fornitura di servizi post-vendita. Tra queste attività, **l'educazione del personale è considerata un'attività primaria poiché ha un impatto diretto sulla qualità del prodotto o servizio offerto dall'azienda.**

In questo libro si affronterà l'argomento web3 e digital assets attraverso diverse lenti colorate, che saranno utilizzate per rappresentare le aree di studio di riferimento per ogni sezione nonché per indicare soft e hard skills.



Questo manuale si concentra sull'importanza delle competenze, sia "soft skills" che "hard skills", nell'ambito della formazione e della preparazione per il mondo del lavoro. Questo approccio didattico, **noto come COMB Model (Competency-Oriented Modular Basic Education)**, riconosce l'importanza di una formazione completa e multidisciplinare che includa sia le competenze tecnologiche che quelle di altre discipline, poiché capaci di dare una idea più completa e più obiettiva di una certa tematica. Il manuale non si limita a presentare il modello didattico COMB, ma si spinge oltre introducendo la teoria della complessità in filosofia. Quest'ultima teoria **si focalizza sull'importanza delle interazioni tra molti elementi nella creazione di oggetti, sistemi e processi complessi.**



Questo metodo di indagine può essere applicato alla relazione **tra denaro e tecnologia** nel mondo contemporaneo, dove le due entità sono interconnesse e interdipendenti, evolvono continuamente e hanno un forte impatto sulla società e sulle economie globali.

La teoria della complessità aiuta a comprendere come fattori esterni ed apparentemente distanti dalla vita di tutti i giorni, quali le politiche economiche e le tendenze sociali, influenzino la vita quotidiana. Inoltre, la stessa teoria suggerisce che il denaro è il prodotto di una complessa interazione tra molteplici fattori economici, sociali, politici e culturali e che, **durante i tempi di crisi**, un sistema monetario diventa particolarmente complesso tanto da dover cercare nuove soluzioni tecnologiche e/o normative che ne garantiscono utilità, liquidità e risparmio alla popolazione.

In ultimo, la teoria della complessità relaziona l'uomo alla tecnologia, mostrando come la crescente adozione di quest'ultima sia fortemente influenzata da come esso vede il mondo.

Il manuale offre quindi una formazione completa e prepara i lettori al meglio, analizzando la società in cui vivono e fornendo loro **una comprensione multidisciplinare**. Nel contesto in cui siamo, l'approccio COMB Model e la teoria della complessità possono essere applicati per fornire una visione più ampia dell'evoluzione di questo fenomeno all'interno dell'innovazione finanziaria.

Capitolo 2

TRUST MACHINE



Introduzione

Il secondo capitolo ha come principale obiettivo formativo quello di analizzare e far comprendere il funzionamento di Internet, delle reti informatiche, delle *distributed ledger technologies* (DLT) e della blockchain. Si approfondiranno le modalità con cui vengono gestite e prodotte le transazioni nelle reti peer-to-peer, senza la necessità di un amministratore centralizzato, nonché i principali modelli di governance utilizzati da una rete decentralizzata. Al fine di spiegare tutto questo, verrà affrontato nel dettaglio il funzionamento della rete di Bitcoin, introducendo analogie e differenze con altre reti blockchain come quella di Ethereum.

Il secondo obiettivo formativo è quello di aiutare il lettore ad immergersi all'interno di una nuova fase storica, ricca di cambiamenti tecnologici, economici e filosofici dovuti principalmente all'avvento dell'informatica e alla progressiva dematerializzazione del denaro, delle forme di scambio e della comunicazione tra individui.

Il terzo obiettivo formativo è quello di comprendere l'evoluzione della moneta e della finanza, approfondendo il ruolo dei digital assets e del web3 in questa fase innovativa, e l'impatto macroeconomico di nuove forme monetarie.

In prima battuta, verrà introdotto il **concetto di valore** e di **comunità economica digitale**. Successivamente, si analizzerà l'architettura tecnologica di Internet e dei protocolli informatici, i quali permettono la comunicazione di informazioni ed il trasferimento di valore tra più utenti sulla rete stessa.

Verrà, inoltre, analizzata più nel dettaglio l'architettura della blockchain di Bitcoin e più generalmente delle reti informatiche peer-to-peer, approfondendo conseguentemente il ruolo di nodi all'interno di una rete senza un amministratore centralizzato. Con riferimento a quest'ultimo punto, ci focalizzeremo sul concetto di consenso distribuito e sul concetto di sicurezza informatica della rete, approfondendo le modalità con cui la crittografia garantisce sicurezza alle transazioni nel database e nonché le modalità con cui la teoria dei giochi può essere applicata alle reti P2P al fine di garantire stabilità e cooperazione tra tutti i nodi.

In sintesi, il capitolo è composto da 7 macro-blocchi e 44 blocchi formativi, creati per aiutare il lettore a fare i primi passi all'interno della tecnologia web3.

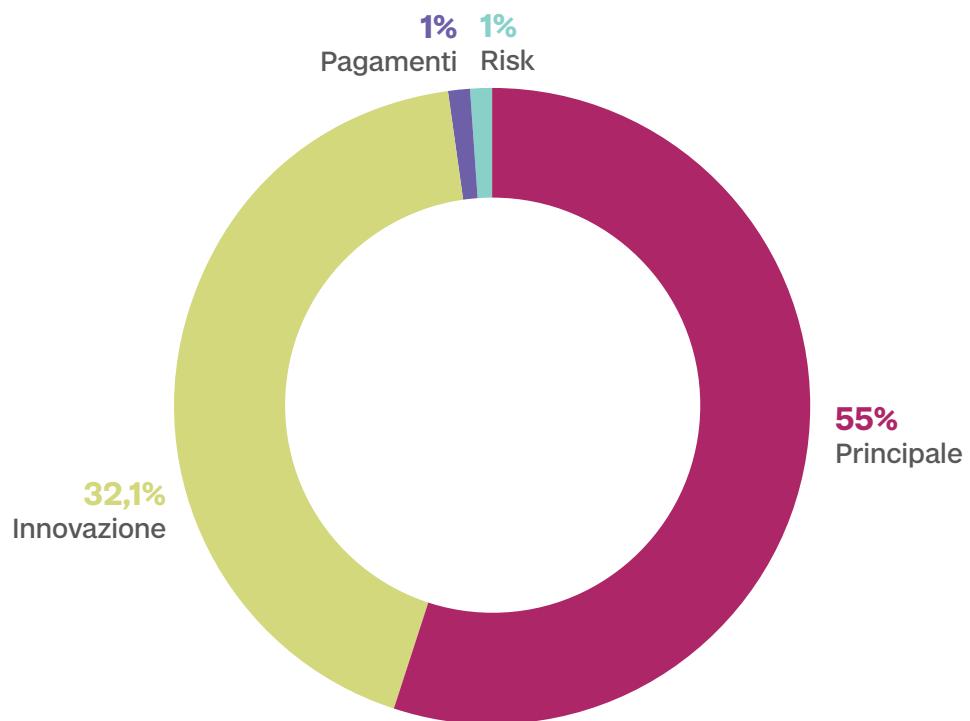
Queste alcune domande a cui cercheremo di rispondere:

- Che cos'è il valore? E come è stato influenzato dalla tecnologia?
- Cos'è Internet? Come funziona il web e che cos'è il web3?
- Come funziona la blockchain?
- Da chi vengono amministrati i dati di una blockchain?
- Cos'è Bitcoin dal punto di vista informatico e qual è il suo scopo?

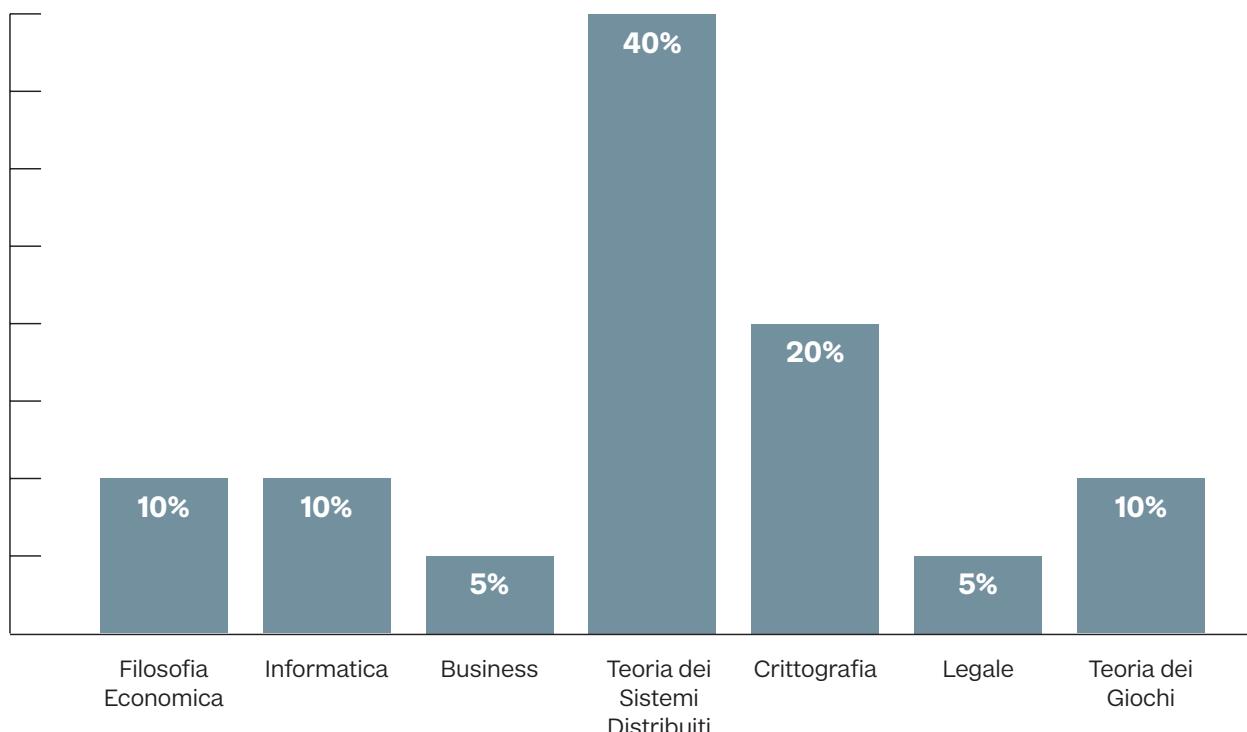
Per poi approfondire con domande più approfondite quali:

- Come viene utilizzata la crittografia, la funzione hash e il PKI Scheme per garantire la sicurezza e l'anonimato nelle transazioni peer-to-peer della blockchain di Bitcoin?
- Quali sono le sfide tecniche e sociali che devono essere affrontate per "scalare" i sistemi informatici?
- In che modo le Distributed Ledger Technologies stanno cambiando il modo in cui vengono gestiti i dati e le transazioni finanziarie?
- Quali sono i rischi e i benefici dell'utilizzo di reti peer to peer aperte, come Bitcoin ed Ethereum, per il sistema finanziario globale?
- Come il modello input-output delle transazioni nel blocco di Bitcoin influenza sulla sicurezza, l'affidabilità e la privacy della rete?
- Quali sono le implicazioni economiche e sociali della valutazione del web3 come un'entità finanziaria e quanto potrebbe valere in futuro?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. Il valore

- 1.1 Il valore come forma di comunicazione
- 1.2 Il concetto di valore come processo bottom-up
- 1.3 Internet e la creazione del valore nella comunità economica

DIFFICOLTÀ DISCIPLINA PERCORSO

●	Filosofia Economica	Principale
●	Filosofia Economica	Principale
●	Filosofia Economica	Principale

2. Internet

- 2.1 Come funziona Internet?
- 2.2 Che cos'è il Word Wide Web?
- 2.3 Che cos'è il Web3?
- 2.4 Quanto potrebbe valere il web?

●	Informatica	Principale
●	Informatica	Principale
●	Informatica	Principale
●	Business	Principale

3. Reti peer to peer

- 3.1 L'architettura del web e gli attori coinvolti
- 3.2 I sistemi distribuiti e l'architettura di rete
- 3.3 L'architettura di una rete peer to peer (p2p)
- 3.4 La rete p2p di BitTorrent
- 3.5 Le controversie verso BitTorrent e l'idea di Spotify
- 3.6 Trasmissione dei dati e performance (Spotify vs BitTorrent)
- 3.7 Come funziona la rete p2p di BitTorrent?
- 3.8 Differenze tra le reti peer to peer: BitTorrent, Bitcoin, Ethereum

●	Informatica	Principale
●	Informatica	Innovazione
●	Informatica	Principale
●	Informatica	Principale
●	Business	Principale
●	Informatica	Innovazione
●	Informatica	Innovazione
●	Informatica	Principale

4. Il nodo nella rete peer to peer

- 4.1 Il nodo nella rete peer to peer di Bitcoin
- 4.2 Come diventare un nodo nella rete di Bitcoin?
- 4.3 L'infrastruttura del database distribuito
- 4.4 La struttura del blocco
- 4.5 Modello input e output delle transazioni nel blocco
- 4.6 Quanti sono i nodi nella rete e che ruolo svolgono?
- 4.7 Quante tipologie di wallet esistono?
- 4.8 Come vengono prioritizzate le transazioni dal nodo minatore?
- 4.9 Ottimizzazione delle transazioni nel blocco
- 4.10 Come avviene il collegamento tra un blocco e l'altro?

●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Innovazione

5. Root of trust e crittografia

- 5.1 Perché la blockchain è sicura?
- 5.2 Basi di crittografia: le funzioni di hashing

●	Crittografia	Principale
●	Crittografia	Innovazione

- 5.3 Basi di crittografia: il Public Key Infrastructure
- 5.4 Come viene utilizzato il PKI Scheme e l'hashing all'interno di un wallet di digital assets?
- 5.5 Dove viene applicata l'hash function e le PKI nella blockchain?
- 5.6 Considerazione di cybersicurezza per un wallet
- 5.7 Cosa vuol dire "possedere" un digital asset come bitcoin?
- 5.8 Considerazioni sul concetto di pseudo-anonimato



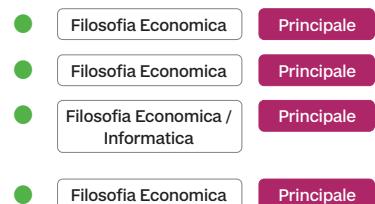
6. Le regole, la governance e il consenso distribuito

- 6.1 Differenze tra le reti: pubblica, privata, con permessi e senza permessi
- 6.2 Perché la rete p2p è sicura e cos'è il consenso distribuito?
- 6.3 Come vengono aggiornate e chi gestisce le regole nella rete?
- 6.4 Che ruolo hanno i full node nelle regole del protocollo?
- 6.5 Come un nodo minatore diventa profittevole?
- 6.6 I modelli matematici del modello ad incentivi della rete
- 6.7 Altri modelli di teoria dei giochi per un equilibrio dinamico



7. The protocol money

- 7.1 A che cosa serve la moneta?
- 7.2 Le caratteristiche di una buona moneta e la standardizzazione
- 7.3 Quali sono le condizioni per cui una tecnologia viene accettata dalla massa?
- 7.4 The Protocol money e la ciclicità nella moneta durante le crisi



1

Il valore

- 1.1 Il valore come forma di comunicazione
- 1.2 Il concetto di valore come processo bottom-up
- 1.3 Internet e la creazione del valore nella comunità economica

1.1

Filosofia Economica

● Basic

Il valore come forma di comunicazione

In ogni epoca, la comunicazione e lo scambio di valore sono state parte integrante della vita umana e il motore di innovazione e progresso.

Il valore è un concetto complesso che può essere definito in molti modi diversi, ma generalmente si riferisce a **qualcosa che è desiderabile, utile o importante per noi**. Il denaro è una delle principali forme di espressione del valore nella società moderna, poiché ci consente di scambiare beni e servizi e di assegnare un prezzo a ciò che è considerato prezioso. Quando una persona trasmette del denaro ad un'altra, sta effettivamente trasferendo del valore, che può essere inteso come un messaggio che comunica l'importanza o il valore di ciò che è stato scambiato.



Valuta

Derivato dal verbo valere. Oggetto che esprime un valore.

In ambito bancario il termine valuta assume anche un'altra accezione: tempo che intercorre tra il momento in cui viene contabilizzata un'operazione bancaria e il momento in cui gli effetti dell'addebito o dell'accredito divengono effettivi ai fini del calcolo degli interessi sul conto corrente in cui il movimento viene registrato

In questo senso, la trasmissione del valore attraverso il denaro può essere vista **come un mezzo per esprimere la reciproca riconoscenza e apprezzamento**, e quindi come un fattore che contribuisce alla costruzione di relazioni sociali basate sulla fiducia e sulla collaborazione. Lo scambio vuole essere una interazione positiva tra due persone, dove si realizza una doppia coincidenza di bisogni dal quale viene generato valore all'interno di una comunità. Le comunità e le masse, nel corso della storia hanno considerato gli oggetti più disparati come strumento per esprimere valore. Alcune comunità chiuse ancora oggi utilizzano forme di **valuta** simboliche quali conchiglie o piume.

Tipologia di Sistema Valutario	Comunità
Sigarette, Vino	Carceri
Piume, Conchiglie	Comunità primitive
Tempo	Liberi professionisti, Comunità Autonome
Sardex	Commercianti Sardegna

Con l'avvento di Internet, la comunicazione e le forme di scambio tra le comunità hanno subito **una radicale evoluzione**. In particolare, il filosofo francese Pierre Lévy ha coniato il termine "cibercultura" per definire la nuova cultura che è emersa dall'uso di Internet e delle tecnologie digitali. La cibercultura è caratterizzata dalla comunicazione e dalla condivisione, e ha aperto nuove opportunità di espressione e partecipazione. Oggi è possibile **connettersi con persone in ogni parte del mondo**, condividere informazioni e conoscenze, partecipare a progetti collaborativi e creare comunità di interesse. All'interno del processo di digitalizzazione e dematerializzazione, lo scambio di valore trova dei nuovi strumenti per diventare più globale. Dal baratto ai sistemi monetari più sofisticati fino ad arrivare Bitcoin, gli individui comunicano tra di loro, attraverso lo scambio di oggetti, per migliorare la loro situazione di partenza. **Anche durante i tempi di guerra**, il mercato libero è sempre stato mantenuto poiché ritenuto una situazione win-win per tutti i partecipanti.

L'evoluzione della tecnologia condiziona come la forma del valore e come si può spostare da un punto all'altro, da una persona all'altra, da un utente all'altro. All'interno della cibercultura, il valore è espresso come informazione, non per questo internet viene definito come un insieme **tecnologie dell'informazione e della comunicazione**.

La questione del valore e del denaro è strettamente legata a questioni etiche e politiche, poiché l'assegnazione del valore e il suo scambio possono influenzare il modo in cui le risorse sono distribuite ed utilizzate all'interno della società. Pertanto, la trasmissione del valore può anche essere vista come un modo per esprimere e promuovere determinati **valori etici e sociali, come la giustizia, l'equità e la solidarietà**.

1.2

Filosofia Economica

● Basic

Il concetto di valore come processo bottom-up

In effetti, la filosofia e la economia hanno in comune alcune domande fondamentali come “che cosa è il valore?” e “come possiamo valutare le cose?”. Tuttavia, la risposta non può che essere dipendente dal contesto storico in cui ci troviamo, e da usi, costumi e tecnologie disponibili.

In alcuni casi però, a prescindere dal contesto storico, il processo con cui assegniamo del valore a qualcosa avviene tramite un processo di condivisione e di ragionamenti comuni. Questa coscienza collettiva crea così nel tempo degli “oggetti standard” ritenuti di valore.

L'oro, per esempio, è uno tra gli oggetti che è stato accettato globalmente in maniera decentralizzata, attraverso un processo di questo tipo, definibile come “processo **bottom up**”. Una delle caratteristiche che ha “messo d'accordo” civiltà distanti sono **le sue molte proprietà fisiche e chimiche** che lo rendono adatto alla conservazione nel tempo. L'oro, infatti, è un metallo inerte e non reattivo, il che significa che non si corrode o si deteriora nel tempo, mantenendo il suo valore per molti anni.



Bottom Up

Definizione: Strategia che regola la gestione di conoscenze e la risoluzione di problemi, applicata in particolare allo sviluppo dei software informatici, ma estesa anche ad altre teorie scientifiche e umanistiche. In generale, l'approccio b.-u. («dal basso verso l'alto») è un processo di sintesi, da elementi base fino a un sistema complesso.

Fonte: [https://www.treccani.it/enciclopedia/bottom-up_%28Dizionario-di-Economia-e-Finanza%29/#:~:text=\(%C2%ABdal%20basso%20verso%20l'alto,fino%20alle%20sue%20componenti%20elementari.](https://www.treccani.it/enciclopedia/bottom-up_%28Dizionario-di-Economia-e-Finanza%29/#:~:text=(%C2%ABdal%20basso%20verso%20l'alto,fino%20alle%20sue%20componenti%20elementari.)

In secondo luogo, l'oro è un materiale raro, il che significa che è difficile da trovare e da estrarre dalla terra. Questo lo rende prezioso e lo ha reso una riserva di valore naturale. L'oro, per effetto delle caratteristiche appena descritte, è diventato nel tempo un elemento in grado di essere utilizzato non solo come mezzo di valore, **ma anche di scambio**.

A partire da molte culture antiche, come gli antichi egizi e/o i Romani, l'oro è stato utilizzato come mezzo di scambio, anche tra popoli di culture differenti. Inoltre, durante il medioevo ed il Rinascimento, il suo utilizzo è stato esteso in tutto il mondo grazie alla espansione del commercio internazionale e grazie alla nascita delle prime banche commerciali. Con il tempo l'oro è divenuto **la misura fondamentale del**

valore nel cosiddetto Gold Exchange standard, in cui il sistema di cambio tra le varie valute di fatto si basava sulla stabilità del dollaro rispetto all'oncia. Fino al 1971, l'oro è stato utilizzato come riserva di valore dai governi e dalle banche centrali, in quanto bene liquido e universalmente accettato.

Anno	Sistema Monetario
1700-1800	Standard oro e argento
1800-1871	Standard oro
1871-1914	Standard oro e argento bimetallismo
1914-1918	Inconvertibilità delle valute
1919-1944	Standard oro e argento bimetallismo
1944-1971	Bretton Woods con standard oro e dollaro come valuta di riserva (cambi fissi)
1971-oggi	Sistema monetario internazionale fluttuante (cambi variabili)

Anche se oggi la **maggior parte delle economie si basano su valute fiat** (cioè valute che non sono influenzate dall'oro o da altre riserve di valore fisiche), l'oro continua a essere utilizzato come riserva di valore dai governi e dagli investitori.

In sintesi, il **valore dell'oro è stato riconosciuto in maniera globale** attraverso un processo dal basso verso l'alto (o bottom-up, per l'appunto) poiché ha soddisfatto le esigenze delle persone come riserva di valore, mezzo di scambio e unità di conto, e proprio per questo è stato accettato e utilizzato dalle persone in tutto il mondo nel corso della storia umana.

Fonti

- ▶ “The Euro: How a Common Currency Threatens the Future of Europe” di Joseph Stiglitz
- ▶ “A Monetary History of the United States, 1867-1960” di Milton Friedman e Anna Jacobson Schwartz
- ▶ “The Evolution of Central Banking: Theory and History” di Stefano Ugolini

1.3

Internet e la creazione del valore nella comunità economica

Filosofia Economica

● Basic

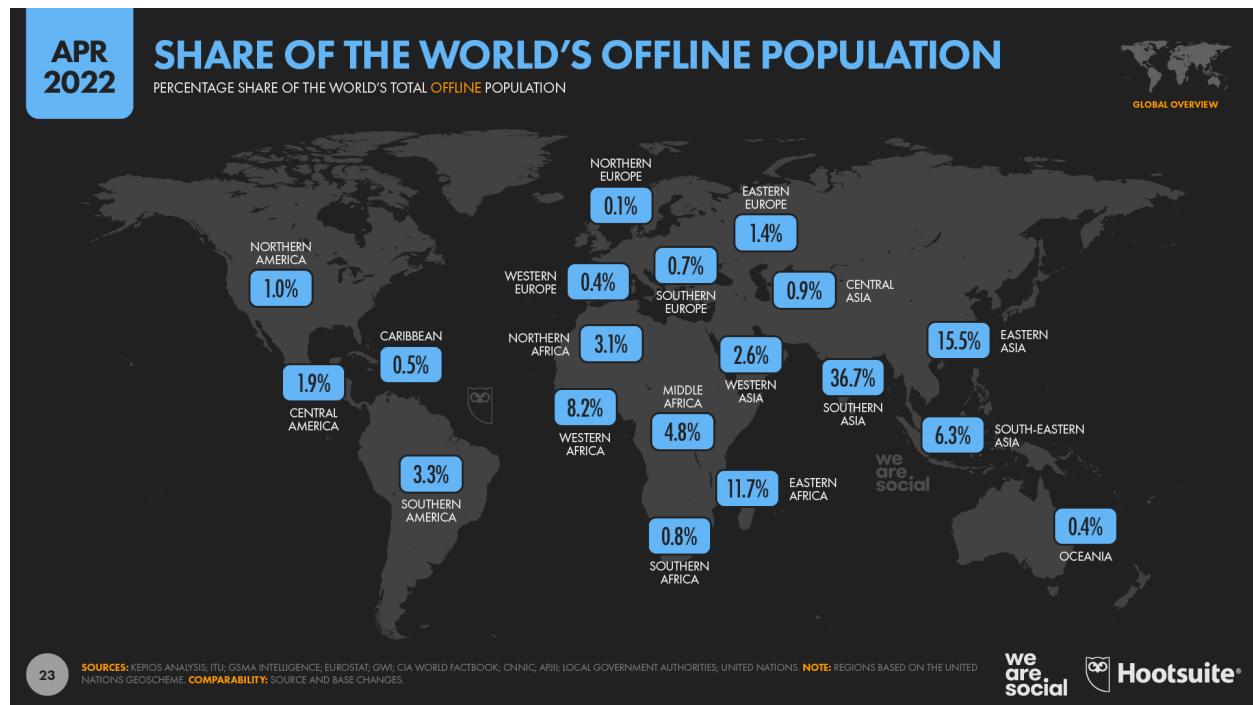
L'avvento di Internet ha rappresentato una svolta epocale nella storia dell'umanità, poiché ha permesso di creare **una rete di comunicazione globale** che ha rivoluzionato il modo in cui le persone interagiscono tra loro e con il mondo circostante. Internet ha aperto nuove opportunità per l'apprendimento, il commercio, la cultura e la politica, sollevando anche importanti questioni etiche e filosofiche.

Già nel 1996, il filosofo francese Jean Baudrillard affermava che internet stava trasformando il mondo in una “società dell’informazione” in cui **le persone si relazionano tra loro attraverso l’immateriale e l’iper-reale**. In seguito, molte altre figure filosofiche hanno analizzato l'impatto di internet sulla società umana, tra cui Manuel Castells, che ha descritto internet come il “mezzo di comunicazione dominante

della nostra epoca”, e Zygmunt Bauman, che ha visto in internet la creazione di una società sempre più “liquida”, de-materiale e decentralizzata.

La dematerializzazione sta modificando **la percezione del valore e conseguentemente sta mettendo in discussione alcuni concetti esistenziali**. Negli ultimi anni, ad esempio, il denaro sta diventando sempre più immateriale, con il passaggio verso società cashless e forme di pagamento digitali, cambiando il nostro rapporto con il valore e l'economia. Come ha sostenuto il filosofo Maurizio Ferraris, “l'intero mondo economico si sta riducendo a un insieme di flussi di informazione, dove l'unico fattore di valore è la velocità della comunicazione”.

In aggiunta a tutto ciò la dematerializzazione sta cambiando anche il nostro concetto di identità, in quanto sempre più **le informazioni personali vengono archiviate e gestite in modo digitale**. Come ha sostenuto il filosofo tedesco Byung-Chul Han, “la società dell'informazione produce una nuova forma di potere che si basa sulla gestione e il controllo delle informazioni personali, che a loro volta definiscono la nostra identità”.



La dematerializzazione sta quindi influenzando in modo significativo alcuni concetti esistenziali, come il denaro, l'identità e l'aggregazione, con implicazioni filosofiche importanti sul nostro rapporto con la realtà e la società.

2

Internet

- 2.1 Come funziona Internet?
- 2.2 Che cos'è il Word Wide Web?
- 2.3 Che cos'è il Web3?
- 2.4 Quanto potrebbe valere il web?

2.1

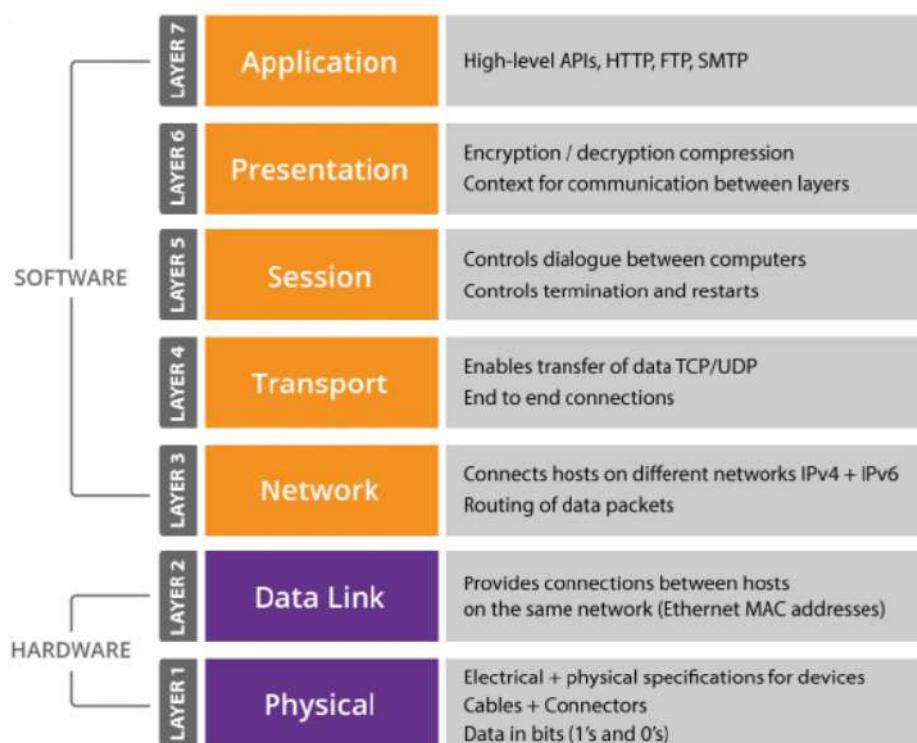
Informatica

• Basic

Come funziona Internet?

L'infrastruttura di Internet può essere considerata come una torta, composta da più strati definiti come livelli. Ogni livello ha specifiche funzioni e differenti tecnologie, definibili a loro volta come reti, le quali, combinate tra loro, permettono il funzionamento complessivo di Internet che conosciamo.

Di seguito una descrizione analitica di ogni livello, utilizzando la tassonomia del modello ISO/OSI, il quale definisce ogni livello in base alla propria funzionalità, e dove ogni livello è arricchito da altre funzionalità grazie all'introduzione di un ulteriore livello soprastante, permettendo la realizzazione di reti via via più complesse.

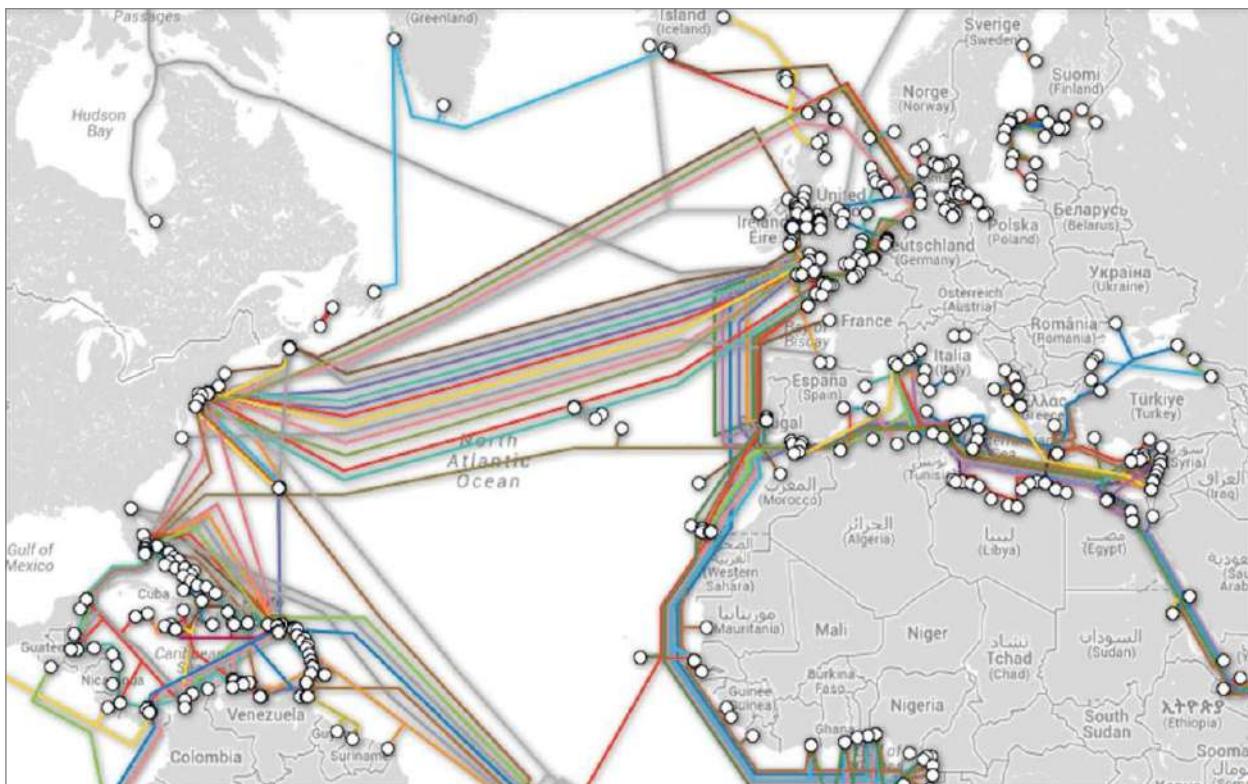


L'infrastruttura di Internet, come da immagine precedente, è **composta da 7 livelli** che lavorano insieme per consentire la trasmissione dei dati su una vasta rete di dispositivi interconnessi. Il web è solo uno dei tanti servizi disponibili su Internet, ma è diventato uno dei più importanti e popolari servizi utilizzati. Il World Wide Web, come lo conosciamo oggi, è costruito al di sopra di altri 6 livelli, che abilitano l'utente a ricevere e trasmettere informazioni globalmente.

L'infrastruttura di Internet si è evoluta nel tempo per rispondere alle esigenze crescenti degli utenti e delle organizzazioni.

- Il primo livello dell'infrastruttura è il **livello fisico**, che include i cavi, i **router di casa** e altri dispositivi di rete.
- Il secondo livello riguarda il **collegamento dati**, che consente alle diverse informazioni di essere trasmesse attraverso i dispositivi di rete.
- Il terzo livello è quello di **rete**, che gestisce la connessione tra i dispositivi connessi alla stessa.
- Il quarto livello dell'infrastruttura di Internet è di **trasporto**, che consente ai dati di essere trasmessi tra dispositivi di rete su larga scala. Il protocollo TCP (Transmission Control Protocol) è il protocollo di trasporto predominante utilizzato su Internet.

5. Il quinto livello è il livello di **sessione**, che consente alle applicazioni di stabilire e gestire sessioni di comunicazione su Internet.
 6. Il sesto livello dell'infrastruttura di Internet è definito di **presentazione**, e si occupa della rappresentazione dei dati, incluso il formato e la crittografia.
 7. Il settimo livello, nonché l'ultimo, è quello di **applicazione**, che comprende una vasta gamma di applicazioni come la posta elettronica, il World Wide Web (web) e i servizi di messaggistica istantanea.



Come da immagini sopra presentata, la rete internet è composta da una serie di cavi (fisici) che hanno l'obiettivo di portare la rete (a livello virtuale) in tutto il globo.

In sintesi, l'infrastruttura di Internet si è evoluta nel tempo per supportare le esigenze crescenti degli utenti e delle organizzazioni, portando alla **creazione di nuovi servizi come i social network**, che utilizzano gli stessi livelli di networking di Internet ma che introducono nuove funzionalità e nuove esigenze di elaborazione e archiviazione. Gli elementi comuni dell'infrastruttura di Internet includono la rete di cavi e collegamenti fisici, il protocollo di trasporto TCP e i protocolli di applicazione utilizzati da una vasta gamma di servizi web.

2.2

Che cos'è il Word Wide Web?

Informatica

Medium

Il World Wide (Web), riprendendo la metafora della torta, si può immaginare come l'ultimo strato di Internet, definito come "livello delle applicazioni". Il Web nasce come **luogo virtuale in cui gli utenti possono condividere informazioni e visualizzarle**. Il World Wide Web è indubbiamente una delle **più importanti conquiste dell'era digitale** e rappresenta una fonte inesauribile di informazioni, conoscenza e opportunità.

tunità. Il Web ha visto la luce grazie ad una serie di innovazioni, tra cui quella del “web server”. Questo concetto è stato sviluppato da Tim Berners-Lee, un informatico britannico, nel 1989. Berners-Lee è anche accreditato come l'inventore del World Wide Web.

Possiamo immaginare che il web server sia come un grande magazzino di oggetti. Quando un utente vuole uno tra questi oggetti, chiede al magazziniere di consegnartelo. Il magazziniere ti dà accesso all'oggetto che hai chiesto, ma mantenendo il controllo su di esso. Allo stesso modo, quando vuoi accedere a un sito web, chiedi al web server di mostrarti il sito. Il web server ti mostra il sito e puoi guardarlo e usarlo come vuoi tu, mentre le informazioni del sito rimangono dentro il web server.

La comunicazione tra il web server e il dispositivo dell'utente, anche noto come **client**, è possibile grazie ad altri 3 protocolli, fondamentali per creare interoperabilità all'interno del web:

1. **HTTP (Hypertext Transfer Protocol)**: è il protocollo di comunicazione utilizzato per trasferire i dati tra il server web e il browser del client. HTTP consente di accedere alle pagine web, di inviare informazioni e di ricevere risposte dal server.
2. **HTML (Hypertext Markup Language)**: è il linguaggio di markup utilizzato per creare le pagine web. HTML permette di definire la struttura e il contenuto delle pagine web, attraverso l'utilizzo di tag e attributi.
3. **URL (Uniform Resource Locator)**: è l'indirizzo che identifica in modo univoco una risorsa sul web. L'URL è composto da diversi elementi, tra cui il protocollo utilizzato (HTTP o HTTPS), il nome del dominio, il percorso della risorsa e il nome del file.



Questi protocolli specializzati hanno consentito la creazione di una vasta gamma di servizi e applicazioni che hanno cambiato il modo in cui le persone lavorano, comunicano e si divertono.

Qui elencati altri protocolli utilizzati all'interno della navigazione giornaliera online, i quali, lavorando insieme in maniera sinergica, permettono agli utenti di accedere ad applicazioni web e altre tipologie di servizi digitali.

Protocollo	Funzione	Porta Predefinita	Tipo di Trasporto
TCP	Fornisce un servizio di connessione affidabile	Varia a seconda del protocollo di livello superiore	Connessione
IP	Indirizzamento e instradamento dei pacchetti	N/A	Datagramma
FTP	Trasferimento di file	20 (dati), 21 (controllo)	Connessione
SMTP	Trasferimento di messaggi di posta elettronica	25	Connessione
HTTP	Trasferimento di dati web	80	Connessione
HTTPS	Trasferimento di dati web sicuro	443	Connessione
UDP	Fornisce un servizio di connessione non affidabile	Varia a seconda del protocollo di livello superiore	Datagramma
DNS	Risoluzione dei nomi di dominio in indirizzi IP	53	Datagramma
TLS/SSL	Fornisce una connessione sicura e crittografata tra due host	Varia a seconda del protocollo di livello superiore, spesso 443 per HTTPS	Connessione
Bitcoin Protocol	Trasferimento di transazioni di Bitcoin tra nodi della rete	8333 (mainnet), 18333 (testnet)	Connessione
SIP	Protocollo di segnalazione per VOIP	5060, 5061 (SIP over TLS)	Connessione
RTP	Trasferimento di dati audio/video per VOIP	Varia, spesso negoziato dinamicamente	Datagramma

Ad esempio, la rete VoIP (Voice over Internet Protocol), consente di effettuare chiamate telefoniche tramite Internet, abilitando app per videoconferenza, come Zoom, Teams, o Skype.

Tutti questi acronimi corrispondono a **protocolli informatici che svolgono diverse funzioni** durante la navigazione su internet. In maniera manuale o automatica, il proprio client, attraverso un **browser**, si collega ad un server aprendo le **porte di rete**.



Browser

In informatica, con il termine **browser** ci si riferisce ad un particolare programma per navigare in Internet, che inoltra la richiesta di un documento alla rete e ne consente la visualizzazione una volta arrivato.

Ecco un esempio di accesso ad un sito web e ad un account e-mail utilizzando i protocolli citati.

1. Apri il browser web sul tuo dispositivo e digita l'URL del sito web a cui desideri accedere.
2. Il tuo dispositivo invierà una richiesta al server **DNS** per la risoluzione del nome di dominio in un indirizzo IP utilizzando il protocollo DNS.
3. Una volta ottenuto l'indirizzo IP, il browser utilizza il protocollo TCP per stabilire una connessione di rete con il server web del sito.
4. Dopo aver stabilito la connessione, il browser invia una richiesta HTTP al server web per ottenere la pagina web richiesta.
5. Il server web invia la pagina web richiesta al browser utilizzando il protocollo HTTP.

6. Se la pagina web richiede il caricamento di file o immagini, il browser può utilizzare il protocollo FTP per scaricare i file dal server FTP del sito.
7. Per accedere all'account e-mail, il browser digita l'URL del sito di posta elettronica nella barra degli indirizzi.
8. Il browser invia una richiesta HTTP al server web del provider di posta elettronica per accedere all'account e-mail.
9. Il server di posta elettronica invia la pagina di accesso all'account e-mail al browser utilizzando il protocollo HTTP.
10. Una volta effettuato l'accesso all'account e-mail, il browser utilizza il protocollo SMTP per inviare e-mail ad altri server di posta elettronica.
11. Per garantire una maggiore sicurezza durante l'accesso all'account e-mail, il browser utilizza il protocollo TLS/SSL per crittografare i dati in transito tra il dispositivo e il server di posta elettronica.



Porte di rete

Rappresentata da un numero intero di 16 bit che ha lo scopo di identificare l'applicazione a cui instradare il flusso di dati, in modo da differenziare le conversazioni tra gli host. Un computer è così in grado di eseguire molteplici applicazioni, discernendo con assoluta certezza quale di esse abbia originato o debba ricevere il flusso di dati. Allo stesso modo, grazie al numero di porta è possibile aprire più connessioni, con la certezza che i dati saranno inviati all'istanza applicativa che li ha richiesti

DNS

DNS sta per **Domain Name System** e si riferisce ai nodi di una rete, per es. Internet, sistema di indirizzamento che traduce i nomi simbolici (più semplici da memorizzare) nei corrispondenti indirizzi IP (Internet Protocol). I nomi simbolici sono divisi in domini gerarchici (separati dal punto), **individuati da destra a sinistra**; il primo nome è il dominio di primo livello (TLD, Top-level domain), che può essere geografico (.it, .uk, .es ecc.) o semantico (.com, .org, .edu ecc.); dal secondo in poi si hanno i domini di secondo, terzo ecc. livello. L'ultimo nome a sinistra è di solito quello del nodo (www, ftp, mail ecc.), ma può essere omesso se è stato definito un default. Il database che compone le associazioni tra nomi e indirizzi è gestito gerarchicamente: ogni livello conosce soltanto il proprio, quello immediatamente sottostante e almeno un 'referente' (DNS server) per il livello superiore. Un utente che, mediante un browser, richiede di visitare una pagina web dà vita a una sequenza di query (interrogazioni) a salire, dalla rete locale al TLD server.

Questa flessibilità è stata sfruttata da molte organizzazioni per creare soluzioni personalizzate per la gestione dei dati e delle applicazioni, la gestione dei processi aziendali e molte altre attività.

Inoltre, il Web è stato utilizzato per creare infrastrutture specifiche per **il supporto di attività collaborative come i social network**. Ad esempio, i wiki sono stati creati utilizzando la struttura del Web, consentendo a gruppi di utenti di collaborare alla creazione di contenuti online. Queste infrastrutture collaborative hanno creato nuove opportunità per la condivisione di informazioni e la creazione di contenuti, portando alla nascita di una crescente gamma di risorse online.

Anche da un punto di vista commerciale, la rete ha creato nuove opportunità di business e ha rivoluzionato il modo in cui le aziende svolgono attività di vario tipo. Basti pensare ai siti web ed ai servizi di e-commerce, tramite i quali le aziende possono raggiungere nuovi clienti in tutto il mondo, **offrendo loro prodotti e servizi online**.

Ultimo ma non ultimo, il web ha portato anche a **nuove forme di intrattenimento**, grazie ai servizi di streaming video e ai giochi online, offrendo un'ampia gamma di opzioni per il divertimento e il relax.

2.3

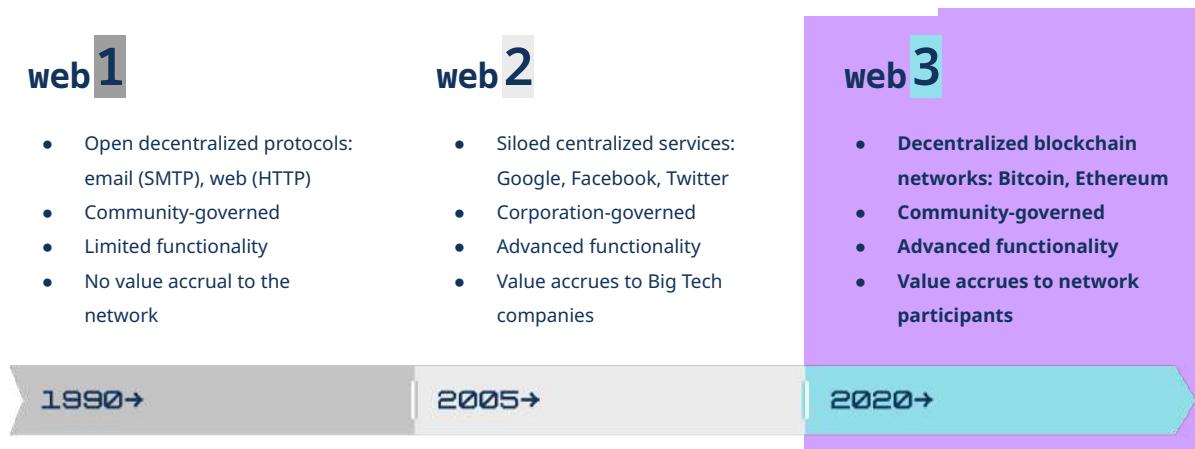
Che cos'è il Web3?

Informatica

Basic

Durante gli ultimi 30 anni, il web ha visto una crescita di nuovi protocolli informatici in grado **di far comunicare le persone con video, messaggistica, audio**. Dalla nascita di Bitcoin, altre reti informatiche hanno sfruttato la tecnologia offerta, creando nuove versioni e portandoci fino all'ultima iterazione del web, nota come web3.

Il web3 può essere definito come un **insieme di nuove reti informatiche costruite sopra l'infrastruttura di internet**. Nuove reti definite da regole di protocollo che abilitano utenti sparsi nel mondo ad interagire l'uno con l'altro attraverso nuove forme di comunicazione. Nuove reti informatiche dove è possibile comunicare sotto forma di transazioni economiche e dove non vi è una autorità centrale che svolge il ruolo da amministratore.



Abbiamo parlato finora, pur non definendoli con questo nome, di web1 e web2. Più precisamente, per web1 si intende la prima versione di Internet, dove i siti erano solo in modalità lettura e non era permessa alcuna interazione con gli stessi. Di contro, nel web2, i siti permettono all'utente non solo di leggere le informazioni ma anche interagire con gli stessi; si pensi, quindi, agli e-commerce o ai social media.

Web1 and web2 democratized information and publishing. Web3 democratizes ownership.



Differentemente, quindi, dalle precedenti iterazioni, il web3:

- È costruito per far interagire l'utente con la blockchain, un database distribuito che funge da libro contabile e da orologio globale per gestire ed organizzare nel tempo i saldi degli utenti all'interno della rete;
- Utilizza i digital assets come strumento per lo scambio di valore all'interno della rete;
- Gli amministratori della rete non sono singole unità ma **interi comunità di persone**, sparse nel mondo, che partecipano nel decidere le regole e nella manutenzione delle informazioni nel tempo.

Nonostante l'innovazione, rimane comunque una costante l'utilizzo di reti già note ed utilizzate nel web tradizionale, o web2, come:

- **TCP e IP:** che fornisce la connessione di rete tra gli utenti del network;
- **HTTP:** che fornisce l'accesso all'interfaccia web per l'utente, consentendo di interagire; con ai software e alle applicazioni
- **TLS/SSL:** che critta i dati in transito tra i dispositivi, fornendo una maggiore sicurezza all'interno di applicazioni e software.

Questi nuovi protocolli come Bitcoin ed Ethereum possono essere considerati alla pari dei protocolli utilizzati nella navigazione Web2, poiché soddisfano il fine di far comunicare le persone in maniera globale su Internet. **La principale differenza con i protocolli precedenti, oltre alle 3 condizioni scritte precedentemente, sono gli obiettivi di questi nuovi protocolli sul Web3.**

Per esempio, il principale obiettivo della rete Bitcoin è quella di essere un protocollo informatico dove gli utenti possono **scambiarsi del valore economico, senza intermediari ed in modo sicuro**. Quando ci riferiamo alla rete Bitcoin, ci riferiamo sia alle regole tra gli utenti nella rete, sia ai bitcoin, ovvero il mezzo di scambio utilizzato nella rete, trasferibile da un utente all'altro senza intermediari. Regole e mezzo di scambio sono chiaramente l'uno frutto dell'altro.

Differentemente, l'obiettivo della rete di Ethereum è quello di diventare un computer globale, simile ad un cloud più distribuito, capace di eseguire del codice informatico, senza intermediari. Anche in questo caso, questa rete informatica utilizza la blockchain per salvare le informazioni sulla rete e un digital assets per far trasferire valore da un utente e l'altro.

Chiunque può partecipare alla rete aprendo una porta di rete del proprio pc e con altri strumenti per il client software che descriveremo in seguito. Nasce, quindi, una nuova idea di web con un nuovo assetto di governance nelle applicazioni online, più *user centric* e volto a fornire maggior controllo e custodia dei propri dati personali.

2.4

Business

• Basic

Quanto potrebbe valere il web?

Calcolare il valore complessivo delle aziende che contribuiscono all'infrastruttura web è un'impresa complessa e difficile, in quanto coinvolge un gran numero di aziende in tutto il mondo che operano in diversi settori. Tuttavia, è **possibile fare un'analisi ad alto livello delle aziende più importanti in ciascun livello dell'infrastruttura di Internet** e dare un'idea approssimativa del loro valore complessivo. Per fare ciò abbiamo utilizzato la tassonomia TC/IP per definire l'infrastruttura di Internet:

- **Livello fisico:** Le aziende più importanti che operano nel livello fisico dell'infrastruttura di Internet sono le società di telecomunicazioni, come AT&T, Verizon e China Mobile, che gestiscono la connettività fisica tra i diversi nodi della rete, come i cavi sottomarini nei mari e oceani.



- **Livello di rete:** Nel livello di rete dell'infrastruttura di Internet, le aziende più importanti includono operatori di backbone come Level 3 Communications e Tata Communications, nonché i fornitori di servizi Internet come Comcast e AT&T.
- **Livello di trasporto:** Le aziende più importanti che operano nel livello di trasporto dell'infrastruttura di Internet includono fornitori di servizi cloud come Amazon Web Services, Microsoft Azure e Google Cloud, nonché fornitori di servizi di hosting per i web server come GoDaddy e Bluehost.
- **Livello di applicazione:** Nel livello di applicazione dell'infrastruttura di Internet, le aziende più importanti includono Google, Facebook e Amazon, che forniscono servizi di ricerca, social networking, e-commerce e molti altri.

È importante sottolineare che questi sono solo alcuni esempi di aziende che operano in ciascun livello dell'infrastruttura di Internet, e che ci sono molte altre aziende che contribuiscono alla rete in modi diversi. Inoltre, il **valore complessivo delle aziende cambia costantemente a seconda delle fluttuazioni del mercato e dell'evoluzione tecnologica**.

In generale il **valore complessivo delle aziende che contribuiscono all'infrastruttura di Internet è enorme e in continua crescita**. Internet è diventata un pilastro fondamentale dell'economia globale e continua a generare opportunità per molte imprese in tutto il mondo.

3

Reti peer to peer

- 3.1 L'architettura del web e gli attori coinvolti
- 3.2 I sistemi distribuiti e l'architettura di rete
- 3.3 L'architettura di una rete peer to peer (p2p)
- 3.4 La rete p2p di BitTorrent
- 3.5 Le controversie verso BitTorrent e l'idea di Spotify
- 3.6 Trasmissione dei dati e performance (Spotify vs BitTorrent)
- 3.7 Come funziona la rete p2p di BitTorrent?
- 3.8 Differenze tra le reti peer to peer: BitTorrent, Bitcoin, Ethereum

3.1

Informatica

● Basic

L'architettura del web e gli attori coinvolti

Il modello client-server, utilizzato dalla maggior parte delle applicazioni all'interno del web, è una **architettura di rete** che permette a diversi dispositivi di comunicare tra loro per scambiare informazioni o per fornire servizi. In questo modello, ci sono due tipi di componenti principali: il client e il server.



Architettura di rete

L'architettura di rete è il modo in cui i servizi e i dispositivi in una rete informatica sono strutturati insieme per soddisfare le esigenze di connettività dei dispositivi e delle applicazioni.

- Il client è un dispositivo che richiede informazioni o servizi, come **un computer o uno smartphone che accede a un sito web da casa**.
- Il server è un dispositivo che fornisce informazioni o servizi, come **un server web che fornisce pagine web o un database server che gestisce un database in un magazzino**.

Il proprietario del server è la persona o l'entità che gestisce e mantiene il server. Questa persona o ente è responsabile di garantire che il server funzioni correttamente e che le informazioni che vengono scambiate tra il client e il server siano protette e sicure.

L'utente è la persona che utilizza il client per accedere alle informazioni o ai servizi forniti dal server. L'utente non ha il controllo diretto sul server, ma può accedere alle informazioni o ai servizi forniti dal server tramite il client. Il server avrà quindi degli **amministratori che gestiranno le regole e le informazioni per quella determinata applicazione web o per quel determinato database**.

Con l'avanzare della tecnologia e l'avvento dei sistemi distribuiti come il cloud e database distribuiti, molte aziende e servizi si basano su diversi server disposti in varie località in modo tale da garantire maggiore sicurezza dei dati e dando ridondanza alle informazioni. Inoltre, come affronteremo in seguito, il web3 ha sfruttato una ulteriore architettura di rete definita come peer to peer, ovvero **pari a pari**: ogni utente e ogni computer collegato alla rete può essere **considerato contemporaneamente alla pari di client e di un server**.

In sintesi, il modello client-server funziona in questo modo: l'utente utilizza il client per inviare una richiesta al server, il server elabora la richiesta e invia una risposta al client, che la visualizza all'utente. Il proprietario del server gestisce e mantiene il server per garantire che funzioni correttamente e che le informazioni siano protette.

3.2

Informatica

● Medium

I sistemi distribuiti e l'architettura di rete

Un sistema distribuito è **un insieme di componenti hardware e software autonomi e interconnessi tra loro**, che cooperano per fornire un servizio o una funzionalità comune. Questi componenti possono essere fisicamente dislocati in diverse posizioni geografiche e comunicano tra di loro attraverso una rete di comunicazione.

I sistemi distribuiti sono progettati per migliorare **la scalabilità, l'affidabilità, la disponibilità e la tolleranza ai guasti del sistema**. Possono essere utilizzati in una vasta gamma di applicazioni, tra cui le reti di sensori, il cloud storage, il cloud computing, le applicazioni web, i servizi di messaggistica e molte altre ancora.

I primi sistemi distribuiti in informatica risalgono agli anni '60 e '70, quando vennero introdotti concetti come la condivisione di risorse e la comunicazione tra computer in reti decentralizzate. Alcuni esempi di tali sistemi includono il sistema operativo TENEX, sviluppato nel 1965, e il progetto ARPANET, il precursore di Internet, sviluppato nel 1969.

Anno	Sistema Distribuito	Descrizione	Esempio
1960	Elaborazione batch distribuita	Sistema in cui un grande lavoro viene diviso in più parti e distribuito a diversi computer per l'elaborazione	Sistema di elaborazione di censimenti
1970	Elaborazione transazionale distribuita	Sistema in cui i dati vengono aggiornati su diversi computer per mantenere la coerenza dei dati	Sistema bancario
1980	Gestione di rete distribuita	Sistema per gestire e controllare i nodi della rete	Sistema di gestione di reti di telecomunicazioni
1990	Elaborazione collaborativa distribuita	Sistema in cui più utenti lavorano insieme su un singolo progetto	Sistema di elaborazione di documenti collaborativi
2000	Elaborazione di dati distribuita	I dati vengono gestiti in una rete di server che comunicano attraverso protocolli sincroni	Apache Hadoop
2009	Distributed Ledger	Registro condiviso e sicuro che consente la registrazione di transazioni tra parti senza intermediari	Bitcoin

Negli anni '80, vennero sviluppati **i primi sistemi di database distribuiti**, che consentivano di **gestire e accedere a dati su diverse macchine**. Un esempio è il sistema di database relazionale Oracle Rdb, sviluppato da Digital Equipment Corporation. Negli **anni '90**, la tecnologia dei sistemi distribuiti ha fatto passi da gigante grazie all'**avvento di Internet e alla diffusione di standard come il protocollo TCP/IP**. Vennero sviluppati molti sistemi di middleware e middleware di messaggistica, che consentivano a diverse applicazioni di interagire tra loro.

I database distribuiti sono progettati per funzionare **su reti di computer e server interconnessi**. La distribuzione dei dati su questi nodi consente ai sistemi distribuiti di essere altamente scalabili (ossia rapidi), ridondanti e tolleranti ai guasti. Tuttavia, la struttura di un database distribuito varia a seconda

del **tipo di rete in cui è creato e della modalità con cui le informazioni vengono gestite, amministrate ed inserite.**

Possiamo definire due principali categorie di reti distribuite, che variano per la loro architettura:

- **Architettura client-server**
- **Architettura peer to peer**

Sistema	Archiviazione	Controllo dei Dati	Scalabilità	Tolleranza ai Guasti
Client/Server	I dati sono archiviati sul server centrale e i client accedono ai dati tramite richieste al server	I dati sono centralizzati e controllati dal server centrale, che è responsabile della sicurezza e dell'integrità dei dati	La scalabilità dipende dalla capacità del server centrale, che può essere scalato verticalmente per aumentare la capacità di elaborazione	La tolleranza ai guasti dipende dalla resilienza del server centrale e della sua capacità di ripristinare i dati in caso di malfunzionamento
P2P	I dati sono distribuiti su tutti i nodi della rete, ognuno dei quali funge da archivio	I dati sono controllati e condivisi tra tutti i nodi della rete, senza un controllo centrale	La scalabilità dipende dalla capacità di elaborazione dei singoli nodi; quindi, la rete può essere scalata orizzontalmente aggiungendo nuovi nodi	La tolleranza ai guasti è alta in quanto i dati sono replicati su più nodi e in caso di malfunzionamento di un nodo, i dati possono essere ripristinati da altri nodi della rete

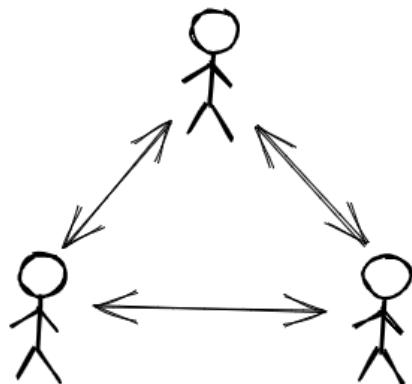
In un ambiente client-server, il database viene archiviato su un server centralizzato e gli utenti accedono ai dati attraverso un'interfaccia client. Ciò significa che **il controllo dei dati rimane centralizzato** e **l'amministratore del server o della rete** ha il pieno controllo su come i dati vengono gestiti e condivisi.



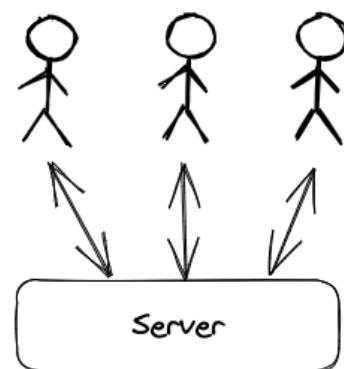
Amministratore del server o della rete

Definizione: L'amministratore di rete (network administrator) è una figura professionale del settore delle reti di telecomunicazioni che si occupa dei problemi inerenti all'interconnessione delle strutture di elaborazione dati in reti di computer.

Peer-to-peer



client-Server



D'altra parte, i sistemi distribuiti peer-to-peer (P2P) sono basati sulla cooperazione tra i nodi nella rete. **Ogni nodo della rete funge da server e client allo stesso tempo**, e i dati vengono distribuiti tra tutti i nodi. In questo modo, la rete non ha un singolo punto di controllo ed è resistente ai guasti e agli attacchi.

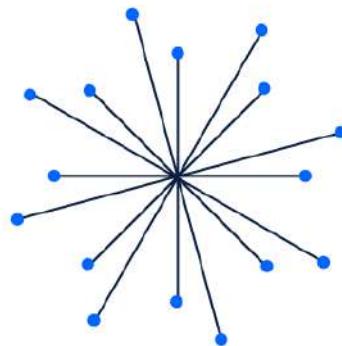
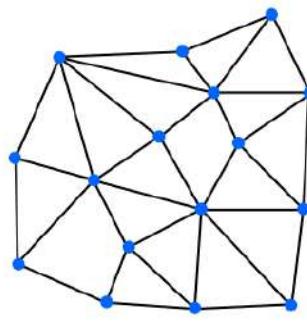
3.3

L'architettura di una rete peer to peer (p2p)

Informatica

• Basic

In una rete P2P, ogni computer o dispositivo connesso alla rete funge sia da client che da server, in quanto ciascun dispositivo può scaricare e/o condividere informazioni direttamente con altri dispositivi sulla rete, **senza la necessità di un server centrale**. All'interno di una rete peer to peer, ogni utente si definisce come "nodo della rete" o semplicemente "nodo". Ogni utente viene definito come nodo della rete, in quanto le informazioni sono distribuite all'interno del network.

**Centralized****Distributed**

Il funzionamento delle reti P2P è basato sulla condivisione di informazioni tra i partecipanti della rete. Per esempio, quando un utente vuole accedere ad informazioni, il dispositivo può collegarsi a più di un nodo per ricevere le fonti contemporaneamente e poter confrontare quest'ultime. In questo modo, **non esiste un unico punto di fallimento tale per cui se il server fallisce**, tutti gli utenti della rete sono colpiti. Un esempio di rete P2P è Torrent il cui sistema distribuito che permette di scaricare file (ad esempio, film, musica, software) a tutti i nodi della rete. Gli utenti caricano i file sui loro computer e consentono ad altri utenti di scaricare parti di quei file, chiamati "pezzi", mentre loro stessi scaricano parti di file da altri utenti. BitTorrent è stato uno dei primi protocolli P2P a **ottenere una grande diffusione**, ma ci sono anche altri protocolli P2P come eMule e Gnutella.

Un altro esempio di rete P2P era la prima versione di Skype. In questo caso, la rete P2P veniva utilizzata per creare **una connessione diretta tra gli utenti effettuando la chiamata direttamente tra i nodi**, anziché passare attraverso un server centrale.

In sintesi, le reti P2P sono una **forma di comunicazione e condivisione di risorse tra utenti che si basano sulla decentralizzazione e l'interazione diretta tra le macchine, senza la necessità di un server centrale**. Sono ampiamente utilizzate per la condivisione di file e per altre attività, ma devono essere utilizzate con cautela poiché possono presentare anche rischi e dei limiti in termini di sicurezza, scalabilità, velocità e privacy.

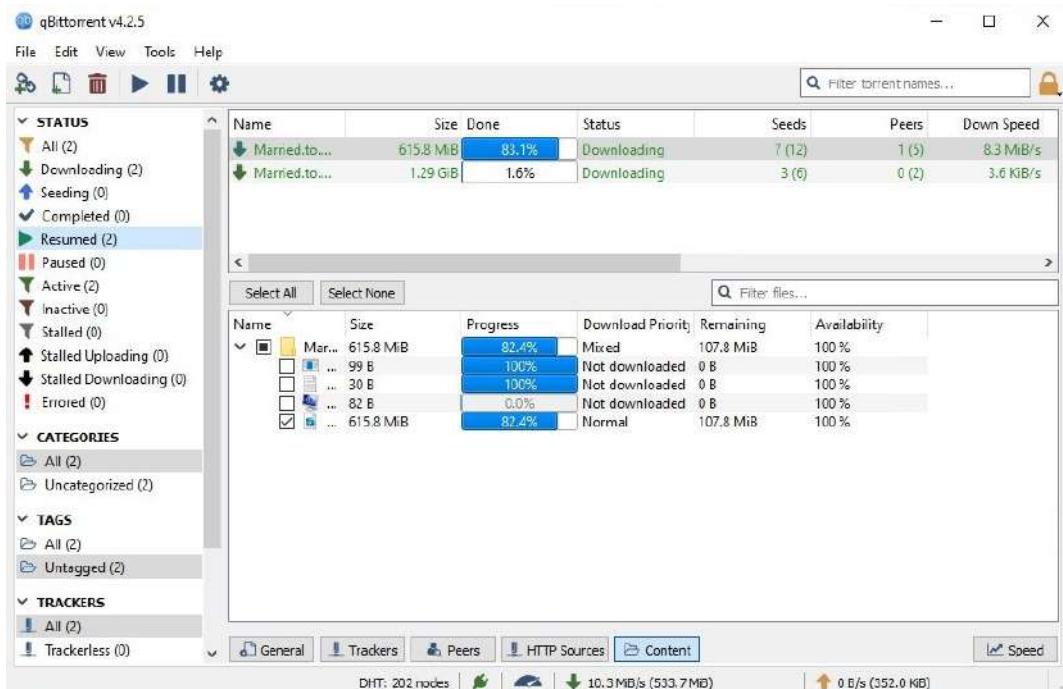
3.4

La rete p2p di BitTorrent

Informatica

Basic

BitTorrent si è diffuso nel web a partire dagli anni 2000, grazie al suo creatore Bram Cohen. Questo protocollo informatico è stato progettato per consentire il download di grandi file da Internet in modo più efficiente rispetto ai metodi di download tradizionali. Invece di scaricare un file da un server centrale, **il protocollo consente ai download di avvenire contemporaneamente da diverse fonti, distribuite sui computer di tutti gli utenti all'interno della rete.** Tutti i computer connessi alla rete diventano un database distribuito da cui vengono scaricati file di qualsiasi tipo.



Questo significa che più persone possono condividere parti di un file simultaneamente, riducendo il carico su un server centrale e accelerando il download complessivo. Tale sistema di condivisione peer-to-peer si basa **su un'infrastruttura distribuita e decentralizzata**, in cui ogni utente che scarica un file diventa automaticamente una fonte di condivisione per altri utenti che desiderano scaricare lo stesso file.

Ma perché le autorità non sono mai riuscite a fermare il network?

Torrent non è stato fermato principalmente **proprio perché utilizza una rete peer-to-peer**, il che rende difficile per le autorità identificare e fermare i singoli utenti che condividono o scaricano file. L'unico modo per "interrompere" la rete sarebbe spegnere e/o confiscare tutti i computer sparsi per il mondo che contribuiscono alla condivisione di risorse.

In generale, le autorità governative si sono concentrate maggiormente sulla rimozione dei siti web che integravano la rete al loro interno e/o sulla sanzione degli utenti che condividono e scaricano contenuti illegali tramite la rete BitTorrent. Tuttavia, come detto in precedenza, l'anonimato e la natura decentralizzata della rete BitTorrent rendono difficile per le autorità perseguire con successo gli utenti che utilizzano la rete.

3.5

Business

● Basic

Le controversie verso BitTorrent e l'idea di Spotify

The Pirate Bay è stato uno dei più **grandi siti di condivisione di file peer-to-peer** al mondo che utilizzava il protocollo Torrent. Tuttavia, è stato al centro di numerose controversie legali con le etichette discografiche e cinematografiche.

Il sito web è stato fondato in Svezia nel 2003 e ha permesso agli utenti di condividere e scaricare file, inclusi film, programmi TV, musica e videogiochi. Tuttavia, molte di queste opere erano protette da copyright e le etichette discografiche e cinematografiche hanno accusato The Pirate Bay di **violazione del diritto d'autore**.

Nel 2009, gli amministratori di The Pirate Bay sono stati condannati a un anno di reclusione e a una multa di 2,7 milioni di euro per aver violato il diritto d'autore. Tuttavia, il sito web è rimasto attivo e continuato ad essere al centro di **controversie legali per molti anni**. Il protocollo Torrent è stato uno dei primi modi per la condivisione peer-to-peer di file digitali su larga scala, tra cui la musica. Questo tipo di condivisione era spesso associato alla pirateria, e molti artisti e case discografiche hanno combattuto contro questa pratica.

La nascita di Spotify si inserisce proprio in questo contesto **come una soluzione legale ed alternativa per l'ascolto di musica in streaming, attraverso un approccio centralizzato**, offrendo agli utenti accesso a una vasta libreria di brani, proprio come dentro The Pirate Bay. Grazie a un modello di business basato sulla pubblicità o su un abbonamento premium, Spotify ha offerto una fonte di reddito per gli artisti e le etichette discografiche, senza violare i diritti d'autore.

Fonti

- ▶ <https://www.italiaoggi.it/archivio/pirate-bay-maxi-multa-e-carcere-1601513>

3.6

Informatica

● Medium

Trasmissione dei dati e performance (Spotify vs BitTorrent)

La velocità di trasmissione dei dati in Spotify è generalmente **molti volte più rapida rispetto alla rete di Torrent** perché Spotify utilizza un modello di distribuzione centralizzato per fornire la musica ai suoi utenti, mentre la rete di torrent utilizza un modello decentralizzato.

In un modello centralizzato come quello utilizzato da Spotify, **la musica viene archiviata su server centrali**, e gli utenti si connettono a questi server per scaricare la musica. Questi server sono generalmente progettati per fornire una grande quantità di dati in modo rapido e affidabile ai client, il che significa che gli utenti di Spotify possono scaricare la musica quasi istantaneamente, a seconda della velocità della loro connessione Internet.

D'altra parte, la rete di torrent è decentralizzata, il che significa che la musica viene distribuita tra gli

utenti che scaricano e condividono i file tramite il protocollo BitTorrent. Mentre questo modello può essere molto efficiente nel distribuire grandi file tra molte persone, **la velocità di download dipende dalla disponibilità dei peer con cui condividere il file** e dalle prestazioni del software utilizzato per scaricare il file.

La velocità dipende dalla grandezza dello Swarm. Il concetto di Swarm, letteralmente “sciame”, si riferisce **l'insieme di tutti i nodi in grado di fornire quel singolo torrent**. Più grande è lo sciame maggiori possibilità ci sono di beccare nodi che dispongono il file all'interno del loro client.

Di seguito, una tabella tecnica di confronto tra Spotify e la rete di torrent:

Caratteristiche	Spotify	Rete di Torrent
Definizione	<i>Spotify è un servizio di streaming musicale che offre accesso a milioni di brani musicali su richiesta, con una vasta gamma di playlist e funzionalità personalizzate.</i>	<i>La rete di Torrent è una rete peer-to-peer utilizzata per lo scambio di file di grandi dimensioni, come film, musica e software, tra gli utenti della rete.</i>
Legittimità	<i>Spotify offre un servizio legale per lo streaming di musica, con un vasto catalogo di brani musicali autorizzati dalle case discografiche.</i>	<i>La rete di Torrent viene spesso utilizzata per condividere illegalmente file protetti da copyright, come film, musica e software.</i>
Qualità audio	<i>Spotify offre un audio di alta qualità, con un bitrate massimo di 320 kbps. Inoltre, il servizio utilizza l'algoritmo di compressione audio Ogg Vorbis per mantenere un audio di alta qualità con un minor utilizzo di dati.</i>	<i>La qualità audio nella rete di Torrent dipende dalla fonte del file e dalla velocità di upload dei peer coinvolti nella condivisione del file. Tuttavia, la qualità audio può variare notevolmente a seconda del file scaricato.</i>
Interfaccia utente	<i>Spotify ha un'interfaccia utente intuitiva e facile da usare, con funzionalità personalizzate come playlist e consigli di brani basati sulle preferenze dell'utente.</i>	<i>La rete di Torrent non ha un'interfaccia utente integrata, ma richiede l'utilizzo di un client di Torrent per accedere alla rete e scaricare i file.</i>
Velocità di download	<i>La velocità di download su Spotify dipende dalla larghezza di banda dell'utente e dalla qualità dell'audio selezionata. Tuttavia, la velocità di download è generalmente rapida grazie all'utilizzo di server dedicati per lo streaming di musica.</i>	<i>La velocità di download nella rete di Torrent dipende dalla fonte del file e dalla velocità di upload dei peer coinvolti nella condivisione del file. Tuttavia, la velocità di download può essere più lenta rispetto allo streaming di musica su Spotify.</i>
Costi	<i>Spotify offre un servizio a pagamento con abbonamenti mensili che in genere vanno da 9,99 a 14,99 euro al mese, ma offre anche un servizio gratuito con pubblicità e funzionalità limitate.</i>	<i>La rete di Torrent è generalmente gratuita, ma l'accesso a contenuti illegali protetti da copyright può comportare conseguenze legali. Inoltre, l'utilizzo di un client di Torrent può richiedere l'acquisto di una licenza.</i>

3.7

Informatica

● Hard

Come funziona la rete p2p di BitTorrent?

Dal punto di vista informatico come viene trasferito un file da un nodo all'altro all'interno della rete peer to peer di BitTorrent?

1. Il file da condividere **viene suddiviso** in più parti di dimensioni variabili, che vengono identificate da un hash univoco.
2. Un utente che desidera scaricare il file cerca il torrent del file su **uno dei siti web di torrent**. Il torrent è un file di piccole dimensioni che contiene le informazioni necessarie per accedere alle diverse fonti che condividono le varie parti del file.
3. L'utente apre il file torrent con un client BitTorrent, che inizialmente **contatta un tracker** che tiene traccia delle fonti che condividono il file all'interno della rete.
4. Il tracker restituisce al client BitTorrent **un elenco di fonti disponibili** che condividono il file, insieme a un elenco delle parti del file che ogni fonte possiede.
5. Il client BitTorrent si connette alle diverse fonti e scarica le parti del file in parallelo. In questo modo, il download viene accelerato, poiché il client può scaricare parti di file da diverse fonti contemporaneamente.
6. Quando il client BitTorrent scarica una parte del file, essa viene verificata con l'**hash univoco corrispondente**. Se l'hash è corretto, la parte viene salvata nel file completo.
7. Quando tutte le parti del file sono state scaricate, il client BitTorrent le combina in un unico file completo.
8. Una volta che l'utente ha scaricato il file completo, il client BitTorrent può continuare a condividere il file con altri utenti che desiderano scaricarlo, utilizzando le parti che ha scaricato come fonti di condivisione.
9. L'utente può scegliere di interrompere la condivisione del file in qualsiasi momento, ma è importante notare che il sistema BitTorrent **si basa sulla condivisione tra utenti e che, quindi, più utenti condividono il file, più velocemente gli altri possono scaricarlo**.



Hash

Definizione: Una funzione di hash è una funzione matematica che da un input (esempio una stringa di lunghezza predefinita) deriva un output (una stringa tipicamente inferiore a quella originaria), definita come hash. Cambiando anche solo un carattere dell'input, l'output cambia completamente.

Fonte

<https://www.borsaitaliana.it/borsa/glossario/hash.html>

Questi sono i **passaggi principali del funzionamento del protocollo torrent**.

Per collegarsi al network BitTorrent e utilizzare il protocollo torrent, di solito non è necessario aprire porte di rete specifiche nel tuo PC, poiché il client BitTorrent utilizza di default alcune porte comuni che sono generalmente aperte sulla maggior parte dei router e dei firewall.

Le **porte sono numeri di riferimento che identificano specifici servizi o programmi** che vengono eseguiti su un computer o su un altro dispositivo connesso a una rete. **Nelle reti peer-to-peer, le porte svolgono un ruolo importante nel consentire la comunicazione tra i diversi computer o dispositivi che partecipano alla condivisione di file.**

In una rete peer-to-peer, ogni computer o dispositivo che partecipa alla condivisione di file utilizza un software client BitTorrent per connettersi ad altri computer o dispositivi che hanno lo stesso software. Il client BitTorrent utilizza le porte per stabilire le connessioni tra i computer e per scambiare dati tra di essi.

In pratica, quando un computer invia una richiesta a un altro computer sulla rete peer-to-peer, la richiesta viene inviata tramite una porta specifica. Il computer ricevente riceve la richiesta sulla porta specifica e risponde inviando i dati richiesti sulla stessa porta.

Pertanto, **quando si utilizza un client BitTorrent per partecipare alla condivisione di file su una rete peer-to-peer, è importante assicurarsi che le porte utilizzate dal client siano aperte sul router o sul firewall del proprio computer.**

3.8

Informatica

● Basic

Differenze tra le reti peer to peer: BitTorrent, Bitcoin, Ethereum

La rete peer-to-peer è l'architettura utilizzata da BitTorrent, ma anche da reti come Bitcoin ed Ethereum. Tutte queste reti P2P si basano sulla **condivisione di dati tra i nodi della rete, senza la necessità di un server centralizzato che svolga il ruolo da amministratore della rete.**

Tuttavia, reti come Bitcoin o Ethereum hanno un livello di **complessità informatica relativamente più alta**, perché l'obiettivo di queste reti è poter scambiare e trasmettere del valore tra i nodi, attraverso unità finite e non duplicabili, definibili come **digital assets**. Anche i nodi della rete hanno dei compiti e dei ruoli differenti, per soddisfare gli obiettivi del protocollo e garantire sicurezza rispetto alle informazioni scambiate e custodite nella rete.

Per esempio, all'interno della rete peer-to-peer di torrent esistono due tipologie di nodi:

- **Seeders:** sono i nodi che dispongono del file completo e lo condividono con gli altri nodi nella rete.
- **Leechers:** sono i nodi che stanno scaricando il file dalla rete e, allo stesso tempo, condividono il pezzo del file che hanno già scaricato con altri nodi nella rete.

Diversamente, per Bitcoin, Ethereum e simili, i nodi hanno ruoli e compiti diversi, **come conservare in sicurezza tutte le transazioni finanziarie avvenute nella rete e garantire che nessuno possa duplicare i propri digital assets**. Inoltre, come vedremo in seguito, ci sono anche delle differenze tra le attività svolte dai nodi della rete Bitcoin con quelle svolte nella rete di Ethereum.

Una ulteriore differenza che possiamo trovare nelle reti peer to peer è relativa alla tipologia di database distribuito che viene utilizzato per conservare le informazioni. Per esempio, nella rete BitTorrent, i nodi utilizzano un database distribuito chiamato Distributed Hash Table (DHT). Il DHT consente di archiviare e cercare le informazioni sulle posizioni dei file e dei nodi nella rete, senza la necessità di un server centrale.

Mentre nella rete Bitcoin ed Ethereum, i nodi utilizzano un database distribuito differente, chiamato **Blockchain**, il quale viene aggiornato tramite la **collaborazione degli utenti** e solo dopo la risoluzione di un **complesso problema matematico**. D'altra parte, la condivisione di file con Torrent non richiede un sistema di sicurezza simile a quello della rete Bitcoin, ma piuttosto si basa sulla semplice condivisione di dati tra i nodi della rete.

Importante avere in mente quindi che esistono anche all'interno delle reti peer to peer delle differenze di architettura, che sposano l'obiettivo della rete stessa. Mentre la rete peer-to-peer di Torrent viene utilizzata principalmente per la condivisione di file digitali, la rete di Bitcoin ed Ethereum sono state progettate per fornire **un sistema sicuro e resistente alla censura per la registrazione di transazioni finanziarie e scambiare digital assets**.

4

Il nodo, il wallet e la blockchain

- 4.1 Il nodo nella rete peer to peer di Bitcoin
- 4.2 Come diventare un nodo nella rete di Bitcoin?
- 4.3 L'infrastruttura del database distribuito
- 4.4 La struttura del blocco
- 4.5 Modello input e output delle transazioni nel blocco
- 4.6 Quanti sono i nodi nella rete e che ruolo svolgono?
- 4.7 Quante tipologie di wallet esistono?
- 4.8 Come vengono prioritizzate le transazioni dal nodo minatore?
- 4.9 Ottimizzazione delle transazioni nel blocco
- 4.10 Come avviene il collegamento tra un blocco e l'altro?

4.1

Teoria dei Sistemi Distribuiti

● Basic

Il nodo nella rete peer to peer di Bitcoin

Un nodo in una rete informatica è un dispositivo connesso ad una rete e che partecipa allo scambio di informazioni o alla fornitura di servizi.

Come abbiamo analizzato in precedenza, in una rete peer-to-peer (P2P), ogni nodo svolge sia il ruolo di client che di server, permettendo ai dispositivi di comunicare direttamente tra loro senza la necessità di un server centrale.

In una rete P2P come Bitcoin, ogni nodo può partecipare alla rete **scaricando un software compatibile con la rete, può aggiornare e mantenere una copia completa della blockchain**, ovvero il registro pubblico e distribuito contenente tutte le transazioni effettuate sulla rete dagli utenti.

Sempre grazie ad altri software dedicati, **un nodo può avere un proprio portafoglio virtuale, attraverso il quale può custodire i propri asset digitali ed effettuare delle transazioni con gli altri nodi della rete**.

Ogni transazione effettuata da un nodo verrà propagata nella rete blockchain, verificata da altri nodi, ed aggiunta dentro il database distribuito.

Possiamo immaginare questo registro distribuito come un orologio globale, il quale viene aggiornato **senza la necessità in un amministratore centrale ma grazie alla collaborazione di tutti i nodi. Ogni nuovo aggiornamento, è collegato al precedente, e mostra la nuova redistribuzione dei digital assets all'interno i nodi della rete**. In questo modello, ogni nodo ha il controllo sulle proprie informazioni, sui propri digital assets e sulle proprie transazioni, rendendo la rete più resistente a eventuali attacchi o malfunzionamenti. Inoltre, non esiste un punto centrale di fallimento, il che significa che la rete è meno vulnerabile rispetto ad una rete client-server.

In sintesi, un nodo in una rete P2P come Bitcoin è un dispositivo che partecipa alla rete mantenendo una copia della blockchain e verificando le transazioni effettuate sulla rete, rendendo la rete più decentralizzata e resistente a eventuali problemi.

4.2

Teoria dei Sistemi Distribuiti

● Basic

Come diventare un nodo nella rete di Bitcoin?

Per poter partecipare alla rete di Bitcoin, basta scaricare un software che permette all'utente di diventare un nodo della rete (analogamente a bitTorrent), scaricando sul proprio computer uno tra i suoi software client come qBittorrent.

Bitcoin Core è uno tra i principali software utilizzati dai nodi della rete. Questi software si collegano alla rete tramite il codice sorgente. Il **codice sorgente** di Bitcoin è **open-source**, cioè a codice sorgente aperto, permettendo a tutti di visionare il codice e di crearsi in locale un eseguibile, senza doversi fidare di qualcuno.



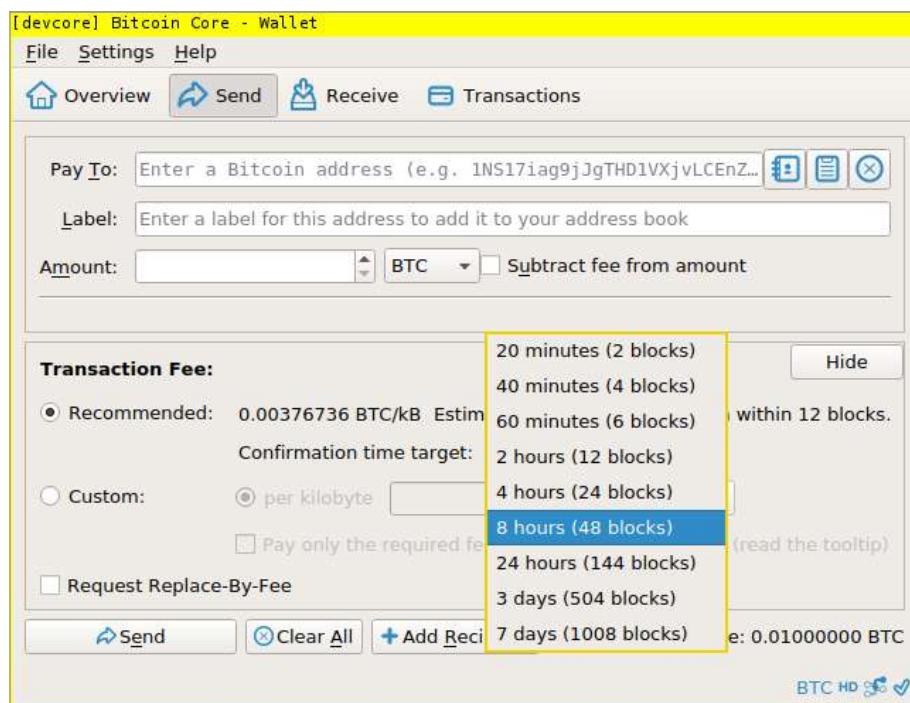
Codice Sorgente

In informatica, il codice sorgente è il testo di un algoritmo di un programma scritto in un determinato linguaggio di programmazione, compreso all'interno di un file sorgente, che definisce il flusso di esecuzione del programma stesso, ovvero la sua codifica software.

Open-Source

Software di cui l'utente finale, che può liberamente accedere al file sorgente, è in grado di modificare a suo piacimento il funzionamento, correggere eventuali errori, ridistribuire a sua volta la versione da lui elaborata. L'esempio più noto è il sistema operativo Linux.

In quanto open-source, il codice sorgente può essere immaginato come un programma informatico con delle regole pubbliche e revisionabili da tutti i nodi della rete (i.e. peer review). Per esempio, tra queste regole, c'è anche chiaramente quella relativa al numero dei digital assets creati dalla rete ed utilizzabili dagli utenti per effettuare le transazioni l'uno con l'altro. Infatti, le regole del codice sorgente di Bitcoin definiscono un numero **finito di 21 milioni di unità di bitcoin, creati dal 2009, con una periodicità programmata e deterministica**. Questa caratteristica di trasparenza garantisce **l'assenza di assimmetria informativa tra i nodi del network**.



La struttura di un software come Bitcoin Core è composta da diversi componenti interconnessi, ognuno dei quali svolge una specifica funzione. Tra questi componenti, si possono citare i seguenti:

- **Interfaccia utente:** fornisce un'interfaccia grafica che permette all'utente di interagire con il software.
- **Client Bitcoin:** è il cuore del software e permette di interagire con il codice sorgente della rete Bitcoin. Il client Bitcoin permette di convalidare le transazioni e i blocchi sulla blockchain, di partecipare al processo di consenso distribuito e di gestire il portafoglio Bitcoin.
- **Database distribuito:** rappresenta la blockchain, un database dove viene conservata l'intera storia della rete, ovvero la lista di tutti i blocchi che sono stati validati dalla rete Bitcoin. Il database di blockchain viene aggiornato in tempo reale su ogni nodo, aggiungo un blocco dopo l'altro, **in maniera periodica come un orologio**.

- **Motore di convalida (consenso):** è la componente che si occupa di verificare la validità delle transazioni e dei blocchi sulla blockchain. In particolare, il motore di convalida verifica che le transazioni rispettino le regole del protocollo Bitcoin, che le firme digitali siano valide e che le transazioni non siano state già utilizzate. Inoltre, il motore di convalida verifica che i nuovi blocchi siano validi e che rispettino le regole del protocollo Bitcoin.
- **Portafoglio di chiavi crittografiche:** rappresenta un contenitore dove si possono visualizzare ed utilizzare delle chiavi crittografiche definite come pubblica e privata. La pubblica è l'indirizzo verso il quale è possibile ricevere i propri digital assets, la privata permette di spendere i digital assets verso terzi, firmando le transazioni. Come vedremo **in seguito alcuni software si limitano nell'offrire solo questo componente, classificando il nodo come "light node".**
- **Strumenti di sviluppo:** sono una serie di strumenti che permettono di sviluppare applicazioni basate su Bitcoin Core come le **API**.



API

API è l'abbreviazione di *interfaccia di programmazione delle applicazioni* (*application programming interface*), un insieme di definizioni e protocolli per la creazione e l'integrazione di software applicativi.

Oltre a Bitcoin Core esistono anche altre tipologie di programmi informatici e dispositivi hardware che permettono all'utente di collegarsi alla rete Bitcoin, scaricando il software all'interno del proprio computer o del proprio smartphone.

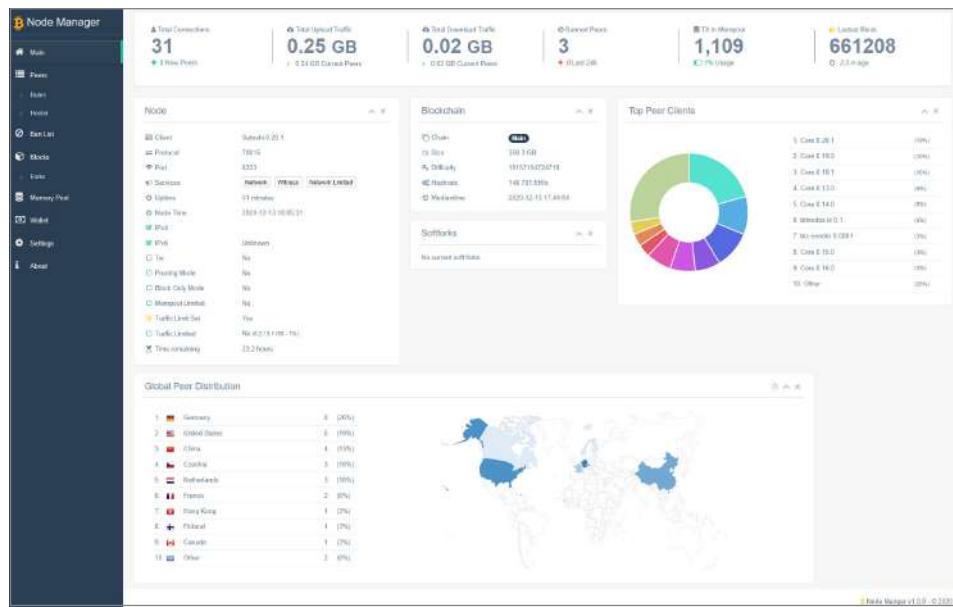
Teoria dei Sistemi Distribuiti

● Medium

4.3 L'infrastruttura del database distribuito

La blockchain è un **database lineare e crescente che segue un modello up-and-only (append)** ovvero i dati vengono inseriti in modo sequenziale e non possono essere modificati o cancellati una volta che sono stati registrati. Questo database può essere immaginato come un registro contabile pubblico all'interno del quale ci sono tutti i saldi finanziari dei singoli nodi e tutte le transazioni finanziarie che sono avvenute all'interno della rete dalla sua nascita.

La blockchain può inserirsi all'interno della più ampia categoria dei Distributed Ledger Technologies (DLT). Coloro che scaricano all'interno del proprio computer tutti i dati del database distribuito vengono definiti come full node. Ogni full node contiene l'intera struttura dati, dal primo blocco creato fino al blocco corrente. Inoltre, ogni full node è collegato all'interno del network con altri nodi, con i quali aggiorna automaticamente ed in maniera sincrona gli aggiornamenti dei saldi e delle transazioni.



Ogni singolo blocco della blockchain contiene le transazioni create dagli utenti della rete, in un certo periodo di tempo, e un codice unico che fa riferimento ai dati del blocco precedente, formando così una lunga catena di blocchi. Grazie a questo codice unico, la catena dei blocchi può rimanere inalterata nel tempo, garantendo l'immutabilità delle transazioni e la loro integrità nel tempo.



Fun Facts

Nel 3 gennaio 2009, il fondatore di Bitcoin, Satoshi Nakamoto, ha creato il primo blocco della blockchain, noto come "Blocco Genesi". Questo blocco contiene un messaggio storico, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Questo messaggio ha una forte rilevanza storica, in quanto fa riferimento a un articolo del quotidiano The Times che parlava di un nuovo piano di salvataggio pubblico per le banche durante la crisi finanziaria del 2008.

Molte delle reti peer to peer nate insieme a Bitcoin o Ethereum utilizzano questa architettura per archiviare le informazioni finanziarie della rete. Tuttavia, possono differire in alcuni aspetti come: la velocità, la dimensione del blocco e ulteriori differenze relative alla programmazione ed alla automazione delle transazioni.

Software	Descrizione
Blockchain di Bitcoin	Un database distribuito all'interno di una rete peer to peer utilizzato per la gestione delle transazioni bitcoin
Oracle RDB	Un database relazionale che utilizza un'architettura client-server tradizionale per catalogare informazioni
Apache Cassandra	Un database distribuito che utilizza una architettura client-server, dove i nodi collaborano per fornire servizi al database.

Nella famiglia delle DLT, si possono includere anche database come Oracle RDB e Apache Cassandra. Oracle RDB è un sistema di gestione di database relazionali distribuiti utilizzato per applicazioni aziendali di livello enterprise, mentre Apache Cassandra è un sistema di database distribuito open source progettato per gestire grandi volumi di dati strutturati e non strutturati.

Nonostante facciano parte della stessa famiglia tecnologica, ciò che differenzia maggiormente la blockchain da questi altri database distribuiti è la modalità con cui le informazioni vengono inserite, validate e visualizzate all'interno del database. Infatti, non vi è **nessun amministratore unico del database a svolgere queste funzioni**, ma come vedremo, il database viene aggiornato attraverso un processo dinamico svolto dalla maggioranza dei nodi che hanno conservato il database sul proprio dispositivo.

4.4

Teoria dei Sistemi Distribuiti

● Medium

La struttura del blocco

Il blocco è quindi **l'unità fondamentale** della blockchain. Mediamente nella software di Bitcoin, ogni singolo blocco viene collegato al precedente ogni 10 minuti circa. Per Ethereum, invece, circa ogni 12 secondi.

La struttura del blocco può variare a seconda dei digital assets o della blockchain specifica, ma in generale è composta da **tre parti principali**: l'intestazione del blocco, il corpo del blocco e il suo valore hash. All'interno dell'intestazione del blocco troviamo diversi parametri che aiutano a identificare il blocco e a garantire la sicurezza della rete.

Campo	Descrizione
Version	La versione del blocco, che indica la versione del software utilizzato per creare il blocco.
Previous Block Hash	L'hash del blocco precedente nella catena di blocchi.
Merkle Root	L'hash della transazione radice Merkle Tree, che rappresenta l'elenco delle transazioni incluse nel blocco.
Timestamp	L'orario in cui il blocco è stato creato, registrato come un timestamp UNIX.
Difficulty Target	Il livello di difficoltà necessario per validare il blocco, che viene regolato automaticamente dalla rete in base alla potenza di calcolo disponibile.
Nonce	Un valore arbitrario utilizzato durante il processo di mining per trovare il valore dell'hash del blocco che soddisfa la difficoltà target.
Transaction Count	Il numero di transazioni incluse nel blocco.

I primi quattro elementi (Version, Previous Block Hash, Merkle Root e Timestamp) vengono utilizzati per verificare l'intera storia della rete e che il software utilizzato nel client sia aggiornato all'ultima versione. Il Difficulty Target e il Nonce sono due parametri definiti dalle regole del protocollo e determinano la difficoltà di generazione del blocco in quel momento nonché la risoluzione del problema matematico svolto da alcuni nodi della rete. La struttura qui presentata è specificamente riferita alla blockchain di Bitcoin. Le transazioni sono contenute nel corpo del blocco e rappresentano **le operazioni che sono state effettuate sulla rete dagli utenti** e possono includere l'invio di digital assets da un indirizzo ad un altro, o la registrazione o l'esecuzione di un comando di un contratto intelligente.

Infine, Il valore hash del blocco è un valore numerico univoco che viene calcolato sulla base dei dati contenuti nel blocco, compreso l'intestazione del blocco, le transazioni e il nonce. Questo valore hash viene utilizzato **per garantire l'immutabilità dei dati del blocco**. Se anche un solo bit di dati all'interno del blocco viene modificato, il valore hash cambia completamente, rendendo evidente la modifica.

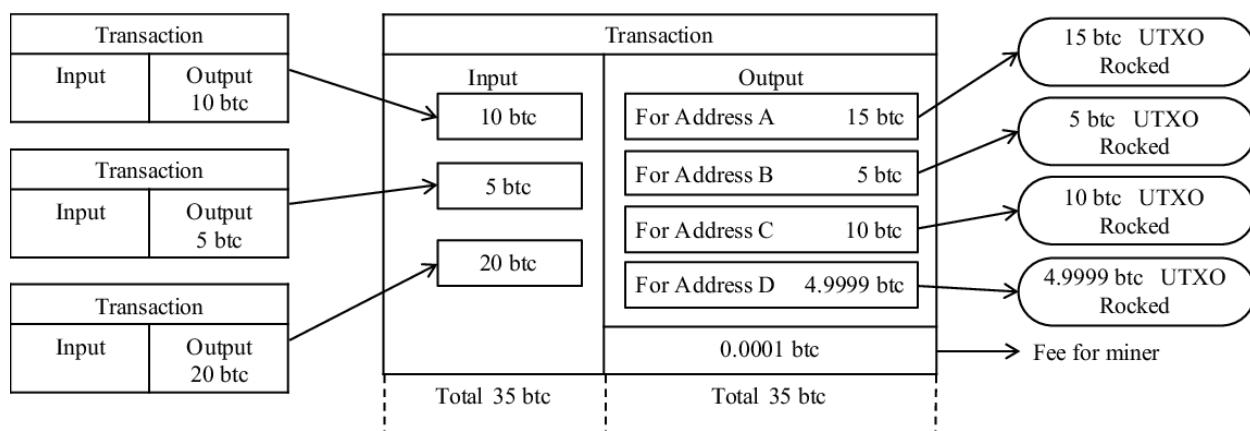
4.5

Teoria dei Sistemi Distribuiti

• Medium

Modello input e output delle transazioni

In generale, le transazioni sulla blockchain di Bitcoin sono **basate su un modello input e output (modello UTXO)**. Ogni transazione, infatti, è composta da un indirizzo che invia dei digital assets (input) e un indirizzo che riceve i digital assets (output). **La differenza di tutti gli input e di tutti gli output all'interno di ogni singolo deve fare zero, mantenendo così il numero degli asset sempre uguali nel tempo.** Ogni input deve essere firmato digitalmente con la chiave privata del mittente per dimostrare che la transazione è stata autorizzata.



Anche per altre blockchain il modello nel gestire le informazioni è abbastanza simile. Tuttavia, alcune reti come Ethereum permettono di creare anche altre tipologie di transazioni. Infatti, come vedremo nel capitolo 3, il **protocollo Bitcoin non è turing complete**, mentre quello di Ethereum lo è. Questo fa sì gli utenti possano gestire e creare altre tipologie di transazioni, grazie all'utilizzo di altri software dedicati all'automatizzazione, chiamati **smart contract**. Approfondiremo nel prossimo capitolo questo concetto.



Turing complete

Definizione: Un linguaggio di programmazione è Turing-complete se la sua semantica permette di implementare una qualsiasi macchina di Turing. Un linguaggio Turing-complete può essere usato per risolvere qualsiasi problema che ammetta soluzione. Quasi tutti i linguaggi di programmazione sono Turing complete.

Fonte: <https://www.unife.it/scienze/informatica/insegnamenti/programmazione-e-laboratorio/materiale-didattico-anni-precedenti/materiale-didattico-a-a-2016-17/diapositive/010-algoritmi-e-programmi#:~:text=Turing%20Completeness,di%20programmazione%20sono%20Turing%20complete.>

Per ogni transazione eseguita, il mittente deve pagare una tassa per farla elaborare e farla inserirla nella blockchain. Esiste infatti una tipologia di nodo chiamato **nodo minatore** che ha il ruolo di creare il corpo del blocco, inserire le transazioni degli altri utenti, compilare l'intestazione del blocco e risolvere un problema matematico. Al raggiungimento dell'obiettivo, il minatore potrà collegare il blocco nuovo a quello precedente, **aggiornando la blockchain e ricevendo tutte le commissioni pagate dai nodi per quelle specifiche transazioni.**

Infine, esiste una ulteriore transazione speciale chiamata **coinbase transaction**, generata direttamente dal protocollo per **ricompensare il minatore (miner) che ha trovato la soluzione al puzzle crittografico per il blocco e che ha aggiornato la rete**. Questa ulteriore transazione non ha input, ma ha un output con una nuova quantità di bitcoin, insieme a eventuali commissioni di transazione. Come vedremo, questa regola è inscritta nel software open-source e determina le unità di bitcoin prodotte per ogni blocco post processo di creazione.

4.6

Teoria dei Sistemi Distribuiti

● Basic

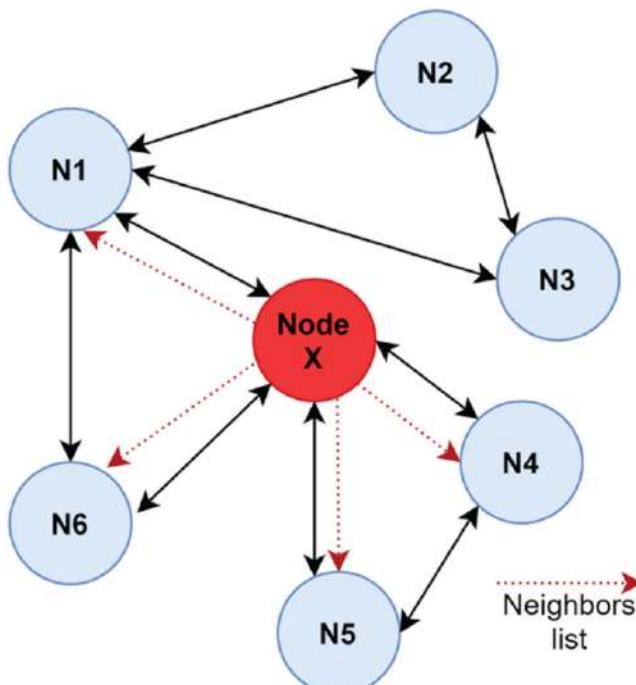
Quanti sono i nodi nella rete e che ruolo svolgono?

Nonostante sia la rete sia piatta, ovvero non esiste un nodo con più potere degli altri, ci sono delle categorizzazioni da fare. In generale, i nodi sulla rete di Bitcoin possono essere suddivisi in tre categorie principali:

- **Light node (nodo leggero)**
- **full node (nodo pieno)**
- **Miner Node (nodo minatore)**

I **light node** sono i nodi che possono solamente inviare e ricevere i bitcoin, senza partecipare a processi di validazione e aggiornamento della rete.

I **full node** sono i nodi che scaricano sul proprio dispositivo l'intera storia della rete, e quindi tutto il database distribuito. Inoltre, si occupano di propagare le informazioni sulla rete, tra un nodo e l'altro. Per esempio, quando un light node invia una transazione questa viene propagata da un full node all'altro. Questa categoria di nodi fa del "**gossip**". Questo termine viene utilizzato per descrivere un **processo di comunicazione decentralizzato** in cui i nodi scambiano informazioni con i loro vicini di rete, diffondendo informazioni a più nodi attraverso la rete.



Il **processo di gossiping** consente di diffondere informazioni in modo rapido ed efficiente nella rete, senza la necessità di un'infrastruttura centralizzata.

Infine, i nodi minatori o miner node hanno dei computer più avanzati e si occupano di costruire i nuovi blocchi della blockchain, attraverso la propria potenza di calcolo. Inoltre, i nodi minatore in cambio del loro lavoro e della energia spesa dai loro computer, guadagnano i nuovi digital assets generati dalla rete e delle commissioni sulle singole transazioni create dagli altri nodi. Come vedremo, il ruolo più attivo nella gestione delle informazioni e dell'aggiornamento della rete, è svolto dalla relazione tra full node e miner.

Tipo di nodo	Descrizione	Funzione principale
Full Node	<i>Un nodo completo (full node) è un nodo che mantiene una copia completa e aggiornata dell'intera blockchain.</i>	<i>La funzione principale di un nodo completo è quella di validare le transazioni e i blocchi della blockchain, e di propagare le informazioni ad altri nodi nella rete. Inoltre, un nodo completo può anche fornire servizi come l'elaborazione di transazioni e la consultazione della blockchain.</i>
Light Node	<i>Un nodo leggero (light node) è un nodo che non mantiene una copia completa della blockchain, ma solo una versione ridotta della stessa.</i>	<i>La funzione principale di un nodo leggero è quella di interrogare i nodi completi per ottenere le informazioni necessarie per validare le transazioni e i blocchi della blockchain. In questo modo, i nodi leggeri possono partecipare alla rete senza dover archiviare l'intera blockchain.</i>
Miner	<i>Un miner è un nodo che utilizza la propria potenza di calcolo per risolvere complessi problemi crittografici e aggiungere nuovi blocchi alla blockchain.</i>	<i>La funzione principale di un miner è quella di validare le transazioni e i blocchi della blockchain, ma anche di competere con gli altri miner per risolvere i problemi crittografici e guadagnare ricompense in digital assets. I miner sono quindi fondamentali per la sicurezza e l'affidabilità della blockchain.</i>

Un elemento che contraddistingue tutti i tre nodi sta nel fatto che per poter comunicare tra loro ed effettuare delle transazioni sulla rete, tutti i nodi hanno bisogno di **un portafoglio digitale (wallet)**, il quale contiene due chiavi, una privata utilizzata per approvare e firmare le transazioni ed una pubblica, immaginabile come un indirizzo, per ricevere i digital assets.

Ecco tutti i passaggi, per effettuare transazione con un wallet all'interno della rete:

1. Il primo passaggio è scaricare e installare un software che consenta di gestire un wallet.
2. Poi, dovrò farmi dare il codice della chiave pubblica dell'utente (indirizzo) a cui voglio inviare i digital assets.
3. Dopo aver ottenuto l'indirizzo del destinatario, devo creare e inviare la transazione utilizzando il mio wallet. La transazione include l'importo che voglio inviare e l'indirizzo del destinatario. Firmo con la chiave privata la transazione, per poi farla propagare in rete.
4. Il wallet diffonde la transazione sulla rete, inviandola ai nodi vicini (full node) a cui è connesso.
5. I nodi vicini ricevono la transazione e la verificano, controllando che la firma fatta dalla chiave privata sia valida e che l'indirizzo del mittente abbia abbastanza fondi per coprire l'importo della transazione e la fee.
6. Se la transazione risulta valida, i nodi la diffondono a loro volta ai nodi vicini a cui sono connessi, creando una sorta di effetto domino.
7. Le transazioni si propagano in modo sempre più ampio, fino a raggiungere i miner della rete.

8. I miner raccolgono le transazioni valide in un blocco e competono per risolvere un problema matematico, al fine di poter pubblicare il blocco sulla blockchain e ricevere la relativa ricompensa in bitcoin.
9. Il primo miner che risolve il problema matematico ha il compito di creare il blocco
10. Le transazioni contenute nel blocco diventano ufficialmente confermate e vengono aggiunte alla blockchain. Le transazioni non confermate rimangono in uno spazio virtuale di transazioni in attesa di essere inserite in un blocco futuro.

Va notato che questa descrizione è **solo un possibile scenario semplificato del funzionamento della rete Bitcoin**, in quanto ci sono diversi fattori che possono influire sulle singole transazioni, come la congestione della rete, la dimensione delle commissioni, il tipo di transazione e altri fattori.

4.7

Teoria dei Sistemi Distribuiti

● Basic

Quante tipologie di wallet esistono?

Per comodità chiameremo nel manuale i light node con il termine wallet. Esistono diverse tipologie di wallet disponibili sul mercato, ognuna delle quali presenta diverse caratteristiche in termini di sicurezza e rischio. In generale, i wallet si possono suddividere in due categorie principali: **online e offline**.

I wallet online sono accessibili tramite una connessione a Internet e sono generalmente più facili da usare, **ma sono anche più vulnerabili agli attacchi informatici**. Tuttavia, alcuni wallet online offrono funzionalità avanzate di sicurezza, come l'autenticazione a due fattori, l'utilizzo di codici pin e l'autorizzazione di transazioni solo da dispositivi autorizzati.

D'altra parte, i wallet offline (o cold wallet) conservano le chiavi private degli utenti in un dispositivo esterno, come un hardware wallet, che non è connesso a Internet. **Ciò significa che il rischio di attacchi informatici è molto ridotto**. Tuttavia, questi wallet sono meno convenienti da usare, poiché gli utenti devono collegare il dispositivo al computer ogni volta che desiderano effettuare una transazione.

In generale, i client wallet possono essere classificati in base al loro modello di gestione delle chiavi e al loro livello di sicurezza come segue:

- **Wallet basati su software installabile**: questi wallet conservano le chiavi private degli utenti su un computer o su un server remoto, che possono essere vulnerabili agli attacchi informatici. Tuttavia, offrono una maggiore convenienza in termini di accesso ai fondi.
- **Wallet hardware**: questi wallet utilizzano dispositivi esterni per conservare le chiavi private degli utenti, il che significa che sono più sicuri dei portafogli basati su software; tuttavia, richiedono un'ulteriore spesa iniziale per l'acquisto del dispositivo.
- **Paper wallet**: questi wallet non conservano le chiavi private in un dispositivo o in una piattaforma online, ma piuttosto stampano le chiavi su carta. Questi wallet sono generalmente considerati tra i più sicuri, poiché le chiavi private sono al sicuro da attacchi informatici. Tuttavia, sono anche i meno convenienti da usare.
- **Multisignature wallet**: questi wallet richiedono l'autorizzazione di più utenti per effettuare una transazione. Ciò significa che i fondi sono più sicuri, poiché i criminali informatici devono violare più chiavi private per accedere ai fondi. Tuttavia, questi wallet sono anche più complessi da usare. Questa funzionalità può essere eseguita sia da wallet basati su software e da wallet basati su hardware.

In sintesi, esistono diverse tipologie di client wallet disponibili sul mercato, ognuna delle quali presenta vantaggi e svantaggi in termini di sicurezza e convenienza. Gli utenti dovranno scegliere un wallet in base alle loro esigenze specifiche e alla loro tolleranza al rischio.

4.8

Teoria dei Sistemi Distribuiti

• Medium

Come vengono prioritizzate le transazioni dal nodo minatore?

All'interno della rete Bitcoin, le transazioni sono ordinate e **priorizzate in base alla quantità di fee pagate dai mittenti per l'inclusione delle transazioni in un blocco**. In pratica, i miners della rete tendono a includere le transazioni che offrono le fee più alte, poiché ciò consente loro di guadagnare di più. Ciò significa che i mittenti che desiderano che la loro transazione venga elaborata rapidamente devono pagare una fee più alta rispetto a chi è disposto ad aspettare un po' di più. In questo modo, il meccanismo di fee costituisce un incentivo per i miners a elaborare le transazioni in modo rapido ed efficiente, mantenendo allo stesso tempo l'integrità e la sicurezza della rete.

Ecco gli stessi passaggi descritti prima ma con qualche dettaglio in più:

- **La transazione viene messa nella mempool:** una volta inviata la transazione, essa viene trasmessa alla rete di blockchain e memorizzata nella mempool, una sorta di "parcheggio" temporaneo dove le transazioni in attesa di essere incluse in un blocco vengono memorizzate.
- **La transazione viene prioritizzata tramite le fee:** le transazioni nella mempool vengono ordinate in base al loro valore in termini di fee. Le transazioni con una fee più alta avranno maggiore priorità nell'essere incluse in un blocco.
- **La transazione inizia a ricevere delle conferme:** una volta che la transazione è stata inclusa in un blocco, inizia a ricevere conferme dalla rete. Le conferme sono la prova che la transazione è stata accettata dalla rete e che il destinatario ha ricevuto i digital assets. Ogni conferma rappresenta un blocco aggiunto alla blockchain dopo quello che contiene la transazione.
- **La transazione viene presa dal miner:** infine, la transazione viene presa dal miner che ha aggiunto il blocco contenente la transazione alla blockchain. Il miner riceve una ricompensa in digital assets per aver aggiunto il blocco alla blockchain e per aver verificato la transazione. Una volta che la transazione viene presa dal miner, il minatore può ottimizzare il corpo del blocco contenente tutte le transazioni avvenute nel network in quell'arco temporale.

4.9

Teoria dei Sistemi Distribuiti

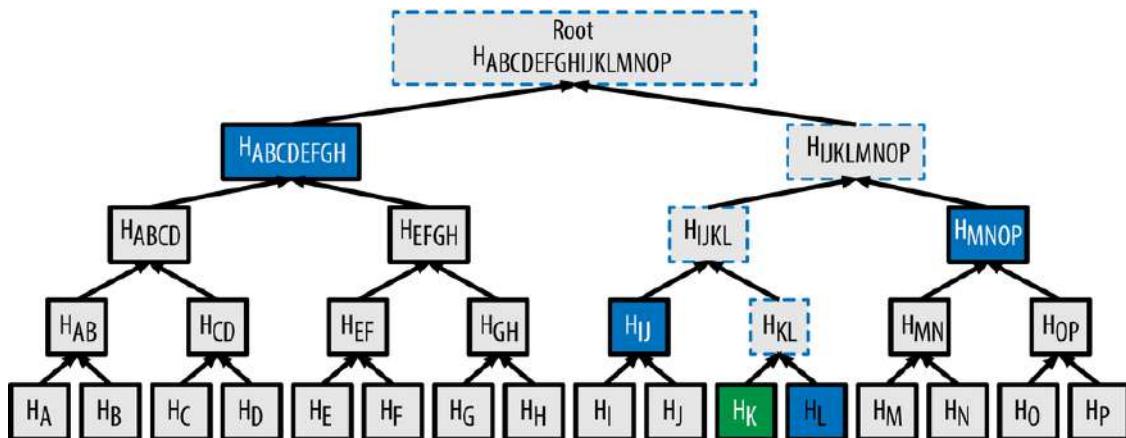
• Medium

Ottimizzazione delle transazioni nel blocco

Il processo di mining in Bitcoin coinvolge diversi passaggi cruciali per l'elaborazione delle transazioni e l'aggiunta di nuovi blocchi alla blockchain. In questo contesto, **i miners sono gli attori che svolgono il ruolo di verificatori e garanti della sicurezza della rete**. Ecco i passaggi che un miner compie nella rete Bitcoin:

- **Scelta delle transazioni dalla mempool:** per costruire un nuovo blocco, il miner deve prima scegliere le transazioni dalla mempool, in cui sono raccolte tutte le transazioni in attesa di essere confermate. Il miner cerca di massimizzare il valore totale delle fee per le transazioni incluse nel blocco, in quanto questo gli consente di guadagnare una ricompensa maggiore.

- **Costruzione del corpo del blocco:** una volta selezionate le transazioni, il miner le organizza all'interno del corpo del blocco in un ordine specifico, utilizzando un algoritmo di hashing crittografico che garantisce l'integrità e la sicurezza delle informazioni. Il miner deve inoltre includere l'hash del blocco precedente e un nonce, un valore arbitrario utilizzato per generare un hash che soddisfi i requisiti di difficoltà della rete.
- **Costruzione del Merkle Tree:** Il miner organizza le transazioni all'interno di un Merkle Tree, una struttura di dati che consente di verificare l'integrità delle informazioni all'interno del blocco. Il miner calcola l'hash di ogni transazione e li organizza in coppie. Successivamente, calcola l'hash di ogni coppia e li organizza in coppie a loro volta, fino a quando non rimane un solo hash, detto root hash. Questo processo permette di garantire l'integrità dei dati nel blocco e semplifica la verifica delle transazioni.



- **Costruzione della testa del blocco:** Infine, il miner calcola l'hash del blocco, che consiste nel combinare l'hash del blocco precedente, il root hash del Merkle Tree, il nonce e altri dati del blocco. Il miner deve continuare a cambiare il nonce fino a quando non trova un valore che consente di generare un hash che soddisfi i requisiti di difficoltà della rete. Questo processo richiede molta potenza di calcolo e, di conseguenza, un miner che trova una soluzione valida viene ricompensato con nuovi Bitcoin. In sintesi, un miner Bitcoin deve selezionare le transazioni dalla mempool, organizzarle all'interno del blocco, costruire il Merkle Tree e la testa del blocco, e infine trovare un nonce valido che permetta di generare un hash soddisfacente i requisiti di difficoltà della rete. Questo processo richiede molta potenza di calcolo e consente ai miners di ricevere ricompense in Bitcoin per la verifica e l'aggiunta di nuovi blocchi alla blockchain.

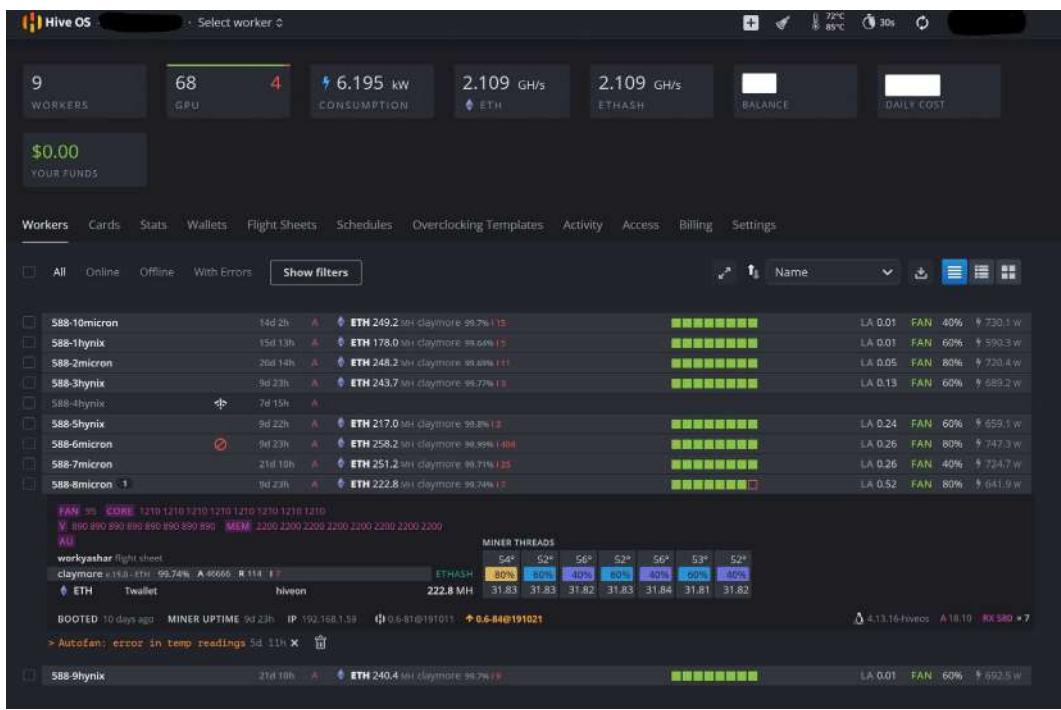
4.10

Teoria dei Sistemi Distribuiti

• Hard

Come avviene il collegamento tra un blocco e l'altro?

I blocchi sono collegati tra loro attraverso il valore hash dell'intestazione del blocco precedente. In altre parole, **il valore hash del blocco precedente viene incluso nell'intestazione del blocco successivo**. In questo modo, ogni blocco contiene il riferimento all'hash del blocco precedente, creando una catena di blocchi (da cui deriva il termine blockchain) che risale all'origine della blockchain. Tuttavia, la sicurezza della blockchain è data dalla energia elettrica che i miner utilizzano per collegare i blocchi. Entriamo nel dettaglio.



Quando un miner risolve un nuovo blocco, invia il blocco alla rete per la validazione. Se la rete (composta da full node e miner) conferma che il blocco è valido, ovvero che tutte le informazioni sono corrette, il miner **viene ricompensato** con un certo numero di digital assets e il blocco viene aggiunto alla blockchain. Un nodo miner specializzato si può collegare ad **un server di mining di Bitcoin, o dispone di un computer specializzato progettato per elaborare transazioni** e creare nuovi blocchi. Il processo di mining richiede una grande quantità di potenza di elaborazione computazionale; quindi, i server di mining sono solitamente equipaggiati con hardware di alto livello, come processori ASIC (Application-Specific Integrated Circuit) e schede grafiche di ultima generazione.



Brute force

Attacco informatico che utilizza metodi per tentativi ed errori per indovinare le credenziali di accesso, le chiavi di sicurezza e altre informazioni sensibili.

Tecnicamente, i minatori all'interno della rete **si sfidano a risolvere un puzzle computazionale complesso**, attraverso un processo di **brute force**, dedicato alla produzione di hash (**hashing power**). L'obiettivo comune è trovare **un hash valido che soddisfi un determinato requisito**. Tale requisito viene espresso dal valore del difficulty target, il quale rappresenta la difficoltà del puzzle computazionale da risolvere. Il primo minatore che riesce a trovare l'hash valido ha il compito di costruire il blocco e collegarlo al precedente.

Per risolvere il puzzle, i miner devono sperimentare diverse combinazioni di nonce. Il **nonce è un valore numerico arbitrario, utilizzato come input all'algoritmo di hashing insieme agli altri elementi del block header**.



Hashing power

Quantità di potenza di calcolo che viene impiegata per risolvere i problemi matematici necessari a confermare le transazioni nella rete Bitcoin.

Il valore del difficulty target viene regolato periodicamente, al fine di mantenere il tempo medio di creazione di un blocco costante, indipendentemente dall'hashing power complessivo della rete. **Se l'hashing power complessivo della rete aumenta, il difficulty target viene aumentato**, al fine di rendere il puzzle computazionale più difficile da risolvere e mantenere il tempo medio di creazione di un blocco costante. Viceversa, se l'hashing power complessivo della rete diminuisce, il difficulty target viene ridotto per rendere il puzzle computazionale più facile da risolvere e mantenere il tempo medio di creazione di un blocco costante.

Questo problema matematico è noto come **Proof of Work (PoW)**, differentemente dall'altro principale modello di consenso, noto come **Proof of Stake (PoS)**.

5

Root of trust e crittografia

- 5.1 Perché la blockchain è sicura?
- 5.2 Basi di crittografia: le funzioni di hashing
- 5.3 Basi di crittografia: il Public Key Infrastructure
- 5.4 Come viene utilizzato il PKI Scheme e l'hashing all'interno di un wallet di digital assets?
- 5.5 Dove viene applicata l'hash function e le PKI nella blockchain?
- 5.6 Considerazione di cybersicurezza per un wallet
- 5.7 Cosa vuol dire “possedere” un digital asset come bitcoin?
- 5.8 Considerazioni sul concetto di pseudo-anonimato

5.1

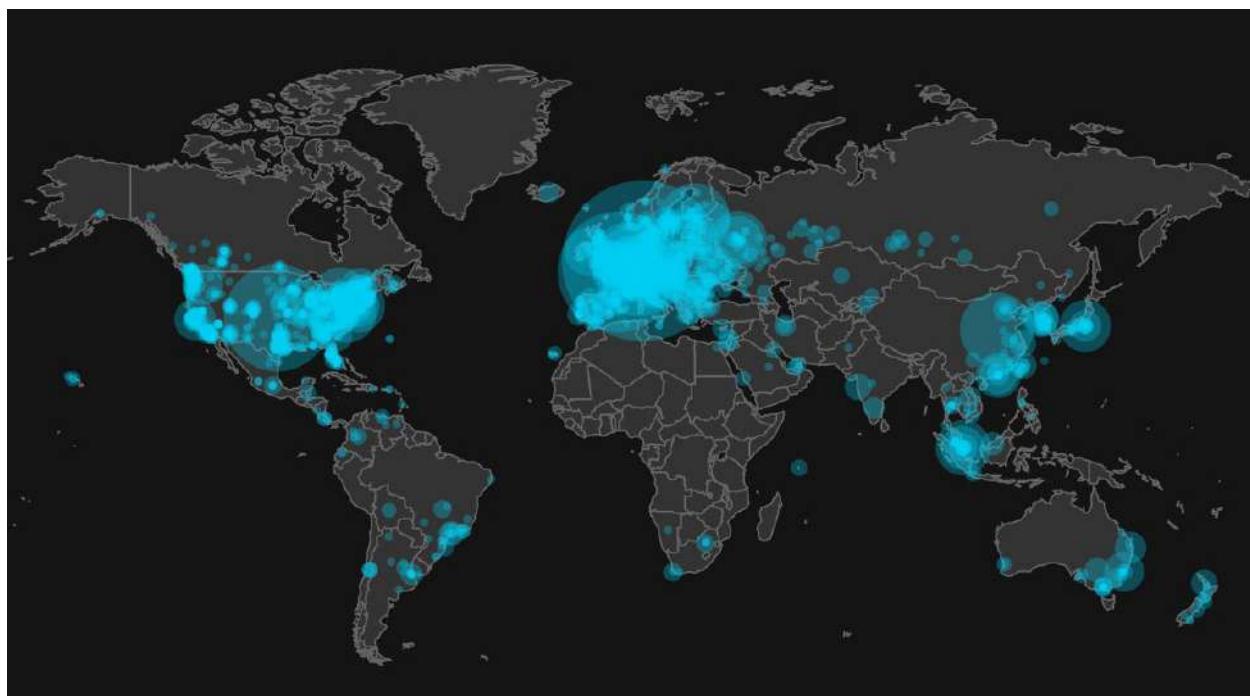
Crittografia

● Basic

Perché la blockchain è sicura?

Nel contesto delle reti peer to peer come Bitcoin, il concetto di sicurezza e affidabilità della rete si basa su due principi cardine della cybersecurity: **l'assenza di singolo punto di fallimento (SPOF) e la sicurezza delle fonti e delle informazioni pregresse (Root of Trust)**.

Il SPOF si riferisce ad un singolo componente o punto di un sistema che, se guasto o disattivato, può causare il fallimento dell'intero sistema. Contestualizzato, la distribuzione dei full node a livello globale garantisce che la rete non abbia un SPOF, poiché se e solo se **tutti i nodi della rete venissero spenti**, ci sarebbe il fallimento dell'intero sistema.



In questa immagine è riportata la **distribuzione dei full node di Bitcoin**, ovvero coloro che tengono l'intera storia della blockchain all'interno di un loro hardware.

Il concetto di **Root of Trust (RoT)**, invece, si riferisce ad un **elemento di un sistema di sicurezza informatica che rappresenta il punto di partenza sicuro e affidabile da cui si estende la catena di fiducia per garantire l'autenticità e l'integrità dei dati**. Contestualizzato, ogni blocco della blockchain è collegato al precedente poiché contiene il "riassunto" del blocco precedente, garantendo un livello di partenza sicuro per ogni blocco creato. Inoltre, come vedremo successivamente, ogni blocco creato è stato validato da molti nodi sparsi per la rete, garantendo un grado di affidabilità condivisa.

Inoltre, SPOF e Root of Trust sono anche garantiti dall'insieme di tecnologie e funzioni matematiche utilizzate per costruire il database e per abilitare i nodi a condividersi le informazioni tra di loro. Infatti, queste reti utilizzano molta crittografia, già validata negli anni ed utilizzata come strumento di sicurezza anche in altri sistemi distribuiti.

Infine, come vedremo in seguito, le reti peer to peer come Bitcoin o Ethereum sono considerate sicure anche perché tutti i nodi che partecipano alla validazione delle transazioni e alla conservazione del database distribuito, **hanno degli incentivi e disincentivi economici che portano quest'ultimi a comportarsi correttamente** e non scrivere delle informazioni "sbagliate", garantendo nel lungo periodo sicurezza e affidabilità della rete.

5.2

Crittografia

● Medium

Basi di crittografia: le funzioni di hashing

La funzione di hash è una tecnica crittografica che consente di generare una stringa di **dimensioni fisse a partire da un messaggio di dimensioni variabili**. Questa stringa, chiamata hash, viene utilizzata per garantire l'integrità dei dati trasmessi, consentendo di verificare che il messaggio originale non sia stato alterato durante la trasmissione. La funzione di hash viene anche utilizzata per verificare l'autenticità di un messaggio e garantire la privacy dei dati.

In gergo informatico le funzioni di hash sono **una funzione di crittografia a senso unico**, in cui un input di lunghezza arbitraria viene trasformato in un output di lunghezza fissa, noto come "digest" o "hash".

Le funzioni di hash sono utilizzate per proteggere la sicurezza dei dati, **poiché anche una minima modifica all'input produce un output completamente diverso**. Questo significa che se un'entità malintenzionata modifica i dati, sarà facile individuare questa modifica confrontando l'hash originale con quello modificato.

Un esempio comune di funzione di hash è SHA-256, che è una funzione di hash crittografica a 256 bit. Questa funzione accetta un input di qualsiasi lunghezza e restituisce un output di 256 bit. SHA-256 è utilizzato in molti contesti, come la firma digitale, la crittografia delle password e la creazione di "checksum" per verificare l'integrità dei file.

In sintesi, le funzioni di hash sono utilizzate per proteggere la sicurezza dei dati e verificare l'integrità dei file. Esse trasformano un input di qualsiasi lunghezza in un output di lunghezza fissa, noto come "digest" o "hash". SHA-256 è un esempio comune di funzione di hash crittografica a 256 bit e viene utilizzata in molti contesti per proteggere la sicurezza dei dati.

5.3

Crittografia

● Hard

Basi di crittografia: il Public Key Infrastructure

Il Public Key Infrastructure, o infrastruttura a chiave pubblica, è un sistema di sicurezza informatica che utilizza un algoritmo di crittografia a chiave pubblica per garantire la confidenzialità, l'integrità e l'autenticità delle informazioni trasmesse. Il PKI si basa sulla creazione di **una coppia di chiavi crittografiche**, una pubblica e una privata, che vengono utilizzate per crittografare e decriptare i dati. La chiave pubblica viene utilizzata per crittografare i dati e può essere condivisa pubblicamente, mentre la chiave privata viene utilizzata per decriptare i dati e deve essere tenuta segreta. Il PKI viene utilizzato in vari contesti, tra cui la sicurezza informatica, la gestione delle identità digitali e la crittografia delle comunicazioni.

RSA è uno dei più comuni sistemi PKI. In questo sistema, la chiave pubblica viene utilizzata per cifrare i messaggi, mentre la chiave privata viene utilizzata per decifrarli. La generazione di una coppia di chiavi RSA è possibile mediante l'utilizzo di un software apposito in grado di sfruttare le proprietà matematiche che stanno alla base di questo sistema.

La sicurezza dei sistemi PKI è basata sulla difficoltà di risolvere problemi matematici complessi, **come la fattorizzazione di grandi numeri**. Ad esempio, nel sistema RSA, cifrare un messaggio richiede la modulazione di un grande numero per una chiave pubblica nota, mentre decifrare richiede la risoluzione

della fattorizzazione di un grande numero per la chiave privata. Questi problemi matematici sono troppo complessi per essere risolti in tempi ragionevoli con le tecnologie attuali, rendendo sicuri i sistemi PKI.

Le funzioni di hash e i sistemi PKI sono spesso utilizzati insieme per garantire la sicurezza dei dati. Prima di inviare un messaggio cifrato con una chiave pubblica, il mittente può calcolare il valore hash del messaggio e cifrarlo con la chiave pubblica. Il destinatario può quindi decifrare il messaggio e confrontare il valore hash decifrato con quello originale per verificare che il messaggio non sia stato modificato durante la trasmissione. In questo modo, la combinazione di funzioni hash e sistemi PKI consente di garantire l'integrità e la privacy dei dati scambiati tra le parti.

Grazie alla loro integrazione, è possibile garantire l'integrità e la privacy dei dati scambiati tra le parti, impedendo a eventuali malintenzionati di intercettare e modificare le informazioni trasmesse.

Ci sono diverse funzioni hash utilizzate per generare gli indirizzi dei wallet di digital assets, tra cui SHA-256 e RIPEMD-160. In particolare, l'**algoritmo più utilizzato per generare gli indirizzi di Bitcoin è il seguente:**

- Calcolare la chiave pubblica del wallet a partire dalla chiave privata utilizzando un algoritmo crittografico di firma digitale (ad esempio, ECDSA).
 - Applicare una funzione hash SHA-256 sulla chiave pubblica ottenuta nel passaggio precedente.
 - Applicare una seconda funzione hash RIPEMD-160 sull'output del primo hash.
 - Aggiungere un byte di versione all'inizio dell'indirizzo (ad esempio, il byte 0x00 per gli indirizzi di Bitcoin).
 - Calcolare il checksum dell'indirizzo (ovvero un hash SHA-256 dell'indirizzo con il byte di versione aggiunto).
 - Aggiungere i primi 4 byte del checksum all'indirizzo, creando così un indirizzo finale di 25 byte.
- L'indirizzo generato è univoco per il wallet e può essere utilizzato per ricevere e inviare digital assets.** Quando si invia una transazione, l'indirizzo del destinatario viene specificato come output della transazione e la chiave privata del wallet viene utilizzata per firmare digitalmente la transazione e autorizzarne l'invio.

5.4

Crittografia

• Hard

Come viene utilizzato il PKI Scheme e l'hashing all'interno di un wallet di digital assets?

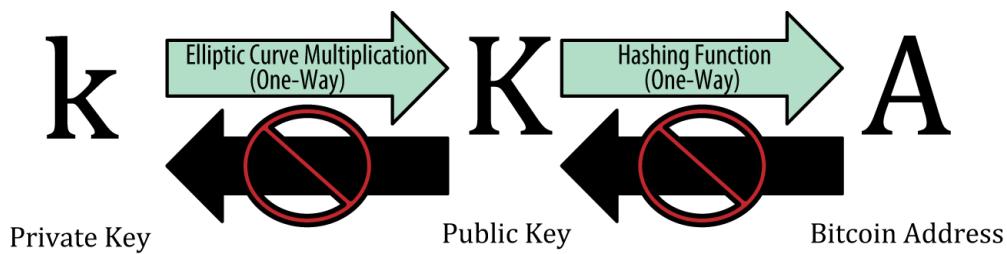
Lo schema PKI (Public Key Infrastructure) viene utilizzato nei wallet di digital assets per gestire le chiavi private e pubbliche che permettono di effettuare transazioni sicure. Tuttavia, le chiavi generate hanno **una funzione diversa da quella del criptare o decriptare i dati.**

I light node come Bitcoin Core e/o altri wallet nel mercato generano una coppia di chiavi pubblica e privata per l'utente, **dove la chiave pubblica viene utilizzata per ricevere fondi e la chiave privata viene utilizzata per firmare le transazioni.**

La creazione di una chiave privata è un processo crittografico che utilizza **l'entropia per generare una sequenza di bit casuali e sicuri.** Inizialmente, si parte da un valore iniziale chiamato "seed" o "seme" che può essere un valore casuale o pseudocasuale. Questo seed viene quindi utilizzato per generare una sequenza di numeri pseudo-casuali utilizzando un algoritmo deterministico, ad esempio un algoritmo di hashing.

Per garantire un alto livello di sicurezza, il seed dovrebbe essere sufficientemente casuale e impreve-

dibile, in modo che la sequenza generata sia altamente casuale e difficile da prevedere per eventuali malintenzionati. In pratica, l'**entropia viene calcolata in base alla complessità del seed e dell'algoritmo di generazione della sequenza**.



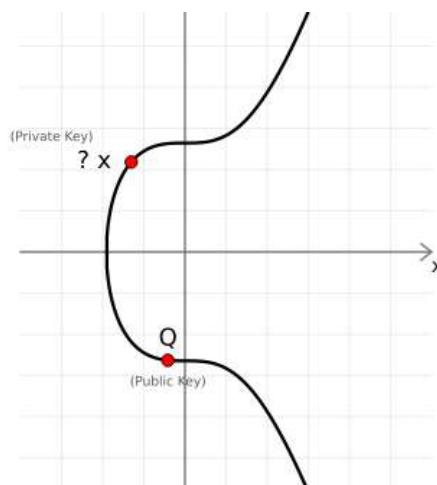
Una chiave pubblica viene generata da una chiave privata attraverso **un processo matematico noto come "crittografia a curva ellittica"** (ECC). Anche questo processo matematica è one-way, ovvero non si può risalire dalla chiave pubblica alla chiave privata.

In questo processo, viene utilizzata una curva ellittica definita su un campo finito, rappresentabile all'interno di un piano cartesiano. La curva ellittica è definita da un'equazione nella forma $y^2 = x^3 + ax + b$, dove a e b sono costanti definite nel campo finito.

Il processo di generazione della chiave pubblica avviene nel seguente modo:

1. Si parte dalla **definizione della curva ellittica e della sua forma**, insieme alla **scelta di un punto base G sulla curva**.
 2. Si **sceglie una chiave privata**, rappresentata da un numero intero casuale k.
 3. La **chiave pubblica si genera moltiplicando il punto base G per la chiave privata k**, attraverso la moltiplicazione scalare: $Q = kG$
 4. Il **risultato della moltiplicazione scalare Q è un altro punto sulla curva ellittica**, che **rappresenta la chiave pubblica**.

Il processo può essere visualizzato su un diagramma cartesiano della curva ellittica, dove il punto base G e la chiave pubblica Q sono rappresentati come punti sulla curva. La chiave privata k è un numero intero che viene utilizzato per moltiplicare il punto base G e generare il punto Q. Infine la chiave pubblica viene moltiplicata per una funzione hash, generando l'address.



La relazione tra chiave privata, chiave pubblica ed address è fondamentale nei wallet per garantire sicurezza **nella gestione dei propri digital assets e per facilitare l'attribuzione dei fondi nei processi di trasferimento di valore nella rete**. La verifica della validità di una transazione in una rete blockchain coinvolge l'uso di crittografia a chiave pubblica. In particolare, il mittente della transazione genera una firma digitale utilizzando la sua chiave privata. La firma viene quindi inclusa nella transazione e inviata alla rete.

I nodi full e i miner della rete verificano che la firma sia valida, utilizzando la chiave pubblica associata all’indirizzo del mittente. L’indirizzo del mittente è derivato dalla chiave pubblica tramite un algoritmo di hash crittografico. In pratica, l’indirizzo è una rappresentazione compressa della chiave pubblica, che consente di verificare la firma in modo efficiente.

La verifica della firma digitale coinvolge l’applicazione dell’algoritmo di crittografia a chiave pubblica alla firma stessa, utilizzando la chiave pubblica del mittente. Se il risultato della verifica è positivo, allora la transazione è considerata valida e viene aggiunta alla blockchain. Altrimenti, la transazione viene respinta e non viene aggiunta alla blockchain.

Per generare una chiave privata in codice, è possibile utilizzare la libreria di crittografia di Ethereum, che fornisce una funzione di creazione di chiavi private.

Per generare la chiave pubblica e l’address, è possibile utilizzare una libreria di crittografia che implementi l’algoritmo Elliptic Curve Digital Signature Algorithm (ECDSA). Questo algoritmo utilizza la chiave privata per generare la corrispondente chiave pubblica e l’address. In questo esempio, importiamo la libreria ECDSA e creiamo un contratto che utilizza la funzione **generatePrivateKey()** per generare una chiave privata a 256 bit. Questa chiave può quindi essere utilizzata per firmare transazioni e accedere ai fondi presenti nel wallet.

In sintesi, la **chiave privata è utilizzata per firmare le transazioni e autorizzare gli acquisti, mentre la chiave pubblica è utilizzata per ricevere le transazioni. L’address è un identificativo pubblico univoco che rappresenta il tuo wallet** e viene utilizzato come destinatario delle transazioni.

5.5

Crittografia

● Hard

Dove viene applicata l’hash function e le PKI nella blockchain?

Come abbiamo visto in precedenza, le **funzioni hash sono fondamentali nella struttura del blocco di Bitcoin**. In particolare, il blocco di Bitcoin è **formato da un’intestazione (header) e da un corpo (body)** contenente le transazioni incluse nel blocco. L’intestazione del blocco contiene diverse informazioni, tra cui:

- La versione del software Bitcoin utilizzata per creare il blocco.
- L’hash del blocco precedente, che crea il collegamento con il blocco precedente nella catena di blocchi.
- Un timestamp che indica l’ora in cui il blocco è stato creato.
- Un valore “bits” che rappresenta la difficoltà di mining del blocco.
- Un valore “nonce” utilizzato nel processo di mining.

Per calcolare l’hash dell’intestazione del blocco, viene utilizzata la funzione hash **SHA-256**. Il valore dell’hash del blocco precedente è incluso nell’intestazione del blocco e viene anch’esso calcolato tramite la funzione hash SHA-256. In questo modo, il collegamento tra i blocchi è garantito dalla crittografia hash.

Il corpo del blocco contiene le transazioni incluse in esso, e l’hash del corpo del blocco viene calcolato tramite la funzione hash SHA-256d, che è una doppia applicazione della funzione SHA-256. Il valore dell’hash del corpo del blocco è incluso nell’intestazione dello stesso e viene utilizzato per garantire l’integrità delle transazioni incluse nel blocco.

Inoltre, le **funzioni hash sono utilizzate anche per la creazione delle firme digitali (PKI)** delle transazioni. Le firme digitali vengono utilizzate per garantire l’autenticità e l’integrità delle transazioni, e vengono create tramite la funzione hash SHA-256 in combinazione con l’algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm).

5.6

Crittografia

• Hard

Considerazioni di cybersicurezza per un wallet

Un wallet sicuro deve garantire diverse funzionalità per proteggere i fondi dell'utente dalle minacce esterne, tra cui:

- **ECDSA e resistenza quantistica:** Il sistema di firma digitale ECDSA (Elliptic Curve Digital Signature Algorithm) è ampiamente utilizzato per garantire la sicurezza delle transazioni crittografiche. Tuttavia, con l'avvento dei computer quantistici, si teme che ECDSA possa essere vulnerabile a future minacce. Un wallet sicuro dovrebbe quindi garantire la resistenza quantistica, cioè la capacità di proteggere le chiavi private dell'utente anche in presenza di computer quantistici avanzati.
- **Replay protection:** Quando si effettua una transazione crittografica, è importante garantire che la transazione venga processata solo una volta e che non possa essere ripetuta o replicata (replay attack). Il replay protection è una funzionalità critica di un wallet sicuro che protegge l'utente da queste minacce.
- **DOS protection:** Un wallet sicuro dovrebbe essere in grado di garantire la protezione contro gli attacchi di tipo DOS (Denial of Service), in cui gli aggressori cercano di sovraccaricare il sistema con un grande volume di richieste. Un wallet ben progettato dovrebbe essere in grado di gestire il traffico in entrata e di prevenire i possibili attacchi DOS.

In sintesi, un wallet sicuro dovrebbe garantire la resistenza quantistica, il replay protection e la DOS protection per garantire che i fondi dell'utente siano al sicuro e protetti da eventuali minacce esterne.

5.7

Legal

• Basic

Cosa vuol dire “possedere” un digital asset come bitcoin?

In realtà, i bitcoin non esistono fisicamente sulla blockchain, **ma vengono rappresentati digitalmente come una transazione all'interno del registro pubblico**. Una transazione bitcoin può essere vista come un messaggio che afferma “trasferisco X bitcoin dalla mia chiave pubblica alla chiave pubblica dell'utente Y”. Quando una transazione viene validata e confermata dalla rete, il registro viene aggiornato per riflettere il nuovo saldo di bitcoin per le due chiavi pubbliche coinvolte nella transazione.

Per muovere i bitcoin da una chiave pubblica a un'altra, l'utente deve utilizzare la sua chiave privata, che permette l'utente di firmare digitale della transazione. La chiave privata è in pratica una stringa di codice segreto che permette all'utente di dimostrare di possedere e di poter quindi spendere e muovere dei bitcoin associati alla chiave pubblica. Quando l'utente invia una transazione, la sua chiave privata viene utilizzata per firmare digitalmente la transazione e creare una prova matematica che dimostra che **l'utente ha il possesso e la possibilità di disporre dei bitcoin associati alla sua chiave pubblica**.

Ciò significa che, in un certo senso, i bitcoin non “esistono” in quanto oggetti fisici o digitali che possono essere spostati da un luogo all'altro. Ma invece, **l'utente possiede solo una chiave privata che gli consente di disporre dei bitcoin associati alla sua chiave pubblica**. Quando l'utente invia una transazione,

la blockchain viene aggiornata per riflettere il nuovo saldo di bitcoin per le due chiavi pubbliche coinvolte nella transazione, ma i bitcoin in sé non escono mai dalla blockchain. La chiave privata diventa quindi il segreto che dobbiamo custodire e proteggere per poter utilizzare i digital assets all'interno della rete. L'accesso ad una chiave privata vuol dire avere accesso ai bitcoin.

5.8

Legal

● Medium

Considerazioni sul concetto di pseudo-anonimato

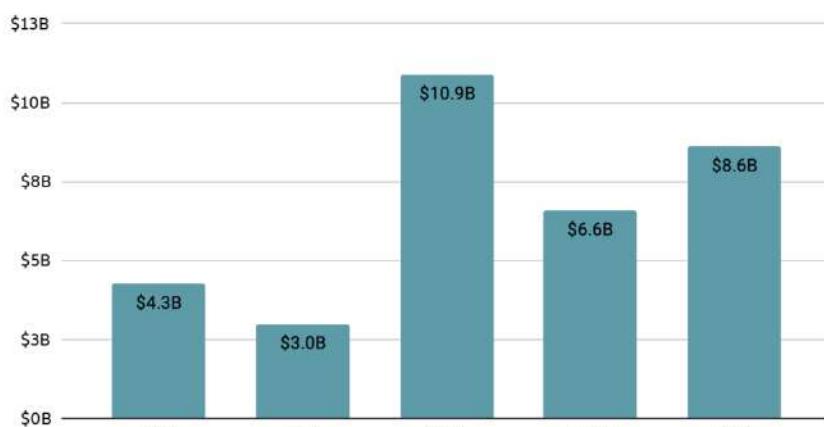
Il concetto di “privacy by design” richiede che la protezione della privacy sia incorporata fin **dall'inizio del processo di sviluppo di qualsiasi prodotto o sistema che tratta dati personali**.

La crittografia asimmetrica (PKI Scheme) e la architettura di pseudo-anonimato dei nodi all'interno della rete possono aiutare a garantire la privacy dei dati finanziari. Infatti, lo schema UTXO della blockchain garantisce l'anonimato delle transazioni. Poiché le transazioni sono pseudo-anonime, ovvero **associate solo a un indirizzo pubblico (ma non necessariamente a una persona fisica), la blockchain garantisce un certo grado di anonimato nelle transazioni**.

Tuttavia, è importante sottolineare che la struttura di pseudo-anonimato, e non di anonimato completo, non garantisce una protezione totale dei dati, poiché le transazioni possono essere analizzate e seguite attraverso analisi forensi della blockchain.

Nonostante l'architettura dei wallet e della blockchain possa essere considerata vicina a ciò che viene generalmente definito **privacy by design** questo aspetto si va a scontrare con la tracciabilità ed il controllo della movimentazione finanziaria, per prevenire fenomeni come il finanziamento al terrorismo e le pratiche di riciclaggio. L'AML viene applicato per prevenire l'uso dei digital assets per attività illecite. Per combattere il riciclaggio di denaro e il finanziamento del terrorismo, le **autorità di regolamentazione stanno lavorando per sviluppare normative e linee guida specifiche per i digital assets**. Ad esempio, il GAFI (Gruppo di azione finanziaria) ha pubblicato delle linee guida per la regolamentazione dei digital assets, che raccomandano l'identificazione e la verifica dell'identità dei soggetti coinvolti nelle transazioni. Chainalysis, società di analisi delle transazioni di digital assets, ha stimato in un suo recente studio che **il 0,34% del volume totale delle transazioni in digital assets è stato utilizzato per scopi illeciti nel 2020**, il che rappresenta una diminuzione rispetto al 2,1% del 2019. Inoltre, la maggior parte di queste transazioni illecite coinvolgeva digital assets come Bitcoin e non stablecoin come Tether.

Total cryptocurrency value laundered by year, 2017 - 2021



6

Le regole, la governance ed il consenso distribuito

- 6.1 Differenze tra le reti: pubblica, privata, con permessi e senza permessi
- 6.2 Perché la rete p2p è sicura e cos'è il consenso distribuito?
- 6.3 Come vengono aggiornate e chi gestisce le regole nella rete?
- 6.4 Che ruolo hanno i full node nelle regole del protocollo?
- 6.5 Come un nodo minatore diventa profittevole?
- 6.6 I modelli matematici del modello ad incentivi della rete
- 6.7 Altri modelli di teoria dei giochi per un equilibrio dinamico

6.1

Informatica

● Basic

Differenze tra le reti: pubblica, privata, con permessi e senza permessi

Un'informazione che dobbiamo avere in mente è che il web è **un insieme di reti informatiche che operano insieme per offrirci la navigazione e tutte le attività di comunicazione tra persone online**. Tutte le reti che compongono il web sono state disegnate con dei modelli di gestione ed amministrazione differenti. In parole semplici, la domanda da porsi quando si analizza una specifica rete è: **quante persone effettivamente amministrano la rete**, decidono le sue regole e quali le operazioni che possono far i partecipanti?

Chiaramente, maggiore sarà il numero di nodi che può “votare” e/o partecipare alla decisione di regole dentro una rete, maggiore sarà decentralizzato il modello di gestione di amministrazione (i.e. governance). In generale, ogni rete può essere classificata in base alla sua apertura e alla presenza di permessi per poter partecipare. Per quanto riguarda la sua apertura, le reti possono essere classificate come:

- **Rete privata:** in una rete privata, l'accesso alla rete e ai suoi servizi è limitato solo a dispositivi e utenti autorizzati. Le reti aziendali, governative e militari sono un esempio di reti chiuse.
- **Rete pubblica:** in una rete aperta, non ci sono restrizioni di accesso e qualsiasi dispositivo o utente può accedere alla rete e ai suoi servizi.

Oltre l'accesso alla rete, la seconda distinzione che le distingue risponde a questa domanda: tutti gli individui hanno pari permessi?

- **Rete senza permessi:** nelle reti senza permessi, non è richiesto alcun tipo di autorizzazione o autenticazione per accedere alla rete o ai suoi servizi. Tutti i nodi sono alla pari.
- **Rete con permessi:** nelle reti con permessi, la gestione della rete e le sue eventuali modifiche è limitato solo a dispositivi e utenti che hanno ottenuto specifici permessi di accesso di amministratore. Alcuni nodi hanno più potere degli altri.

All'interno del Web3, la maggioranza delle reti informatiche nell'industria possono essere classificabili in questi tre modi, qui alcuni esempi:

- **Rete aperta e senza permessi:** Bitcoin, Ethereum, Litecoin, Monero, Solana, Algorand,
- **Rete con private e con permessi:** Ethereum Enterprise Alliance (EEA), Hyperledger Suite, Corda
- **Rete aperta con permessi:** Binance, Ripple, POA

In generale, **le reti senza permessi come Bitcoin e la versione originale di Ethereum tendono ad essere più decentralizzate** in quanto le regole del software e la governance di queste sono sempre soggetta a votazione da parti dei nodi della rete durante gli aggiornamenti e i cambiamenti, e più resistenti perché più distribuite rispetto alle reti con permessi o chiuse. Ma come scegliere la tipologia di una rete? Facciamo un esempio.

In passato Skype ha utilizzato il protocollo peer-to-peer “Joltid” sviluppato da Joltid Ltd., una società fondata dagli stessi creatori di Skype per il suo servizio. Tuttavia, quando Microsoft ha acquisito Skype nel 2011 e ha deciso di migrare la piattaforma da una rete peer-to-peer a una rete centralizzata proprietaria.

Questo perché:

- **Aveva problemi di scalabilità:** con l'aumentare del numero di utenti, la rete peer-to-peer possono mostrare dei limiti in termini di prestazioni e scalabilità.
- **Poteva avere maggiore controllo sulla piattaforma:** con una rete proprietaria centralizzata, Microsoft ha potuto avere un maggiore controllo sulla piattaforma e sulla gestione delle comunicazioni degli utenti.

- **Poteva garantire maggiore sicurezza:** una rete centralizzata proprietaria può essere più sicura di una rete peer-to-peer, dove ogni utente può essere vulnerabile ad attacchi esterni.
- **Creare nuove funzionalità:** una rete centralizzata proprietaria può consentire di aggiungere nuove funzionalità alla piattaforma, come ad esempio la possibilità di registrare le chiamate o di inviare messaggi di testo.

La scelta di migrare da una rete peer-to-peer a una rete centralizzata proprietaria è stata fatta per migliorare la scalabilità, la sicurezza e la gestione della piattaforma, consentendo a Microsoft di offrire un servizio di comunicazione di alta qualità ai suoi utenti. Tuttavia, **ci sono alcuni casi in cui la scelta di una rete peer to peer può essere migliore rispetto ad una chiusa**. Per esempio, su progetti di comunicazione aperta e globale, una rete peer to peer risulta più appetibile per gli utenti e più sicura a livello di governance e distribuzione del rischio.

Analizzeremo nei prossimi capitoli quale rete utilizzare per un progetto in base allo scopo del progetto ed ai suoi aspetti legati a sicurezza e scalabilità.

6.2

Teoria dei giochi

• Basic

Perché la rete p2p è sicura e cos'è il consenso distribuito?

In una rete aperta e senza permessi non vi è alcun ente centrale che garantisce la manutenzione della rete e che le regole vengano rispettate. Ma quindi come viene gestita la governance dentro queste reti? E come possiamo garantire che tutti i nodi della rete seguano le regole comuni?

Non essendoci una autorità centrale, la maggioranza dei nodi della rete deve auto-gestire la propria rete attraverso processi di votazioni e aggiornamento del software. Reti come Bitcoin garantendo la sicurezza delle transazioni tra le persone del network attraverso un meccanismo che è chiamato **consenso distribuito**. Per consenso distribuito si intende la capacità dei nodi della rete di raggiungere **un accordo su un insieme comune di informazioni o decisioni**, senza affidarsi ad un'autorità centrale. Ma come possono fidarsi i nodi l'uno dell'altro? E soprattutto, dato che nessuno conosce nessuno, come è possibile sapere che un nodo malevolo non abbia creato tante copie di sé stesso per votare più volte e compromettere le decisioni?

Questo problema non è stato risolto in matematica, teoria dei giochi e distributed science per lungo tempo. In particolare, è stato dimostrato che, in un sistema distribuito come una rete peer to peer, può risultare impossibile raggiungere un consenso perfetto, compromettendo la sicurezza della rete, con **più versioni delle informazioni o decisioni in circolazione contemporaneamente**.

Tuttavia, con l'introduzione di Bitcoin nel 2009, questo problema è stato risolto con successo **grazie all'uso dell'incentivazione economica**. Ogni nodo si comporterà in maniera corretta e non scriverà informazioni sbagliate sul database distribuito poiché:

- **è incentivato** dall'ottenere un **signoraggio** dei nuovi digital assets, come bitcoin, prodotti dal software della rete;
- **è disincentivato** poiché il processo di validazione di un nuovo blocco comporta l'utilizzo di energia elettrica che corrisponde ad un costo fisso;
- **è disincentivato** poiché se la rete venisse compromessa, automaticamente il digital asset dato come ricompensa perderebbe di valore e di conseguenza anche gli investimenti fatti dal minatore.



Signoraggio

Persignoraggio viene comunemente inteso l'insieme dei redditi derivanti dall'emissione di moneta.

Cerchiamo adesso di declinare queste due considerazioni rispetto alle attività che svolgono i full node e i nodi minatori nella rete:

- I full nodi sono gli attori che **conservano** tutti gli aggiornamenti della rete e di tutte transazioni dentro la blockchain, all'interno del proprio computer;
- I nodi minatori sono gli attori che **aggiornano** periodicamente le informazioni nella blockchain con la creazione di nuovi blocchi, grazie ai computer specializzati;

Tra questi due attori vi è una relazione, in quanto:

- I nodi minatori prendono le transazioni avvenute in una temporale, le inseriscono nel nuovo blocco, e lo collegano al blocco precedente, aggiornando i bilanci dei nodi del network;
- I nodi minatori controllano che l'ammontare dei bitcoin spesi sia minore o uguale dell'ammontare dei bitcoin associati all'indirizzo e che la firma della transazione sia valida;
- I full node controllano che l'intero lavoro svolto dal nodo minatore sia corretto matematicamente, permettendo al nodo minatore di accedere alla ricompensa economica in bitcoin.

Entrambi sanno che la collaborazione tra loro garantisce il buon funzionamento del sistema, e il valore dei digital assets dentro la rete. I miner, possono guadagnare dal signoraggio, **poiché la loro attività costa di più di quella dei full node, in quanto necessità di molta più energia elettrica e potenza computazionale.**

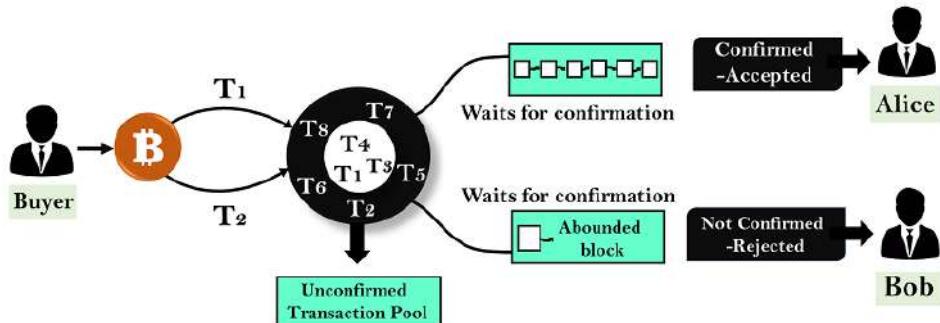


Qui un'immagine di una mining farm utilizzata nel 2023 per “minare” i bitcoin. **Queste interrelazioni incoraggiano tutti nodi a collaborare per raggiungere un consenso distribuito sulla versione corretta della storia della rete, garantendo immutabilità alla blockchain.**

Inoltre, ogni nodo minatore che partecipa alla rete sfida gli altri nodi minatori nel risolvere un problema matematico prima degli altri, aggiudicandosi l'onore e l'onere di aggiornare la blockchain. In parole semplici, la collaborazione tra full node e miner, la sfida tra i minatori e gli incentivi e disincentivi economici garantiscono che, nonostante non ci sia un amministratore centrale, tutte le regole siano sempre rispettate e che la rete sia sicura.

Contestualizzando ad una rete che vuole diventare una rete per le transazioni economiche, cosa vuol dire che la rete è sicura?

Innanzitutto, la prima regola da far rispettare è che nessun nodo possa duplicare i propri digital assets all'interno del proprio wallet, effettuando una **“doppia spesa”**. **Nessun utente può aumentare il proprio bilancio di digital assets in maniera indipendente e nessuno utente può inviare una singola unità a più persone contemporaneamente.**



Facciamo un esempio per capire il problema della doppia spesa e come viene risolto all'interno di una rete privata e con permessi, come Paypal, rispetto ad una rete pubblica senza permessi, come Bitcoin. PayPal è un sistema di pagamento che utilizza una rete chiusa e con permessi, dove la società PayPal funge da intermediario tra i partecipanti alla transazione. In questo caso, il problema della doppia spesa viene risolto **tramite il sistema centralizzato di gestione dei pagamenti, in cui PayPal tiene traccia di tutte le transazioni e delle somme di denaro disponibili per ogni utente**. Quando viene effettuata una transazione, PayPal si assicura che l'importo trasferito sia disponibile sul conto dell'utente che lo invia, e quindi trasferisce l'importo al conto del destinatario.

Bitcoin non ha nessuna azienda che si occupa di validare le transazioni, tuttavia attraverso il sistema di incentivazione, **garantisce livelli di sicurezza** paragonabili a quelli del sistema Paypal. Quando parte la transazione, i nodi della rete verificano il saldo e lo storico dei pagamenti, ed una volta che un certo numero di nodi verifica che è valida, la transazione viene poi inserita del database distribuito dal nodo minatore

Ecco una tabella che confronta i sistemi di Bitcoin e PayPal:

Caratteristiche	Bitcoin	PayPal
Valuta	Bitcoin è una valuta digitale decentralizzata basata su blockchain, creata nel 2009.	PayPal è un sistema di pagamento online che consente di effettuare transazioni in diverse valute, tra cui dollari, euro e altre valute locali.
Decentralizzazione	Bitcoin è decentralizzato, il che significa che non è controllato da un'autorità centrale come una banca o un governo.	PayPal è centralizzato, il che significa che è controllato da una società privata.
Anonimato	Bitcoin offre un certo grado di anonimato, in quanto le transazioni non sono legate alle identità reali degli utenti.	PayPal richiede che gli utenti forniscano le loro informazioni personali, il che significa che le transazioni sono legate alle identità reali degli utenti.
Commissioni	Le commissioni di transazione di Bitcoin sono basse e dipendono dalla quantità di dati inclusi nella transazione.	PayPal addebita commissioni sulle transazioni, che dipendono dal tipo di transazione e dal paese di provenienza dell'utente.
Velocità delle transazioni	Le transazioni di Bitcoin possono richiedere alcuni minuti per essere elaborate, ma le conferme successive aumentano la sicurezza.	Le transazioni di PayPal sono generalmente più veloci, poiché PayPal è un sistema centralizzato con una maggiore capacità di elaborazione delle transazioni.

Per concludere, il meccanismo di consenso distribuito su reti aperte e senza permessi garantisce che i nodi, attraverso una loro collaborazione, possano gestire le regole e le informazioni in modo corretto tra tutti i partecipanti.

6.3

Teoria dei giochi

● Medium

Come vengono aggiornate e chi gestisce le regole nella rete?

In quest'altro blocco educativo, cercheremo di rispondere a queste domande che molto spesso il lettore può chiedersi:

- Chi decide le regole della rete e come vengono votate?
- Che come si applica il consenso distribuito alle regole della rete?
- Come si raggiunge il consenso distribuito tecnicamente?

Nella rete pubblica e senza permessi, **ogni utente all'interno della rete ha la possibilità di partecipare alle attività della stessa**, come ad esempio votare per decidere le regole del codice sorgente.

Durante ogni processo decisionale, i nodi della rete devono prendere decisioni (accetto, non accetto) e raggiungere un consenso distribuito.

I due attori principali sono: i full node e i miner. I full node sono i nodi della rete che **archiviano l'intera blockchain** e verificano ogni transazione che viene aggiunta alla rete. Questi nodi sono responsabili di convalidare ogni blocco e di accettare solo quelli che rispettano le regole del protocollo. I miner, d'altra parte, sono coloro che utilizzano la propria potenza di calcolo per competere **tra loro nella creazione di nuovi blocchi**. Questi blocchi devono rispettare le regole del protocollo e includere solo transazioni valide. Oltre alla gestione giornaliera della rete, i nodi devono occuparsi anche della gestione delle regole e l'eventuale modifica e/o aggiornamento.

Una modifica del protocollo deve avere le seguenti caratteristiche:

- **deve essere accettata da altri nodi**
- **deve essere accettata dai miners**
- **nodi e miners che la accettano devono essere la maggioranza qualificata**

Nel dettaglio, una **modifica proposta viene attivata solo quando viene raggiunto un consenso della maggioranza qualificata dei nodi della rete Bitcoin**. In particolare, la maggioranza qualificata viene definita come il 95% dei nodi che elaborano blocchi, misurati in base alla potenza di calcolo della rete.

Dal punto di vista tecnico, la proposta di un cambiamento “fork” può essere distinta attraverso il tipo di cambiamenti che verranno apportati al protocollo della blockchain.

Un **soft fork** richiede un **cambiamento relativamente minore al protocollo esistente**, in modo da mantenere la compatibilità con le versioni precedenti del software. In altre parole, le regole del protocollo vengono aggiornate in modo tale da essere compatibili con le regole precedenti. In pratica, un soft fork prevede di introdurre nuove regole che vanno ad aggiungersi alle regole esistenti, piuttosto che sostituire completamente quelle precedenti. Per esempio, nel 2016, il Bitcoin ha subito un soft fork chiamato Segregated Witness (SegWit). Questo cambiamento ha introdotto un nuovo modo di memorizzare le transazioni all'interno dei blocchi, senza modificare la dimensione massima dei blocchi.

Un **hard fork**, invece, richiede un **cambiamento più radicale al protocollo esistente**. In pratica, questo significa che le regole del protocollo vengono sostituite completamente, rendendo i blocchi generati in base alle vecchie regole invalidi sulla nuova catena di blocchi. Durante un hard fork, invece, l'aggiornamento del software è obbligatorio per tutti i full node e i miner. In caso contrario, l'aggiornamento non si propaga nella rete. Alcune volte, **i fork possono essere controversi, con portando a dividere in due progetti differenti la rete**.

Per esempio, nell'**agosto 2017, alcuni nodi della rete hanno proposto un hard fork che ha portato alla creazione del Bitcoin Cash**. Questo è accaduto perché alcuni sviluppatori e miner di Bitcoin hanno proposto di aumentare la dimensione massima dei blocchi da 1 MB a 8 MB per migliorare la scalabilità della rete. Tuttavia, questo cambiamento non è stato accettato dalla maggioranza qualificata della rete. La minoranza ha comunque aggiornato la propria rete, spezzando la catena di due, e portando alla creazione di Bitcoin Cash come un nuovo digital asset.

	Hard Fork	Soft Fork
Compatibilità	Non retrocompatibile	Retrocompatibile
Blocchi precedenti	Invalidi	Validi
Aggiornamento richiesto	Da tutti i nodi	Dalla maggioranza dei nodi
Impatto sulla catena	Separazione permanente	Continuità della catena
Esempi	Bitcoin Cash e Bitcoin SV	SegWit

Nella maggior parte dei casi, la proposta di un fork viene fatta dai membri della comunità di sviluppatori che lavorano sul software della blockchain. Questa proposta viene solitamente pubblicata su un forum pubblico, come ad esempio Reddit o GitHub, dove gli utenti possono discuterne e fornire feedback. Se la proposta riceve un ampio consenso, i membri della comunità iniziano a lavorare sulla realizzazione del fork.

La possibilità di discutere e fornire feedback ad un eventuale aggiornamento della rete è fondamentale **per avere una peer review tale da ridurre il rischio operativo di un errore umano che potrebbe compromettere il valore del digital asset basato su quella rete.**

Ogni regola è dettata dalla volontà dei nodi partecipanti della rete. Ogni votazione comporta una scelta, e la maggioranza qualificata della rete deve esprimersi, senza nessun ente centralizzato.

Per garantire nel tempo l'equilibrio e il mantenimento di una convergenza di interessi, si deve raggiungere un consenso distribuito di attori a sostegno della rete, e per raggiungere ciò i sistemi informatici come Bitcoin **si fondano sulla teoria dei giochi e su meccanismi di incentivi.**

6.4

Teoria dei giochi

• Medium

Che ruolo hanno i full node nelle regole del protocollo?

I nodi non minatori sulla rete Bitcoin possono partecipare al processo di voto sui processi di aggiornamento, come l'integrazione di **Taproot**, attraverso il processo di “attivazione dell'utente”. Questo processo è stato progettato per consentire agli utenti di esprimere il loro sostegno per un aggiornamento della rete, e di conseguenza fornire un feedback agli sviluppatori e ai miner sulla volontà della comunità di implementare un determinato cambiamento. BIP è la sigla delle proposte sulla rete Bitcoin, definite come Bitcoin Improvement Proposal.



Taproot

Taproot è una tecnologia che mira a migliorare la privacy e la capacità di Bitcoin di creare contratti intelligenti complessi. Questo per migliorare i suoi benefici e aiutare l'evoluzione del suo ecosistema in crescita.

Durante il processo di attivazione dell'utente, gli **utenti possono esprimere il loro sostegno per un aggiornamento della rete modificando il file di configurazione del loro nodo Bitcoin per includere una**

serie di opzioni che indicano il loro supporto per l'aggiornamento. Queste opzioni possono includere l'attivazione del segnale di versione, che indica che il nodo supporta l'aggiornamento, o l'impostazione di un bit di attivazione, che indica che il nodo ha visto un numero sufficiente di blocchi che includono il segnale di versione.

Una volta che un numero sufficiente di nodi hanno espresso il loro sostegno per l'aggiornamento, la rete può procedere con l'attivazione dello stesso. Se l'aggiornamento richiede un fork soft, i nodi non aggiornati non subiranno alcun danno o perdita di fondi, ma non saranno in grado di utilizzare le nuove funzionalità o beneficiare di eventuali miglioramenti di sicurezza o privacy.

6.5

Teoria dei giochi

● Medium

Come un nodo minatore diventa profittevole?

Se si vuole partecipare alla rete come nodo minatore, sfidando gli altri nodi minatori nel trovare il nonce corretto prima degli altri, un utente deve tenere in considerazioni molti aspetti per poter essere profittevole e collaborare in maniera win-win con la rete Bitcoin.

Differentemente dai full node, la scelta di partecipare nel network da parte dei miner comporta l'utilizzo di energia e quindi dei costi fissi. Il modello di incentivi può permettere al miner di creare un business model per calcolare la profitabilità del minare. L'obiettivo del nodo minatore è duplice:

- Dare sicurezza alle transazioni e alla rete nel suo complessivo
- Guadagnare i nuovi bitcoin creati dalla coin base transaction generata dal protocollo

Dati e Benchmark	Descrizione
Hash Rate	<i>La velocità a cui un miner può elaborare i problemi crittografici per risolvere un nuovo blocco nella blockchain. Misurato in hash al secondo (H/s), terahash al secondo (TH/s), o petahash al secondo (PH/s).</i>
Difficoltà	<i>La difficoltà della blockchain di Bitcoin è regolata automaticamente ogni 2016 blocchi per mantenere una velocità di estrazione costante di circa 10 minuti per blocco. Maggiore è il hashrate della rete, maggiore sarà la difficoltà.</i>
Consumo di energia	<i>L'estrazione di Bitcoin richiede una grande quantità di energia elettrica. Il consumo di energia dei miner può variare a seconda del loro hashrate e dell'efficienza del loro hardware.</i>
Costo dell'hardware	<i>L'hardware necessario per l'estrazione di Bitcoin può essere costoso, in quanto i miner hanno bisogno di potenti processori grafici (GPU) o di circuiti integrati specifici per l'applicazione (ASIC).</i>
Guadagni	<i>I guadagni dei miner dipendono dalla potenza di calcolo che forniscono alla rete e dal prezzo del Bitcoin. Il valore dei guadagni può variare considerevolmente nel tempo.</i>
Pool di mining	<i>I miner possono unirsi a pool di mining per aumentare le loro possibilità di guadagno. In un pool di mining, i miner lavorano insieme per risolvere i problemi crittografici e dividere i guadagni in base alla loro potenza di calcolo.</i>
ROI	<i>Il ritorno sull'investimento (ROI) per l'estrazione di Bitcoin dipende dal costo dell'hardware, dal costo dell'energia elettrica, dalla difficoltà della blockchain, dal prezzo del Bitcoin e dal valore dei guadagni. Il ROI può richiedere diversi mesi o anni, a seconda delle condizioni di mercato.</i>

Per calcolare se il mining di Bitcoin è profittevole è necessario utilizzare una calcolatrice di mining di Bitcoin, che può essere facilmente trovata online. Ci sono molte variabili da considerare, ma alcuni dei fattori più importanti includono:

- **Quantità di bitcoin prodotti in quell'era:** ogni 210.000 blocchi creati (circa 4 anni) la quantità di bitcoin dentro la coinbase transactions viene dimezzata. Per esempio, nel 2009 erano 50, nel 2023 sono 5,75 bitcoin.
 - **Prezzo corrente del Bitcoin:** il valore di mercato attuale del Bitcoin influisce direttamente sui profitti del mining.
 - **Hash rate del minatore:** la velocità a cui il minatore risolve problemi matematici complessi, necessari per confermare le transazioni e aggiungere nuovi blocchi alla blockchain.
 - **Consumo energetico del minatore:** maggiore è il consumo energetico, maggiore sarà il costo dell'energia elettrica necessario per far funzionare il minatore.
 - **Costo dell'energia elettrica:** il costo dell'energia elettrica necessaria per far funzionare il minatore influisce direttamente sui costi di mining.
 - **Tasso di hash rate incrementale annuo:** il tasso di incremento dell'hash rate indica l'incremento del numero di minatori che entrano nel mercato, il che può aumentare la difficoltà di mining.
 - **Difficoltà di mining attuale:** la difficoltà di mining cambia costantemente in base alla quantità di potenza di calcolo dedicata all'estrazione di Bitcoin. Maggiore è la difficoltà, maggiore sarà il tempo e la potenza di calcolo necessari per confermare le transazioni e aggiungere nuovi blocchi alla blockchain.
- In generale, **il mining di Bitcoin richiede un investimento significativo di tempo, denaro ed energia.** Inoltre, la **difficoltà di mining può aumentare rapidamente**, il che può rendere il mining meno profittevole nel tempo. Per questo motivo, è **importante effettuare una valutazione accurata dei costi e dei profitti** potenziali prima di investire in attrezzature di mining di Bitcoin.

6.6

Teoria dei giochi

• Medium

I modelli matematici del modello ad incentivi della rete

In teoria dei giochi, un gioco è un **modello matematico di interazione strategica tra due o più giocatori che cercano di massimizzare il loro guadagno o minimizzare le loro perdite**. Ogni gioco ha un insieme di regole e un insieme di strategie disponibili per ciascun giocatore. In un gioco, gli eventi rappresentano le situazioni specifiche che possono verificarsi durante il gioco, come la scelta di una strategia da parte di un giocatore o il risultato di una mossa.

Un sistema di eventi e giochi dei modelli dinamici e statici rilevanti all'interno del protocollo Bitcoin:

- **Proof-of-Work (PoW)** - il gioco in cui i miner devono risolvere problemi matematici complessi per confermare le transazioni e creare nuovi blocchi nella blockchain.
- **Incentivi (block reward)** - il sistema di incentivi per i miner che risolvono i problemi matematici, in cui ricevono una ricompensa in bitcoin.
- **Consenso distribuito** - il gioco in cui i nodi della rete cercano di raggiungere un accordo sulla validità delle transazioni, sulla creazione di nuovi blocchi e sull'aggiornamento delle regole
- **Attacchi a doppia spesa** - il gioco in cui un utente cerca di spendere lo stesso bitcoin due volte, cercando di manipolare la blockchain.
- **Algoritmo di consenso** - il gioco in cui i nodi della rete cercano di scegliere la versione corretta della blockchain in caso di divergenza o conflitto di versioni.

- **Proof-of-Stake (PoS)** - un modello alternativo a PoW in cui il mineraggio è basato sulla quantità di digital assets posseduta, anziché sulla potenza di calcolo.
- **Hard Fork** - il gioco in cui si verifica una divergenza nella blockchain e si crea una nuova versione della stessa.

Nella teoria dei giochi, si studiano i giochi di strategia in cui i giocatori prendono decisioni basandosi sulla conoscenza degli altri giocatori e sull'obiettivo di massimizzare il proprio guadagno. **L'obiettivo dei miner è massimizzare la loro utilità, ovvero ottenere il massimo profitto possibile dal mining.**

In teoria dei giochi, il processo di mining dei digital assets, come Bitcoin, può essere descritto come un **gioco tra i vari miner che partecipano alla rete**. Il gioco consiste nell'effettuare calcoli matematici per risolvere un complesso problema crittografico, con l'obiettivo di trovare una stringa alfanumerica corretta, chiamata nonce, per validare un nuovo blocco nella blockchain. Il modello di consenso Proof-of-Work (PoW) è utilizzato in molti digital assets, come Bitcoin, per validare le transazioni in modo decentralizzato.

La relazione tra la potenza di hashing della rete e quella dei singoli miner è molto importante in questo gioco, poiché determina la probabilità che un determinato miner possa trovare il nonce corretto per validare un blocco e ricevere la relativa ricompensa.

In un ambiente competitivo, in cui i miner cercano di **massimizzare i loro profitti**, il miner deve decidere quale quantità di hashing power impiegare per partecipare alla rete. In generale, la scelta del miner dipenderà dalla potenza di hashing della rete complessiva e dalla sua potenza di hashing personale.

Se la potenza di hashing personale del miner è relativamente piccola rispetto alla potenza di hashing della rete, allora la probabilità di trovare il nonce corretto e validare un nuovo blocco sarà molto bassa. In questo caso, il miner potrebbe decidere di unirsi a un pool di mining per aumentare la propria potenza di hashing effettiva.

Se, d'altra parte, la potenza di hashing personale del miner è relativamente grande rispetto alla potenza di hashing della rete, allora la probabilità di trovare il nonce corretto e validare un nuovo blocco sarà molto alta. In questo caso, il miner potrebbe decidere di lavorare in solitaria invece di unirsi a un pool di mining per massimizzare i propri profitti.

Il concetto importante in teoria dei giochi è quello di **equilibrio di Nash**, ovvero **l'insieme di strategie che rappresentano la migliore risposta di ciascun giocatore alle strategie degli altri giocatori**. In PoW, l'equilibrio di Nash viene raggiunto quando ogni miner sceglie la strategia più efficiente in base alla difficoltà di mining e al tasso di creazione di blocchi. Quando tutti i miner adottano la stessa strategia, si raggiunge l'equilibrio di Nash. Questo equilibrio mantiene la rete sicura e il consenso distribuito tra i nodi minatori.

Tuttavia, l'**equilibrio di Nash può essere instabile e può essere influenzato dalla comparsa di nuovi miner o dal cambiamento del premio in monete digitali**.

Il **sistema di incentivi** (o “block reward”) è un elemento fondamentale del modello Bitcoin e gioca un ruolo chiave nel raggiungimento dell'equilibrio dinamico della rete. Questo meccanismo di incentivi è progettato per garantire che i miner agiscano nell'interesse della rete e mantengano l'integrità del sistema.

Al giorno d'oggi, non sarebbe conveniente per un miner malevolo attaccare la rete Bitcoin, poiché ciò richiederebbe molte risorse e non garantirebbe il successo dell'attacco. Inoltre, se l'attacco riuscisse, il valore di Bitcoin potrebbe diminuire, riducendo i guadagni futuri del miner stesso. Di conseguenza, la scelta razionale per un miner sarebbe quella di partecipare alla rete in modo onesto, rispettando le regole e contribuendo alla sicurezza della rete, al fine di raggiungere un equilibrio stabile e sicuro all'interno della rete peer to peer.

6.7

Teoria dei giochi
● Hard

Altri modelli di teoria dei giochi per un equilibrio dinamico

Concetto	Descrizione
Equilibrio di Nash	Situazione in cui i giocatori in un gioco strategico hanno scelte ottimali date le scelte degli altri giocatori. In altre parole, nessun giocatore può migliorare la sua posizione unilateralmente.
Dilemma del prigioniero	Situazione in cui due giocatori, che agiscono in modo indipendente, sono in grado di migliorare la loro posizione complessiva cooperando, ma entrambi scegliendo di non cooperare per paura di essere traditi dal loro partner.
Equilibrio di Stackelberg	Situazione in cui un leader sceglie le sue azioni in modo strategico in base alle possibili risposte dei seguaci. Il leader ha il vantaggio di sapere le azioni dei seguaci prima di prendere le sue decisioni.
Teoria dei giochi cooperativi	Ramo della teoria dei giochi in cui i giocatori cercano di massimizzare un obiettivo comune e lavorare insieme per raggiungere tale obiettivo.
Equilibrio di Bertrand	Situazione in cui due aziende concorrenti scelgono il prezzo più basso per ottenere la maggior parte del mercato. Se le aziende hanno costi simili, il prezzo di mercato scende fino al costo marginale e le aziende non hanno alcun guadagno.
Teoria della negoziazione	Teoria dei giochi che si concentra sulla negoziazione tra due parti in cui entrambe cercano di ottenere il miglior accordo possibile.
Modello di Hotelling	Situazione in cui due aziende concorrenti cercano di massimizzare il profitto scegliendo la loro posizione in un segmento di mercato. Se le aziende sono vicine l'una all'altra, i clienti preferiranno l'azienda più conveniente in termini di prezzo.
Equilibrio di Cournot	Situazione in cui due o più aziende concorrenti scelgono la quantità di prodotto che desiderano offrire. In una situazione di equilibrio, le aziende offriranno la quantità ottimale di prodotto, tenendo conto delle azioni delle altre aziende.
Modello di Bertrand-Edgeworth	Estensione del modello di Bertrand in cui le aziende concorrenti scelgono il prezzo e la quantità di prodotto in modo simultaneo. In una situazione di equilibrio, le aziende offriranno la quantità ottimale di prodotto al prezzo più basso possibile.

In alto, una tabella con le definizioni di alcuni equilibri e modelli che avvengono nel gioco dinamico del mining e della validazione delle regole all'interno di una rete peer come Bitcoin. Mentre qui di seguito, le **applicazioni teorica di questi modelli nella rete**, con alcune considerazioni di carattere generale:

- **Equilibrio di Nash:** nel protocollo Bitcoin, gli incentivi economici (come il block reward) incoraggiano i miner a competere tra loro per risolvere il puzzle crittografico e validare le transazioni. L'equilibrio di Nash viene raggiunto quando i miner decidono di aderire alle regole del protocollo Bitcoin e di cercare di risolvere il puzzle crittografico in modo onesto, in modo da massimizzare il loro guadagno complessivo.
- **Modello di Prisoner's Dilemma:** il dilemma del prigioniero può essere applicato alla scelta tra cooperazione e competizione tra i miner. Se tutti i miner collaborano e lavorano insieme per risolvere i puzzle crittografici, la blockchain sarà aggiornata più velocemente e tutti i miner riceveranno un guadagno. Tuttavia, se un miner decide di lavorare da solo e guadagnare il block reward da solo, potrebbe avere un vantaggio a breve termine, ma a lungo termine tutti i miner perderanno. Pertanto, è nell'interesse di tutti i miner collaborare e lavorare insieme per aggiornare la blockchain.

- **Equilibrio di Stackelberg:** nel protocollo Bitcoin, i miner possono agire come leader e scegliere di adottare un approccio diverso per la validazione delle transazioni, ad esempio utilizzando una versione diversa del software di mining. Tuttavia, se il loro approccio non viene adottato dagli altri miner, il loro guadagno potrebbe diminuire. Pertanto, i miner che agiscono da leader devono essere in grado di prevedere come gli altri miner reagiranno alle loro scelte e agire di conseguenza.
- **Teoria dei giochi cooperativi:** i miner possono lavorare insieme in pool di mining, condividendo le risorse e il guadagno. In questo modo, possono collaborare per risolvere i puzzle crittografici più velocemente e ricevere il block reward in modo più regolare. Tuttavia, se un miner decide di lasciare il pool e lavorare da solo, potrebbe avere un vantaggio a breve termine ma a lungo termine, il suo guadagno complessivo potrebbe diminuire.
- **Equilibrio di Bertrand:** nel mercato dei mining di Bitcoin, i miner competono tra loro per offrire la tariffa di transazione più bassa per l'inclusione nella blockchain. Tuttavia, se tutti i miner offrono la stessa tariffa di transazione, il guadagno complessivo diminuisce. Pertanto, i miner devono essere in grado di prevedere le scelte degli altri miner e decidere la tariffa di transazione da offrire in modo da massimizzare il guadagno complessivo.
- **Teoria della negoziazione:** i miner possono collaborare e negoziare per dividere il guadagno del block reward in modo equo. In questo modo, possono evitare di competere tra loro e migliorare la loro efficienza complessiva. Tuttavia, se un miner rifiuta di collaborare, gli altri miner potrebbero decidere di escluderlo dal pool.
- **Modello di Hotelling:** nel mercato dei mining di Bitcoin, i miner cercano di trovare il punto migliore per posizionarsi per massimizzare il loro guadagno. Questo può essere visto come una variazione del modello di Hotelling, in cui i negozi si posizionano lungo una strada per massimizzare il numero di clienti. I miner cercano di posizionarsi in modo da avere la tariffa di transazione più bassa e massimizzare il loro guadagno.
- **Equilibrio di Cournot:** nel mercato dei mining di Bitcoin, i miner producono quantità di hash power in modo indipendente. Tuttavia, se tutti i miner producono la stessa quantità di hash power, il guadagno complessivo potrebbe diminuire. Pertanto, i miner devono essere in grado di prevedere le scelte degli altri miner e produrre la quantità di hash power giusta per massimizzare il guadagno complessivo.
- **Modello di Stackelberg dinamico:** il protocollo Bitcoin è in continua evoluzione e i miner devono essere in grado di prevedere come gli aggiornamenti del protocollo influenzino il loro guadagno. Il modello di Stackelberg dinamico può essere applicato alla scelta del momento migliore per aggiornare il software di mining per massimizzare il guadagno.
- **Modello di Bertrand-Edgeworth:** nel mercato dei mining di Bitcoin, i miner possono offrire diverse opzioni di tariffe di transazione e di tempo di elaborazione. Il modello di Bertrand-Edgeworth può essere utilizzato per prevedere quale combinazione di tariffe di transazione e di tempo di elaborazione massimizzerà il guadagno complessivo dei miner.
- **Modello di ultimatum:** i miner possono scegliere di includere o escludere determinate transazioni dalla blockchain. Se un miner esclude una transazione che altri miner hanno incluso, potrebbe causare problemi di coordinamento e un potenziale danno per il sistema. Il modello di ultimatum può essere utilizzato per prevedere come i miner decideranno di includere o escludere le transazioni.
- **Teoria delle coalizioni:** i miner possono coalizzarsi per aumentare la loro capacità di hashing e il guadagno complessivo. Tuttavia, se la coalizione diventa troppo grande, potrebbe diventare troppo costosa da gestire e diminuire il guadagno complessivo. La teoria delle coalizioni può essere utilizzata per prevedere quale combinazione di miner si unirà per massimizzare il guadagno complessivo.
- **Modello di competizione multi-agente:** nel protocollo Bitcoin, ci sono molti miner che competono tra loro per risolvere i puzzle crittografici. Il modello di competizione multi-agente può essere utilizzato per prevedere come i miner reagiranno alle scelte degli altri e come la loro strategia di mining influenzera il guadagno complessivo.
- **Modello di disuguaglianza di Bertrand:** nel mercato dei mining di Bitcoin, i miner possono utilizzare la loro capacità di hashing per sfruttare i prezzi più bassi e aumentare il loro guadagno.
- **Effetti di rete:** Gli effetti di rete in Bitcoin si riferiscono all'idea che il valore della rete aumenta man mano che più persone la usano. Ciò crea un loop di feedback positivo, poiché più utenti portano a più transazioni, maggiore domanda di mining e una rete più sicura. Gli effetti di rete possono anche rendere più difficile per nuovi protocolli blockchain ottenere visibilità, poiché gli utenti e i miner sono già investiti nella rete esistente.

- **Eliminazione di strategie dominate:** In Bitcoin, i miner possono scegliere quali transazioni includere nei blocchi che stanno minando. Tuttavia, ci sono alcune transazioni che non sono redditizie da includere a causa delle loro basse commissioni di transazione o bassa priorità, e i miner possono eliminare tali transazioni dalla considerazione per risparmiare risorse di calcolo. Ciò può aiutare a raggiungere un equilibrio in cui i miner si concentrano su transazioni con commissioni o priorità più elevate, aumentando l'efficienza complessiva della rete.
- **Giochi ripetuti:** Il processo di mining di un blocco in Bitcoin è un gioco ripetuto, poiché i miner sono incentivati a minare blocchi nel tempo per guadagnare ricompense. Questo gioco ripetuto può contribuire a garantire che i miner continuino ad agire nell'interesse della rete e a mantenere la sicurezza della blockchain.
- **Teoria dei meccanismi:** La teoria dei meccanismi si riferisce alla progettazione di un sistema che incoraggi i giocatori a comportarsi in modo desiderabile. In Bitcoin, la progettazione del sistema di incentivazione attraverso il block reward e le commissioni di transazione potrebbe essere considerata una forma di teoria dei meccanismi.

In generale, **il raggiungimento di tutti gli equilibri e modelli di teoria dei giochi nel protocollo Bitcoin può contribuire a garantire la sicurezza e l'affidabilità della rete.** Ogni equilibrio e modello rappresenta una sfida specifica per i miner e gli utenti della rete, ma attraverso l'interazione e la collaborazione, può essere raggiunto un equilibrio di Nash stabile e sostenibile. L'obiettivo finale è di garantire che la blockchain Bitcoin sia aggiornata in modo affidabile e che le transazioni siano verificate correttamente, evitando comportamenti fraudolenti o attacchi alla sicurezza della rete. La teoria dei giochi fornisce un quadro utile per comprendere questi processi e raggiungere un equilibrio che beneficia l'intera rete Bitcoin.

7

The money protocol

- 7.1 A che cosa serve la moneta?
- 7.2 Le caratteristiche di una buona moneta e la standardizzazione
- 7.3 Quali sono le condizioni per cui una tecnologia viene accettata dalla massa?
- 7.4 The Protocol money e la ciclicità nella moneta durante le crisi

7.1

A cosa serve la moneta?

Filosofia Economica

• Basic

La moneta è uno strumento di scambio che consente di facilitare le transazioni commerciali tra le persone. La sua nascita risale a tempi antichi, in maniera complementare **alle prime forme di scambio basate sul baratto, lo scambio diretto di beni e servizi**. A poco a poco, con l'aumentare della complessità delle attività economiche e l'espansione del commercio internazionale, si è reso necessario un mezzo di scambio più portatile e socialmente quantificabile, sostituendo quasi del tutto le forme di baratto. La teoria economica classica, rappresentata da Adam Smith, sostiene che la funzione del denaro è quella di facilitare la doppia coincidenza dei bisogni, ovvero la possibilità di **scambiare beni e servizi senza dover necessariamente trovare un'altra persona che abbia esattamente ciò che si desidera e che sia disposta a scambiarlo**.

La doppia coincidenza dei bisogni è un concetto fondamentale per l'economia, poiché consente di superare il problema della **mancanza di fiducia** reciproca tra gli individui e di promuovere lo sviluppo del commercio e dell'economia in generale. Tuttavia, la teoria economica moderna ha messo in discussione la visione classica del denaro come semplice mezzo di scambio, sostenendo che esso abbia anche una funzione di riserva di valore e di unità di conto. Inoltre, l'evoluzione della tecnologia ha portato alla nascita di nuove forme di moneta digitale, che stanno rivoluzionando il mondo finanziario.

Il ruolo del denaro per aiutare la doppia coincidenza dei bisogni può essere spiegato anche attraverso i **modelli di teoria dei giochi**. In un modello di teoria dei giochi con informazioni complete, senza asimmetria informativa, due individui scambieranno due beni se il valore associato dei rispetti è considerato simile e/o se l'esito crea un equilibrio di interessi tra le controparti. Tuttavia, se solo uno dei due individui ha bisogno del bene dell'altro, **l'equilibrio può essere ottenuto solo se il possessore del bene è in grado di fornire un ulteriore bene socialmente accettato** che può essere scambiato in un successivo scambio per ottenere un bene desiderato.

In sintesi, la doppia coincidenza dei bisogni è un concetto fondamentale per il funzionamento del mercato e dell'economia in generale, poiché consente di superare il problema della mancanza di fiducia reciproca tra gli individui. Tuttavia, la sua realizzazione può essere influenzata da fattori come la presenza di informazioni incomplete o la selezione avversa nel mercato.

7.2

Le caratteristiche di una buona moneta e la standardizzazione

Filosofia Economica

• Basic

Alcuni punti da avere bene in mente per proseguire la lettura dei prossimi blocchi:

- Che Internet è composto da molte reti informatiche e il web3 è un nuovo insieme di reti informatiche dove si può trasferire valore da un punto all'altro della rete senza autorità centrali.
- Che Bitcoin, Ethereum e altre reti utilizzano reti peer to peer ed un database distribuito chiamato blockchain.
- Che la blockchain è sicura perché utilizza la crittografia come root of trust e i nodi della rete raggiungono un consenso distribuito grazie a un modello ad incentivi e disincentivi.

- Che si possono effettuare transazioni finanziarie online, senza una controparte centrale che gestisca i processi di **clearing e settlement** tra individui su Internet.



Clearing and settlement

Liquidazione e regolamento sono fasi del post-trading, ossia ciò che avviene dopo che una transazione è stata eseguita sul mercato. La liquidazione (o clearing) avviene dopo le fasi di conferma e riscontro ed è finalizzata a definire gli obblighi di acquirente e venditore circa le transazioni concluse andando a ridurre il rischio di mercato. Il processo di regolamento riguarda tempi e modalità con le quali acquirente e venditore si scambiano rispettivamente il contante e i titoli. In Italia l'istituzione che si occupa di organizzare e gestire tutte le fasi del post-trading (e quindi anche liquidazione e regolamento) delle operazioni aventi ad oggetto titoli non derivati è Monte Titoli. La liquidazione delle operazioni aventi ad oggetto strumenti derivati è invece gestita dalla Cassa di Compensazione e Garanzia.

La domanda che molti si stanno ponendo adesso è: Bitcoin può diventare un sistema di pagamento e contemporaneamente un sistema monetario globale? Sicuramente non basta che sia sicuro, ma soprattutto che le persone accettino i digital assets, come i bitcoin, come mezzo di scambio per beni e servizi.

Un buon sistema monetario è essenziale per garantire la stabilità economica di un paese. Una moneta instabile o un sistema monetario inefficiente possono portare a svalutazioni e fluttuazioni di valore, che a loro volta possono avere conseguenze negative sull'economia, sui consumatori e sui mercati finanziari.

Definizione	Spiegazione
Riserva di valore	La capacità della moneta di mantenere il suo valore nel tempo, consentendo alle persone di risparmiare e investire per il futuro.
Unità di conto	La capacità della moneta di rappresentare il valore di beni e servizi in modo standardizzato. In altre parole, la moneta viene utilizzata come un'unità di conto per misurare il valore di ciò che viene acquistato o venduto.
Mezzo di scambio	La capacità della moneta di essere utilizzata per effettuare transazioni commerciali, ovvero per acquistare beni e servizi.
Fungibilità	La capacità della moneta di essere intercambiabile con altre unità della stessa valuta, in modo che ogni unità sia indistinguibile dalle altre.
Trasportabilità	La capacità della moneta di essere trasportata facilmente da un luogo all'altro.
Divisibilità	La capacità della moneta di essere divisa in piccole unità per permettere transazioni di importi variabili.
Durabilità	La capacità della moneta di durare nel tempo e mantenere le proprie caratteristiche, ad esempio resistenza all'usura e alla corrosione.

Una buona moneta deve avere alcune caratteristiche fondamentali. Innanzitutto, deve essere **ampiamente accettata come mezzo di pagamento**, ovvero deve essere riconosciuta come forma di pagamento valida in molti contesti e luoghi. Inoltre, la moneta deve **fungere da riserva di valore**, ossia deve essere in grado di conservare il suo valore nel tempo. Infine, deve essere un **buon "metro" per misurare il valore degli oggetti, garantendo da unità di conto**.

La moneta deve inoltre essere **divisibile, fungibile, trasportabile e duratura**. La sua divisibilità permette

di effettuare transazioni di varie dimensioni e valori. La fungibilità, invece, indica che ogni unità della moneta deve essere intercambiabile con altre unità della stessa moneta. La trasportabilità indica che la moneta deve essere facilmente trasportabile, mentre la durabilità assicura che la moneta sia abbastanza resistente e duratura da conservare il suo valore nel tempo.

La moneta diventa uno standard se le viene attribuito corso legale da un'autorità, come uno stato o un'organizzazione internazionale, oppure se viene considerata buona da una comunità attraverso un processo bottom-up. Ad esempio, l'euro è stato introdotto dal trattato di Maastricht nel 1992 e adottato come valuta comune dell'Unione Europea. D'altra parte, il **bitcoin è una moneta proposta dal basso**, grazie all'adozione da parte di una comunità di utenti online in tutto il mondo.

La sfida principale del bitcoin è quella di diventare uno standard monetario accettato a livello globale, in modo da poter essere utilizzato come mezzo di pagamento ampiamente diffuso. Questo comporta una serie di sfide, tra cui la necessità di sviluppare infrastrutture finanziarie che supportino l'uso del bitcoin e la creazione di un'ampia base di utenti che lo accettino come forma di pagamento.

7.3

Filosofia Economica / informatica

● Basic

Quali sono le condizioni per cui una tecnologia viene accettata dalla massa?

L'uomo deve essere sempre al centro dell'analisi per comprendere se una tecnologia può essere utilizzata nel lungo periodo, o è semplicemente una moda passeggera. Ogni sistema complesso come quello odierno, può essere studiato e compreso attraverso alcuni concetti che aiutano a comprendere l'adozione e la diffusione di una tecnologia come:

- Il **concetto di scalabilità sociale** si riferisce alla **capacità di un sistema o di un'organizzazione di adattarsi e crescere in modo efficiente e sostenibile**, man mano che aumenta la sua dimensione e la sua portata. In particolare, la scalabilità sociale si riferisce alla capacità di un sistema di mantenere la sua efficienza, la sua qualità e la sua capacità di soddisfare le esigenze dei suoi utenti, man mano che il numero di utenti o l'ambito delle attività aumenta.
- Il concetto di scalabilità tecnologica, ovvero la capacità di un sistema informatico di crescere in maniera organica, garantendo sicurezza ed interoperabilità al crescere degli attori coinvolti e delle attività interne.

Contestualizzando questi due concetti rispetto alle reti tecnologiche, ci viene in aiuto un modello definito come **Legge di Metcalfe**. Questo modello afferma che il **valore di una rete cresce esponenzialmente al quadrato del numero di utenti connessi alla rete stessa**. In altre parole, una rete tende a diventare sempre più utili e preziose man mano che il loro numero di utenti cresce, poiché c'è un aumento esponenziale delle possibilità di connessione, di scambio di informazioni e di valore generato dalla rete. La Legge di Metcalfe è stata formulata da Robert Metcalfe, uno dei co-fondatori di Ethernet, una tecnologia di rete usata per collegare computer in una LAN (rete locale) ed ha importanti implicazioni per lo sviluppo e la crescita delle reti.

Facciamo degli esempi:

- La rete HTTP ha una buona scalabilità tecnologica in quanto il protocollo si basa su un modello client-server, che consente di gestire un elevato numero di richieste in modo efficiente.
- La scalabilità sociale dell'HTTP è elevata in quanto il protocollo è stato adottato da quasi tutti i siti web.

- La legge di Metcalfe è applicabile in quanto il valore della rete HTTP aumenta con il numero di utenti che lo utilizzano.

Analizziamo lo stesso modello per reti sociali come il social network LinkedIn:

- Il social network LinkedIn si basa su un modello client-server ed ha una buona scalabilità tecnologica se l'azienda LinkedIn in grado di aumentare il numero di web-server all'aumentare delle richieste dei client.
- La scalabilità sociale è elevata in quanto LinkedIn è diventata la principale piattaforma di social networking professionale al mondo.
- La legge di Metcalfe è applicabile in quanto il valore e l'utilità del social network aumenta con il numero di utenti.

Queste considerazioni sono perfettamente applicabili alle reti di pagamento come SWIFT, Mastercard o Visa e alla creazione di standard monetari come l'euro, il dollaro e bitcoin. Maggiore sarà il numero di utenti di un sistema monetario, maggiore sarà il valore del sistema monetario. Questo concetto viene spesso definito anche come **network effect**. Questi concetti sono importanti per la progettazione e la gestione di sistemi complessi e possono essere utilizzati per valutare il potenziale di crescita e il valore delle reti sociali e digitali.



Network Effect

L'effetto rete è un fenomeno economico che descrive un prodotto o un servizio, in cui l'arrivo di un maggior numero di utenti aggiunge valore alla rete. Quando è presente l'effetto rete, ogni nuovo utente aggiunge valore al prodotto entrando a far parte del network

Un'altra chiave di lettura per comprendere la diffusione di una tecnologia tra una popolazione o una organizzazione è stata proposta dal crittografo moderno Nick Szabo. Szabo ha sviluppato una teoria di scalabilità sociale basata sul concetto di "wet code" e "dry code".

Per Szabo:

- Il **wet code** si riferisce ai protocolli e alle istituzioni che regolano le interazioni sociali umane, come ad esempio le leggi, le norme sociali, le convenzioni e le istituzioni.
- Il dry code, invece, si riferisce alle tecnologie e ai protocolli digitali che regolano le interazioni su internet

Szabo sostiene che la scalabilità sociale dipende dalla capacità di combinare efficacemente wet code e dry code, in modo da creare sistemi che siano sia efficienti dal punto di vista tecnologico, sia efficaci nel regolare le interazioni sociali. Secondo questa teoria, la **scalabilità sociale può essere migliorata attraverso la progettazione di wet code e dry code che siano compatibili tra loro e che siano in grado di evolversi insieme**, man mano che il sistema cresce e si evolve.

7.4

Filosofia Economica

● Basic

The Protocol money e la ciclicità nella moneta durante le crisi

La complessità di questo nuovo protocollo come Bitcoin non sta solamente nella sua diffusione come sistema di pagamento peer to peer, ma soprattutto nella sua comprensione da parte delle persone. Le domande aperte sono molte:

- **Può un digital asset come bitcoin diventare una valuta?**
- **I bitcoin che ruolo avranno nell'economia del futuro? Sostituiranno le valute fiat o verranno utilizzati in maniera complementare?**
- **Può essere una valuta definita da un sistema informatico senza una autorità centrale che definisce le regole di emissione?**
- **Può la rete Bitcoin essere considerato un nuovo sistema monetario indipendente?**

Ray Dalio, uno degli investitori più famosi e influenti del mondo, ha sviluppato l'idea che i sistemi monetari nascano e muoiano in risposta alle crisi economiche. Infatti, le crisi economiche rappresentano un momento di transizione tra un sistema monetario esistente e uno nuovo.

Dalio sostiene che i sistemi monetari si alternano tra due fasi definite come: la fase “hard money” e la fase “soft money”.

- **L'hard money** è una valuta stabile, solida e affidabile che mantiene il suo valore nel tempo e ha **una bassa inflazione**. Generalmente, l'hard money è supportato da un collaterale, come oro o argento, e ha un'offerta limitata sul mercato. Le valute “hard” sono spesso utilizzate in periodi di crisi o di instabilità economica per fornire una forma di stabilità monetaria.
- **Il “soft money”,** invece, è una valuta meno stabile e affidabile che ha **una maggiore propensione all'inflazione** e può essere svalutata rapidamente. Il soft money è spesso emesso senza un collaterale ed è caratterizzato da una maggiore offerta sul mercato.

Qui di seguito è riportata una lista di esempi di come le fasi “hard” e “soft” si sono intercambiate durante i periodi di crisi e di guerra:

- **Crisi del Panico del 1837:** la crisi economica degli Stati Uniti portò alla svalutazione della valuta e a una forte inflazione. In risposta, il governo degli Stati Uniti passò al sistema monetario hard money, stabilendo il gold standard.
- **Guerra civile americana (1861-1865):** la guerra portò alla svalutazione della valuta e all'inflazione negli Stati Uniti. Dopo la guerra, il governo degli Stati Uniti passò al sistema monetario hard money, basato sull'oro.
- **Prima Guerra Mondiale:** La valuta tedesca (mark) era una valuta “hard” sostenuta da un collaterale in oro fino alla Prima guerra mondiale. Successivamente, dopo le condizioni stabilite dal Trattato di Versailles, la repubblica tedesca dovette cedere parte delle sue riserve in oro togliendo il collaterale alla valuta domestica.
- **Crisi del 1929:** la Grande Depressione portò a una forte deflazione e alla svalutazione della valuta negli Stati Uniti. In risposta, il governo degli Stati Uniti passò al sistema monetario hard money, stabilendo il gold standard.
- **Crisi Energetica 1971:** Il dollaro americano (USD) era una valuta “hard” fino al 1971 quando gli Stati Uniti hanno abbandonato il sistema del gold standard, a seguito dell'aumento dei costi dell'energia dopo l'**embargo dell'OPEC**.



Embargo OPEC

L'embargo dell'OPEC si riferisce al periodo tra il 1973 e il 1974 in cui i paesi membri dell'Organizzazione dei Paesi Produttori di Petrolio (OPEC) hanno deciso di bloccare le esportazioni di petrolio verso i paesi occidentali, in seguito alla decisione di questi ultimi di appoggiare Israele nella guerra del Kippur. Ciò ha causato un aumento dei prezzi del petrolio e ha avuto gravi conseguenze economiche per molti paesi, in particolare quelli dipendenti dal petrolio importato.

In generale, le valute “hard” tendono ad essere preferite in situazioni di instabilità economica o politica, mentre le valute “soft” possono essere più vantaggiose in periodi di crescita economica e stabilità. Tuttavia, troppa libertà nello stampare può portare ad una perdita del potere d'acquisto, creando fenomeni di inflazione e iperinflazione che tendono a far perdere potere d'acquisto alla maggioranza delle persone.

Ancora oggi, in paesi in via di sviluppo dove la gestione dei sistemi monetari è opaca, dove ci sono crisi economiche e politiche, la popolazione tende a convertire la propria valuta domestica “soft” con valute internazionali “hard” per tutelare il proprio risparmio.

Nei paesi elencati in cui vi sono delle crisi monetarie in corso, si è inoltre riscontrato come i bitcoin siano stati utilizzati come moneta di rifugio e riserva di valore da parte della popolazione.

- **Venezuela** - L'iperinflazione in Venezuela è stata causata principalmente dalla politica monetaria del governo, che ha portato ad una stampa eccessiva di denaro senza un'adeguata copertura economica. Inoltre, l'economia del paese è stata fortemente colpita dalla caduta dei prezzi del petrolio, che ha ridotto significativamente le entrate del governo. Secondo il sito di monitoraggio dei prezzi CoinDance, il prezzo di Bitcoin in Venezuela ha superato il livello di \$ 100.000 nel 2021.
- **Argentina** - L'Argentina ha subito ripetute crisi economiche e finanziarie, causate da una combinazione di fattori, tra cui l'elevato debito pubblico, la corruzione e la svalutazione della valuta nazionale. Questi fattori hanno portato a un'iperinflazione che ha colpito duramente la popolazione. Secondo il sito di monitoraggio dei prezzi BitcoinAverage, il prezzo di Bitcoin in Argentina ha superato i \$ 60.000 nel 2021.
- **Zimbabwe** - L'iperinflazione in Zimbabwe è stata causata dalla politica monetaria del governo, che ha stampato eccessivamente denaro per finanziare le spese pubbliche. Inoltre, il paese ha subito una crisi economica e politica a seguito della riforma agraria, che ha ridotto significativamente la produzione agricola e le entrate del governo. Secondo il sito di monitoraggio dei prezzi CoinDesk, il prezzo di Bitcoin in Zimbabwe ha superato i \$ 75.000 nel 2021.

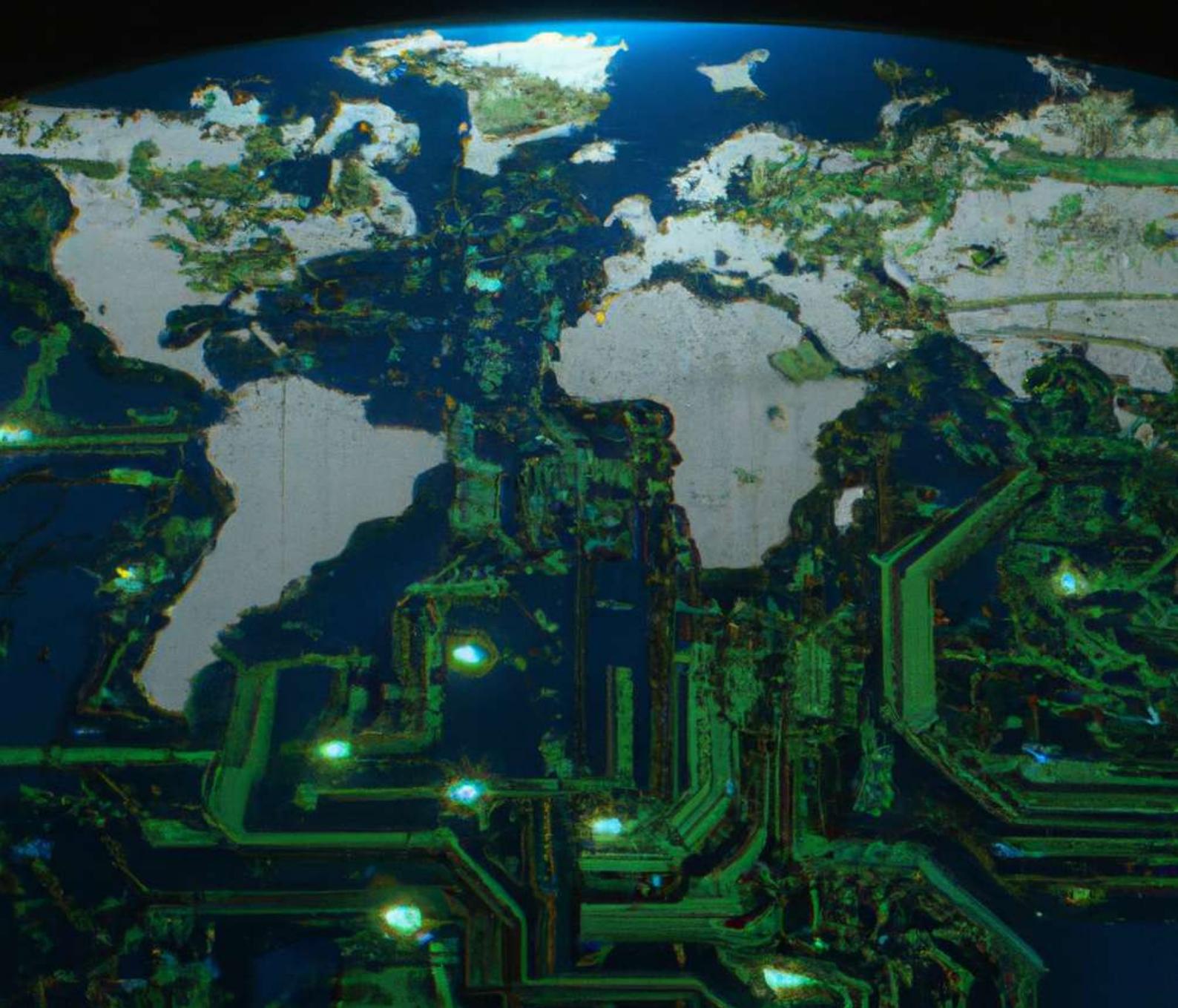
La sua natura aperta, globale e senza permessi ha dato la possibilità a queste popolazioni di scambiare la propria valuta domestica con questo digital asset.

Fonti

- ▶ Local Bitcoin Volume Chart. Fonte: <https://coin.dance/volume/localbitcoin/VES>
- ▶ Valore di Bitcoin nel tempo. Fonte: <https://bitcoinaverage.com/en/bitcoin-price/btc-to-ars>
- ▶ Ndlovu, R. (2020). Zimbabwe Annual Inflation Soars to 837%, Statistics Agency Says. Bloomberg, Fonte: <https://www.bloomberg.com/news/articles/2020-08-15/zimbabwe-annual-inflation-soars-to-837-statistics-agency-says>
- ▶ Tasso d'inflazione del Venezuela tra il 1985 ed il 2023. Statista, Fonte: <https://www.statista.com/statistics/371895/inflation-rate-in-venezuela/>
- ▶ Reuters (2023). Argentina's inflation rate soars past 100%, its worst in over 30 years. The Guardian, Fonte: <https://www.theguardian.com/world/2023/mar/15/argentina-inflation-rate-100-percent>

Capitolo 3

WEB3



Introduzione

Il terzo capitolo ha come principale obiettivo formativo quello di analizzare e far comprendere il funzionamento di un protocollo programmabile come Ethereum, o più generalmente, il funzionamento della maggior parte dei protocolli di “seconda generazione” basati sulla blockchain, che permettono lo sviluppo di software definiti come smart contract e di applicazioni web3 decentralizzate (dApps).

Il secondo obiettivo formativo è quello di aiutare il lettore a comprendere la vasta gamma di possibili applicazioni informatiche da sviluppare utilizzando la blockchain, i digital assets e le DLT e quali di queste hanno generato maggior interesse all’interno del mercato, creando delle comunità solide attorno al progetto. Il terzo obiettivo formativo è quello di comprendere il funzionamento tecnico della rete di Ethereum, delle applicazioni decentralizzate relative alla finanza decentralizzata, e di come poter iniziare a costruire una dApps attraverso smart contract e tokens con logiche di governance interne innovative.

Il capitolo inizia con una spiegazione formale del concetto di programmabilità e di economia di rete, declinando poi questi due aspetti all’interno di reti informatiche peer to peer come Ethereum.

Successivamente, verrà affrontato più nel dettaglio l’architettura della macchina virtuale di Ethereum, in grado di eseguire il codice degli smart contract ed abilitare il corretto funzionamento delle applicazioni decentralizzate che formano il web3.

All’interno del testo, verranno poi analizzate: quali sono le principali tipologie di applicazioni decentralizzate presenti nel web3, con un verticale sui servizi finanziari senza intermediazione, cos’è un token e qual è il suo ruolo in una rete peer to peer, che differenza c’è tra un token fungibile e non fungibile, e l’importanza della tokenomics, ovvero lo studio delle modalità con cui viene creato un nuovo token nel mercato. Infine, approfondiremo l’impatto degli NFT nell’economia digitale e cosa sono e come funzionano le Decentralized Autonomous Organization (DAO).

In sintesi, il capitolo è composto da 7 macro-blocchi e 45 blocchi formativi, che aiutano a comprendere l’insieme delle tecnologie e realtà che compongono il web3.

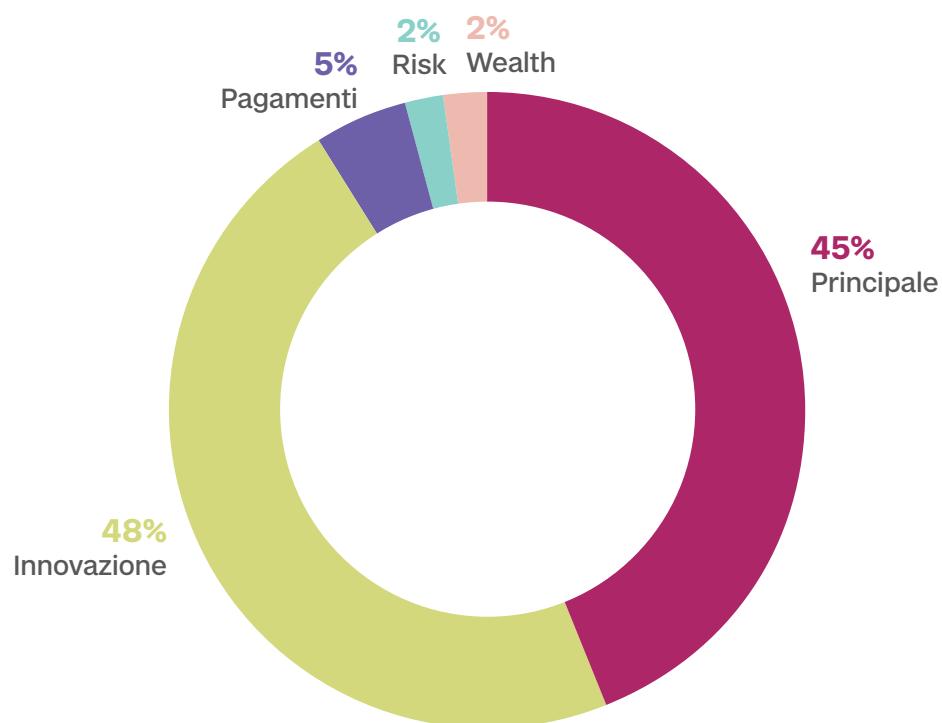
Queste alcune domande a cui cercheremo di rispondere:

- Qual è il ruolo delle aziende, startup e fondazioni nell’ecosistema Web3?
- In che modo la programmabilità permette lo sviluppo di applicazioni web sulle reti peer to peer?
- Cosa si intende per economia di rete e perché è importante?
- Quali sono le principali differenze tra le applicazioni decentralizzate rispetto a quelle centralizzate?
- Come funziona la Ethereum Virtual Machine?
- Quali sono le differenze tra un software tradizionale rispetto ad uno smart contract sviluppato all’interno di un ambiente web3?
- Come viene inserito uno smart contract nella blockchain?
- Quali sono i diversi livelli di architettura delle dApps?

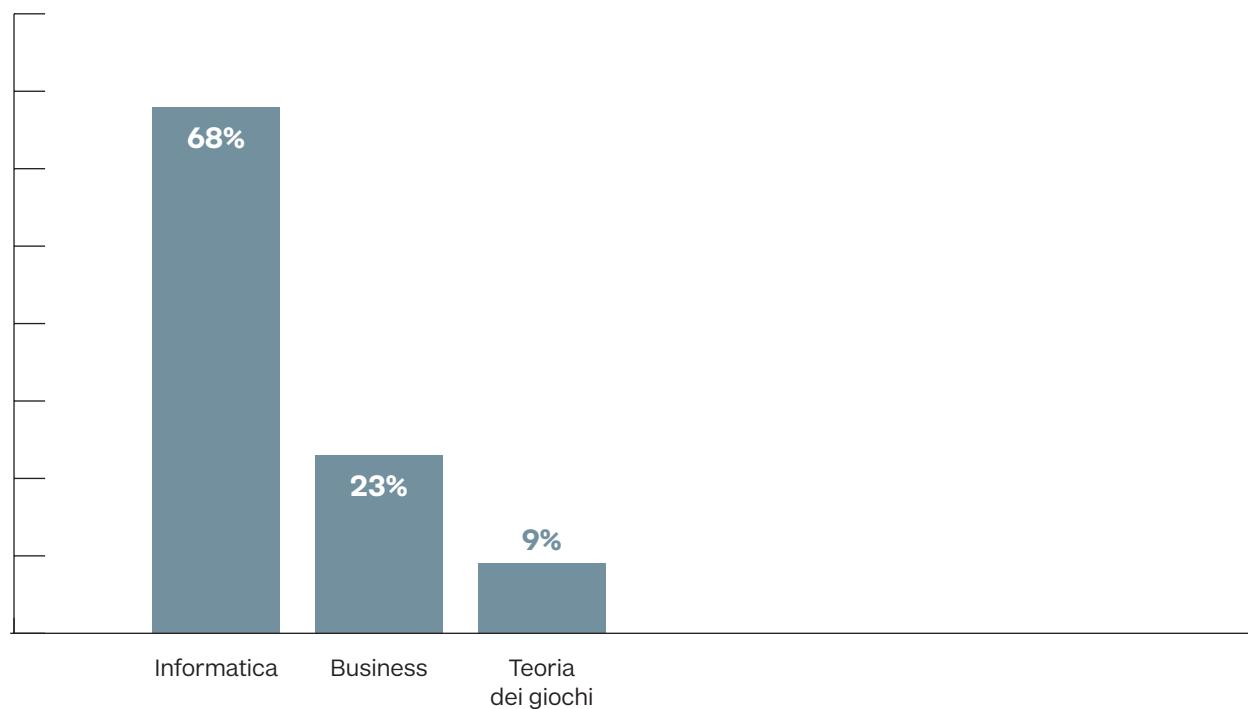
Andremo, inoltre, più in profondità, cercando di rispondere a domande quali:

- Come interagisce un client con uno smart contract nell’ecosistema Web3?
- Che cosa si intende per tokenomics? Quali sono i modelli di tokenomics più presenti all’interno del mercato dei digital assets?
- Qual è il ruolo dei token nella programmabilità delle reti peer to peer e come vengono gestiti dagli smart contract?
- Quali sono le differenze tra i diversi tipi di dApps?
- In che modo le community influenzano il mercato degli NFT?
- Come viene utilizzata la teoria dei giochi nelle reti peer to peer e nelle tokenomics delle dApps?
- Quali sono gli smart contract utilizzati per sviluppare un’applicazione e come viene gestita l’interazione tra front-end, back-end e smart contract?
- Quali sono le differenze tra i token ERC20 e ERC721 e in che modo influenzano la tokenomics delle dApps?
- Quali sono i vantaggi e le sfide dell’utilizzo di IPFS come sistema di clouding decentralizzato nell’ecosistema Web3?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. L'economia nel Web3

- 1.1 Come si è evoluto l'ecosistema del Web3?
- 1.2 Che cosa si intende per programmabilità sopra una rete peer to peer?
- 1.3 Che cos'è l'economia di rete e perché è importante?
- 1.4 Quali sono le differenze con i servizi centralizzati per lo sviluppo di applicazioni?
- 1.5 I nodi della rete di Ethereum e il suo modello di consenso distribuito

DIFFICOLTÀ	DISCIPLINA	PERCORSO
●	Business	Principale
●	Informatica	Principale
●	Informatica/Business	Principale
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr.	Principale

2. La programmabilità degli smart contract

- 2.1 Macchine virtuali in reti peer to peer: la Ethereum Virtual Machine
- 2.2 Dentro la Ethereum Virtual Machine
- 2.3 Il software sulle reti peer to peer: smart contract e dApps
- 2.4 Software on chain vs software off chain
- 2.5 Come viene inserito uno smart contract nella blockchain?
- 2.6 Gli ambienti di test per gli sviluppatori
- 2.7 Aggiornamento del network e modello di contabilità delle transazioni con smart contract
- 2.8 La programmabilità sulla rete Bitcoin

●	Informatica	Innovazione

3. Applicazioni Decentralizzate (dApps)

- 3.1 Applicazioni Web3 vs Applicazioni Web2
- 3.2 Le applicazioni decentralizzate (dApps)
- 3.3 La finanza decentralizzata
- 3.4 Finanza centralizzata e finanza decentralizzata a confronto
- 3.5 Smart Contract e standardizzazione
- 3.6 Che relazione c'è tra digital asset e smart contract?
- 3.7 La programmabilità dei token

●	Informatica/Business	Principale
●	Informatica/Business	Principale
●	Informatica/Business	Principale
●	Informatica/Business	Risk
●	Informatica	Innovazione
●	Informatica	Principale
●	Informatica	Innovazione

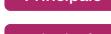
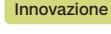
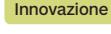
4. dApps e tokenomics

- 4.1 Cos'è la tokenomics e come fanno profitto le applicazioni decentralizzate?
- 4.2 L'uso degli ERC20 nelle dApps
- 4.3 Approfondimento sulla tokenomics: modello deflattivo o inflattivo (ERC20)

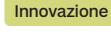
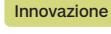
●	Informatica/Business	Principale
●	Informatica/Business	Principale
●	Teoria dei giochi	Pagamenti

- | | | |
|---|---|---|
| 4.4 Tokenomics e la teoria dei giochi
4.5 Tokenomics e la teoria dei giochi: il modello tragedy of commons scenario
4.6 Tokenomics con i token non fungibili (ERC721) |  Teoria dei giochi
 Teoria dei giochi
 |  Pagamenti
 Wealth
 Principale
 Principale |
|---|---|---|

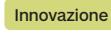
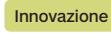
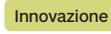
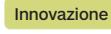
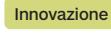
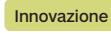
5. NFT

- | | | |
|--|--|--|
| 5.1 Il fenomeno NFT nel pop market
5.2 I mercati di riferimento degli NFT
5.3 Il ruolo della community nei progetti NFT
5.4 Social tiering ed esclusività con gli NFT
5.5 Come si gestiscono i token non fungibili dentro un wallet?
5.6 Token non fungibili per accedere a servizi esclusivi: il caso Spotify
5.7 Single Sign-On (SSO) con NFT nel Web2 e nel Web3
5.8 I metadati dentro gli NFT |  Business
 Business
 Business
 Business
 Informatica
 Informatica
 Informatica
 |  Principale
 Principale
 Principale
 Principale
 Principale
 Principale
 Innovazione
 |
|--|--|--|

6. Decentralized Autonomous Organization (DAO)

- | | | |
|--|--|--|
| 6.1 Che cosa sono le DAO?
6.2 Quali applicazioni possono nascere con una DAO?
6.3 Quali sono i tokens utilizzati da una DAO?
6.4 Considerazioni sulla tokenomics e la governance in una DAO |  Informatica/Business
 Informatica/Business
 Informatica
 |  Principale
 Principale
 Innovazione
 |
|--|--|--|

7. Approfondimenti su Token e Smart Contract

- | | | |
|--|--|--|
| 7.1 Costruire nel Web3
7.2 Tipologia di smart contract per lo sviluppo di dApps
7.3 Approfondimento Tether (ERC20)
7.4 Approfondimento Compound (DeFi)
7.5 Approfondimento IPFS (InterPlanetary File System)
7.6 Approfondimento CryptoKitties (ERC721) |  Informatica
 Informatica
 Informatica
 Informatica
 Informatica
 |  Innovazione
 Innovazione
 Innovazione
 Innovazione
 Innovazione
 |
|--|--|--|

1

L'economia del Web3

- 1.1 Come si è evoluto l'ecosistema del Web3?
- 1.2 Che cosa si intende per programmabilità sopra una rete peer to peer?
- 1.3 Che cos'è l'economia di rete e perché è importante?
- 1.4 Quali sono le differenze con i servizi centralizzati per lo sviluppo di applicazioni?
- 1.5 I nodi della rete di Ethereum e il suo modello di consenso distribuito

1.1

Business

Basic

Come si è evoluto l'ecosistema del Web3?

Dopo il 2009, in seguito alla pubblicazione del **white paper** di Bitcoin, il settore dell'innovazione, globalmente, ha iniziato ad interessarsi alla materia, offrendo diverse applicazioni e servizi per aziende private e consumatori finali. Storicamente, le prime aziende entrate nel mercato sono state:

- BitPay, creando **un carrello digitale** per facilitare l'uso dei bitcoin per i pagamenti online
- Coinbase, creando **una piattaforma di scambio** (exchange) per aiutare lo scambio tra privati di digital assets.
- BitGo, che ha creato dei **wallet digitali** per aiutare a custodire i propri digital assets.

Da lì a poco, il mercato si è iniziato a popolare. L'obiettivo comune di queste nuove aziende è stato:

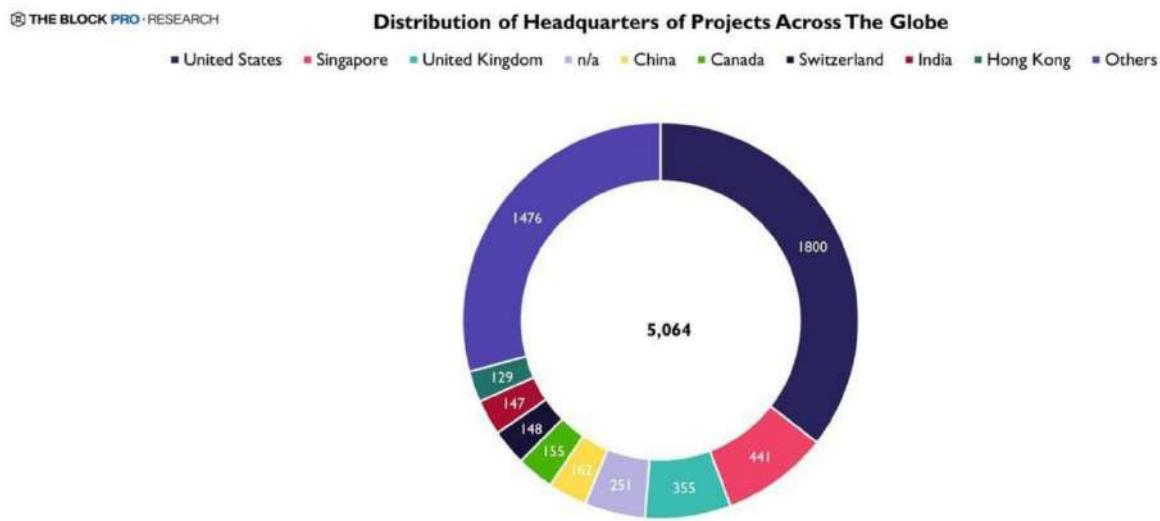
- Migliorare l'usabilità dell'utente finale per interagire con il protocollo
- Migliorare la sicurezza nella gestione delle proprie chiavi private
- Espandere l'offerta di casi di applicazione per questi protocolli informatici
- Espandere l'uso di questo nuova rete informatica in nuovi mercati



White Paper

Un *white paper* è un documento informativo, solitamente emesso da un'azienda o da un'organizzazione no-profit, per promuovere o evidenziare le caratteristiche di una soluzione, di un prodotto o di un servizio. Nel caso di Bitcoin è stato pubblicato da uno pseudonimo, Satoshi Nakamoto, il 31 Ottobre 2008.

L'interesse crescente verso la tecnologia spinse altri sviluppatori a creare altri protocolli informatici simili a Bitcoin, con caratteristiche simili, come Dogecoin, Litecoin e altre centinaia di progetti. Solitamente questi progetti pubblicano un white paper, all'interno del quale vi sono alcuni dettagli rispetto alla modalità di emissione del loro digital asset e il campo applicativo coperto dal progetto, con proiezioni di crescita e il team e/o come partecipare pubblicamente al progetto. Molti di questi fallirono poiché poco utilizzati e con poco valore, **se non essere una semplice copia del protocollo originale**. Tuttavia, a fine 2013, dopo la pubblicazione della prima documentazione di Ethereum, si capì che lo sfruttamento della rete peer to peer e della blockchain era possibile per implementare **nuove logiche con cui costruire applicazioni web**, senza la necessità di un ente centrale. Questa nuova gamma di protocolli, differentemente da Bitcoin, sarà costruita con un linguaggio di programmazione completo, permettendo agli sviluppatori di scrivere codice per automatizzare le transazioni e creare delle nuove applicazioni. **La somma di tutte queste nuove reti peer to peer, definite come programmabili, e la somma di tutte le applicazioni su di esse costruite, può essere definito, oggi, come l'industria del web3.**



All'interno dell'industria web3, ci sono diverse tipologie di iniziative, alcune a scopo di lucro realizzate da aziende private, altre senza scopo di lucro realizzate da fondazioni, gruppi di sviluppatori indipendenti e cooperative fisiche o virtuali, con l'unico scopo di diffondere sapere ed innovazione. Qui di seguito alcuni esempi:

- **Le reti peer to peer e open-source sono tecnologie pubbliche e gratuite che possono essere utilizzate e modificate da chiunque.** Per esempio, il protocollo Bitcoin non è nato né da una azienda privata, né da una fondazione, ma da una comunità decentralizzata.
- Le **fondazioni sono organizzazioni senza scopo di lucro** che svolgono un ruolo chiave nello sviluppo e nella **promozione di una particolare tecnologia**, al contrario le **aziende private, sono società con scopo di lucro che forniscono servizi e tecnologie basate su blockchain**. Per esempio, Ethereum, è nata insieme alla fondazione Ethereum Foundation, che si occupa di organizzare iniziative per la community e luogo di scambio di proposte. Nel tempo molte altre realtà hanno seguito questa modalità per far crescere il proprio progetto.
- Le aziende private, come **startup o tech company**, che sviluppano nuovi servizi sopra i protocolli peer to peer o offrono soluzioni che aiutano aziende e privati a gestire i propri digital assets. ConsenSys è una azienda privata che ha sviluppato Metamask, uno dei principali wallet per interagire con la rete di Ethereum.
- Le **cooperative** invece sono **organizzazioni in cui i membri hanno una proprietà collettiva dell'organizzazione stessa e partecipano alla sua gestione e ai suoi profitti**.
- Le **DAO sono organizzazioni autonome decentralizzate, create dal web in maniera distribuita e con un approccio bottom up**, in cui le decisioni sono prese in modo democratico dalla comunità di membri che partecipano alla rete attraverso votazioni.

Assetto Societario	Esempi
Aziende Private	Consensys, Coinbase, Chainlink, Uniswap
Fondazione	Zcash Foundation, Cardano Foundation, Ethereum Foundation
Protocollo Open Source	Bitcoin, Ethereum, Polkadot, Solana
Cooperative	Gnosis, Aragon, Gitcoin, MetaCartel
DAO	MakerDAO, Aave, Compound, Yearn.finance

Questi sono solo alcuni esempi di assetti societari all'interno del web3, ma ci sono molte altre tipologie di organizzazioni che possono essere trovate all'interno di questo spazio in continua evoluzione.

1.2

Informatica

● Basic

Che cosa si intende per programmabilità sopra una rete peer to peer?

Nel capitolo precedente, abbiamo analizzato cosa sono le reti peer to peer e come queste funzionano. Abbiamo anche visto che l'architettura della rete e il ruolo dei nodi della rete può differenziare in funzione dello scopo che la rete vuole raggiungere ed offrire. Da qui in avanti, per comprendere a pieno come funziona il web3, dobbiamo aggiungere un nuovo concetto: **la programmabilità**.

La programmabilità nelle reti peer-to-peer (P2P) si riferisce alla capacità di personalizzare e gestire il comportamento della rete attraverso l'uso di un software programmabile. Ciò significa che **utenti, fondazioni, organizzazioni ed aziende possono creare applicazioni web (programmi) personalizzate o estensioni per la rete che eseguono funzionalità specifiche**. Il codice di questi nuovi programmi è distribuito nella rete e la loro esecuzione avviene tramite potenza computazionale offerta dalla rete, senza appoggiarsi ad un server o cloud privato, come AWS o Azure Cloud.

La programmabilità rende Ethereum un computer globale sopra il quale sviluppatori e aziende possono creare delle nuove applicazioni chiamate dApps (o anche applicazione decentralizzate). Dal punto di vista tecnologico, rispetto a Bitcoin, protocolli come Ethereum hanno un nuovo elemento, ovvero una macchina virtuale che insieme al database distribuito, la blockchain, rende possibile l'esecuzione del codice direttamente sul protocollo. **Una semplice analogia possiamo farla con il nostro computer di casa, il quale possiede una memoria da cui pescare le informazioni e un calcolatore (macchina virtuale) che esegue le informazioni memorizzate**. Anche il cloud, per esempio, è un insieme di macchine virtuali che permette alle aziende di far funzionare le applicazioni offerte sul web.

La programmabilità è importante nelle reti P2P poiché consente agli utenti di personalizzare la rete in base alle loro esigenze specifiche, migliorandone flessibilità e scalabilità. Inoltre, la **programmabilità può essere utilizzata per migliorare la sicurezza** della rete e garantire la privacy degli utenti.

Da Ethereum in avanti, la maggior parte delle reti peer to peer nel web3 hanno incluso linguaggi di programmazione più semplici, nuove interfacce di programmazione delle applicazioni (API) e framework di sviluppo volti a facilitare creazione di servizi ed aggiungere nuove funzionalità per gestire e creare digital assets.

1.3

Informatica / Business

● Basic

Che cos'è l'economia di rete e perché è importante?

Quando si parla di economia di rete si fa riferimento a **tutti quei servizi e prodotti che possono essere monetizzati attraverso la rete internet**. Ogni applicazione sul nostro computer o smartphone genera una economia di rete, ovvero una economia sopra una rete informatica che coinvolge:

- Un utente pagante
- Un'azienda o un ente che offre e mantiene il servizio (in cambio di un pagamento)

Con riferimento al web3 ed a protocolli programmabili come Ethereum bisogna considerare che:

- Ogni utente che vuole fornire informazioni sulla rete è un utente pagante, poiché dovrà spendere un piccolo ammontare dei digital assets della blockchain stessa (es: ETH per Ethereum, BTC per Bitcoin etc..) per poter registrare informazioni sulla rete;
- Ogni sviluppatore e/o azienda diventa un utente pagante quando inserisce un programma sopra la rete, per creare delle applicazioni decentralizzate e/o dei nuovi digital assets
- I minatori offrono e mantengono il servizio, in cambio di un pagamento. Importante sottolineare come i cosiddetti “full node” possono, però, essere creati da tutti gli utenti, con il solo fine di interrogare la blockchain e senza offrire un servizio che punti a validare le transazioni.
- Ogni sviluppatore e/o azienda che offre nuove applicazioni personalizzate e/o dei nuovi digital assets, può ricevere in cambio un pagamento a fronte del servizio offerto.

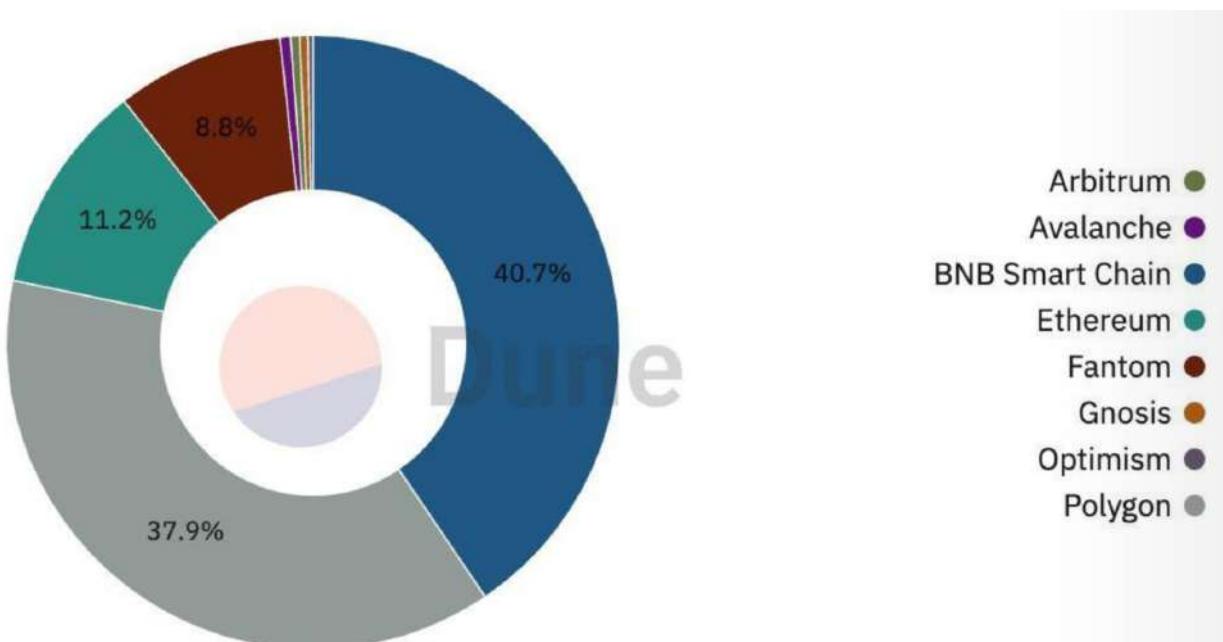
Le applicazioni decentralizzate utilizzano un insieme di nuovi software e programmi logici definiti come smart contract. Questi contratti intelligenti possono essere considerati dei nuovi componenti logici, inseriti all'interno della rete che automatizzano transazioni tra i nodi e/o abilitano nuove funzionalità tra gli utenti, seguendo la logica “if this, then that”: “se succede questo, allora attiva questo”.



Funny Facts

Nick Szabo ha introdotto il concetto di smart contract ispirandosi alla macchinetta del caffè. Come una macchinetta del caffè, uno smart contract è un meccanismo automatico che esegue automaticamente un'azione quando vengono soddisfatte determinate condizioni. In pratica, uno smart contract è un codice informatico che si autoesegue quando viene raggiunto un certo stato o condizione, senza bisogno di un intermediario umano.

Prendendo un recente report di Dune aggiornato al 2022, solamente il 11,2% degli smart contract sviluppati sul web3 sono stati costruiti sulla rete di Ethereum. Molti di questi sono stati sviluppati su altre reti P2P come Binance Smart Chain, Arbitrum, Polygon. Una buona parte delle nuove reti su cui sono stati sviluppati Smart Contract sono, però, dei layer 2, ovvero layer secondari e compatibili con la blockchain di Ethereum (si dicono EVM compatible, ovvero Ethereum Virtual Machine Compatible), costruiti sulla stessa tecnologia. La nascita di nuove reti ha permesso a sviluppatori e aziende di creare nuove tipologie di applicazioni decentralizzate, aiutando la crescita dell'industria e la gamma delle possibili funzionalità.



In tutte queste reti e dApps, l'economia di rete è sostenuta da incentivi monetari tramite digital assets non duplicabili. Per facilità di comprensione, possiamo distinguere i digital assets in due macrocategorie:

- gli asset **nativi della rete** sono noti come Digital Assets;
- gli **asset generati tramite degli smart contract** sono noti come token.

Per esempio, sulla rete Ethereum, **esiste Ether**, digital asset che viene utilizzato per pagare i nodi validatori per garantire la sicurezza nella rete, ed esistono altri token, utilizzati dalle applicazioni decentralizzate costruite sopra la piattaforma, con scopi diversi e con una tokenomics completamente diversa. La creazione di applicazioni web decentralizzate (dApp) è vitale per la creazione di una più ampia definizione di economia di rete all'interno di reti peer to peer programmabili come Ethereum.

Il **valore di una rete peer to peer dipende quindi dalla adozione da parte di una vasta comunità di nodi partecipanti, quali sviluppatori, aziende e utenti**. In altre parole, quanto più persone utilizzano una determinata rete, tanto maggiore sarà il valore che questa fornisce a ciascuno degli utenti. **L'uso di Ethereum consente di creare applicazioni che non richiedono l'intermediazione di una terza parte per approvare lo sviluppo e la diffusione della applicazione nella rete.**

Ciò significa che le **dApp possono essere sviluppate e utilizzate senza dover fare affidamento su un'autorità centrale**, il che le rende molto interessanti per una vasta gamma di utilizzi, dalle applicazioni finanziarie ai giochi online. Inoltre, l'utilizzo di Ethereum come infrastruttura di base consente alle dApp di beneficiare dell'economia di rete, poiché l'aumento del numero di utenti che partecipano alla rete aumenta il valore di ciascuna delle applicazioni che vi si appoggiano.

1.4

Teoria dei Sistemi Distribuiti

• Medium

Quali sono le differenze con i servizi centralizzati per lo sviluppo di applicazioni?

Il **Web3** è la terza generazione del World Wide Web, che si differenzia dalle precedenti per l'**utilizzo di sistemi di computazione distribuiti basati sulla tecnologia blockchain**. In questo sistema, le applicazioni non sono più ospitate su server centralizzati, ma vengono eseguite su una rete di computer interconnessi tra loro (nodi) che lavorano insieme per fornire servizi e risorse.

Dal punto di vista informatico, possiamo immaginare che il web3 si basa su:

- Un sistema di computazione distribuita (Distributed Computing System, DCS)
- Un sistema di clouding distribuito (Distributed Cloud Computing, DCC)

Il **DCS** è un sistema in cui il carico di lavoro viene suddiviso tra diversi nodi della rete, che lavorano insieme per eseguire un'elaborazione distribuita. In questo modo, il DCS può garantire una maggiore affidabilità e disponibilità rispetto ad un sistema centralizzato, in cui la mancata disponibilità del server potrebbe impedire l'accesso ai servizi.

Il **DCC**, invece, è una **forma di cloud computing basata sulla condivisione di risorse di calcolo, archiviazione e rete tra più nodi della rete, senza l'intermediazione di un provider di servizi cloud centralizzato**. In questo modo, il DCC può garantire una maggiore sicurezza e privacy dei dati, poiché i dati sono distribuiti su più nodi della rete.

L'uso dei **token** nativi della piattaforma Ethereum, come Ether, vengono utilizzati dagli sviluppatori come **una nuova forma di commodity volta ad usufruire delle risorse computazionali e di memoria** offerte dai nodi della rete peer to peer. Questo avviene quando viene eseguito del codice sulla blockchain

(smart contract). Una domanda da porsi è se, nel lungo periodo, questo sistema decentralizzato potrà diventare un'alternativa valida ai sistemi distribuiti in cloud.

Ad oggi, uno dei principali limiti sta nelle dimensioni e nella continua crescita della blockchain, la quale sta obbligando gli sviluppatori ad utilizzare servizi cloud come quelli di AWS, per scaricare integralmente tutta la storia blockchain di Ethereum. Sarà interessante nel lungo periodo capire la relazione tra la distribuzione dei nodi di una rete e la sua sicurezza ed accessibilità rispetto alla dipendenza dei sistemi cloud offerti da Google, AWS, Azure e altri player tech.

1.5

Teoria dei Sistemi Distribuiti

● Basic

I nodi della rete di Ethereum e il suo modello di consenso distribuito

Esistono, anche per la protocollo peer to peer di Ethereum, diverse opzioni per partecipazione come nodo della rete:

- Light Node (nodo leggero)
- Full Node (Nodo Pieno)
- Archive Node (Nodo Archivio)
- Staker Node (svolge in maniera simile alcune funzioni del minatore per la rete di Bitcoin)

I nodi leggeri (i.e. wallet), consentono agli utenti di partecipare senza l'hardware potente o l'elevata larghezza di banda, come gli **hard e i cold wallet**. Eseguendo transazioni anche dal proprio smartphone e computer portatile. Anche nella rete di Ethereum, i light node non partecipano al consenso distribuito.



Hard e cold wallet

Con i termini *hard* e *cold*, si classificano i wallet in due macrocategorie che si differenziano rispetto alla possibilità di connettersi online e la sicurezza. Infatti, gli *hard wallet* sono strumenti meno sicuri rispetto ai *cold wallet*, in quanto scambiano la possibilità di operare online con la loro potenziale vulnerabilità ad attacchi su Internet. Il *cold wallet*, invece, viene sviluppato senza la possibilità di connettersi ad Internet, ma con la sicurezza di creare le chiavi private in un ambiente virtuale sterile.

I full node e i nodi archivio hanno entrambi il compito di salvare sul proprio computer il database distribuito come nella rete di Bitcoin, ma con alcune differenze. Il full node registra solo parte della storia della blockchain, mentre il nodo archivio memorizza l'intero storico dei dati. Per esempio, un nodo archivio può essere utile **per le aziende che offrono servizi come esploratori di blocchi, venditori di portafogli e analisi della catena**. Entrambi i nodi possono partecipare al consenso distribuito durante gli aggiornamenti di software e modifiche del codice sorgente.



Proof of stake

È detto proof-of-stake (PoS, vagamente traducibile in italiano come “prova che si ha un interesse in gioco”) un tipo di protocollo per la messa in sicurezza di una rete di digital assets e per il conseguimento di un consenso distribuito.

Con l'introduzione del **Proof of Stake** nella rete di Ethereum, anche il ruolo del nodo minatore cambia significativamente rispetto a quello di Bitcoin. Invece di utilizzare la potenza di calcolo per vincere la competizione tra i minatori, risolvendo un problema matematico, **i nodi staker utilizzano parte del loro capitale in Ether come garanzia per essere sorteggiati, come nodo validatore, per creare il nuovo blocco e guadagnare il signoraggio.** In altre parole, i nodi staker devono possedere una quantità sufficiente di Ether per poter partecipare al processo di validazione delle transazioni e ricevere ricompense in base alla loro partecipazione.

Molte reti simili ad Ethereum hanno progressivamente adottato questo modello di consenso distribuito al posto alla prova di lavoro (i.e. Proof of Work) fatta dai minatori. Entrambi i modelli possono essere considerati una sorta di lotteria, in cui la probabilità del nodo minatore/staker di validare il prossimo blocco e ottenere nuovi digital assets come ricompensa, è rappresentata da:

- **Proof of work:** % di potenza di calcolo sul totale della potenza di calcolo della rete
- **Proof of stake:** % di capitale in digital asset nativo sul totale dei digital assets

In entrambi i casi, ci sono dei meccanismi di disincentivi per facilitare il raggiungimento del consenso distribuito e che la validazione delle informazioni sia corretta. Infatti, se nel caso della POW il disincentivo di validare informazioni non corrette è il costo dell'energia elettrica, nella POS il disincentivo è quello che il proprio capitale venga bloccato sulla rete, rendendolo inutilizzabile.

2

La programmabilità degli smart contract

- 2.1 Macchine virtuali in reti peer to peer: la Ethereum Virtual Machine
- 2.2 Dentro la Ethereum Virtual Machine
- 2.3 Il software sulle reti peer to peer: smart contract e dApps
- 2.4 Software on chain vs software off chain
- 2.5 Come viene inserito uno smart contract nella blockchain?
- 2.6 Gli ambienti di test per gli sviluppatori
- 2.7 Aggiornamento del network e modello di contabilità delle transazioni con smart contract
- 2.8 La programmabilità sulla rete Bitcoin

2.1

Informatica

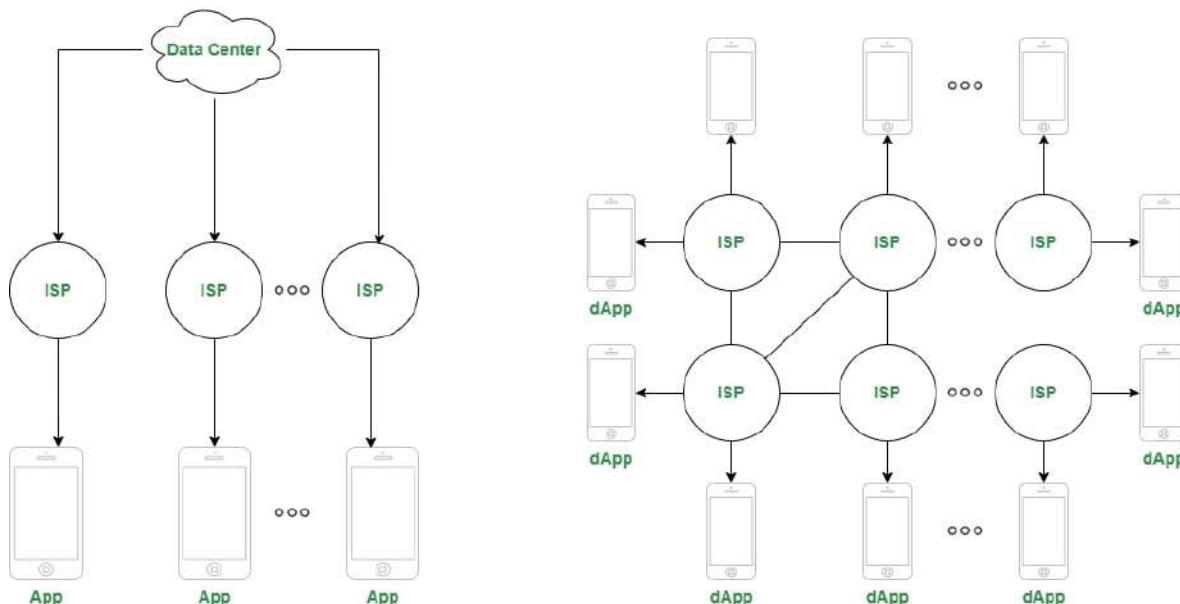
• Medium

Macchine virtuali in reti peer to peer: la Ethereum Virtual Machine

Una **macchina virtuale in una rete peer-to-peer (P2P)** è un software che simula il comportamento di un computer fisico, consentendo l'esecuzione di programmi e l'elaborazione di dati su più nodi della rete, in modo distribuito e cooperativo.

In una rete P2P, le macchine virtuali possono essere utilizzate per **creare e gestire applicazioni decentralizzate (dApp)**. Differentemente dalle applicazioni centralizzate le dApps, non utilizzano un modello client server, ma pescano le informazioni dai nodi vicini attraverso protocolli di comunicazione quali, ad esempio, il modello di gossiping (di cui abbiamo parlato precedentemente).

Normal Apps VS dApps



Nella tabella in alto, il termine ISP sta per Internet Service Provider: **un'organizzazione che fornisce servizi per l'accesso a Internet e/o alla rete di riferimento per poter far funzionare la logica della applicazione.**

Nel contesto delle reti client-server e peer-to-peer, gli ISP svolgono un ruolo fondamentale nel facilitare la comunicazione tra i nodi di queste reti.

- **Per le applicazioni client-server (app),** gli ISP forniscono la connettività necessaria per consentire ai client di comunicare con i server. In molti casi, i server sono ospitati in data center, che sono strutture fisiche progettate per ospitare e gestire grandi quantità di hardware di rete e di server. Gli ISP forniscono la connessione tra i client (ad esempio, il tuo smartphone o il tuo computer) e il data center in cui è ospitato il server dell'app.
- **Per le applicazioni decentralizzate (dApps),** che utilizzano reti peer-to-peer, gli ISP svolgono un ruolo simile. Forniscono la connettività necessaria per consentire ai nodi della rete di comunicare tra loro. Tuttavia, a differenza delle app client-server, le dApps non dipendono da un singolo server o data center, in quanto, le informazioni e le funzionalità dell'applicazione sono distribuite tra tutti i nodi della rete. Nonostante ciò, gli ISP rimangono fondamentali per fornire la connessione Internet che consente a questi nodi di comunicare tra loro.

I nodi Archive e Full ospitano delle macchine virtuali nella rete, permettendo così all'utente di connettersi al codice di una dApps dal proprio client e chiamando il codice dello smart contract in esecuzione in maniera distribuita negli archive e full node. Le macchine virtuali in reti P2P sono spesso basate su tecnologie di virtualizzazione, come ad esempio la **virtualizzazione** a livello di sistema operativo (OS-level virtualization) o la virtualizzazione basata su container. Questi approcci consentono la creazione di ambienti virtuali isolati l'uno dall'altro, in cui i programmi e i dati possono essere eseguiti in sicurezza senza interferenze esterne.

L'utilizzo di macchine virtuali in reti P2P offre numerosi vantaggi, tra cui una maggiore sicurezza e affidabilità, la possibilità di eseguire programmi su qualsiasi nodo della rete e l'eliminazione della necessità di dipendere da un'unica autorità centrale per la gestione e l'elaborazione dei dati.

Parametri	Macchine virtuali P2P	Macchine virtuali non P2P
Topologia di rete	Mesh o fully connected	Gerarchica o a stella
Scalabilità	Ottime (teorico)	Limitate
Prestazioni di rete	Buone	Dipende dal tipo di rete
Sicurezza della rete	Bassa	Elevata
Capacità di condivisione delle risorse	Elevata	Limitata
Complessità di configurazione	Elevata	Bassa
Affidabilità	Bassa	Elevata
Utilizzo di larghezza di banda	Elevato	Limitato
Comunicazione inter-processo	Supportata	Non supportata
Utilizzo di CPU	Elevato	Limitato
Utilizzo di memoria	Elevato	Limitato

2.2

Informatica

● Hard

Dentro la Ethereum Virtual Machine

Vitalik Buterin, il **21 novembre 2013**, ha pubblicato lo **yellow paper** di Ethereum, all'interno del quale spiegava la relazione tra la blockchain e la sua macchina virtuale, EVM.

EVM, o Ethereum Virtual Machine, è una macchina virtuale che esegue il codice per automatizzare e gestire le transazioni, utilizzando quelli che vengono definiti come smart contract all'interno della blockchain di Ethereum. EVM è progettato per eseguire in modo sicuro un codice scritto in un linguaggio di programmazione speciale, come il linguaggio di programmazione Solidity, e garantisce che tutti i nodi sulla rete Ethereum eseguano lo stesso codice e producano risultati coerenti.

Inoltre, la **EVM è un ambiente sandboxed**, il che significa che i contratti intelligenti e le transazioni eseguite su di essa non possono interagire con l'esterno o influenzare altre applicazioni o parti della rete Ethereum.

L'architettura della EVM è costituita da diversi strati, ognuno dei quali svolge una funzione specifica all'interno del sistema. Ecco una descrizione dettagliata degli strati:

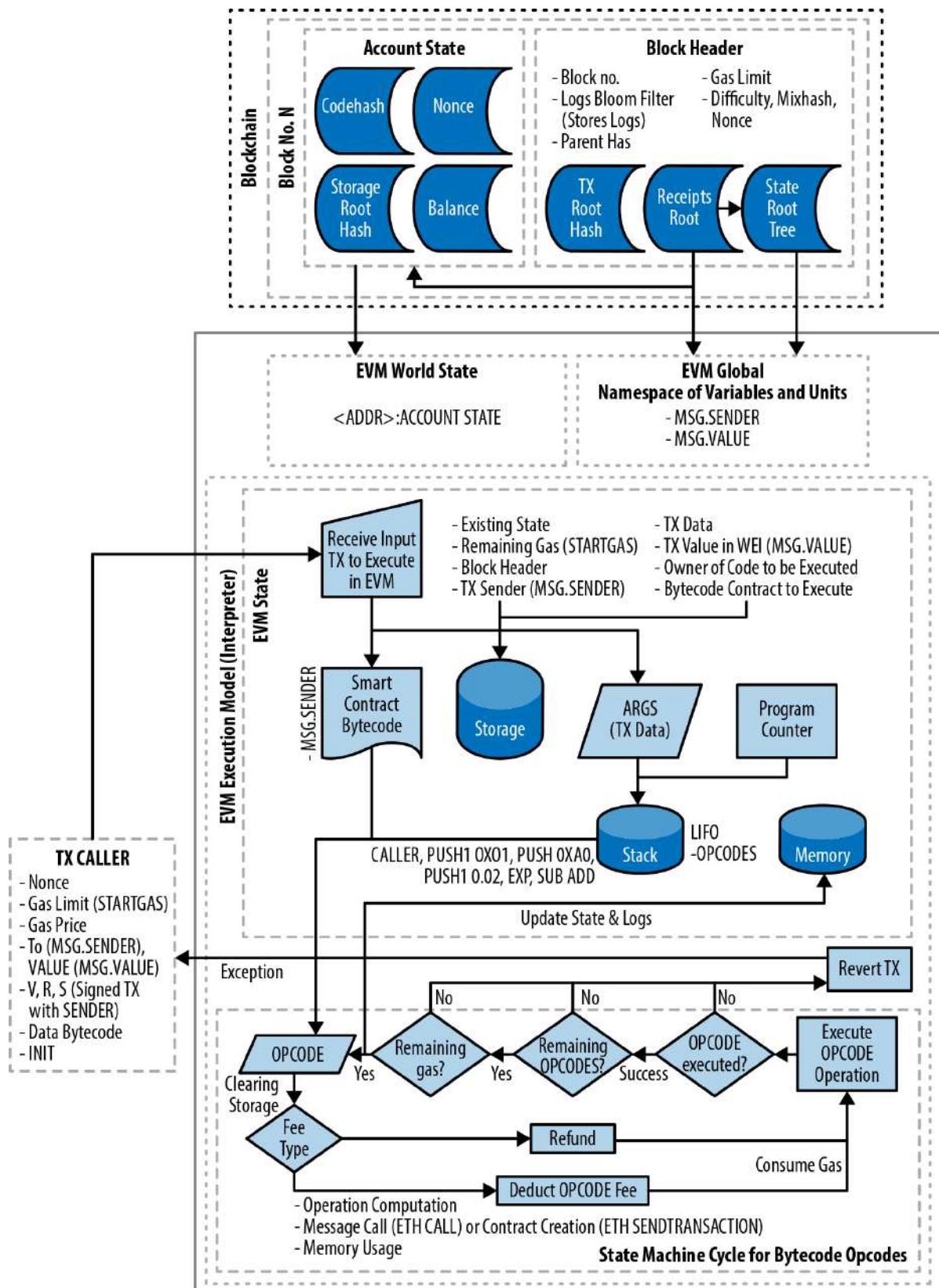
- **Linguaggio di programmazione:** come Solidity, che viene utilizzato per scrivere i contratti intelligenti. Questo linguaggio viene poi compilato in codice byte e quindi caricato sulla EVM per l'esecuzione.
- **Strato di memoria:** dove vengono memorizzati i dati che vengono utilizzati e modificati durante l'esecuzione del contratto intelligente.

- **Strato di esecuzione:** dove viene eseguito il codice del contratto intelligente. Questo strato utilizza un registro, una pila e un program counter per tenere traccia dello stato dell'esecuzione e dei dati utilizzati.
- **Strato di storage:** dove vengono memorizzati i risultati dell'esecuzione del contratto intelligente e le informazioni sul suo stato. Questi dati sono permanenti e vengono archiviati sulla blockchain.

Questi strati costituiscono lo stack tecnologico della EVM, che consente di eseguire contratti intelligenti in modo affidabile e sicuro sulla blockchain di Ethereum.

L'immagine di seguito presentata rappresenta l'architettura e il contesto di esecuzione della Ethereum Virtual Machine (EVM). Ecco una descrizione del flusso logico:

- **Block Header:** questo è l'intestazione del blocco che contiene informazioni come il numero del blocco, il limite di gas, il nonce e l'hash del blocco genitore.
- **EVM World State:** rappresenta lo stato globale della rete Ethereum. Ogni account (indirizzo) ha uno stato associato che include informazioni come il saldo di Ether, lo storage, e il codice del contratto (se l'account è uno smart contract).
- **EVM State:** questo corrisponde allo stato corrente dell'EVM durante l'esecuzione di uno smart contract. Include informazioni come il mittente del messaggio (MSG.SENDER), il valore del messaggio (MSG.VALUE), e lo stato esistente.
- **Smart Contract:** con esso si intende il codice dello smart contract che viene eseguito, ed è rappresentato come bytecode, che è il formato di codice che l'EVM può eseguire.
- **Modello (Interpreter):** componente dell'EVM che interpreta ed esegue il bytecode dello smart contract. Ogni operazione nel bytecode ha un costo di gas associato, che viene detratto dal gas totale disponibile.
- **EVM Execution:** processo di esecuzione del bytecode che include operazioni come PUSH e CALLER, che sono istruzioni nel linguaggio di programmazione di basso livello utilizzato dall'EVM.
- **Aggiornamento dello Stato e dei Logs:** dopo che ogni operazione è stata eseguita, lo stato dell'EVM viene aggiornato. Questo può includere il trasferimento di Ether, la modifica dello storage di uno smart contract, o la creazione di nuovi log.
- **Memory:** questa è la memoria temporanea utilizzata dall'EVM durante l'esecuzione di uno smart contract, in cui vengono memorizzate le variabili e i dati temporanei.
- **Operazione di Calcolo:** rappresenta il calcolo effettivo eseguito dall'EVM. Ogni operazione nel bytecode viene eseguita in sequenza, con il costo di gas appropriato detratto dal gas totale disponibile.
- **Ciclo di Stato della Macchina per Bytecode OpCodes:** ciclo di esecuzione dell'EVM. Ogni operazione nel bytecode viene eseguita una alla volta, con lo stato dell'EVM aggiornato dopo ogni operazione.



L'immagine fornisce una panoramica di alto livello di come funziona l'EVM e di come esegue gli smart contract sulla rete Ethereum.

Infine, la **EVM include anche meccanismi di sicurezza, come la limitazione del gas per impedire l'esecuzione eccessiva di codice e la gestione degli errori per gestire situazioni impreviste durante l'esecuzione del contratto intelligente**. Questi meccanismi garantiscono che la EVM sia un ambiente sicuro.

e affidabile per lo sviluppo e l'esecuzione di contratti intelligenti e applicazioni decentralizzate. Inoltre, questo porta gli sviluppatori a ben calcolare la logica e la lunghezza del proprio codice, cercando così di ottimizzare i costi di ogni operazione eseguita dalla EVM.



GAS FEE

Definizione: // Gas è l'unità di misura utilizzata per calcolare le “gas fee” la tariffa necessaria a concludere una transazione o per eseguire gli smart contract di Ethereum.

Fonte: <https://www.btc sentinel.com/blog/Gas-fee-cosa-sono-Digital Assets-blockchain-ethereum>

Fonte

► <https://github.com/ethereumbook/ethereumbook>

2.3

Informatica

● Medium

Il software sulle reti peer to peer: smart contract e dApps

I software dentro una piattaforma come Ethereum vengono definiti come smart contract. **La EVM permette quindi agli sviluppatori di scrivere del codice e farlo eseguire in maniera autonoma e deterministica.** Questo permette di automatizzare transazioni nella rete ed applicare nuove logiche per coloro che utilizzano Ethereum.

Ecco un elenco delle principali caratteristiche degli smart contract su Ethereum:

1. **Autonomia:** Uno smart contract esegue automaticamente una volta che viene attivato, senza la necessità di alcun intervento umano.
2. **Codice immutabile:** Il codice di uno smart contract viene immesso sulla blockchain e diventa immutabile, ovvero non può essere modificato o cancellato.
3. **Sicurezza:** Gli smart contract sono costruiti per essere sicuri e resistere ad attacchi esterni, grazie alla crittografia e alla decentralizzazione.
4. **Trasparenza:** Tutte le operazioni eseguite su uno smart contract sono pubbliche e possono essere verificate sulla blockchain.
5. **Decentralizzazione:** Gli smart contract sono eseguiti su una rete di nodi decentralizzati, il che significa che non ci sono autorità centrali che controllano l'elaborazione dei dati.
6. **Programmabilità:** Gli smart contract sono programmi, quindi possono essere scritti in diversi linguaggi di programmazione e utilizzati per eseguire una vasta gamma di operazioni.
7. **Interoperabilità:** Gli smart contract possono interagire con altri smart contract o applicazioni decentralizzate, creando un'infrastruttura di applicazioni interconnesse.
8. **Costi di transazione:** Le transazioni che coinvolgono gli smart contract richiedono l'utilizzo di un digital asset come il token Ethereum, che viene utilizzato come carburante per l'esecuzione delle operazioni.

Uno smart contract è un programma autonomo (software) che esegue automaticamente, sulla base di una serie di regole predefinite, determinate azioni in modo sicuro, affidabile e trasparente. Quando questo viene invocato da un utente o da uno sviluppatore, allora questo paga del gas alla rete. Uno smart contract su Ethereum interagisce con indirizzi, spostamento di token e applicazioni su front-end come il login con il wallet in vari modi. Ecco una descrizione passo-passo di come avviene questo processo:

- **Creazione dello Smart Contract:** prima di tutto, uno sviluppatore scrive lo smart contract utilizzando un linguaggio di programmazione chiamato Solidity. Questo smart contract può includere funzioni per interagire con indirizzi Ethereum, trasferire token e altro ancora.
- **Deploy dello Smart Contract:** una volta scritto, lo smart contract viene “deployato” sulla rete Ethereum. Questo significa che viene inviata un’operazione speciale alla rete che registra il contratto nello stato globale di Ethereum. Ogni smart contract ha un indirizzo Ethereum associato, proprio come un account normale.
- **Interazione con gli Indirizzi:** gli smart contract possono interagire con altri indirizzi Ethereum in vari modi. Ad esempio, possono inviare Ether ad un indirizzo, o possono chiamare funzioni su altri smart contract utilizzando il loro indirizzo.
- **Spostamento di Token:** gli smart contract possono anche gestire il trasferimento di token ERC-20, che è uno standard comune per i token su Ethereum. Questo può includere funzioni per trasferire token da un indirizzo all’altro, o per consentire ad altri indirizzi di prelevare una certa quantità di token.
- **Interazione con il Front-End:** gli smart contract possono interagire con applicazioni front-end attraverso l’uso di librerie come Web3.js o Ethers.js. Queste librerie forniscono funzioni che consentono al codice front-end di inviare transazioni e leggere i dati dallo stato del contratto.
- **Login con il Wallet:** per interagire con uno smart contract, gli utenti devono prima “loggarsi” con il proprio wallet Ethereum. Questo di solito implica la selezione del wallet che l’utente desidera utilizzare (ad esempio, MetaMask), e poi la firma di una transazione o un messaggio per dimostrare che controllano l’indirizzo del wallet. Una volta che l’utente è loggato, il front-end può inviare transazioni allo smart contract in nome dell’utente.
- **Invio di Transazioni:** quando il front-end invia una transazione allo smart contract, include i dettagli di quale funzione vuole chiamare e quali argomenti vuole passare. Questa transazione viene poi firmata con la chiave privata dell’utente e inviata alla rete Ethereum.
- **Esecuzione dello Smart Contract:** quando la rete Ethereum riceve la transazione, esegue lo smart contract. Questo significa che esegue la funzione specificata nella transazione, aggiornando lo stato del contratto o trasferendo token come descritto nel codice del contratto.
- **Risposta al Front-End:** dopo che la transazione è stata confermata, i dettagli della transazione, compresi eventuali output dello smart contract, possono essere letti dal front-end. Questo permette al front-end di aggiornare l’interfaccia utente per riflettere i cambiamenti nello stato del contratto.

2.4

Software on-chain vs software off-chain

Informatica

• Medium

Nello sviluppo di applicazioni decentralizzate (dApps), il codice può essere scritto sia on-chain che off-chain. Questi termini si riferiscono a dove viene eseguito il codice e dove vengono memorizzati i dati.

On-Chain: Il codice on-chain è il **codice che viene eseguito sulla blockchain stessa**. Quando un’azione

viene eseguita in uno smart contract (come il trasferimento di token), quella azione è registrata in un blocco sulla blockchain, rendendola immutabile e verificabile pubblicamente. Questo è il cuore della programmabilità e della trasparenza della blockchain.

Tuttavia, eseguire il codice on-chain ha dei costi. Ogni operazione che viene eseguita sulla blockchain (come calcoli o modifiche allo stato) costa una certa quantità di “gas” in Ethereum. Il gas è un meccanismo che limita la quantità di lavoro che può essere eseguito in un blocco e serve a prevenire abusi come attacchi DDoS. Il costo del gas può diventare significativo, specialmente quando la rete è congestionata.

Off-Chain: Il codice off-chain è il **codice che viene eseguito al di fuori della blockchain**. Questo può includere il codice del server o del client in un'applicazione web, o può essere codice eseguito in una rete peer-to-peer separata. I dati generati o modificati dal codice off-chain non sono registrati sulla blockchain, il che significa che non sono soggetti ai costi del gas e possono essere eseguiti più rapidamente e in modo più scalabile.

Tuttavia, **il codice off-chain non ha le stesse garanzie di sicurezza e trasparenza del codice on-chain**.

Ad esempio, i dati off-chain possono essere modificati o falsificati senza che nessuno se ne accorga. Per questo motivo, è importante scegliere attentamente quali parti del codice eseguire off-chain.

Nello sviluppo di una dApp, è comune utilizzare una combinazione di codice on-chain e off-chain per ottenere il giusto equilibrio tra sicurezza, trasparenza, velocità e costo. Ad esempio, è sicuramente opportuno scegliere di eseguire le transazioni finanziarie e le operazioni critiche per la sicurezza on-chain, mentre le operazioni meno critiche e più intensive dal punto di vista computazionale in maniera off-chain.

Parametri	Software On-chain	Software Off-chain
Sicurezza	<i>Elevata: tutte le transazioni e le operazioni vengono eseguite direttamente sulla blockchain utilizzando criptografia avanzata per garantire l'integrità dei dati. La decentralizzazione della blockchain contribuisce a garantire la sicurezza e l'immutabilità dei dati</i>	<i>Variabile: la sicurezza dipende dalla soluzione adottata e dalle misure di sicurezza implementate sui server esterni</i>
Costi	<i>Elevati: lo sviluppo e l'esecuzione del software on-chain richiedono risorse hardware e software specifiche. Inoltre, l'utilizzo di digital assets per l'accesso alla blockchain può aumentare i costi</i>	<i>Bassi: lo sviluppo e l'esecuzione del software off-chain sono più economici rispetto al software on-chain. Inoltre, l'accesso alla soluzione può avvenire tramite applicazioni web o mobili senza l'utilizzo di digital assets</i>
Interazione utente	<i>Limitata: l'accesso alla blockchain richiede l'utilizzo di digital assets, rendendo l'interazione utente più limitata. Inoltre, il tempo di conferma delle transazioni può essere lungo</i>	<i>Elevata: l'accesso alla soluzione può avvenire tramite applicazioni web o mobili senza la necessità di digital assets. Inoltre, il tempo di conferma delle operazioni è più veloce rispetto al software on-chain</i>
Scalabilità	<i>Limitata: il carico di lavoro della blockchain è distribuito tra tutti i nodi della rete, il che può portare a problemi di scalabilità in caso di un aumento significativo del traffico</i>	<i>Elevata: il carico di lavoro del software off-chain può essere distribuito tra più server esterni, il che permette di gestire un elevato volume di traffico senza problemi di scalabilità</i>

In generale, il **software on-chain offre un livello di sicurezza elevato**, ma **può essere costoso in termini di transazioni**. L'interazione con la blockchain può essere limitata e la scalabilità può essere un problema. D'altra parte, il **software off-chain offre costi più bassi e una maggiore facilità di interazione utente, oltre che una scalabilità più elevata, ma a costo di una sicurezza minore**.

Non sempre l'utilizzo di una rete peer to peer è la scelta corretta per sviluppare la propria applicazione. Molte volte, la scelta di sviluppare una applicazione che segua logiche web2 può essere la scelta migliore per costo, complessità, interoperabilità e scalabilità del sistema.

2.5

Informatica

• Medium

Come viene inserito uno smart contract nella blockchain?

Per **inserire uno smart contract nella blockchain di Ethereum**, uno sviluppatore deve scrivere il codice del contratto utilizzando un linguaggio di programmazione supportato da Ethereum, come **Solidity** o **Vyper**.

Una volta scritto il codice, il contratto deve essere **compilato in bytecode** che può essere eseguito sulla macchina virtuale Ethereum.

Successivamente, il bytecode del contratto deve essere **caricato sulla blockchain di Ethereum** utilizzando uno strumento di distribuzione di contratti intelligenti come **Truffle**, **Remix**, o **Hardhat**.

Questi **strumenti consentono agli sviluppatori di creare, compilare, testare e distribuire contratti intelligenti sulla blockchain di Ethereum**.

In particolare, Truffle è un framework per lo sviluppo di contratti intelligenti e applicazioni decentralizzate, Remix è un IDE online per la scrittura, la compilazione e il debug di contratti intelligenti, mentre Hardhat è un ambiente di sviluppo locale per la creazione di applicazioni decentralizzate su Ethereum. Una volta caricato sulla blockchain di Ethereum, il contratto intelligente è **accessibile al pubblico e può essere eseguito da chiunque abbia l'accesso alla blockchain di Ethereum**.

Una volta che le informazioni vengono caricate sulla blockchain di Ethereum, diventano accessibili al pubblico e possono essere recuperate da chiunque abbia accesso alla blockchain. Il processo di salvataggio di informazioni sulla blockchain richiede l'esecuzione di transazioni.

Per salvare informazioni sulla blockchain, è necessario creare e inviare una transazione contenente i dati che si desidera memorizzare. Questa transazione deve essere inviata alla rete Ethereum e verificata dai partecipanti della rete, chiamati "nodi". I nodi validano la transazione, assicurandosi che sia conforme alle regole e alle politiche della blockchain. Una volta che la transazione viene accettata e confermata dai nodi, le informazioni vengono inclusi in un nuovo blocco e aggiunti alla catena di blocchi. Scrivere informazioni sulla blockchain di Ethereum comporta alcuni aspetti importanti. Innanzitutto, le informazioni sono immutabili, il che significa che non possono essere modificate o cancellate una volta che sono state confermate e aggiunte alla blockchain. Questo rende la blockchain un registro affidabile e sicuro per la conservazione di dati critici.

Inoltre, l'archiviazione di informazioni sulla blockchain di Ethereum comporta costi. Ogni transazione inviata richiede il pagamento di una commissione di gas, che rappresenta il costo computazionale necessario per l'esecuzione delle operazioni sulla rete Ethereum. Più complessa è l'operazione da eseguire e più gas viene richiesto. Pertanto, scrivere grandi quantità di dati sulla blockchain può comportare costi elevati.

D'altro canto, è importante notare che la blockchain di Ethereum offre anche la possibilità di archiviare informazioni pubbliche che possono essere recuperate senza richiedere transazioni o l'uso di un wallet. Questo significa che alcune informazioni possono essere accessibili liberamente a chiunque abbia accesso alla blockchain senza necessità di transazioni o di possedere un wallet.

2.6

Informatica

● Medium

Gli ambienti di test per gli sviluppatori

Prima di caricare lo smart contract all'interno di Ethereum, pagando delle commissioni in gas, la maggior parte degli sviluppatori utilizzano ambienti di test, per validare le logiche del loro contratto.

Gli ambienti di Testnet su Ethereum sono reti simili alla rete principale di Ethereum, ma utilizzano un digital asset fittizio chiamata “Ether di prova” anziché l'Ether reale. Alcuni esempi di Testnet sono Görli, Ropsten, Rinkeby e Kovan.

Questi ambienti sono **utili per gli sviluppatori e gli utenti per testare i loro contratti intelligenti** e le applicazioni decentralizzate su una rete simile a quella principale di Ethereum, senza dover utilizzare l'Ether reale (gas). In questo modo, gli sviluppatori possono identificare e risolvere i problemi di sicurezza e di funzionalità prima di pubblicare il loro codice sulla rete principale, evitando potenziali perdite di denaro o problemi per gli utenti.

Inoltre, gli ambienti di Testnet sono **utili anche per testare nuove funzionalità o aggiornamenti della rete Ethereum prima di implementarli sulla rete principale**, garantendo che tutto funzioni correttamente prima della messa in pratica effettiva.

2.7

Informatica

● Medium

Aggiornamento del network e modello di contabilità delle transazioni con smart contract

La differenza principale tra l'aggiornamento degli stati della blockchain di Ethereum e quella di Bitcoin è che **Ethereum utilizza la EVM** (Ethereum Virtual Machine). La EVM è progettata per essere un ambiente di esecuzione completamente isolato dal resto della rete, in modo che l'esecuzione del codice di un contratto non possa influire sul resto del sistema.

Ciò significa che **quando un contratto intelligente viene eseguito sulla rete Ethereum, la sua esecuzione viene gestita dalla EVM**. Quando una transazione viene inviata per eseguire una funzione all'interno del contratto, la EVM esegue il codice del contratto, che può includere la modifica dello stato del contratto stesso o l'invio di transazioni ad altri contratti.

Ogni volta che una funzione di un contratto viene eseguita, lo stato del contratto viene aggiornato, ma l'aggiornamento non diventa ufficiale fino a quando non viene incluso in un blocco valido. Ciò significa che **l'aggiornamento degli stati avviene solo quando viene effettivamente minato un blocco sulla blockchain, mentre i nodi della rete conservano solo la copia dell'ultimo stato della blockchain**.

Al contrario, **Bitcoin utilizza solamente un modello di contabilità utxo** (Unspent Transaction Outputs) per registrare gli stati delle transazioni. In questo modo, Bitcoin **non utilizza un ambiente di esecuzione isolato come la EVM di Ethereum**, ma piuttosto si basa sulle semplici transazioni che modificano gli utxo per determinare lo stato del sistema.

Questa è la differenza primaria rispetto all'architettura del blocco e di come vengono catalogate le informazioni nel registro distribuito di Ethereum e Bitcoin. Questo anche perché il design della rete è specifico per due purpose differenti.

2.8

La programmabilità sulla rete Bitcoin

Informatica

• Medium

Sfatiamo un mito: **anche su Bitcoin è possibile sfruttare dei contratti intelligenti** per automatizzare delle transazioni sulla rete. La complessità, tuttavia, è maggiore, e anche le funzionalità inferiori, rispetto al linguaggio turing complete di Ethereum, il che porta ad avere una community di sviluppatori più ridotta sulla rete Bitcoin.

Per scrivere un contratto intelligente su Bitcoin, è necessario conoscere il codice sorgente di Bitcoin e comprenderne il funzionamento a livello di basso livello. Inoltre, è necessario essere in grado di scrivere codice in linguaggi come il C++ o il Python per interagire con la blockchain di Bitcoin. In generale, lo **sviluppo di contratti intelligenti su Bitcoin è più complesso e tecnico rispetto allo sviluppo su Ethereum**. Un esempio di contratto intelligente su Bitcoin è **“Hash Time Lock Contract” (HTLC)**, che consente di creare un canale di pagamento a due vie in cui le transazioni devono essere autorizzate da entrambi i partecipanti prima che i fondi vengano trasferiti.

Oltre al “Hash Time Lock Contract”, ci sono altri esempi di contratti intelligenti su Bitcoin:

- **Multisig:** un contratto intelligente che **richiede più di una chiave per autorizzare una transazione**. Questo aumenta la sicurezza delle transazioni, poiché non basta avere una sola chiave per trasferire i fondi.
- **Escrow:** un contratto intelligente che **ti permette di tenere i fondi in attesa fino a quando non vengono soddisfatte determinate condizioni**. Questo è utile per le transazioni online in cui non si conosce la controparte o non si ha la certezza che la transazione verrà completata come previsto.

La differenza principale tra i contratti intelligenti su Bitcoin e quelli su Ethereum riguarda la capacità di programmazione. Ethereum ha un linguaggio di programmazione completo, chiamato Solidity, che ti consente di scrivere contratti intelligenti complessi e flessibili. Al contrario, Bitcoin ha una **capacità di programmazione molto più limitata e non esiste un modo per eseguire direttamente codice sul protocollo**. Ciò significa che i contratti intelligenti su Bitcoin possono soddisfare logiche meno elaborate e molto più semplici e limitate rispetto a quelli su Ethereum, ma rappresentano comunque un'importante area di sviluppo per la blockchain di Bitcoin.

3

Applicazioni decentralizzate (dApps)

- 3.1 Applicazioni Web3 vs Applicazioni Web2
- 3.2 Le applicazioni decentralizzate (dApps)
- 3.3 La finanza decentralizzata
- 3.4 Finanza centralizzata e finanza decentralizzata a confronto
- 3.5 Smart Contract e standardizzazione
- 3.6 Che relazione c'è tra digital asset e smart contract?
- 3.7 La programmabilità dei token

3.1

Applicazioni Web3 vs Applicazioni Web2

Informatica / Business

• Basic

Il Web3 rappresenta una nuova generazione di internet, che si basa sulla tecnologia blockchain e sull'idea di decentralizzazione. Rispetto al Web2, che ha visto la crescita di giganti centralizzati come Google, Facebook e Amazon, il **Web3 si presenta come un nuovo paradigma** in cui i dati e i servizi sono distribuiti e gestiti in modo decentrato, senza la necessità di intermediari centralizzati.

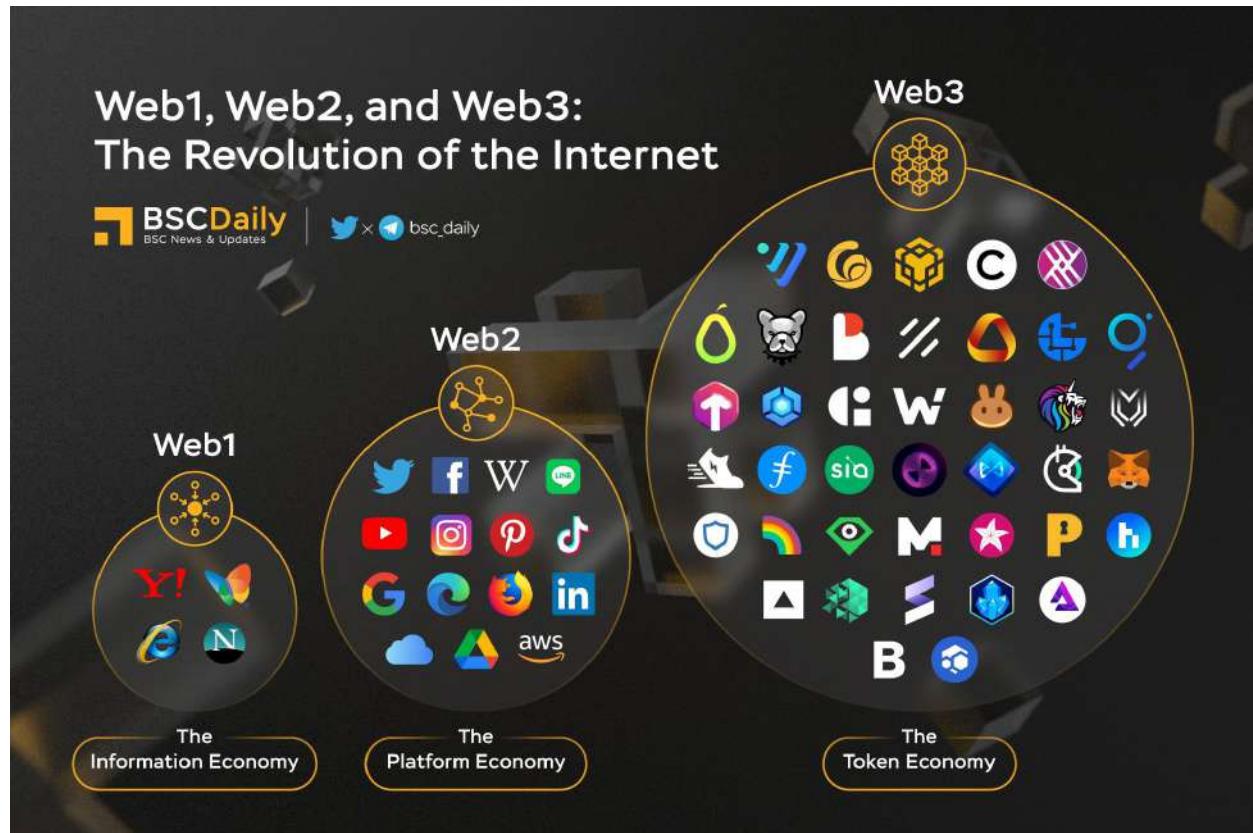
Durante gli anni 2000, la **diffusione dei GAFAM può essere attribuita ad una solida economia di rete all'interno delle piattaforme**, ad un continuo migliorarsi nella usabilità per utenti di qualsiasi età ed infine ad una forte scalabilità sociale delle applicazioni, standardizzando alcuni mercati come quello della ricerca online e dei social network.



GAFAM

Definizione: Acronimo utilizzato per indicare Google, Apple, Facebook, Amazon e Microsoft, ossia le più grosse ed influenti società nel settore tech.

Fonte: <https://www.collinsdictionary.com/it/submission/20994/GAFAM>



Per confrontare i servizi del Web3 e del Web2 rispetto all'economia di rete, all'usabilità e alla social scalability, abbiamo creato la seguente tabella:

Caratteristiche	Web 2.0	Web 3.0
Economia di rete	<i>La maggior parte dei servizi e delle applicazioni sono centralizzati, controllati da un'entità o da un'azienda, che gestisce l'accesso e la distribuzione dei dati.</i>	<i>L'economia di rete è decentralizzata e si basa sulla condivisione di risorse, dati e servizi tramite protocolli open-source e blockchain. Ciò significa che gli utenti possono partecipare direttamente alla rete, senza dover passare attraverso intermediari centralizzati.</i>
Usabilità	<i>L'usabilità del Web 2.0 è generalmente elevata, grazie alla semplicità e alla familiarità delle interfacce utente.</i>	<i>L'usabilità del Web 3.0 è inizialmente complessa, poiché richiede la conoscenza di protocolli decentralizzati e di digital assets. Tuttavia, gli sviluppatori stanno lavorando per creare interfacce utente più intuitive e semplici da usare per gli utenti meno esperti.</i>
Social scalability	<i>La social scalability del Web 2.0 è limitata dalla natura centralizzata delle applicazioni e dei servizi. Ciò significa che il numero di utenti che possono partecipare è limitato dalla capacità dell'azienda che controlla la piattaforma.</i>	<i>La social scalability del Web 3.0 è potenzialmente illimitata, poiché la rete è decentralizzata e basata sulla condivisione di risorse. Ciò significa che gli utenti possono partecipare direttamente alla rete e condividere risorse in modo aperto e trasparente. Inoltre, la tecnologia blockchain offre la possibilità di creare reti completamente autonome e decentralizzate, che possono essere gestite e utilizzate da chiunque abbia accesso a internet.</i>

La sfida del web3 è quella di prendersi del market share rispetto ai player dominanti, rispetto a servizi e prodotti online, costruiti sopra reti peer to peer. Tuttavia, sarà interessante se e come le aziende tradizionali del web2, vorranno entrare in questo nuova industria, adattando o modificando i loro business model.

3.2

Informatica / Business
● Basic

Le applicazioni decentralizzate (dApps)

Aziende, fondazioni e altre forme di organizzazioni hanno creato una vastissima gamma di applicazioni decentralizzate dal 2014 in avanti con l'avvento di Ethereum e di altre reti programmabili “competitor” come Binance Smart Chain, Polygon e altre.



Queste dApps sono caratterizzate dalla loro **trasparenza e sicurezza**. Differentemente dalla blockchain, non sono completamente immutabili poiché un update agli smart contract sulla rete di riferimento porterebbe al completo aggiornamento delle dApps stesse.

All'interno delle dApps, l'esecuzione del codice è deterministica, poiché le regole sono conservate nella blockchain. Il codice delle applicazioni è scritto e distribuito sulla rete, quindi il codice è legge (“code is law” è un mantra nell'ecosistema blockchain). Le dApps possono essere suddivise in diverse categorie, a seconda del loro utilizzo e dei servizi che forniscono. Ecco alcune delle categorie più comuni:

- **Finanza decentralizzata:** le dApps di finanza decentralizzata utilizzano la blockchain per **creare un mercato finanziario decentralizzato**, dove gli utenti possono prestare, prendere in prestito o scambiare digital assets in modo sicuro e trasparente.
- **Giochi ed Intrattenimento:** i giochi decentralizzati utilizzano la **blockchain per creare un mondo virtuale dove gli utenti possono giocare** e possedere token che rappresentano asset virtuali collezionabili (i.e. NFT).
- **Gestione della Identità:** le dApps per l'identità utilizzano la **blockchain per creare un sistema di identità decentralizzato** che fornisce agli utenti il controllo e la proprietà dei loro dati personali.
- **Decentralized cloud:** le dApps per il content management utilizzano la **blockchain per creare un sistema di archiviazione decentralizzato** che permette agli utenti di pubblicare e condividere file in modo sicuro e privato. Tra le applicazioni decentralizzate più diffuse, **IPFS**.
- **Sistemi di voto:** le dApps per il voto utilizzano la **blockchain per creare un sistema di voto decentralizzato** che fornisce agli utenti un modo sicuro e trasparente per esprimere la loro opinione.



IPFS

L'InterPlanetary File System (IPFS) è un protocollo di comunicazione e una rete peer-to-peer per l'archiviazione e la condivisione di dati in un file system distribuito. L'IPFS utilizza uno spazio di archiviazione associativo per identificare univocamente ogni file in uno spazio di nomi globale che connette tutti i dispositivi di calcolo.

Queste sono solo alcune delle categorie di dApps presenti nel mercato. Un elemento che le contraddistingue è l'uso di un nuovo token all'interno della logica del funzionamento, per premiare gli utenti e/o per far fruire quest'ultimi i propri servizi. L'industria sta continuando a evolversi e ad espandersi in nuovi settori, sarà infatti probabile che emergano nuove categorie di dApps nel futuro.

3.3

Informatica / Business

● Basic

La finanza decentralizzata

La finanza decentralizzata, o **DeFi**, è un nuovo modello di servizi finanziari basato sulla tecnologia **blockchain** e su reti peer-to-peer. A differenza del modello client-server tradizionale, che prevede un'interazione centralizzata tra il computer del cliente e il server di un'istituzione finanziaria, la DeFi permette agli utenti di interagire tra di loro direttamente attraverso smart contract su una blockchain pubblica. In questo modello, le **transazioni finanziarie** non sono gestite da una singola autorità centrale, ma vengono **validate e registrate sulla blockchain in modo distribuito, senza la necessità di intermediari**. Ciò permette di abbattere i costi e di aumentare la trasparenza e la sicurezza delle transazioni.

La DeFi comprende una **vasta gamma di servizi finanziari decentralizzati, come prestiti, scambi di digital assets, tokenizzazione di beni, assicurazioni, derivati e molto altro ancora**. Tutti questi servizi sono basati su smart contract, che stabiliscono le regole e le condizioni delle transazioni.

Esempi di mercati finanziari decentralizzati:

- **Decentralized Exchanges (DEXs)**: Sono una versione decentralizzata di un exchange centralizzato, dove gli **utenti possono scambiare token direttamente l'uno con l'altro senza la necessità di intermediari**.
- **Lending & Borrowing Platforms**: Piattaforme che consentono agli **utenti di prestare o richiedere prestiti utilizzando token digitali come garanzia**.
- **Stablecoins**: Monete digitali che **mantengono un valore stabile** rispetto ad un'altra valuta, ad esempio il dollaro statunitense.
- **Yield Farming**: Consiste nel **prestare o depositare token su piattaforme DeFi per generare interessi**.
- **Insurance Protocols**: Protocolli di **assicurazione decentralizzati** che forniscono copertura ai rischi associati agli investimenti in DeFi.

Alcuni esempi dei protocolli di finanza decentralizzata più popolari e utilizzati costruiti sopra Ethereum sono:

- **Uniswap**: un decentralized exchange automatizzato che utilizza gli smart contract per effettuare gli scambi.
- **Aave**: una piattaforma decentralizzata che consente agli utenti di prestare e di ricevere in prestito token digitali.

- **MakerDAO**: un sistema decentralizzato di prestito stabile che utilizza il DAI, una stablecoin legata al dollaro, come mezzo di prestito.
- **Compound**: una piattaforma di prestito decentralizzata che utilizza gli smart contract per automatizzare i tassi di interesse e la gestione delle posizioni di prestito.
- **Yearn Finance**: una piattaforma di yield farming che offre ai suoi utenti opportunità di investimento automatizzate per generare rendimenti elevati.

3.4

Informatica / Business

● Medium

Finanza centralizzata e finanza decentralizzata a confronto

Tra le innovazioni più interessanti all'interno dei servizi offerti dalla Finanza Decentralizzata, possiamo sicuramente menzionare ed approfondire il concetto di Decentralized Exchange (DEX). Iniziamo questo approfondimento partendo dalla distinzione tra CEX e DEX

- Una **Centralized Exchange (CEX)** è una **piattaforma di scambio di digital assets** che funziona come un intermediario centrale tra i suoi utenti. Ciò significa che la piattaforma controlla la maggior parte delle transazioni che avvengono su di essa, e che gli utenti devono depositare le loro valute in un portafoglio sulla piattaforma stessa. CEX sono i primi tipi di piattaforme di scambio di digital assets che sono state create e sono ancora molto popolari.
- Un Decentralized Exchange (DEX) è una piattaforma di scambio di digital assets che **non utilizza un intermediario centrale**. Invece di utilizzare un intermediario centrale, i **DEX utilizzano la blockchain per gestire le transazioni e garantire la sicurezza degli scambi**. Questo tipo di piattaforme di scambio è stato creato per fornire un'**alternativa più sicura e decentralizzata ai CEX**, e sta guadagnando sempre più popolarità.

Per elaborare ulteriormente, possiamo dire che CEX sono molto semplici da usare perché forniscono un'interfaccia utente intuitiva e gestiscono tutte le transazioni per conto degli utenti. Tuttavia, questo significa anche che gli utenti devono affidare la propria sicurezza ai CEX, il che comporta un rischio di sicurezza e di perdita di fondi. D'altra parte, i DEX forniscono un **livello di sicurezza maggiore** perché le transazioni sono gestite direttamente dalla blockchain e non c'è alcun intermediario centrale che controlla i fondi degli utenti. Tuttavia, i DEX possono essere **più complessi da utilizzare** e richiedono una certa conoscenza tecnica per essere utilizzati in modo efficiente.

Parametri	CeFi	DeFi
Controllo dei fondi	Centralizzato	Decentralizzato
Regolamentazione	Forte	Variabile
Compatibilità con la blockchain	Limitata	Totalità
Accessibilità finanziaria	Limitata	Aperta
Garanzie finanziarie	Forti	Variabili
Interesse degli investitori	Elevato	In crescita
Autonomia decisionale dell'utente	Bassa	Alta
Velocità di esecuzione	Elevata	Variabile

In sintesi, entrambi i tipi di piattaforme di scambio hanno i loro vantaggi e svantaggi, e la scelta dipenderà dalle preferenze individuali in termini di sicurezza, semplicità d'uso e altri fattori.

- **Sicurezza:** La sicurezza è un aspetto cruciale da considerare quando si parla di scambi crittografici. I CEX sono spesso visti come meno sicuri rispetto ai DEX poiché i fondi degli utenti sono conservati sui server centralizzati dell'exchange. Questo significa che i fondi sono a rischio di attacchi informatici o di furto da parte di criminali informatici. D'altra parte, i **DEX utilizzano la tecnologia blockchain per garantire che i fondi degli utenti siano conservati in modo sicuro in un portafoglio crittografico**. Tuttavia, poiché i **DEX sono più difficili da vigilare rispetto ai CEX, potrebbero esserci maggiori rischi di frodi o di problemi tecnici**.
- **Privacy:** La privacy è un altro aspetto importante da considerare quando si parla di scambi crittografici. I CEX richiedono spesso che gli utenti forniscano informazioni personali, come il nome, l'indirizzo e-mail e il numero di telefono, per verificare l'identità dell'utente. Queste informazioni possono essere condivise con le autorità o utilizzate per scopi pubblicitari, potenzialmente in violazione della normativa in materia di privacy. Al contrario, i **DEX sono spesso anonimi e non richiedono informazioni personali per creare un account**. Tuttavia, poiché i **DEX sono più difficili da vigilare**, potrebbero essere meno sicuri rispetto ai CEX.
- **Liquidità:** La liquidità è un fattore importante da considerare quando si parla di scambi crittografici poiché **influenza la facilità con cui è possibile scambiare valute crittografiche**. I CEX hanno solitamente una maggiore liquidità poiché sono più grandi e più popolari rispetto ai DEX. Ciò significa che gli utenti possono effettuare scambi più rapidamente e a prezzi più competitivi. Tuttavia, i DEX stanno diventando sempre più popolari e stanno aumentando la loro liquidità, offrendo un'alternativa più decentralizzata ai CEX.

Con l'incremento del mercato e della adozione delle digital assets, la finanza decentralizzata potrà essere di beneficio per gli utenti e per coloro che vi **partecipano a livello globale in diversi modi come:**

- **Accessibilità:** la finanza decentralizzata è accessibile a chiunque abbia accesso a Internet e una conoscenza minima della tecnologia blockchain, indipendentemente dalla loro ubicazione geografica o status finanziario.
- **Sicurezza:** la natura decentralizzata della finanza decentralizzata rende i fondi degli utenti più sicuri, poiché non dipendono da un singolo intermediario che potrebbe essere vulnerabile a furti o attacchi informatici.
- **Trasparenza:** tutte le transazioni e i contratti sono registrati immutabilmente sulla blockchain, rendendo trasparente il funzionamento dei servizi DeFi.
- **Neutralità:** poiché la finanza decentralizzata non dipende da intermediari centralizzati, non esiste alcun bias o preferenze verso determinati utenti o gruppi.
- **Flessibilità:** la finanza decentralizzata offre una maggiore flessibilità rispetto alla finanza tradizionale, poiché gli utenti hanno il pieno controllo sulle loro attività finanziarie e possono effettuare transazioni 24/7 senza il bisogno di intermediari.
- **Innovazione:** la finanza decentralizzata sta spingendo i limiti delle attuali capacità finanziarie e sta aprendo la strada a nuove opportunità e soluzioni innovative.

Ad oggi, tuttavia, vi sono ancora delle **limitazioni** in quanto:

- Vi è ancora una **parziale regolamentazione e standardizzazione** a livello globale
- La **volatilità dei prezzi dei token digitali** può rendere difficile la valutazione delle attività in maniera completamente decentralizzata
- La **natura decentralizzata rende difficile la risoluzione dei problemi** e la gestione delle dispute tra due attori dentro il DEX
- La **complessità tecnica** può rendere difficile per molti utenti comprendere e utilizzare i servizi DeFi

3.5

Informatica

• Medium

Smart Contract e standardizzazione

Il futuro della finanza decentralizzata è ancora incerto, ma ci sono molte opportunità di crescita e sviluppo. Per facilitare la standardizzazione tra le applicazioni decentralizzate e per aumentare la sicurezza degli smart contract all'interno della rete, la community ha proposto di seguire alcune **linee guida per lo sviluppo di applicazioni decentralizzate definite come Ethereum Request for Comments (ERC).** Queste proposte vengono analizzate dalla community, implementate dentro il codice sorgente, diventando poi dei modelli che aiutato gli sviluppatori a creare soluzioni decentralizzate compatibili l'una con l'altra.

Titolo dell'ERC	Autore
ERC-20	Fabian Vogelsteller
ERC-721	William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs
ERC-1155	Philippe Castonguay
ERC-777	Jordi Baylina, Jacques Dafflon, Thomas Shababi, Thomas Bertani
ERC-1337	Joshua Mir
ERC-1400	Thomas Euler, Pablo Ruiz, Fabian Vogelsteller
ERC-223	Dexaran
ERC-2981	William Entriken, David Rugendyke, Shane Fontaine
ERC-3000	Fabian Vogelsteller

Ecco qui alcuni standard di ERC che si possono trovare all'interno di questo sito (<https://eips.ethereum.org/erc>). Tra gli standard più utilizzati all'interno di Ethereum vi sono lo ERC20 e lo ERC721, utilizzati per creare sopra nuovi digital assets e/o token, scambiati e custodibili all'interno del proprio wallet. Prima di divenire ERC, queste proposte devono essere approvate con votazione da parte della rete (come avviene sulla rete di Bitcoin) e vengono definite EIP, Ethereum Improvements Proposals (BIP nel caso di Bitcoin, Bitcoin Improvements Proposals).

3.6

Informatica

• Basic

Che relazione c'è tra digital asset e smart contract?

Per creare i token sopra le reti peer to peer, gli sviluppatori hanno deciso di realizzare degli standard per facilitare la diffusione e la semplicità di utilizzo. **Gli standard ERC20 e ERC721 sono i due smart contract maggiormente utilizzati per creare nuovi token sopra Ethereum.** Possiamo dunque comprendere che gli smart contract sono gli strumenti utilizzati per creare e programmare un token e/o un digital asset. **I token sono una rappresentazione digitale di un valore, di uno strumento di pagamento o di un as-**

set, utilizzati nelle applicazioni decentralizzate per rappresentare una varietà di attività finanziarie, di diritti di proprietà, di accesso e molto altro ancora. Gli smart contract ERC20 e ERC721 sono spesso associati ad altri smart contract, che gestiscono altre logiche per gli utenti che utilizzano una applicazione web3.

- **ERC20** è uno standard di token fungibile, ovvero **ogni unità di un token è uguale a tutte le altre unità di quel token**. Solitamente, questo standard viene utilizzato per generare grandi quantità di token. Gli esempi di token ERC20 includono i digital assets come ETH, DAI e USDT. Spesso utilizzato dentro una applicazione decentralizzata come moneta del sistema, definito come utility.
- **ERC721**, d'altra parte, è uno standard di token non fungibile, ovvero **ogni unità di un token è unica e ha un valore specifico**. Solitamente, questo standard viene utilizzato per generare un singolo token alla volta. Gli esempi di token ERC721 includono token di gioco, come CryptoKitties, dove ogni token rappresenta un gatto unico con caratteristiche uniche. Spesso utilizzato per fare associazione univoca tra un oggetto digitale e/o fisico e il token.

Questi esempi ci permettono di comprendere **cos'è un token sulla blockchain di Ethereum e come può essere programmato per ogni condizione e per ogni scenario**. Infatti, uno sviluppatore può costruire il design di un token avendo la possibilità di decidere:

- A chi farlo utilizzare
- Per quali condizioni può essere utilizzato
- La tipologia di pagamento ed applicare politiche e condizionalità durante il trasferimento
- Automatizzare un pagamento in base alle regole e gli input deterministici, come l'accesso ad una risorsa
- Se cancellarlo, bloccarlo e bruciarlo
- La quantità e la distribuzione iniziale del token all'interno della community o network di riferimento

La scelta se utilizzate una rete come Ethereum, una competitor e/o rimanere su un modello client/server, stile punti fragola o crediti di piattaforma dentro i video-game è da analizzare nel dettaglio. L'utilizzo di questi token comporta un costo e una serie di complessità che i modelli centralizzati risolvono più facilmente.

In sintesi, i **token sono un nuovo strumento all'interno delle dApps che consentono agli utenti di partecipare alla governance della stessa, effettuare pagamenti digitali e generare revenue per i creatori della dApp stessa**. Inoltre, con l'infrastruttura di Ethereum possibile dare programmabilità alla moneta e far gestire in maniera self e distribuita agli utenti i propri crediti/diritti, in maniera differente dai modelli client server di applicazioni all'interno del web2.

3.7

Informatica

● Medium

La programmabilità dei token

Entrambi gli standard di token ERC20 e ERC721 utilizzano smart contract per definire le regole e le funzionalità del token. Ad esempio, **uno smart contract può definire il numero totale di token creati, la quantità massima di token che un utente può detenere, le regole per le transazioni di token e altro ancora**. In questo modo, gli smart contract garantiscono che i token siano utilizzati in modo sicuro e affidabile sulla blockchain.

```

1 // -----
2 // ERC Token Standard #20 Interface
3 // https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
4 // -----
5 contract ERC20Interface {
6     function totalSupply() public constant returns (uint);
7     function balanceOf(address tokenOwner) public constant returns (uint balance);
8     function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
9     function transfer(address to, uint tokens) public returns (bool success);
10    function approve(address spender, uint tokens) public returns (bool success);
11    function transferFrom(address from, address to, uint tokens) public returns (bool success);
12
13    event Transfer(address indexed from, address indexed to, uint tokens);
14    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
15 }

```

La programmabilità di un token è la **capacità di definire le regole e le funzionalità specifiche del token attraverso il codice**, che viene eseguito sulla blockchain in cui il token è emesso. Questo consente di creare token personalizzati con funzionalità uniche e specifiche, oltre ai tradizionali scambi e trasferimenti.

Questa interfaccia definisce un insieme di funzioni che un token ERC20 deve implementare. Ecco una descrizione di ciascuna funzione:

- **totalSupply()**: questa funzione restituisce il numero totale di token in circolazione. È una funzione di sola lettura, il che significa che non modifica lo stato del contratto.
- **balanceOf(address tokenOwner)**: funzione che restituisce il saldo di token dell'indirizzo specificato. Come totalSupply(), è una funzione di sola lettura.
- **allowance(address tokenOwner, address spender)**: questa funzione indica il numero di token che lo "spender" è autorizzato a prelevare dall'account del "tokenOwner". Questo è utile per situazioni in cui si desidera permettere ad un altro account di spendere token per conto altri.
- **transfer(address to, uint tokens)**: funzione che trasferisce un numero specifico di token dall'account che chiama la funzione all'indirizzo specificato. Restituisce un booleano per indicare se il trasferimento è stato eseguito con successo.
- **approve(address spender, uint tokens)**: questa funzione consente allo "spender" di prelevare un numero specifico di token dall'account che chiama la funzione. Restituisce un booleano per indicare se l'approvazione è stata eseguita con successo.
- **transferFrom(address from, address to, uint tokens)**: questa funzione consente ad uno "spender" autorizzato di trasferire un numero specifico di token da un account all'altro. Restituisce un booleano per indicare se il trasferimento è stato eseguito con successo.

Inoltre, l'interfaccia ERC20 definisce due eventi:

- **Transfer(address indexed from, address indexed to, uint tokens)**: questo evento viene invocato quando i token sono trasferiti. Include gli indirizzi del mittente e del destinatario, e il numero di token trasferiti.
- **Approval(address indexed tokenOwner, address indexed spender, uint tokens)**: evento che viene invocato quando vi è l'approvazione di un prelievo di token. Include l'indirizzo del proprietario dei token, l'indirizzo dello spender e il numero di token approvati.

Queste funzioni ed eventi costituiscono l'interfaccia standard ERC20, che è ampiamente utilizzata per la creazione di token su Ethereum.

Esistono anche altre funzioni che permettono altre logiche dei token. Ad esempio, l'implementazione di una funzionalità **Soulbound** in un token può **vincolare i token di un determinato account in modo che non possano essere trasferiti a nessun altro**, garantendo la sicurezza dei fondi e impedendo eventuali frodi o attacchi. Al contrario, la funzionalità di **Burn** consente di ridurre il numero di token in circolazione, eliminandoli in modo permanente dal sistema.

Inoltre, la programmabilità di un token consente di **implementare regole specifiche per l'uso del token**, come limitazioni sull'utilizzo o la quantità di token che possono essere spesi in un determinato periodo di tempo.

4

dApps e tokenomics

- 4.1 Cos'è la tokenomics e come fanno profitto le applicazioni decentralizzate?
- 4.2 L'uso degli ERC20 nelle dApps
- 4.3 Approfondimento sulla tokenomics: modello deflattivo o inflattivo (ERC20)
- 4.4 Tokenomics e la teoria dei giochi
- 4.5 Tokenomics e la teoria dei giochi: il modello tragedy of commons scenario
- 4.6 Tokenomics con i token non fungibili (ERC721)

4.1

Informatica / Business

● Basic

Cos'è la tokenomics e come fanno profitto le applicazioni decentralizzate?

Prima che una dApp venga lanciato nel mercato web3 sopra rete programmabile, il team di sviluppo deve creare un design di incentivi all'interno della applicazione, tale per cui vi sia una situazione di win-win game per tutti gli attori che compreranno il token e che lo utilizzeranno all'interno della applicazione. Questo concetto si definisce come "disegno di una tokenomics".

Il concetto di **tokenomics** si riferisce alla **creazione e gestione di token all'interno di un ecosistema decentralizzato, in particolare delle applicazioni decentralizzate (dApp)**. Si tratta di un nuovo modello di business e di revenue model per le dApp, che permette di creare un ecosistema virtuoso, dove gli utenti sono incentivati a partecipare e contribuire alla crescita del progetto.

In pratica, la **tokenomics mira a creare un sistema di incentivi per gli utenti**, dove i token sono utilizzati come mezzo di scambio all'interno della piattaforma e come strumento per la partecipazione e la governance della stessa. I token possono essere utilizzati per accedere a servizi premium, per votare sulle decisioni del progetto, per ottenere diritti di proprietà, per partecipare a programmi di incentivazione, e così via.

Il **whitepaper di una dApp spiega in dettaglio la sua tokenomics, cioè come i token sono emessi, distribuiti, utilizzati e valorizzati all'interno del progetto**.

ECCO UNA POSSIBILE STRUTTURA DI UN WHITE PAPER, precisando che non ci si riferisce in questo caso al "white paper", inteso quale documento informativo richiesto dalla normativa MiCAR:

I. Introduzione

- Descrizione generale del progetto e degli obiettivi del white paper
- Contesto del progetto e breve storia della rete programmabile scelta (per esempio Ethereum)

II. Descrizione del problema

- Descrizione del problema o della necessità che la dApp vuole risolvere o soddisfare
- Descrizione dei limiti delle soluzioni attuali

III. Descrizione della soluzione

- Descrizione della soluzione proposta e come la dApp risolve il problema
- Descrizione delle funzionalità principali della dApp

IV. Descrizione tecnica

- Descrizione delle tecnologie utilizzate nella creazione della dApp
- Descrizione di come la dApp utilizza gli smart contract per gestire le transazioni e le interazioni sulla blockchain di Ethereum
- Descrizione delle specifiche di ERC20 e/o ERC721 e come vengono utilizzate nella dApp

V. Tokenomics

- Descrizione dei token emessi e come vengono utilizzati nella dApp
- Distribuzione iniziale dei token nel network e nel team
- Attività di **airdrop** pre lancio
- Soft Cap e Hard Cap per raggiungere gli obiettivi del progetto
- Prezzo in FIAT o ETH del token al momento del lancio
- Descrizione della roadmap e dei piani futuri per il progetto

VI. Team e partnership

- Descrizione del team di sviluppo e delle partnership attuali o future

VII. Conclusioni

- Riassunto delle principali idee presentate nel white paper
- Invito alla partecipazione e alla collaborazione

VIII. Bibliografia

- Riferimenti utilizzati per la creazione del white paper.



Airdrop

Un airdrop è la distribuzione di un token, in maniera gratuita, a diversi indirizzi (o address) di utenti. In un ecosistema affollato come quello dei digital assets, regalare asset gratuiti è uno dei modi migliori per farsi notare.

Infine, per far sì che un token ERC20 o ERC721, possa essere facilmente scambiato tra gli shareholders del progetto, quest'ultimo viene listato sopra il mercato dei digital assets. Quest'ultimo può essere all'interno di piattaforme centralizzata, come gli exchange, o all'interno di servizi di finanza decentralizzata come i DEX. Il lancio a mercato di token viene definito come Initial Coin Offering o Initial Token Offering. Per concludere, dopo avere creato un token, un'azienda è solita “listare” i proprio token in altri mercati, fornendo a quest'ultimo il suo valore tramite l'incrocio tra domanda ed offerta.

4.2

Informatica / Business

● Basic

L'uso degli ERC20 nelle dApps

Le dApps (Decentralized Applications) utilizzano i token ERC20 soprattutto come **strumenti di partecipazione, utilizzo e revenue in diverse modalità**. Una volta che questi token vengono creati (i.e. mintati), questi possono essere utilizzati come:

1. **Mezzi di pagamento** all'interno di una dApp per l'acquisto di servizi o prodotti. In questo caso, i token fungono da valuta digitale e possono essere scambiati tra gli utenti della DApp.
2. **Strumenti di governance** all'interno di una DApp. Gli utenti possono utilizzare i token per partecipare alle decisioni di governance, ad esempio per votare su proposte di cambiamento della dApp o per eleggere i membri del consiglio di amministrazione.
3. **Strumenti di revenue** per i creatori di una DApp. I creatori possono emettere i token iniziali e trattenere una quota di essi come incentivo per il loro lavoro di sviluppo. Inoltre, i creatori possono guadagnare entrate dalle transazioni all'interno della dApp che richiedono l'utilizzo dei token.

L'ICO di EOS è iniziata nel giugno 2017 e si è conclusa nel giugno 2018, con la raccolta di quasi 4 miliardi di dollari, che la rende l'ICO di maggior successo di sempre fino ad oggi. Il token ERC-20 di EOS è stato poi convertito nel token nativo di EOS quando il progetto è stato lanciato sulla sua piattaforma di blockchain mainnet.

Fonte

- ▶ <https://it.cointelegraph.com/news/eos-about-to-secure-a-record-4-bln-in-year-long-ico>

4.3

Teoria dei giochi

● Medium

Approfondimento sulla tokenomics: modello deflattivo o inflattivo (ERC20)

La tokenomics è lo studio del **valore economico generato dai digital assets**, analizzando gli aspetti economici e finanziari di un progetto blockchain. La tokenomics si concentra sulla **creazione di un modello di incentivazione per i partecipanti del sistema**, che spesso prevede l'emissione di un digital asset o di un token. In questo senso, la tokenomics può essere vista come una combinazione di teoria economica, matematica, finanza e tecnologia.

Uno dei concetti chiave della tokenomics è il **modello di supply**, ovvero il **modo in cui i token vengono emessi e distribuiti nel tempo**. In genere, ci sono due tipologie di modelli di supply:

- il **modello inflationary** - la quantità di token in circolazione aumenta nel tempo;
- il **modello deflationary** - la quantità di token in circolazione diminuisce nel tempo.

Il modello di tokenomics di Bitcoin può essere considerato deflationary. Ciò significa che la quantità di Bitcoin in circolazione diminuisce nel tempo, poiché la quantità massima di Bitcoin che possono essere estratti è limitata a 21 milioni. Infatti, il tasso di inflazione annuale diminuisce continuamente e raggiungerà lo zero quando verranno estratti tutti i Bitcoin. Questo rende **Bitcoin un bene deflazionario**. Un ulteriore esempio di modello di supply deflationary è quello di token come Binance Coin (BNB) o Maker (MKR), dove i token vengono bruciati ad ogni transazione, riducendo quindi la quantità di token in circolazione nel tempo.

Un esempio di token con **supply inflazionaria** è il token XRP emesso dalla società Ripple. Il token XRP ha una fornitura massima di 100 miliardi, ma a differenza di molte altre digital assets, la fornitura in circolazione aumenta gradualmente ogni anno, a una velocità del 1% della fornitura totale. Ciò significa che la supply di XRP aumenta di circa 1 miliardo di token ogni anno.

Un altro concetto chiave della tokenomics è la **teoria dei giochi**, che viene utilizzata per analizzare l'**e-quilibrio tra i partecipanti del sistema**. Un esempio di gioco utilizzato in tokenomics è quello del “Tragedy of the Commons”, dove c’è un bene comune (come l’ambiente o il network) che tutti i partecipanti del sistema possono utilizzare. Tuttavia, se ciascun partecipante cerca di massimizzare il proprio profitto, il bene comune potrebbe essere distrutto. In questo senso, la tokenomics cerca di creare incentivi per i partecipanti a collaborare e mantenere il bene comune.

I **giochi dinamici** sono un altro concetto importante nella tokenomics, e si riferiscono al **modo in cui i partecipanti del sistema si adattano alle variazioni dei prezzi e delle quantità di token in circolazione**.

Un esempio di gioco dinamico è quello del “stagflation”, dove il valore dei token diminuisce mentre la quantità di token in circolazione aumenta. In questo caso, i partecipanti potrebbero decidere di vendere i loro token, ma questo potrebbe ulteriormente abbassare il prezzo dei token. Tuttavia, se tutti i partecipanti decidono di vendere, il prezzo dei token potrebbe crollare drasticamente.

In sintesi, la tokenomics si occupa di creare un ecosistema economico sostenibile per i partecipanti del sistema, utilizzando modelli di supply, teoria dei giochi e giochi dinamici.

4.4

Teoria dei giochi

● Hard

Tokenomics e la teoria dei giochi

In termini di tokenomics, i **modelli deflationary e inflationary si riferiscono alla gestione dell'offerta di un digital asset o di un token, e come questa può influire sul valore e sulla liquidità di tale asset.**

Un **modello deflationary prevede che l'offerta di token diminuisca nel tempo**, spesso attraverso un meccanismo di bruciatura (anche noto come “burn”) di token o una supply che tende a diminuire nel tempo fino ad arrivare a 0. Questo significa che la quantità di token in circolazione diminuisce, ma la domanda può rimanere costante o addirittura aumentare, il che porta ad un aumento del valore del token. In questo modello, l'offerta limitata di token è il fattore principale che supporta il valore dell'asset. D'altra parte, un **modello inflationary prevede che l'offerta di token aumenti nel tempo**, spesso attraverso la distribuzione di nuovi token ai partecipanti del network come ricompensa per la partecipazione o il mining. Questo può aumentare la liquidità del token, ma se la domanda non aumenta in proporzione all'offerta, il valore del token può diminuire. In questo modello, la domanda di token è il fattore principale che supporta il valore dell'asset.

In termini matematici, il modello deflationary può essere rappresentato dall'equazione:

$$V = M/Q$$

Mentre, il modello inflationary può essere rappresentato dall'equazione:

$$V = M \times V/Q$$

Dove

- **V rappresenta la velocità di circolazione della moneta**, ovvero il numero di volte in cui una determinata unità di moneta viene utilizzata in un certo periodo di tempo.
- **M rappresenta la quantità di moneta in circolazione.**
- **Q rappresenta la quantità di beni e servizi prodotti nell'economia durante lo stesso periodo di tempo.**

Alcuni modelli utili per analizzare una tokenomics:

- Modello di Fisher: il modello di Fisher prevede una relazione diretta tra il tasso di inflazione e il tasso di interesse nominale.
- Modello di Black-Scholes: il modello di Black-Scholes è utilizzato per valutare le opzioni finanziarie.
- Modello di Regressione: il modello di regressione può essere utilizzato per analizzare la relazione tra la quantità di token in circolazione ed il prezzo di mercato.
- Modello di Sopraffazione: il modello di sopraffazione prevede che il prezzo di un bene aumenti in modo esponenziale man mano che la domanda supera l'offerta.
- Modello di Crescita Logistica: il modello di crescita logistica prevede una crescita iniziale esponenziale seguita da una crescita più lenta, ma ancora sostenuta.
- Analisi del mercato: la valutazione della tokenomics può essere effettuata attraverso l'analisi del mercato e la valutazione delle dinamiche di offerta e domanda.
- Modelli di domanda e offerta: i modelli di domanda e offerta possono essere utilizzati per valutare le variazioni dei prezzi e dei volumi delle transazioni.
- Analisi di rete: l'analisi di rete può essere utilizzata per valutare la tokenomics di un digital asset attraverso l'analisi delle transazioni e dei nodi di rete.
- Modelli di previsione dei prezzi: i modelli di previsione dei prezzi possono essere utilizzati per valutare le tendenze di prezzo e la volatilità dei digital assets. Ad esempio, è possibile utilizzare i modelli ARIMA o le reti neurali per effettuare previsioni sui prezzi futuri dei digital assets.
- Analisi di correlazione: l'analisi di correlazione può essere utilizzata per valutare le relazioni tra i digital assets e altri asset.
- Modelli di equilibrio dei giochi: i modelli di equilibrio dei giochi possono essere utilizzati per valutare le dinamiche di mercato dei digital assets.

4.5

Teoria dei giochi

• Basic

Tokenomics e la teoria dei giochi: il modello tragedy of commons scenario

Il “Tragedy of the Commons” è un concetto che si riferisce ad una **situazione in cui molte persone utilizzano in comune una risorsa limitata**, come ad esempio un prato pubblico, **senza preoccuparsi del fatto che il loro comportamento possa danneggiare la risorsa stessa**.

Nel contesto della tokenomics, il Tragedy of the Commons si può **manifestare quando i titolari di un particolare digital asset sono incentivati a vendere o a scambiare le loro monete in modo aggressivo**, senza considerare gli effetti di questo comportamento sul valore della moneta stessa.

In altre parole, se molti titolari di un digital asset decidono di vendere le loro monete allo stesso tempo, il prezzo dei digital assets può diminuire rapidamente, causando un crollo del valore della moneta e danneggiando tutti i titolari.

Per prevenire questo tipo di scenario, molti progetti di tokenomics includono meccanismi per **ridurre gli incentivi per i titolari di vendere in modo aggressivo le loro monete**, come ad esempio l’implementazione di una periodica bruciatura di token (token burning), dei vesting period in cui il token non può essere trasferito e/o altri meccanismi per incentivare i titolari a mantenere le loro monete invece di venderle. **Questi meccanismi possono contribuire ad alleviare il Tragedy of the Commons e a mantenere il valore dei digital assets stabile**.

4.6

Informatica / Business

• Basic

Tokenomics con i token non fungibili (ERC721)

Nel contesto dei token non fungibili (NFT), la **tokenomics si riferisce all’analisi e alla progettazione delle strategie economiche che influenzano il valore e la liquidità dei NFT**.

Il **prezzo minimo** (price floor) di un NFT è una delle **principali componenti** della tokenomics. Il prezzo minimo rappresenta il **prezzo più basso a cui un NFT può essere acquistato e può essere determinato da una serie di fattori**, tra cui l’offerta e la domanda, la rarità, la qualità e l’esclusività dell’opera d’arte digitale. Le piattaforme NFT, come ad esempio OpenSea, spesso consentono agli utenti di impostare un prezzo minimo per le loro opere d’arte digitali.

La **quantità di NFT in circolazione è un altro fattore che influenza la tokenomics**. In generale, un numero limitato di NFT può aumentare il loro valore e la loro rarità, ma può anche limitare la liquidità e la disponibilità degli NFT. Al contrario, una grande quantità di NFT può aumentare la disponibilità e la liquidità degli NFT, ma può anche ridurre il loro valore.

La **tipologia di NFT può anche influenzare la tokenomics**. Ad esempio, gli NFT che rappresentano **opere d’arte digitali uniche possono avere un valore più elevato rispetto a quelli che rappresentano elementi di gioco o collezionabili digitali**. Inoltre, le opere d’arte digitali di artisti famosi o di grande valore possono aumentare il valore degli NFT associati.

Inoltre, nella tabella a seguito riportata è stata creata una divisione degli NFT in 5 categorie, ciascuna delle quali applicabile a diversi business model:

Tipologia di NFT	Descrizione
Statico	Gli NFT statici sono semplici rappresentazioni digitali di un'opera d'arte o di un oggetto virtuale. Questi NFT non cambiano mai e non hanno funzionalità aggiuntive.
Dinamico	Gli NFT dinamici contengono dati aggiuntivi che cambiano nel tempo. Questi NFT possono essere utilizzati per rappresentare oggetti virtuali che possono essere utilizzati in giochi online o per rappresentare le prestazioni di un artista o di un musicista in un determinato momento.
Con royalties	Gli NFT con royalties permettono all'artista o al creatore di ricevere una percentuale delle transazioni successive che coinvolgono il loro NFT. In questo modo, l'artista o il creatore continua a guadagnare dalla loro opera d'arte o dall'oggetto virtuale anche dopo la vendita iniziale.
Senza royalties	Gli NFT senza royalties non offrono alcuna percentuale di royalties all'artista o al creatore. Questi NFT possono essere utilizzati in casi in cui l'artista o il creatore non desidera ricevere alcuna percentuale delle transazioni future.
Frazionario	Gli NFT frazionati sono divisi in parti più piccole che possono essere vendute separatamente. In questo modo, più persone possono possedere una parte dell'opera d'arte o dell'oggetto virtuale e possono beneficiare delle transazioni future che coinvolgono quel NFT.

L'applicazione decentralizzata **che supporta gli NFT può anch'essa avere un impatto significativo sul design della tokenomics**. Infine, anche la **governance della piattaforma può influire sulla regolamentazione degli NFT e sui loro prezzi**.

5

NFT

- 5.1 Il fenomeno NFT nel pop market
- 5.2 I mercati di riferimento degli NFT
- 5.3 Il ruolo della community nei progetti NFT
- 5.4 Social tiering ed esclusività con gli NFT
- 5.5 Come si gestiscono i token non fungibili dentro un wallet?
- 5.6 Token non fungibili per accedere a servizi esclusivi: il caso Spotify
- 5.7 Single Sign-On (SSO) con NFT nel Web2 e nel Web3
- 5.8 I metadati dentro gli NFT

5.1

Business

Basic

Il fenomeno NFT nella cultura pop

Negli ultimi anni, gli NFT (Non-Fungible Token) sono diventati una vera e propria tendenza nel mondo della cultura pop. Gli NFT sono stati **utilizzati da artisti, celebrità e influencer per creare e vendere oggetti digitali unici**, come immagini, video, musica e molto altro ancora.

Uno dei primi esempi di successo nel mondo degli NFT è rappresentato dalle **CryptoPunks**, una collezione di 10.000 immagini pixelate di personaggi unici, che sono stati venduti attraverso un'asta online. Successivamente, altre collezioni di NFT hanno fatto la loro comparsa sul mercato, tra cui i **Bored Ape Yacht Club**, i **Pudgy Penguins** e molti altri.

Oltre agli artisti, anche i **musicisti hanno iniziato ad abbracciare il mondo NFT**, creando collezioni di oggetti digitali unici. Ad esempio, il rapper americano Post Malone ha creato una collezione di NFT chiamata "Posty Drops", che includeva oggetti digitali ispirati alle sue canzoni. Anche altri artisti come Deadmau5, Grimes e Kings of Leon hanno creato collezioni di NFT.

Gli NFT (Non-Fungible Tokens) sono rappresentazioni digitali di beni unici e irripetibili, che utilizzano la tecnologia blockchain per garantire l'autenticità e la proprietà degli stessi. Gli **NFT hanno rivoluzionato il mondo dell'arte, della musica e dell'intrattenimento**, offrendo un modo completamente nuovo per creare, condividere e scambiare opere d'arte e beni digitali.

Il codice in Solidity degli ERC721 è relativamente semplice e si concentra principalmente sulla definizione degli attributi del token, come l'identificativo unico, il proprietario, il prezzo e il metadata del token, come foto, video o musica.

5.2

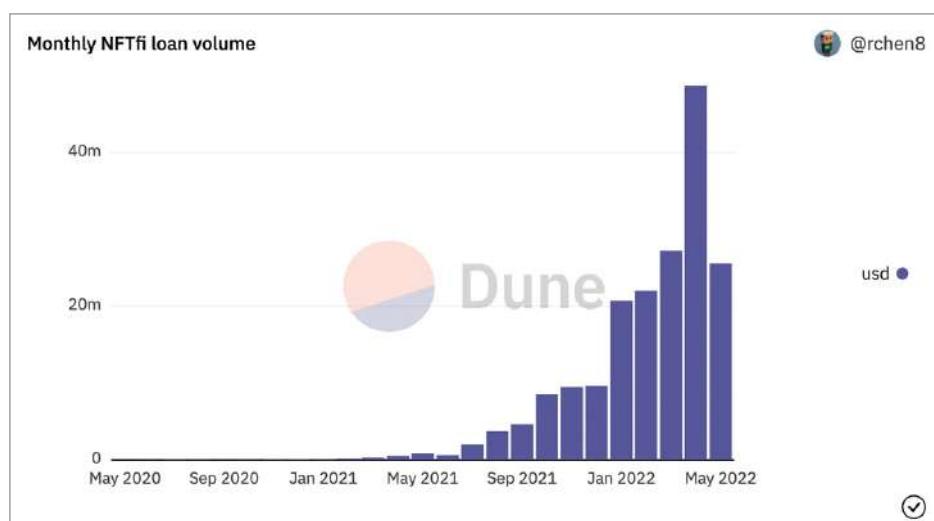
Business

Basic

I mercati di riferimento degli NFT

Il **mercato degli NFT ha avuto una crescita esplosiva negli ultimi anni**, con volumi di transazioni che hanno raggiunto cifre impressionanti. Secondo il sito di monitoraggio dei digital assets CoinMarketCap, il volume totale delle transazioni NFT è aumentato in modo significativo a partire dal 2020, raggiungendo un picco di oltre 4 miliardi di dollari nel mese di maggio 2021.

Dal grafico a fianco è inoltre possibile vedere la forte crescita nel 2022 con riferimento all'NFT lending ecosystem.



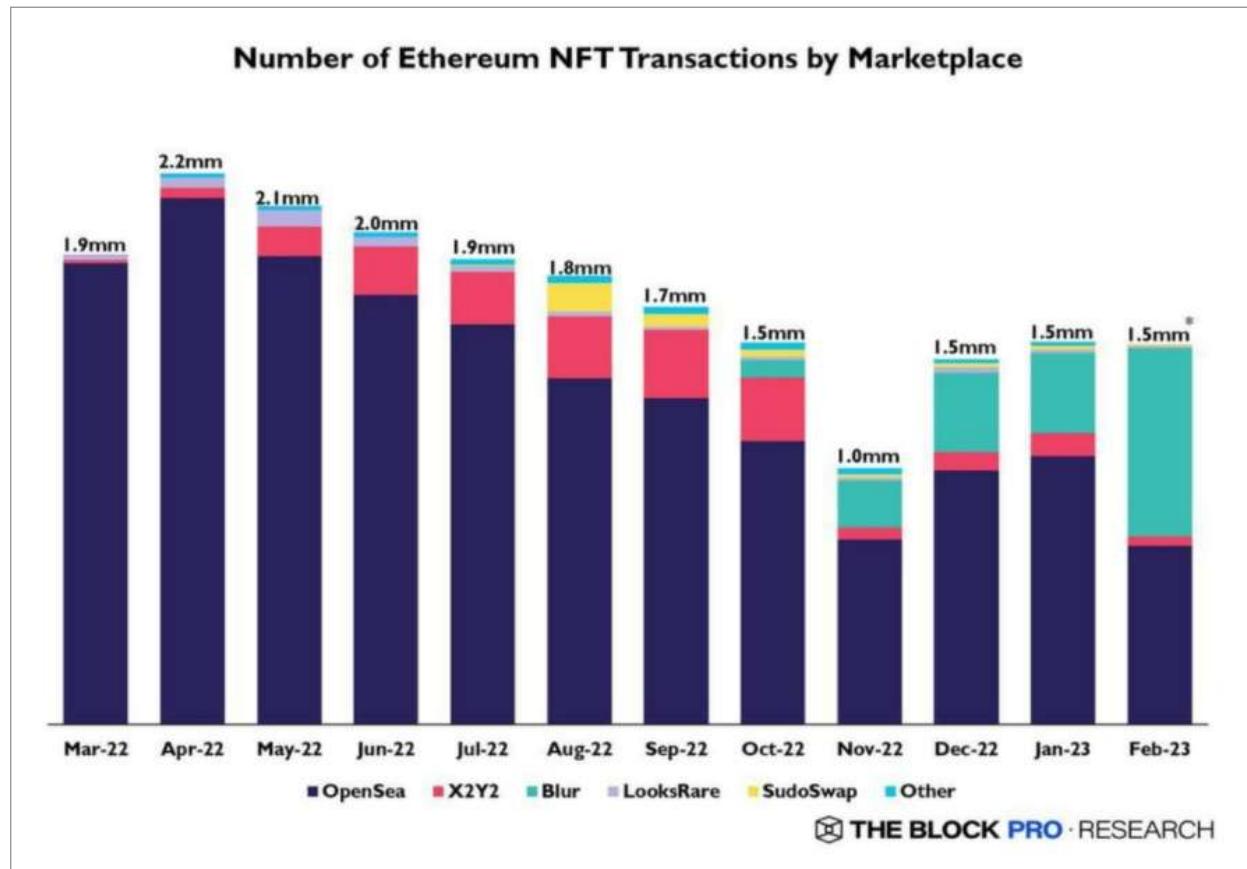
Ci sono state diverse aziende e piattaforme che hanno contribuito alla crescita del mercato degli NFT. **Uno dei primi progetti NFT**

di successo è stato CryptoKitties, lanciato nel 2017 su Ethereum. Il gioco ha permesso ai giocatori di acquistare, collezionare, allevare e commerciare gatti virtuali unici sotto forma di NFT.

Altri progetti NFT di successo includono **Axie Infinity**, una piattaforma di gioco basata su NFT che consente ai giocatori di combattere con creature uniche, e NBA Top Shot, una piattaforma di collezionismo di NFT dei momenti salienti dell’NBA.

Oltre alle piattaforme di gioco e di collezionismo, ci sono state molte altre applicazioni degli NFT in vari settori, tra cui l’arte, la musica, il cinema, lo sport e molti altri.

Nel settore dell’arte, l’artista digitale **Beeple** ha venduto un’opera d’arte sotto forma di NFT per la cifra record di 69 milioni di dollari nel marzo 2021. Nel mondo della musica, Grimes ha venduto una collezione di NFT per 6 milioni di dollari.



In questa tabella sono riportate il numero di transazioni avvenute nei principali marketplace di digital assets sul mercato. Come possiamo osservare OpenSea, è stato fino al 2023 il principale mercato di riferimento, mentre dal 2023, Blur ha iniziato a prendersi parte del marketshare complessivo.

5.3

Business

● Basic

Il ruolo della community nei progetti NFT

Il concetto di community online è strettamente legato all'economia intorno ai social network. Le comunità online si basano sulla creazione di gruppi di persone con interessi comuni, che interagiscono tra di loro attraverso le piattaforme social. Queste comunità possono essere create intorno a interessi specifici, come hobby, sport, musica o anche semplicemente la condivisione di idee e opinioni comuni. L'obiettivo di queste community è quello di creare un ambiente in cui i membri si sentano parte di un gruppo e possano interagire tra loro in modo significativo.

Gli influencer hanno un ruolo importante all'interno delle comunità online, in quanto in grado di influenzare le opinioni e le decisioni delle persone.

Un esempio di mercato che utilizza le community sui social network è **Freeda**, una **piattaforma che si rivolge alle donne con una forte presenza sui social network e utilizza una combinazione di analisi dati e machine learning per identificare e valutare l'influenza e l'engagement delle donne nella propria rete.**

Community online	Round di finanziamento	Importo	Fonte
Freeda	Serie A	16 milioni di euro	https://startupitalia.eu/114471-20190909-freeda-chiude-un-round-da-16-milioni-di-dollari
Peanut	Serie A	11 milioni di euro	https://www.eu-startups.com/2020/05/london-based-peanut-snaps-up-e11-million-to-become-the-leading-womens-social-network/
Nextdoor	Serie H	170 milioni di dollari	https://startupitalia.eu/114782-20190913-nextsoor-round-170-milioni-dollari

Freeda rappresenta un esempio di come le aziende possono utilizzare le community sui social network per ottenere un valore economico. In questo modo, le aziende possono ottenere una migliore comprensione dei loro pubblici di riferimento e creare campagne di marketing più efficaci.

Tipo di applicazione	Descrizione	Esempi di mercato
Arte	Applicazioni che permettono di acquistare, vendere e possedere opere d'arte digitali uniche e autenticabili attraverso NFT.	SuperRare, Nifty Gateway, Async Art
Giochi	Applicazioni che offrono esperienze di gioco decentralizzate, utilizzando NFT per rappresentare oggetti, personaggi e risorse all'interno dei giochi.	Axie Infinity, Decentraland, Gods Unchained
Social	Applicazioni che utilizzano blockchain e crittografia per proteggere la privacy degli utenti e incentivare la creazione di contenuti di alta qualità.	Minds, Steemit, LBRY
Mercati	Applicazioni che consentono a utenti e aziende di vendere e acquistare beni e servizi utilizzando digital assets e NFT.	OpenBazaar, Rarebits, Origin Protocol
Identità e reputazione	Applicazioni che consentono agli utenti di creare e controllare la propria identità digitale e la propria reputazione online.	uPort, Civic, Sovrin

Stiamo assistendo al progressivo avvicinamento del web2 con il web3, in quanto molte community web2 stanno provando ad utilizzare nuovi strumenti tecnologici, quali ed esempio gli NFT, per attrarre

nuovi utenti e generare revenue dai propri followers, dando in cambio un certificato unico digitale che abilità nuove attività all'interno della stessa community.

Per esempio, il mercato delle community sportive è in rapida crescita, con collezioni di NFT che rappresentano squadre, atleti, eventi sportivi e momenti memorabili. Alcune collezioni popolari includono NBA Top Shot, una collezione di clip video in edizione limitata che rappresentano le migliori giocate della NBA, e Sorare, una collezione di carte collezionabili di calcio che rappresentano giocatori e squadre di tutto il mondo. Le community che si sono formate intorno a queste collezioni sono composte da appassionati di sport e collezionisti di tutto il mondo.

Gli NFT hanno una vasta gamma di applicazioni, dalle opere d'arte digitali ai video di gioco fino alle collezioni virtuali. Sono utilizzati anche come un mezzo per rappresentare la proprietà di beni digitali, per proteggere i diritti d'autore e per garantire l'autenticità delle opere d'arte. Inoltre, gli NFT possono essere utilizzati per creare incentivi e ricompense all'interno delle comunità online, dove l'esclusività e il tiering sociale possono svolgere un ruolo importante.

5.4

Business

● Basic

Social tiering ed esclusività con gli NFT

Gli NFT stanno diventando sempre più diffusi come strumento per rappresentare beni digitali unici come opere d'arte o oggetti di gioco. Al centro del **concetto di esclusività degli NFT c'è la loro unicità**. Ogni token è creato in modo univoco e rappresenta un bene digitale specifico. Inoltre, gli **NFT sono spesso accompagnati da una certificazione di autenticità**, che attesta l'unicità del token e la sua proprietà.

Ma gli NFT **non sono solo un mezzo per rappresentare beni digitali unici**. Essi possono anche essere **utilizzati per creare una gerarchia all'interno delle comunità online**. Ad esempio, i membri che possiedono NFT di livello superiore possono ottenere accesso esclusivo a contenuti speciali o ricevere ricompense speciali all'interno della comunità. Questo tipo di tiering sociale può creare incentivi per i membri della comunità ad investire in NFT e può aumentare l'interesse e l'attività all'interno della comunità.

L'utilizzo degli NFT per creare una gerarchia sociale all'interno delle comunità può essere particolarmente efficace in contesti in cui i membri desiderano distinguersi dagli altri e ottenere una certa posizione sociale. Ad esempio, all'interno di comunità di appassionati di giochi o sport, i membri che possiedono gli NFT di livello superiore possono essere considerati "leader" della comunità e acquisire una maggiore influenza.

5.5

Informatica

● Basic

Come si gestiscono i token non fungibili dentro un wallet?

La gestione di un token ERC721 all'interno di un wallet è simile a quella di un token ERC20, poiché entrambi i tipi di token sono basati sulla tecnologia blockchain Ethereum e sono gestiti attraverso un portafoglio digitale. Tuttavia, ci sono alcune differenze significative tra i due tipi di token che ne influenzano la gestione.

In particolare, i token ERC20 rappresentano un'unità di valore fungibile all'interno di un sistema, mentre i token ERC721 rappresentano un'unità di valore non fungibile. Ciò significa che ogni token ERC721 è unico e ha un valore unico, a differenza dei token ERC20 che sono intercambiabili.

La tabella seguente illustra le **principali differenze tra i token ERC20 e ERC721** in termini di gestione all'interno di un wallet:

Descrizione	Token ERC20	Token ERC721
<i>Tipo di token</i>	Fungibile	Non fungibile
<i>Identificazione</i>	Identificati da un simbolo univoco	Identificati da un ID univoco
<i>Quantità</i>	Sono emessi tipicamente in quantità maggiori	Sono emessi in quantità limitate
<i>Possesso</i>	Possono essere posseduti in massa	Sono posseduti uno alla volta
<i>Gestione del wallet</i>	Possono essere gestiti in un unico portafoglio	Richiedono un portafoglio dedicato per ogni NFT
<i>Interoperabilità</i>	Scambiabili tra diverse piattaforme	Meno interoperabili tra diverse piattaforme
<i>Utilizzo principale</i>	Monete utilizzate per lo scambio di valore	Utilizzati per rappresentare oggetti digitali unici

In sintesi, sebbene la gestione di un token ERC721 all'interno di un wallet sia simile a quella di un token ERC20, ci sono alcune differenze significative dovute alla natura unica e non fungibile dei token ERC721. Queste differenze richiedono una gestione separata dei token all'interno del portafoglio e una maggiore attenzione alle transazioni di singoli token unici.

5.6

Informatica

● Basic

Token non fungibili per accedere a servizi esclusivi: il caso Spotify

Il concetto di accesso token-gated può essere descritto come un meccanismo di autenticazione e autorizzazione basato su token non fungibili (NFT), che limita l'accesso a determinate funzionalità o contenuti all'interno di applicazioni decentralizzate (dApps) o di piattaforme di comunicazione (tra le più note ci sono Discord e Telegram). In questo contesto, i token funzionano come una forma di "tessera d'in-

gresso” o di “abbonamento”, che garantisce ai detentori dei token l’accesso ad alcuni servizi premium. Questa nuova forma di accesso viene utilizzata come metodo di autenticazione molto simile al social login web2 ma sfruttando la tecnologia dei wallet digitali, richiedendo agli utenti di firmare una transazione per confermare il possesso di un NFT specifico. Il possesso permette, conseguentemente, di accedere a funzionalità o contenuti altrimenti protetti.

Rispetto alle tradizionali forme di autenticazione basate su username e password, **gli NFT offrono un maggiore livello di sicurezza e protezione per gli utenti, poiché sono basati su crittografia e tecnologie blockchain.** L’utilizzo di un sistema token-gated può offrire diversi vantaggi sia per gli utenti che per gli sviluppatori. Alcuni utenti acquistano token come **forma di investimento** al fine di accedere a servizi esclusivi, di guadagnare ricompense o di acquisire oggetti virtuali di valore. Per gli sviluppatori, invece, l’utilizzo di un sistema token-gated può essere **un’opportunità per monetizzare il proprio servizio o per incentivare l’utilizzo della propria piattaforma.**

Le applicazioni token-gated sono particolarmente comuni in diversi settori, come ad esempio quello dei giochi online, delle piattaforme di social networking e dei servizi di streaming. In questi casi, i token possono essere utilizzati per sbloccare nuovi livelli, acquistare oggetti virtuali o accedere a funzionalità esclusive.

Il gigante dello streaming musicale Spotify ha lanciato un nuovo test pilota per le playlist basate su token come il suo ultimo esperimento su Web3. Il pilota coinvolge alcuni progetti NFT, tra cui Overlord e Kingship, che permettono ai detentori di ciascun progetto di testare un’innovativa integrazione crittografica con la piattaforma di streaming.

Il nuovo pilota “token-gated playlist” rappresenta un’innovativa applicazione dell’uso di token non fungibili (NFT) all’interno della piattaforma di streaming musicale. Offrendo playlist esclusive e accessibili solo ai detentori di specifici NFT, Spotify potrebbe attirare un pubblico più ampio e appassionato di tecnologia blockchain e digital assets.

5.7

Informatica

● Medium

Single Sign-On (SSO) con NFT nel Web2 e nel Web3

Il Single Sign-On (SSO) è un meccanismo di autenticazione che consente agli utenti di accedere a diverse applicazioni o servizi con un unico set di credenziali di accesso. Nel contesto di una dApp token-gated, il SSO consente agli utenti di accedere alla dApp utilizzando un unico token di autenticazione, anziché dover effettuare l’autenticazione per ogni singola applicazione o servizio. Ad oggi i principali servizi online che utilizziamo per loggarci sono quelle offerte da social network e altre piattaforme che gestiscono per noi i nostri dati personali.

L’implementazione del SSO in una dApp token-gated può comportare diversi vantaggi, tra cui una maggiore comodità per l’utente, una maggiore sicurezza e una migliore gestione delle autorizzazioni. Infatti, il SSO consente di semplificare il processo di autenticazione per gli utenti, che non devono più ricordare diverse coppie di nome utente e password per accedere alle diverse funzionalità della DApp. Inoltre, **l’utilizzo di un singolo token di autenticazione consente di ridurre il rischio di attacchi di phishing o di furto di credenziali,** in quanto le informazioni di accesso dell’utente sono registrate nella blockchain tramite l’associazione token e address.

Ad oggi è facile trovare dei modelli di autorizzazione ed accesso token-gated nelle applicazioni web3, ma più difficile trovare questi social login web3 all’interno di applicazioni e piattaforme online tradizionali.

5.8

Informatica

● Medium

I metadati dentro gli NFT

Un NFT (Non-Fungible Token) è un token crittografico che rappresenta un'entità unica e irripetibile, come ad esempio un'opera d'arte digitale o un pezzo di musica. **Una delle caratteristiche distintive degli NFT è la loro capacità di incorporare qualsiasi formato all'interno del loro smart contract ERC721.** In pratica, quando un artista crea un'opera d'arte digitale e la trasforma in un NFT, può incorporare il file dell'opera all'interno del contratto dell'NFT stesso. In questo modo, **il file dell'opera viene “incapsulato” all'interno del token e può essere facilmente accessibile e visualizzato dai proprietari dell'NFT.** Per custodire il file dell'opera d'arte digitale, gli NFT utilizzano spesso IPFS (InterPlanetary File System), un sistema distribuito di archiviazione dei dati che **consente di memorizzare grandi quantità di informazioni in modo sicuro e affidabile.** In pratica, quando l'artista crea l'NFT, il file dell'opera viene caricato su IPFS e il contratto dell'NFT viene programmato per puntare a quel file. In questo modo, quando un acquirente acquista l'NFT, può accedere facilmente al file dell'opera d'arte digitale tramite IPFS. Questo rende gli NFT estremamente flessibili e adatti per rappresentare qualsiasi tipo di entità digitale, dal momento che possono incorporare qualsiasi formato all'interno del loro contratto e utilizzare IPFS per la sua memorizzazione.

Per far comunicare uno smart contract con IPFS su Ethereum, sono necessari i seguenti campi:

- **Una libreria IPFS:** è necessario importare una libreria IPFS nel contratto intelligente per consentire al contratto di comunicare con la rete IPFS.
- **Un campo per il CID:** il CID (Content Identifier) è un identificatore univoco del file archiviato su IPFS. Il contratto intelligente deve contenere un campo per il CID del file associato all'NFT.
- **Un metodo per recuperare il file:** il contratto intelligente deve contenere un metodo che consente di recuperare il file associato all'NFT utilizzando il CID. Questo metodo può essere utilizzato dagli utenti per accedere al file e visualizzare l'entità digitale rappresentata dall'NFT.

6

Decentralized Autonomous Organization (DAO)

- 6.1 Che cosa sono le DAO?
- 6.2 Quali applicazioni possono nascere con una DAO?
- 6.3 Quali sono i tokens utilizzati da una DAO?
- 6.4 Considerazioni sulla tokenomics e la governance in una DAO

6.1

Che cosa sono le DAO?

Informatica / Business

● Basic

Il concetto di **DAO** (Decentralized Autonomous Organization) è strettamente legato alla nascita delle comunità economiche digitali, ovvero gruppi di individui che si uniscono attraverso una piattaforma digitale per collaborare e perseguire obiettivi economici comuni. Le DAO sono **organizzazioni decentralizzate che si basano su blockchain e digital assets, e che hanno l'obiettivo di creare un ecosistema economico autogovernato e completamente autonomo**.

Le DAO si basano sul principio della **governance distribuita**, dove **ogni membro della comunità ha un peso uguale nella gestione delle decisioni dell'organizzazione**. Ciò significa che le decisioni sono prese in modo democratico attraverso meccanismi di voto, e che tutti i membri della comunità hanno la possibilità di partecipare attivamente alla gestione dell'organizzazione.

Oltre ai vantaggi economici, le DAO sono spesso associate ad un aspetto filosofico e sociale, che promuove l'**idea di un sistema più equo e decentralizzato, in cui il potere non è concentrato nelle mani di pochi, ma è distribuito tra tutti i membri della comunità**. Inoltre, le DAO si basano su tecnologie open source, che permettono a chiunque di partecipare e contribuire allo sviluppo dell'organizzazione.

Ecco di seguito una tabella con i concetti chiave relativi alle DAO:

Concetto	Descrizione
Governance distribuita	<i>La governance distribuita è un sistema in cui le decisioni sono prese in modo decentralizzato e democratico da tutti i membri della comunità. In una DAO, i membri possono votare per decidere le azioni e le decisioni da prendere.</i>
Autonomia	<i>Le DAO sono organizzazioni autonome, che si gestiscono da sole senza la necessità di un amministratore centrale. Questo permette una maggiore agilità nella presa delle decisioni e nella loro attuazione.</i>
Blockchain	<i>Le DAO si basano su una blockchain, che rappresenta un registro pubblico e immutabile delle transazioni e delle decisioni prese all'interno dell'organizzazione. La blockchain garantisce la trasparenza e la sicurezza delle operazioni effettuate dalla DAO.</i>
Meccanismi di voto	<i>I membri della DAO possono votare per prendere decisioni. Esistono diversi meccanismi di voto, come il voto ponderato, il voto a maggioranza, il voto quadratico e altri ancora.</i>
Open source	<i>Le DAO utilizzano spesso software open source per la loro gestione, che garantisce la trasparenza e la partecipazione della comunità nello sviluppo e nella gestione dell'organizzazione.</i>
Equità	<i>Le DAO garantiscono l'equità nella distribuzione dei diritti di voto e di partecipazione all'interno dell'organizzazione. Tutti i membri della comunità hanno gli stessi diritti e le stesse opportunità di partecipazione e di guadagno.</i>
Partecipazione	<i>Le DAO promuovono la partecipazione attiva dei membri della comunità nella presa delle decisioni e nella gestione dell'organizzazione. Tutti i membri possono proporre nuove idee e progetti e votare per le decisioni da prendere.</i>

Per concludere uno dei potenziali rischi delle DAO, se non verranno regolamentate correttamente, sarà quello dell'anonymato e della sua vulnerabilità durante scelte strategiche, determinate da grandi detentori di token, che potranno alterare il corretto funzionamento delle logiche sottostanti.

6.2

Quali applicazioni possono nascere con una DAO?

Informatica / Business

● Basic

Una DAO (Decentralized Autonomous Organization) può **operare in molte aree di business diverse**, a seconda degli obiettivi e delle necessità della comunità che la gestisce. Di seguito sono elencate alcune delle possibili aree di business in cui una DAO potrebbe operare, tralasciando in questa sede gli aspetti di natura legale e regolamentare del fenomeno:

- **Crowd-funding platform:** una DAO può operare come piattaforma di crowd-funding, consentendo ai membri della comunità di investire in progetti e startup in modo decentralizzato, senza l'intermediazione di una banca o di altri intermediari finanziari.
- **Beneficenza:** una DAO può operare come organizzazione benefica, raccogliendo fondi e donazioni per sostenere cause sociali, ambientali o sanitarie, e distribuendo i fondi in modo trasparente e democratico tra i progetti selezionati dalla comunità.
- **Grant e bounty program:** una DAO può operare come programma di sovvenzioni e premi per incoraggiare lo sviluppo di progetti open source, di ricerca o di innovazione tecnologica, premiando i partecipanti che raggiungono determinati obiettivi o che contribuiscono in modo significativo al progresso dell'organizzazione.
- **Fondi partecipativi:** una DAO può operare come fondo partecipativo, consentendo ai membri della comunità di investire in modo decentralizzato in progetti di sviluppo economico, infrastrutture e servizi pubblici, consentendo ai cittadini di partecipare attivamente alle decisioni che riguardano il loro territorio e la loro comunità.
- **Piattaforme di voting:** una DAO può operare come piattaforma di voto, consentendo ai membri della comunità di partecipare attivamente alla gestione dell'organizzazione, votando sulle decisioni strategiche, le politiche interne e la selezione dei progetti da finanziare.

La **trasparenza** è un **vantaggio fondamentale per le DAO** perché consente ai membri della comunità di tenere traccia di come i fondi vengono spesi. Grazie alla trasparenza, i membri della comunità possono vedere chi riceve i fondi, come vengono utilizzati e come vengono assegnati i premi e le sovvenzioni. Questo aiuta a prevenire la corruzione e assicura che i fondi vengano utilizzati in modo efficace e per il bene della comunità.

Lo **pseudo-anonimato** è un'altra caratteristica importante per le DAO perché agevola i **membri della comunità nella tutela della loro privacy e della loro sicurezza**. I membri possono partecipare alle attività della DAO senza rivelare la loro identità reale, il che può essere particolarmente importante quando si tratta di questioni sensibili come le donazioni o la partecipazione a progetti politici o sociali.

Il **pay-to-delivery**, infine, è un **vantaggio per le DAO** perché consente di **effettuare transazioni in modo sicuro e immediato**. Quando un membro della comunità effettua una transazione, i fondi vengono immediatamente consegnati all'altro membro senza la necessità di intermediari. Questo può ridurre i costi delle transazioni e aumentare la velocità di esecuzione delle attività, migliorando l'efficienza complessiva della DAO.

Modello di business	Vantaggi di trasparenza	Vantaggi di pseudo-anonimato	Vantaggi di pay-to-delivery
Crowd-funding	<i>I contribuenti possono vedere esattamente come il loro denaro viene utilizzato</i>	<i>Gli utenti possono partecipare senza dover rivelare la propria identità</i>	<i>Il denaro viene rilasciato solo quando l'obiettivo di finanziamento è stato raggiunto</i>
Bandi e grant	<i>I finanziamenti pubblici sono soggetti a una rigorosa supervisione e trasparenza</i>	<i>Gli utenti possono partecipare senza dover rivelare la propria identità</i>	<i>Il finanziamento viene rilasciato solo dopo che il progetto è stato completato con successo</i>
Beneficenza	<i>I donatori possono vedere esattamente come il loro denaro viene utilizzato</i>	<i>Gli utenti possono partecipare senza dover rivelare la propria identità</i>	<i>Il denaro viene rilasciato solo quando viene soddisfatta la necessità del destinatario</i>

In sintesi, i vantaggi di trasparenza, pseudo-anonimato e pay-to-delivery possono fornire valore alle DAO nella gestione dei fondi e nella governance della comunità. Consentono di prevenire la corruzione, proteggere l'anonymato dei membri e migliorare l'efficienza delle transazioni.

6.3

Informatica

● Medium

Quali sono i tokens utilizzati da una DAO?

Nel contesto dei token di governance, le modalità di voto possono essere di due tipi principali: **proporzionale** e **non proporzionale**.

Nel caso degli **ERC20**, il **voto proporzionale** è il **modello più comune**. In questo caso, ogni token conferisce un diritto di voto e il numero di voti che un detentore di token può esercitare è proporzionale al numero di token che possiede. In questo modo, i detentori di token che possiedono una maggiore quantità di token hanno un maggiore potere di voto.

Per quanto riguarda gli **ERC721**, il **modello di voto non proporzionale** è più comune. In questo caso, ogni token rappresenta un diritto di voto e il detentore del token ha un voto a prescindere dal numero di token che possiede. In questo modo, il potere di voto è equamente distribuito tra tutti i detentori di token. Inoltre, i token ERC721 possono essere utilizzati in modo più flessibile per rappresentare particolari diritti di voto o diritti di proprietà, come nel caso di token di governance che rappresentano quote di proprietà in un bene fisico.

Ad esempio, una DAO potrebbe possedere un'opera d'arte sotto forma di NFT e i membri potrebbero votare sulla sua vendita o sulla sua conservazione. In questo modo, gli NFT possono essere utilizzati per rappresentare la proprietà di asset e dare ai proprietari il diritto di voto sulla loro gestione all'interno della DAO.

In generale, il modello di **voto proporzionale** può essere considerato più democratico rispetto al **modello non proporzionale**, in quanto consente ai detentori di token con una maggiore partecipazione finanziaria di avere un maggiore peso nelle decisioni. Tuttavia, questo modello può anche portare ad una concentrazione del potere nelle mani di pochi detentori di token.

Il modello di **voto non proporzionale** può essere considerato più inclusivo e meno soggetto ad influenze di pochi detentori di token. Tuttavia, può essere critico per le DAO che richiedono un'ampia partecipazione finanziaria per raggiungere gli obiettivi comuni.

In entrambi i casi, il potere di voto dipende dal numero di token detenuti e dal modello di voto adottato dalla DAO. La scelta del modello di voto può avere un impatto significativo sul potere decisionale e sull'equità della DAO.

Alcuni esempi di token di governance nel mercato della DeFi includono:

- **MKR**: un token di governance utilizzato nella piattaforma **MakerDAO**, che consente ai suoi detentori di votare sulle decisioni riguardanti il sistema di prestiti stabili Dai.
- **COMP**: un token di governance utilizzato nella piattaforma **Compound**, che consente ai suoi detentori di votare sulle decisioni riguardanti la governance della piattaforma e la distribuzione dei premi.
- **UNI**: un token di governance utilizzato nella piattaforma **Uniswap**, che consente ai suoi detentori di votare sulle decisioni riguardanti la governance della piattaforma e la distribuzione dei premi.
- **DAO**: un token di governance utilizzato nella piattaforma **DAOstack**

6.4

Informatica

• Hard

Considerazioni sulla tokenomics e la governance in una DAO

I token, come già detto precedentemente, sono unità di valore che rappresentano un'assegnazione di diritti e funzioni all'interno di un'applicazione decentralizzata. I token possono essere utilizzati come valuta, come titolo, come partecipazione a un progetto o come voto per la governance.

Esistono **diversi tipi di token, come i token di sicurezza, i token utilitari, i token di accesso e i token di asset**. Ogni tipo di token ha una sua funzione specifica all'interno di un'applicazione o di un progetto. Il modello di emissione è uno degli aspetti più importanti della tokenomics. Esistono tre modelli di emissione principali: emissione fissa, emissione basata sull'utilizzo e emissione basata sul tempo.

- Nel **modello di emissione fissa**, una **quantità fissa di token viene creata all'inizio** del progetto e non viene creato alcun nuovo token in futuro.
- Nel **modello di emissione basata sull'utilizzo, i token vengono creati e distribuiti in base all'utilizzo della piattaforma**. Ad esempio, un utente che utilizza la piattaforma più di frequente riceverà una maggiore quantità di token.
- Nel **modello di emissione basata sul tempo, i token vengono creati e distribuiti nel corso del tempo**, con una quantità di token che viene creata ogni unità di tempo.

La tokenomics ha un **impatto significativo sulla governance e sulle decisioni prese all'interno della DAO, poiché la detenzione dei token dà diritto ai voti nelle decisioni prese dalla comunità e può influenzare la direzione strategica della DAO stessa**.

Inoltre, la **tokenomics può anche essere utilizzata per incentivare i membri della comunità a partecipare attivamente** alle attività della DAO, ad esempio offrendo ricompense in token per il lavoro svolto o per le decisioni prese.

La governance dei token può essere realizzata utilizzando **smart contract, che permettono di automatizzare le decisioni sull'utilizzo dei token**. Ad esempio, uno smart contract potrebbe essere utilizzato per stabilire regole sul numero massimo di token che possono essere emessi e su come questi token possono essere utilizzati.

- L'**emissione dei token riguarda la decisione su quando e come emettere nuovi token**. Ad esempio, una piattaforma potrebbe decidere di emettere nuovi token solo in risposta ad un aumento della domanda o per finanziare nuove funzionalità.
- La **modalità di emissione dei token può avere un impatto significativo sul valore** degli stessi. Ad esempio, un'emissione troppo rapida potrebbe portare a un'inflazione eccessiva, mentre un'emissione troppo lenta potrebbe rendere difficile finanziare nuove funzionalità.

In entrambi i casi, è **importante che la piattaforma fornisca trasparenza sulla propria politica di emissione e che utilizzi smart contract per garantire che le regole siano seguite in modo automatico e immutabile.**

Per quanto riguarda la **governance**, può essere implementata tramite un **sistema di voto decentralizzato** dove i token holder possono votare sulle modifiche al progetto o alla tokenomics stessa. Questo tipo di governance può essere implementato utilizzando un contratto intelligente basato sulla blockchain. Ad esempio, sulla blockchain Ethereum, è possibile utilizzare un contratto chiamato DAO (Decentralized Autonomous Organization) per implementare la governance.

Questo contratto consente ai partecipanti di votare su una proposta con un voto “sì” o “no”, e se il numero di voti “sì” supera una soglia di quorum, il contratto trasferirà una quantità specifica di fondi ad un destinatario specifico.

In conclusione, è quindi possibile affermare che la governance di un DAO è interamente decentralizzata e trasparente, e le decisioni sono prese dai partecipanti tramite meccanismi di voto che utilizzano la blockchain come registro immutabile. Tuttavia, **questo modello presenta anche alcuni limiti, tra cui la difficoltà di modificare il contratto una volta pubblicato e la difficoltà di garantire che i partecipanti siano davvero rappresentativi della comunità a cui servono.** Inoltre, la governance decentralizzata può essere **influenzata da problemi di centralizzazione e di partecipazione limitata**, il che può rendere difficile la decisione di modificare la tokenomics.

7

Approfondimenti su token e smart contract

- 7.1 Costruire nel Web3
- 7.2 Tipologia di smart contract per lo sviluppo di dApps
- 7.3 Approfondimento Tether (ERC20)
- 7.4 Approfondimento Compound (DeFi)
- 7.5 Approfondimento IPFS (InterPlanetary File System)
- 7.6 Approfondimento CryptoKitties (ERC721)

7.1

Informatica
● Basic

Costruire nel Web3

Il processo logico con cui uno sviluppatore inizia a creare una dApps dipende dalle specifiche esigenze del progetto. In linea generale, il processo può essere suddiviso in diverse fasi:

1. **Identificazione dell'obiettivo della dApps**
2. **Scelta della rete su cui sviluppare (in questo caso Ethereum)**
3. **Scelta degli smart contract da utilizzare**
4. **Implementazione degli smart contract**
5. **Integrazione degli smart contract nella dApps**
6. **Testing e deploy della dApps**

Per quanto riguarda il testing e il deploy della dApps sulla blockchain Ethereum, esistono diverse testnet disponibili per i developer.



Per il deploy della dApps sulla rete Ethereum, **esistono diversi strumenti a disposizione dei developer, come ad esempio Truffle, Remix e Ganache**. Truffle è un framework di sviluppo per Ethereum che offre uno strumento di deploy chiamato Truffle Deploy. Remix è un IDE online che permette di scrivere, testare e deployare i contratti intelligenti direttamente dalla piattaforma. Ganache è un ambiente di sviluppo locale che permette di creare una blockchain privata per testare le dApps.

Inoltre, prima di fare il deploy, solitamente si va a calcolare quanto costa in termini di gas. **Maggiore è la lunghezza e la complessità degli smart contract, maggiore sarà il costo di deploy sulla rete**. In sintesi, La quantità di gas richiesta, e quindi il costo di rilasciare una dApps, dipende quindi dalla complessità della dApps e dal carico della rete Ethereum al momento del deploy.

Secondo il rapporto di Alchemy, il numero di contratti intelligenti implementati **nel quarto trimestre del 2022 è cresciuto del 453% da un trimestre all'altro, raggiungendo l'incredibile cifra di 4,6 milioni**. Inoltre, l'implementazione di contratti intelligenti sulla testnet Goerli di Ethereum è cresciuta del 187% negli ultimi tre mesi del 2022 e fino al 721% su base annua, raggiungendo il massimo storico di 2,7 milioni e segnalando che più applicazioni decentralizzate (dApps) potrebbe entrare nel mercato in futuro.

7.2

Informatica

• Medium

Tipologia di smart contract per lo sviluppo di dApps

Come abbiamo visto in precedenza, uno smart contract non è altro che una nuova tipologia di software che automatizza le transazioni sulla rete e crea nuove logiche capaci di generare applicazioni decentralizzate. Ecco una lista dei principali smart contract utilizzati per creare un'applicazione decentralizzata:

1. **Proxy smart contract:** questo tipo di smart contract viene utilizzato per delegare le funzioni di un contratto a un altro contratto, senza dover modificare il codice sorgente del contratto originale.
2. **Token smart contract:** questo tipo di smart contract viene utilizzato per creare un token su una blockchain, come ad esempio un token ERC-20 su Ethereum.
3. **Oracle smart contract:** questo tipo di smart contract viene utilizzato per ottenere dati esterni, come ad esempio i prezzi dei digital assets, e renderli disponibili all'interno della blockchain.
4. **Yield farming smart contract:** questo tipo di smart contract viene utilizzato all'interno delle dApps DeFi per incentivare gli utenti a fornire liquidità alla piattaforma in cambio di rendimenti.
5. **Staking smart contract:** questo tipo di smart contract viene utilizzato per incentivare gli utenti a mantenere i propri token in un determinato wallet o sulla piattaforma, in cambio di rendimenti o diritti di voto.
6. **Governance smart contract:** questo tipo di smart contract viene utilizzato per consentire agli utenti di votare su decisioni importanti all'interno della piattaforma, come ad esempio l'aggiornamento del protocollo o l'introduzione di nuove funzionalità.
7. **Collateralized debt position (CDP) smart contract:** questo tipo di smart contract viene utilizzato per creare stablecoin, come ad esempio DAI su Ethereum, garantendo il valore della stablecoin attraverso il deposito di digital assets come garanzia.

Tra i contratti elencati, quello proxy, è di particolare importante per poter collegare diversi smart contract, facilitando la creazione di logiche più complesse. Inoltre, risulta di particolare importanza per creare interfacce collegabili e fruibili per l'utente. La struttura di uno smart contract proxy può variare a seconda delle esigenze specifiche dell'applicazione. Tuttavia, di solito è composto da diversi blocchi logici e funzionali, tra cui:

1. **Interfaccia utente:** questo blocco gestisce l'interazione tra l'utente e lo smart contract proxy. L'interfaccia può essere implementata tramite una GUI (interfaccia grafica utente) o attraverso una API (interfaccia di programmazione delle applicazioni).
2. **Verifica delle autorizzazioni:** questo blocco verifica se l'utente ha le autorizzazioni necessarie per eseguire una determinata operazione. Ad esempio, potrebbe verificare se l'utente ha abbastanza fondi per eseguire una transazione.
3. **Validazione dei dati:** questo blocco verifica se i dati inseriti dall'utente sono validi e conformi alle regole del contratto.
4. **Esecuzione del contratto:** questo blocco esegue il contratto effettivo, utilizzando gli altri smart contract necessari per completare l'operazione richiesta dall'utente.
5. **Gestione degli errori:** questo blocco gestisce gli errori che possono verificarsi durante l'esecuzione del contratto, ad esempio quando si verifica un errore di convalida dei dati o di autorizzazione.
6. **Gestione degli eventi:** questo blocco gestisce gli eventi generati dal contratto, ad esempio quando viene eseguita una transazione o quando viene raggiunto un determinato stato.

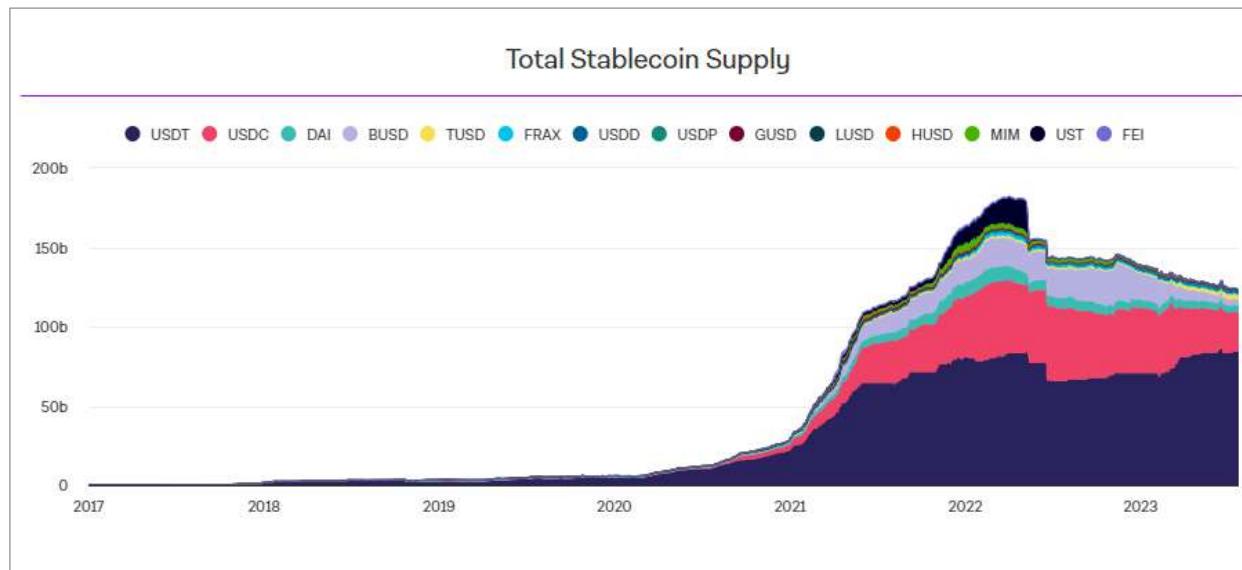
In sintesi, uno smart contract proxy funge da intermediario tra gli utenti e la logica del contratto, semplificando l'interazione e migliorando la sicurezza dell'applicazione.

7.3

Informatica
● Hard

Approfondimento Tether (ERC20)

Tether è una stablecoin che mira a mantenere un valore pari a 1 dollaro USA per token. La stabilità di Tether viene mantenuta attraverso il processo di ancoraggio, che implica il deposito di una quantità di denaro equivalente in dollari USA in una banca. Tether utilizza la tecnologia blockchain per emettere e gestire i propri token, e questo processo avviene attraverso la creazione di uno smart contract.



Lo smart contract di Tether è un contratto autonomo e autoregolamentato che esegue le transazioni in modo automatizzato e senza la necessità di un intermediario. È costruito sulla blockchain di Ethereum, che consente la creazione di smart contract personalizzati. In particolare, **Tether utilizza il protocollo ERC-20, che definisce gli standard per l'emissione e la gestione di token su blockchain Ethereum.**

Il contratto Tether ERC-20 definisce la quantità massima di token Tether emessi e in circolazione, insieme alle regole per la creazione, il trasferimento ed il controllo dei token. Inoltre, il contratto stabilisce il rapporto 1:1 tra ogni token Tether e il dollaro USA, garantendo la stabilità del valore del token.

L'infrastruttura dello smart contract di Tether è **distribuita su più nodi della rete Ethereum, il che significa che il contratto viene eseguito simultaneamente su più computer**. Questa distribuzione garantisce che il contratto Tether sia resistente ad eventuali attacchi o malfunzionamenti di un singolo nodo della rete.

Infine, tale smart contract viene costantemente monitorato e aggiornato per garantire la sicurezza e la stabilità dei token Tether emessi. Questo è particolarmente importante data la natura critica della funzione di ancoraggio che Tether svolge, il quale richiede che il valore dei token rimanga stabile e che i fondi siano protetti.

Elemento	Descrizione
Nome	<i>Tether Token</i>
Simbolo	<i>USDT</i>
Tipo di Token	<i>Stablecoin</i>
Valore di Tether	<i>Collegato al dollaro USA (1 USDT = 1 USD)</i>
Backing	<i>Garantito da riserve in contanti e conti bancari equivalenti</i>
Tipo di blockchain	<i>Omni Layer su Bitcoin, Ethereum, Tron e altre blockchain</i>
Obiettivo	<i>Fornire una stablecoin che possa essere utilizzata come alternativa alle valute fiat nelle transazioni crittografiche</i>
Regolamentazione	<i>Soggetto alla normativa sui digital assets e alle leggi sulle valute in diversi paesi</i>
Trasparenza	<i>Periodicamente pubblica una conferma delle riserve per dimostrare la copertura totale</i>
Fungibilità	<i>Tutti i token Tether sono intercambiabili e fungibili</i>
Accettazione	<i>Ampiamente accettato in diverse borse crittografiche e utilizzato come forma di pagamento in vari settori</i>

Lo smart contract proxy per una stablecoin come Tether è un tipo di smart contract che funge da intermediario tra il protocollo principale di Tether e le applicazioni esterne che vogliono utilizzare la stable coin. La struttura di uno smart contract proxy per Tether è composta da diversi blocchi logici e funzionali.

- Il primo blocco è quello che **gestisce la creazione e la distruzione dei token USDT**. Questo blocco prevede la creazione di nuovi token USDT in base alla domanda del mercato e la distruzione dei token quando vengono venduti.
- Il secondo blocco è quello che **gestisce il trasferimento dei token USDT da un utente all'altro**. Questo blocco prevede la registrazione delle transazioni sulla blockchain di Tether e garantisce la sicurezza e l'integrità delle transazioni.
- Il terzo blocco è quello che **gestisce il sistema di riserve di denaro reale**. Questo blocco prevede la gestione del fondo di denaro reale che viene mantenuto in banche e che corrisponde al valore totale dei token USDT in circolazione. In questo modo, Tether garantisce che ogni token USDT possa essere convertito in un dollaro americano in qualsiasi momento.
- Il quarto blocco è quello che **gestisce le interazioni con le applicazioni esterne**. Questo blocco prevede la creazione di un'interfaccia per le applicazioni esterne che vogliono utilizzare la stable coin. L'interfaccia fornisce informazioni sul valore dei token USDT e permette alle applicazioni esterne di effettuare transazioni con la stable coin.

Oltre allo smart contract proxy, una stable coin come Tether può utilizzare altri smart contract per gestire altre funzionalità. Ad esempio, può essere utilizzato uno smart contract per la gestione dei diritti di voto e decisionali sulla governance della stable coin, o uno smart contract per la gestione dei programmi di incentivazione e ricompensa per gli utenti che utilizzano la stable coin. Inoltre, possono essere utilizzati smart contract per la gestione degli oracoli, ovvero i sistemi che forniscono informazioni esterne alla blockchain, come il prezzo dei digital assets o delle valute fiat, necessari per garantire la stabilità del valore della stable coin.

7.4

Informatica

● Hard

Approfondimento Compound (DeFi)

Gli smart contract per i servizi di peer to peer landing sulla blockchain Ethereum operano **come intermediari tra le parti**. Gli utenti possono accedere alla piattaforma attraverso un'interfaccia utente web o mobile, dove possono richiedere un prestito oppure offrire un prestito, specificando il tasso di interesse, la durata e le garanzie richieste.

Una volta che un prestito è stato negoziato tra lender e borrower, il contratto intelligente del lending P2P viene attivato. **Il prestatore trasferisce i fondi alla blockchain Ethereum come deposito di garanzia, mentre il prestito viene distribuito al richiedente mediante una transazione sulla blockchain.**

Il contratto intelligente gestisce automaticamente i pagamenti del prestito, **controllando se il prestatore ha ricevuto i pagamenti degli interessi e il rimborso del prestito in tempo**. Se il mutuatario (colui che richiede il prestito) non adempie alle sue obbligazioni di rimborso, il contratto intelligente utilizzerà il deposito di garanzia per il rimborso.

Inoltre, gli smart contract P2P per il lending possono anche utilizzare la tecnologia degli oracoli per verificare la solvibilità del mutuatario e l'accuratezza dei dati che ha fornito, **ad esempio verificando la sua reputazione creditizia o il suo reddito**. In questo modo, il contratto intelligente può ridurre il rischio di default del prestito e aumentare la fiducia.

Tra i servizi nel mercato, **Compound è una piattaforma DeFi (Decentralized Finance) che utilizza gli smart contract di Ethereum** per fornire servizi di prestito e prestito di digital assets in modo decentralizzato. Gli smart contract utilizzati da Compound sono progettati per gestire il prestito di digital assets tra utenti, senza la necessità di intermediari centralizzati come le banche.

Uno smart contract di dApps di peer to peer lending come Compound potrebbe essere suddiviso **in diversi blocchi logici**, ognuno dei quali svolge una funzione specifica. Di seguito sono elencati alcuni possibili blocchi logici che potrebbero essere presenti in uno smart contract di questo tipo:

1. **Blocco di inizializzazione:** questo blocco viene eseguito una sola volta all'avvio del contratto e ha lo scopo di inizializzare le variabili e le strutture dati necessarie per il funzionamento del contratto.
2. **Blocco di gestione degli utenti:** questo blocco contiene le funzioni per la gestione degli utenti del contratto, come la registrazione degli utenti, la verifica dell'identità e la gestione dei prestiti e dei prestiti ricevuti.
3. **Blocco di gestione dei prestiti:** questo blocco contiene le funzioni per la gestione dei prestiti, come la richiesta di un prestito, la valutazione del rischio di credito dell'utente e la definizione delle condizioni del prestito.
4. **Blocco di gestione dei prestiti ricevuti:** questo blocco contiene le funzioni per la gestione dei prestiti ricevuti, come il pagamento degli interessi e la restituzione del prestito alla scadenza.
5. **Blocco di gestione delle garanzie:** questo blocco contiene le funzioni per la gestione delle garanzie fornite dagli utenti per garantire il rimborso dei prestiti. Queste funzioni includono l'accettazione delle garanzie, il monitoraggio della loro valutazione e la loro restituzione agli utenti una volta che il prestito è stato rimborsato.
6. **Blocco di gestione dei tassi di interesse:** questo blocco contiene le funzioni per la gestione dei tassi di interesse sui prestiti. Queste funzioni includono il calcolo dei tassi di interesse in base al rischio di credito dell'utente e alla durata del prestito, nonché la definizione delle regole per l'aggiornamento dei tassi di interesse nel tempo.
7. **Blocco di gestione delle transazioni:** questo blocco contiene le funzioni per la gestione delle transazioni tra gli utenti del contratto, come il trasferimento di digital assets o altre valute da un utente all'altro.

All'interno degli smart contract, ci sono alcune funzioni logiche da studiare nel dettaglio per garantire che il meccanismo di peer to peer landing funzioni e garantisca sicurezza alle controparti coinvolte. Qui alcune funzioni da inserire nei contratti:

- Funzioni per l'aggiunta e la rimozione di digital assets dallo smart contract
- Funzioni per il calcolo degli interessi e la distribuzione degli interessi ai partecipanti
- Funzioni per la gestione delle garanzie e la liquidazione in caso di default di un partecipante
- Funzioni per la gestione delle votazioni e delle decisioni prese dalla comunità di partecipanti
- Funzioni per la gestione dei prestiti e delle richieste di prestito tra i partecipanti
- Funzioni per la gestione dei token ERC20 associati al blocco logico.

Questi sono solo alcuni esempi di blocchi logici che potrebbero essere presenti in uno smart contract di dApps di peer to peer lending come Compound. Il linguaggio utilizzato per implementare questi blocchi logici potrebbe essere Solidity, un linguaggio di programmazione specifico per gli smart contract su Ethereum.

In sintesi, gli smart contract utilizzati da Compound sono progettati per consentire agli utenti di depositare e prelevare e di prendere in prestito digital assets da altri utenti e di pagare gli interessi sui prestiti stessi. La piattaforma utilizza la tecnologia blockchain e gli smart contract per garantire la sicurezza e la trasparenza delle transazioni.

7.5

Informatica

● Hard

Approfondimento IPFS (InterPlanetary File System)

IPFS è un sistema di archiviazione decentralizzato che permette di memorizzare e accedere ai contenuti in maniera distribuita. Invece di archiviare i dati su un server centrale, IPFS utilizza una rete di nodi che contribuiscono a mantenere i file sincronizzati. Questo significa che i dati non sono più controllati da un singolo soggetto, ma da una rete globale.

I blocchi logici di uno smart contract o più smart contracts di dApps di decentralized storage come IPFS possono essere implementati in Solidity utilizzando diverse funzioni e strutture dati. Ad esempio, un blocco logico potrebbe essere implementato come un contratto che contiene una lista di nodi IPFS, ciascuno dei quali rappresenta un file o una directory archiviati sulla rete IPFS. Questo contratto potrebbe includere le seguenti funzioni:

- Una funzione **per l'aggiunta di un nuovo nodo IPFS alla lista**, che richiede l'hash del nodo come parametro e verifica che il nodo non sia già presente nella lista.
- Una funzione **per la rimozione di un nodo IPFS dalla lista**, che richiede l'hash del nodo come parametro e verifica che il nodo sia presente nella lista.
- Una funzione **per la ricerca di un nodo IPFS nella lista**, che richiede l'hash del nodo come parametro e restituisce true se il nodo è presente nella lista e false altrimenti.
- Una funzione **per la gestione delle autorizzazioni di accesso ai nodi IPFS**, che permette ai proprietari dei nodi di concedere o revocare l'accesso ad altri utenti sulla base di determinate condizioni.
- Una funzione **per la gestione dei pagamenti per l'accesso ai nodi IPFS**, che permette ai proprietari dei nodi di impostare un prezzo per l'accesso ai loro contenuti e di ricevere pagamenti in digital assets o in altre valute.

- Una funzione per la gestione della condivisione dei nodi IPFS tra più utenti, che permette ai proprietari dei nodi di creare gruppi di utenti autorizzati ad accedere ai loro contenuti e di gestire le autorizzazioni di accesso di ciascun utente all'interno del gruppo.

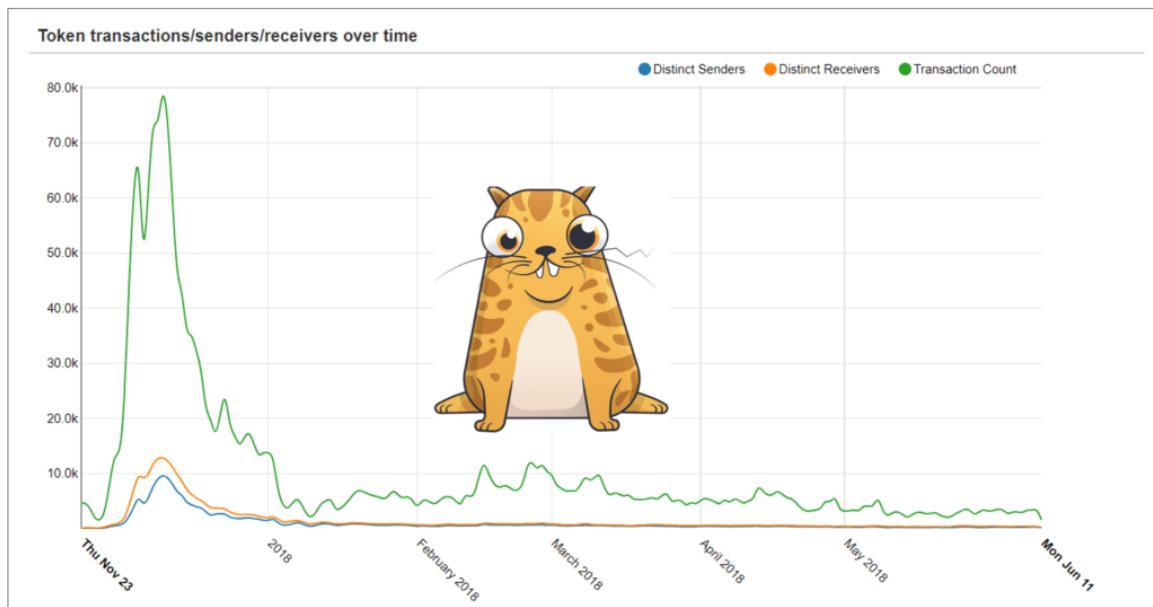
Inoltre, uno smart contract di dApps di decentralized storage come IPFS potrebbe utilizzare altre funzioni e strutture dati per implementare funzionalità aggiuntive come la crittografia dei dati, la compressione dei dati, la gestione delle versioni dei file, la ricerca dei file sulla rete IPFS e molto altro ancora.

7.6 Approfondimento Cryptokitties (ERC721)

Informatica

● Hard

CryptoKitties è un gioco basato su blockchain in cui gli utenti possono acquistare, scambiare e allevare gattini virtuali unici, chiamati "CryptoKitties". La piattaforma è costruita su Ethereum, una blockchain che consente la creazione di smart contract, ovvero programmi eseguiti sulla blockchain.



Lo smart contract di CryptoKitties è responsabile della gestione delle transazioni di acquisto, vendita e riproduzione di CryptoKitties. Quando un utente acquista o vende un CryptoKitty, il contratto intelligente esegue automaticamente la transazione e si occupa di trasferire i fondi e la proprietà del gattino.

Inoltre, il contratto intelligente di CryptoKitties utilizza un sistema di generazione di numeri casuali per determinare le caratteristiche uniche di ogni CryptoKitty. Questo sistema è fondamentale per assicurare l'unicità di ogni gattino e impedire la creazione di duplicati.

Il contratto intelligente di CryptoKitties è stato scritto in Solidity, il linguaggio di programmazione utilizzato per creare smart contract su Ethereum. Esso definisce la struttura e la logica del gioco, come la creazione di nuovi gattini, il calcolo dei prezzi di vendita e riproduzione, e la gestione delle proprietà dei gattini. Inoltre, il contratto intelligente include meccanismi di sicurezza per garantire che le transazioni vengano eseguite correttamente e senza frodi.

Elemento	Descrizione
Nome	CryptoKitties
Simbolo	Non ha un simbolo ufficiale
Tipo di Token	Non è un token, ma un'applicazione decentralizzata basata su Ethereum
Valore	Il valore di ogni gatto è determinato dalla domanda del mercato
Backing	Non è supportato da riserve, ma da una comunità attiva di utenti
Tipo di blockchain	Basato su Ethereum
Obiettivo	Creare e scambiare gatti digitali unici e rari utilizzando la tecnologia blockchain
Regolamentazione	Soggetto alla normativa sui digital assets in diversi paesi
Trasparenza	Trasparente per quanto riguarda la creazione e la proprietà dei gatti, ma non per i guadagni degli sviluppatori
Fungibilità	I gatti CryptoKitties non sono intercambiabili in modo diretto con altri token
Accettazione	Accettati solo in piattaforme di trading crittografiche e tra utenti che desiderano scambiare i loro gatti

I blocchi logici di uno smart contract o più smart contracts di dApps di gaming come CryptoKitties con gli NFT possono essere implementati in Solidity utilizzando diverse funzioni e strutture dati. Questi contratti potrebbero includere le seguenti funzioni:

- Una funzione **per la creazione di un nuovo gatto NFT**, che richiede diversi parametri come il nome del gatto, il colore, la rarità e altri attributi. Questa funzione dovrebbe generare un ID univoco per il gatto e aggiungerlo alla lista dei gatti NFT. Il contratto includerà una funzione **mint** che consente agli utenti di creare un nuovo CryptoKitty specificando il nome e il destinatario dell'NFT.
- Una funzione per la vendita di un gatto NFT, che **permette ai proprietari dei gatti di metterli in vendita sulla piattaforma**. Questa funzione dovrebbe gestire il prezzo di vendita del gatto e le transazioni monetarie tra il venditore e l'acquirente.
- Una funzione per l'acquisto di un gatto NFT, che permette **agli utenti di acquistare i gatti messi in vendita dagli altri utenti**. Questa funzione dovrebbe gestire il prezzo di acquisto del gatto e le transazioni monetarie tra l'acquirente e il venditore.
- Una funzione per la visualizzazione dei gatti NFT, che permette agli utenti di visualizzare i propri gatti e quelli degli altri utenti sulla piattaforma, **recuperando le informazioni sopra IPFS o altri database dove vengono inseriti i metadati**. Questa funzione dovrebbe gestire la ricerca e la visualizzazione dei gatti sulla base di diversi criteri come la rarità, il colore, il nome e altri attributi.
- Una funzione per la gestione delle autorizzazioni di accesso ai gatti NFT, **che permette ai proprietari dei gatti di concedere o revocare l'accesso ad altri utenti sulla base di determinate condizioni**.
- Una funzione per la gestione dei pagamenti per l'accesso ai gatti NFT, che **permette ai proprietari dei gatti di impostare un prezzo per l'accesso ai loro personaggi e di ricevere pagamenti in digital assets o in altre valute**.
- Una funzione per la gestione degli eventi, che permette agli utenti **di creare eventi in-game come tornei, sfide, battaglie e altro ancora**. Questa funzione dovrebbe gestire la registrazione degli utenti all'evento, il pagamento delle quote di partecipazione e la distribuzione dei premi.

Fonti

- Steinmetz, R., Wehrle, S. (2012). Peer-to-Peer Systems and Applications. Springer.
- Shen, X., Yu, H. (2010: Handbook of Peer-to-Peer Networking. Springer.
- Khalaf, R., Kotz, D. (2005). Peer-to-Peer Computing: The Evolution of a Disruptive Technology.
- Oram, A., Rosenblatt, B. (2001). Peer-to-Peer: Harnessing the Power of Disruptive Technologies

Capitolo 4

COSTRUIRE SUL WE³



Introduzione

Il quarto capitolo ha come principale obiettivo formativo quello di aiutare il lettore a creare una matrice decisionale completa da utilizzare durante il processo di analisi e di progettazione di una applicazione decentralizzata o un servizio di finanza sul Web3, sopra una rete come Bitcoin, Ethereum o altre reti simili.

Il secondo obiettivo formativo è quello di illustrare alcuni dei problemi relativi ai protocolli come Bitcoin ed Ethereum, come scalabilità, privacy e interoperabilità, e quali sono, ad oggi, le soluzioni e/o alternative proposte dalle aziende sul mercato. Inoltre, verrà analizzata in maniera approfondita l'importanza della gestione del nodo all'interno di un network e l'importanza della gestione di chiavi private da parte di un utente, con alcuni riferimenti a modelli di business applicabili per queste attività sostanziali.

Il capitolo inizia con alcune considerazioni preliminari che un qualsiasi sviluppatore, project manager o in generale un team, deve porsi prima di progettare una soluzione finanziaria all'interno del Web3. Successivamente si approfondiranno nel dettaglio alcune soluzioni sul mercato utilizzate per garantire la scalabilità sociale, l'interoperabilità con il Web3, e la sicurezza tecnologica per le soluzioni globali.

All'interno del testo, verranno raccontati alcuni esempi di progetti, utili per comprendere alcune applicazioni secondarie delle blockchain e dei DLT come la notarizzazione, la supply chain e il metaverso, insieme ad una breve analisi sui rischi e sui paradossi tecnologicamente riscontrabili.

In sintesi, il capitolo è composto da 8 macro-blocchi e 49 blocchi formativi, creati per aiutare il lettore a comprendere la complessità del web e quali possibili considerazioni bisogna fare per sviluppare una applicazione decentralizzata.

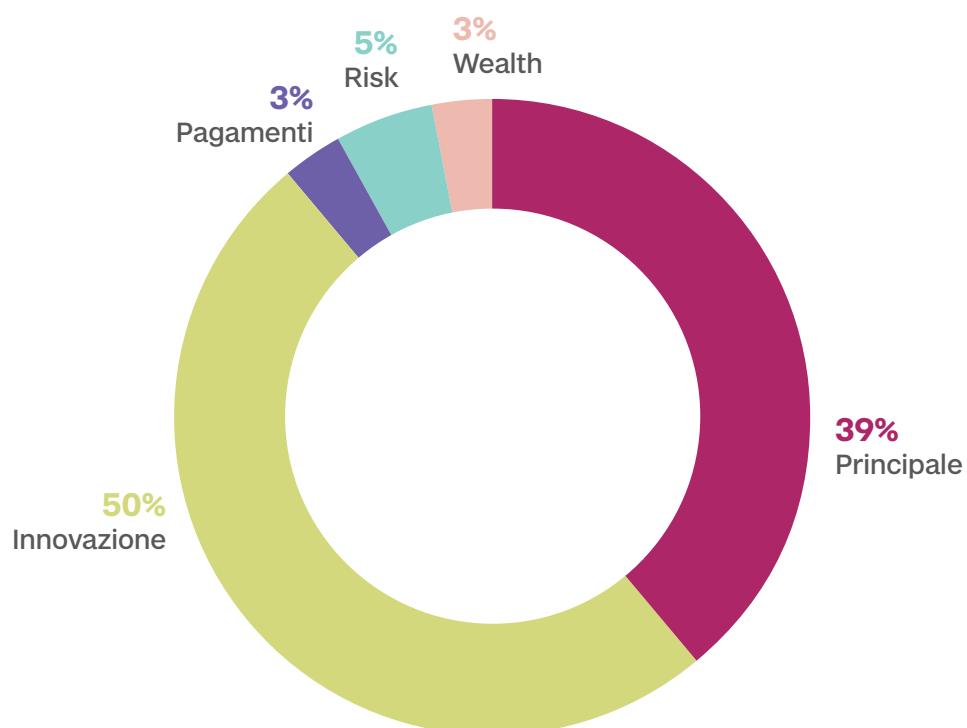
Queste alcune domande a cui cercheremo di rispondere:

- Quali sono i criteri da considerare nella scelta del network per un'azienda o una startup?
- Quali sono i tipi di attacchi informatici che possono colpire un network decentralizzato?
- Come il modello di governance può impattare sul business model di una applicazione Web3?
- Come viene gestito il nodo e quali sono i servizi offerti attraverso l'analisi dei dati della rete?
- Come vengono gestite le chiavi private e quali possono essere le best practice per un operatore di questo servizio?
- Come influisce la gestione e la dimensione del nodo sulla scalabilità e la sicurezza del network?
- Quali sono le soluzioni per la scalabilità del mercato e come vengono implementate e quali opportunità possono offrire all'industria
- In che modo la interoperabilità tra Web3 e Web2 può favorire lo sviluppo di nuove applicazioni?

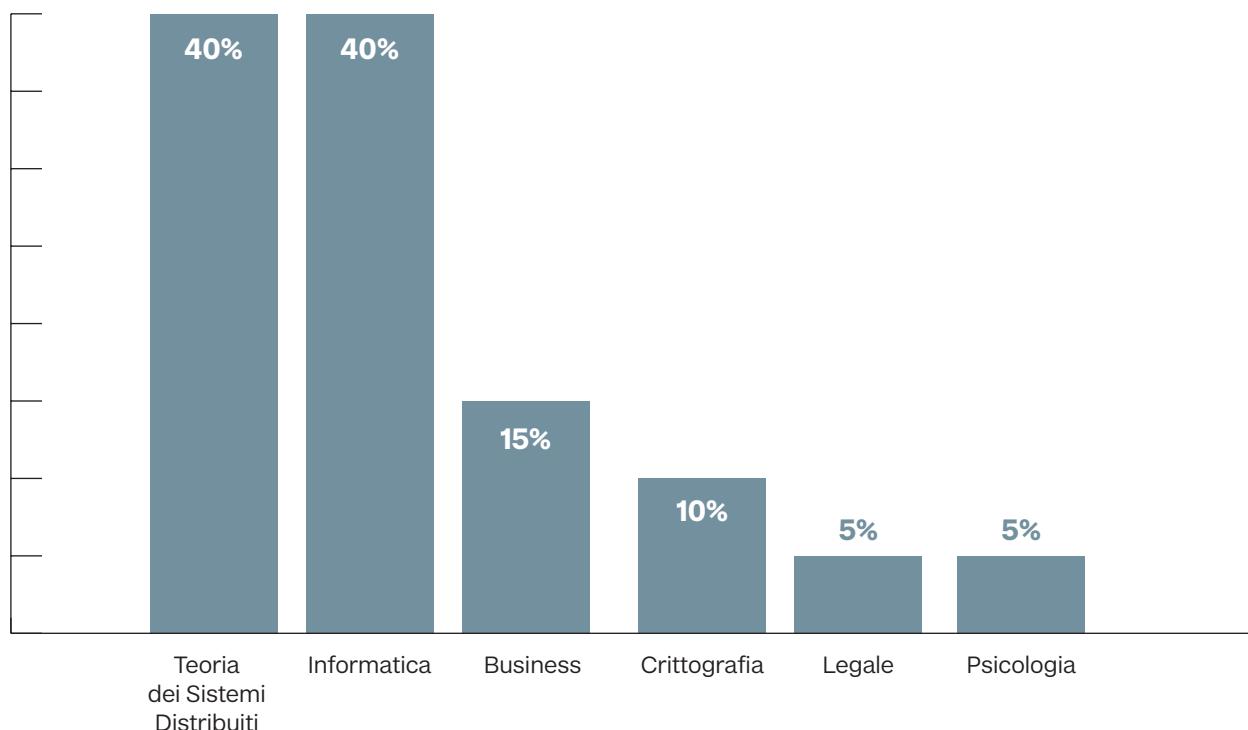
Per poi approfondire con domande più in profondità come:

- Quali sono le tecniche per garantire una privacy maggiore nelle transazioni su Bitcoin ed Ethereum?
- Come possono essere utilizzati i dati pubblici dei network blockchain come trigger per applicazioni Web2 e viceversa?
- Qual è il ruolo dei token nei modelli di business del metaverso e come sono utilizzati per generare revenue?
- In che modo la gamification è utilizzata nel Web3 e come si collega al mondo del gaming?
- Qual è il ruolo dei sistemi di trustless timestamp sulla blockchain e quali limiti possono avere?
- Come la supply chain può beneficiare dell'utilizzo della blockchain e quali sono le sfide principali da affrontare?
- Come si possono creare dei contratti bancari direttamente con il linguaggio di programmazione di uno smart contract?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. Da dove parto a costruire nel Web3?

- 1.1 Come faccio a scegliere una rete su cui costruire?
- 1.2 Quali sono gli attacchi informatici di una rete peer to peer?
- 1.3 Perché i progetti aperti possono aiutare l'economia di rete?

DIFFICOLTÀ	DISCIPLINA	PERCORSO
●	Business	Principale
●	Informatica	Innovazione Risk
●	Business/Informatica	Principale

2. Chi gestisce il nodo e le informazioni?

- 2.1 Come viene gestito un full node?
- 2.2 Quali sono le modalità di gestione delle chiavi private?
- 2.3 Che cosa si intende per analisi dei dati sulla blockchain?
- 2.4 Come si possono creare dei business model con i dati?
- 2.5 Neutrino e il caso Coinbase
- 2.6 La gestione dei server per il mining e per lo staking pool
- 2.7 Ethereum Name Service con IPFS

●	Teoria Sistemi Distr.	Innovazione Risk
●	Crittografia	Innovazione Risk
●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Pagamenti Wealth
●	Legale	Principale
●	Teoria Sistemi Distr.	Innovazione Risk
●	Informatica	Innovazione

3. Scalabilità

- 3.1 I problemi della dimensione del blocco e l'introduzione del secondo livello
- 3.2 Il trilemma dei sistemi P2P ed il CAP Theorem
- 3.3 Le soluzioni di secondo livello nel mercato Web3
- 3.4 I modelli di consenso nelle soluzioni di secondo livello
- 3.5 Approfondimento LN su Bitcoin (payment contract)
- 3.6 Approfondimento Abstraction (smart contract wallet e bundle)
- 3.7 Approfondimento Arbitrum (roll up)
- 3.8 Il secondo livello Base dentro l'exchange di Coinbase

●	Teoria Sistemi Distr.	Principale
●	Teoria Sistemi Distr.	Innovazione Risk
●	Teo. Sist. Distr./Busin.	Innovazione
●	Teoria Sistemi Distr.	Innovazione
●	Teoria Sistemi Distr./ Informatica	Innovazione Pagamenti
●	Teoria Sistemi Distr./ Informatica	Innovazione Pagamenti
●	Teoria Sistemi Distr./ Informatica	Innovazione Pagamenti
●	Teoria Sistemi Distr./ Business	Innovazione Pagamenti

4. Privacy

- 4.1 Che valore ha la privacy per gli utenti del Web3?
- 4.2 Che cos'è un protocollo di mixing?
- 4.3 Approfondimento protocollo di mixing su Ethereum:
Tornado Cash

●	Crittografia	Principale
●	Crittografia	Innovazione Risk
●	Informatica	Innovazione Risk

4.4 Il caso Tornado Cash in USA

● Legale Principale
5. Interoperabilità

- | | | | |
|--|--------------------------------------|-------------|-------------|
| 5.1 Perchè è importante l'interoperabilità tra Web2 e Web3? | ● | Informatica | Principale |
| 5.2 Cosa sono i trigger e gli oracoli? | ● | Informatica | Innovazione |
| 5.3 Come possono interagire i protocolli Web3 tra di loro? | ● | Informatica | Innovazione |
| 5.4 Approfondimento libreria WEB3.JS | ● | Informatica | Innovazione |
| 5.5 Cos'è la compatibilità EVM? | ● | Informatica | Innovazione |
| 5.6 Come funziona uno scambio atomico (Atomic Swap) tra due reti? | ● | Informatica | Innovazione |
| 5.7 Perchè gli Atomic swap possono offrire sicurezza nella finanza decentralizzata? | ● | Informatica | Innovazione |
| 5.8 Perchè gli Atomic swap possono essere una vulnerabilità nella finanza decentralizzata? | ● | Informatica | Innovazione |
| 5.9 Approfondimento Atomic Swap su Ethereum | ● | Informatica | Innovazione |
| 5.10 Che cosa si intende per Wrapped Token? | ● | Informatica | Innovazione |

6. Cosa posso salvare sulla blockchain?

- | | | | |
|---|--------------------------------------|---------------------|-------------|
| 6.1 Come funziona la notarizzazione su una rete peer to peer come Bitcoin? | ● | Crittografia/Legale | Innovazione |
| 6.2 Approfondimento sulla marcatura temporale senza permessi (trustless timestamping) | ● | Informatica | Innovazione |
| 6.3 I paradossi della blockchain nella supply chain | ● | Business | Principale |
| 6.4 Il caso di IBM Merks | ● | Business | Principale |
| 6.5 Come si possono scrivere degli Smart Legal Contract? | ● | Informatica/Legale | Innovazione |
| 6.6 Decreto semplificazioni e lo stallo dell'Agid | ● | Legale | Principale |

7. Metaverso

- | | | | |
|---|--------------------------------------|---------------------|------------|
| 7.1 La gamification nel Web3 | ● | Business | Principale |
| 7.2 Dal gaming al metaverso | ● | Business | Principale |
| 7.3 L'architettura del metaverso | ● | Informatica | Principale |
| 7.4 Tokenomics di un metaverso | ● | Business | Principale |
| 7.5 Come funziona il modello play to earn? | ● | Psicologia/Business | Principale |
| 7.6 Industrie correlate ed i rischi nella realtà virtuale | ● | Psicologia/Business | Principale |

8. Identità digitale

- | | | | |
|---|--------------------------------------|----------------------|------------|
| 8.1 La dematerializzazione del portafoglio | ● | Filosofia digitale | Principale |
| 8.2 Gli attori e i modelli di gestione dell'identità digitale | ● | Informatica | Principale |
| 8.3 La sovranità della propria identità digitale | ● | Filosofia digitale | Principale |
| 8.4 Il paradigma Self-Sovereign Identity | ● | Informatica | Principale |
| 8.5 Singolo wallet o due wallet per identità e denaro? | ● | Business/Informatica | Principale |

1

Da dove parto a costruire nel Web3?

- 1.1 Come faccio a scegliere una rete su cui costruire?
- 1.2 Quali sono gli attacchi informatici di una rete peer to peer?
- 1.3 Perché i progetti aperti possono aiutare l'economia di rete?

1.1

Business

● Basic

Come faccio a scegliere una rete su cui costruire?

La scelta di una rete programmabile per sviluppare una dApp è una decisione importante perché ci sono molte opzioni tra cui scegliere e ogni opzione ha i suoi pro e contro. Tra i fattori da considerare ci sono:

- i modelli di governance della rete
- la scalabilità sociale
- la tecnologica della rete
- lo scopo del progetto.

I **modelli di governance** si riferiscono alla **struttura di potere e decisionale all'interno del network**. I modelli centralizzati, in cui l'autorità centrale prende le decisioni, possono essere più efficienti ma anche meno trasparenti e vulnerabili ai problemi di sicurezza. Al contrario, i modelli decentralizzati, in cui il potere decisionale è distribuito tra gli utenti del network, possono essere più sicuri e trasparenti ma anche molto più complessi.

La **social scalability** si riferisce alla **capacità del network di crescere e adattarsi al cambiamento senza compromettere le prestazioni o la sicurezza**. Una buona social scalability richiede un'architettura flessibile e la capacità di adottare rapidamente nuove tecnologie e protocolli. Inoltre, una buona social scalability facilita l'effetto network, aiutando la crescita degli utenti all'interno dell'applicazione.

La **scalabilità tecnica** si riferisce alla capacità del network di **elaborare un gran numero di transazioni in modo rapido ed efficiente**. Una buona scalabilità tecnica richiede un'infrastruttura solida e la capacità di adattarsi alle esigenze degli utenti in rapida crescita.

Tuttavia, la scelta più importante è chiaramente quella relativa al *purpose* dell'applicazione che vogliamo costruire. Il **purpose** di una specifica dApp si riferisce all'**obiettivo per cui la dApp è stata creata**. Ad esempio, se la dApp è destinata al settore finanziario, la sicurezza e la trasparenza possono essere particolarmente importanti, se invece la dApp è destinata al settore dei giochi, la scalabilità e la flessibilità dovrebbero essere prioritari. In generale, la scelta del network si basa sull'obiettivo della dApp stessa e dalle sue esigenze specifiche.

In questa tabella vengono riassunti i pro e contro rispetto alla scelta di utilizzare una rete programmabile aperta e senza permessi:

Concetto	Descrizione	Pro	Contro
Purpose del progetto dApps	<i>Lo scopo principale di un progetto dApps è quello di creare una piattaforma decentralizzata che consenta agli utenti di accedere a servizi e applicazioni in modo sicuro, trasparente e privato.</i>	<i>Offre un ambiente sicuro e privato per l'elaborazione dei dati.</i>	<i>Le applicazioni decentralizzate sono ancora in fase sperimentale, quindi potrebbero non essere completamente affidabili.</i>
Social Scalability	<i>La capacità di una dApps di crescere e adattarsi ad una vasta gamma di utenti senza compromettere l'efficienza e la sicurezza.</i>	<i>La scalabilità sociale può consentire ad un gran numero di utenti di accedere alla piattaforma.</i>	<i>La scalabilità sociale richiede un grande investimento in infrastrutture per supportare un gran numero di utenti.</i>
Scalabilità tecnica	<i>La capacità di una dApps di elaborare grandi quantità di transazioni e dati in modo efficiente e affidabile.</i>	<i>La scalabilità tecnica può consentire alla piattaforma di supportare un gran numero di transazioni.</i>	<i>La scalabilità tecnica richiede una notevole quantità di risorse di elaborazione e archiviazione.</i>

In questa tabella sono presenti alcuni dei parametri che possono essere utilizzati per confrontare le diverse piattaforme come la tipologia di rete (con permessi e senza permessi), la velocità delle transazioni, il linguaggio di programmazione e altri parametri utili per analizzare e scegliere il network giusto per l'applicazione giusta.

Piattaforma	Anno di lancio	Tipo di Consenso	Linguaggio di programmazione	Scalabilità	Smart Contract	Privacy	Flessibilità
Bitcoin	2009	Proof of Work	C++	Bassa	Limitati	Bassa	Bassa
Ethereum	2015	Proof of Stake	Solidity	Media	Completi	Bassa	Media
Algorand	2019	Pure Proof of Stake	Java, Go	Elevata	Completi	Media	Media
Hyperledger Fabric	2017	Consenso basato su ordine	Go	Elevata	Limitati	Elevata	Elevata
Corda	2016	Consenso basato su validità	Java	Elevata	Completi	Elevata	Media
Quorum	2016	Proof of Authority	Solidity	Elevata	Completi	Elevata	Media

1.2

Informatica

• Medium

Quali sono gli attacchi informatici di una rete peer to peer?

Ogni network, prima di essere scelto, deve avere un grado di sicurezza elevato per garantire la continuità di servizio nel lungo periodo. Da notare come una rete peer to peer come Bitcoin ha quasi un 100% di continuità di servizio dal 2009 al 2023, contando pochissimi momenti di **downtime**.



Downtime

Definizione: Periodo morto, o momento in cui una macchina come un computer non funziona o non è operativo.

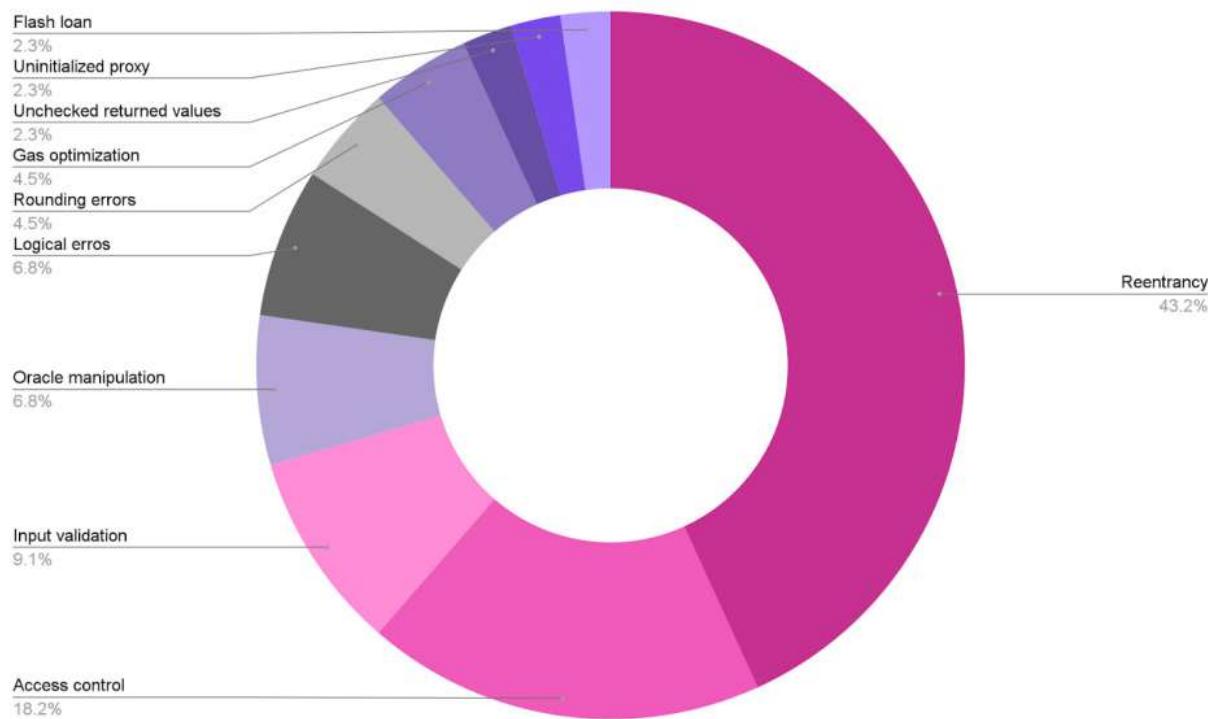
Fonte: <https://www.collinsdictionary.com/it/dizionario/inglese/downtime>

Tuttavia, un sistema distribuito può essere vulnerabile ad una serie di attacchi, tra cui:

- **Attacco al 51%**: questo è un tipo di attacco dove un soggetto controlla oltre il 50% della potenza di calcolo della rete. Ciò consente all'**attaccante di controllare la maggioranza delle conferme delle transazioni e di manipolare la blockchain a proprio vantaggio**.
- **Attacco DDoS** (Distributed Denial of Service): questo è un tipo di **attacco che mira a rendere inaccessibile un servizio online inviando una quantità eccessiva di richieste al sistema, sovraccaricandolo**. Questo tipo di attacco può essere lanciato da molte fonti diverse, rendendolo difficile da identificare e causando in conseguenza problemi nella protezione contro di esso.
- **Attacco di re-spending**: questo è un tipo di attacco in cui un **attaccante tenta di spendere la stessa moneta digitale due volte**. Questo può essere fatto manipolando la blockchain per far credere che una transazione non sia stata confermata o facendo una copia della transazione originale.
- **Attacco Sybil**: questo è un tipo di attacco in cui un **soggetto crea molte identità false sulla rete per influire sul voto o sulla decisione del sistema**.
- **Attacco alla privacy**: questo è un tipo di attacco in cui un **soggetto cerca di raccogliere informazioni riservate sugli utenti del sistema**, ad esempio tramite analisi dei dati delle transazioni.
- **Attacco di race condition**: questo è un tipo di attacco che **sfrutta la concorrenza tra transazioni per manipolare il sistema**. Ad esempio, un attaccante può inviare due transazioni in rapida successione che dipendono l'una dall'altra e sfruttare la concorrenza per eseguire la transazione in un ordine specifico.
- **Attacco di replay**: questo è un tipo di attacco in cui un **soggetto copia e riutilizza una transazione valida sulla stessa o su una blockchain diversa**. Questo può causare la duplicazione delle transazioni o il trasferimento non autorizzato di fondi.
- **Attacco di “nothing at stake”**: questo è un tipo di attacco che **sfrutta la natura proof-of-stake di alcune blockchain**. Un attaccante può creare molte identità e utilizzare la loro potenza di calcolo per votare per diverse catene allo stesso tempo, influendo sulla decisione del sistema.
- **Attacco di front-running**: questo è un tipo di attacco in cui un **soggetto utilizza informazioni sulle transazioni in corso per trarre vantaggio sul mercato**. Ad esempio, un attaccante potrebbe acquistare un asset prima che un ordine di acquisto di grandi dimensioni influenzi il prezzo.
- **Attacco di Phishing**: questo è un tipo di attacco in cui un **soggetto crea un sito falso, all'apparenza legittimo, per convincere gli utenti a condividere le loro informazioni private, come le credenziali di accesso**.

Questi sono solo alcuni esempi degli attacchi che possono essere eseguiti su un sistema distribuito. È importante che i progetti di blockchain adottino misure di sicurezza adeguate a proteggere contro questi attacchi e garantire l'integrità e la sicurezza della rete.

Inoltre, se consideriamo anche gli attacchi relativi agli errori sugli smart contract, la lista di potenziali vulnerabilità di un'applicazione decentralizzata aumenta in larga misura. Qui una tabella dove viene riportato il numero di attacchi avvenuti all'interno l'industria del Web3.



La maggior parte degli sviluppatori intervistati menzionano, all'interno del Report di Immunefy, la reentrancy (43,2%) come la più comune vulnerabilità che incontrano durante la revisione del codice di uno smart contract, seguita dal controllo degli accessi (18,2%). Altre vulnerabilità menzionate includono la convalida dell'input (9,1%), Oracle manipolazione (6,8%) ed errori logici (6,8%). Errori di arrotondamento (4,5%), gas ottimizzazione (4,5%), valori restituiti non controllati (2,3%), proxy non inizializzato (2,3%) e prestito flash (2,3%).

1.3

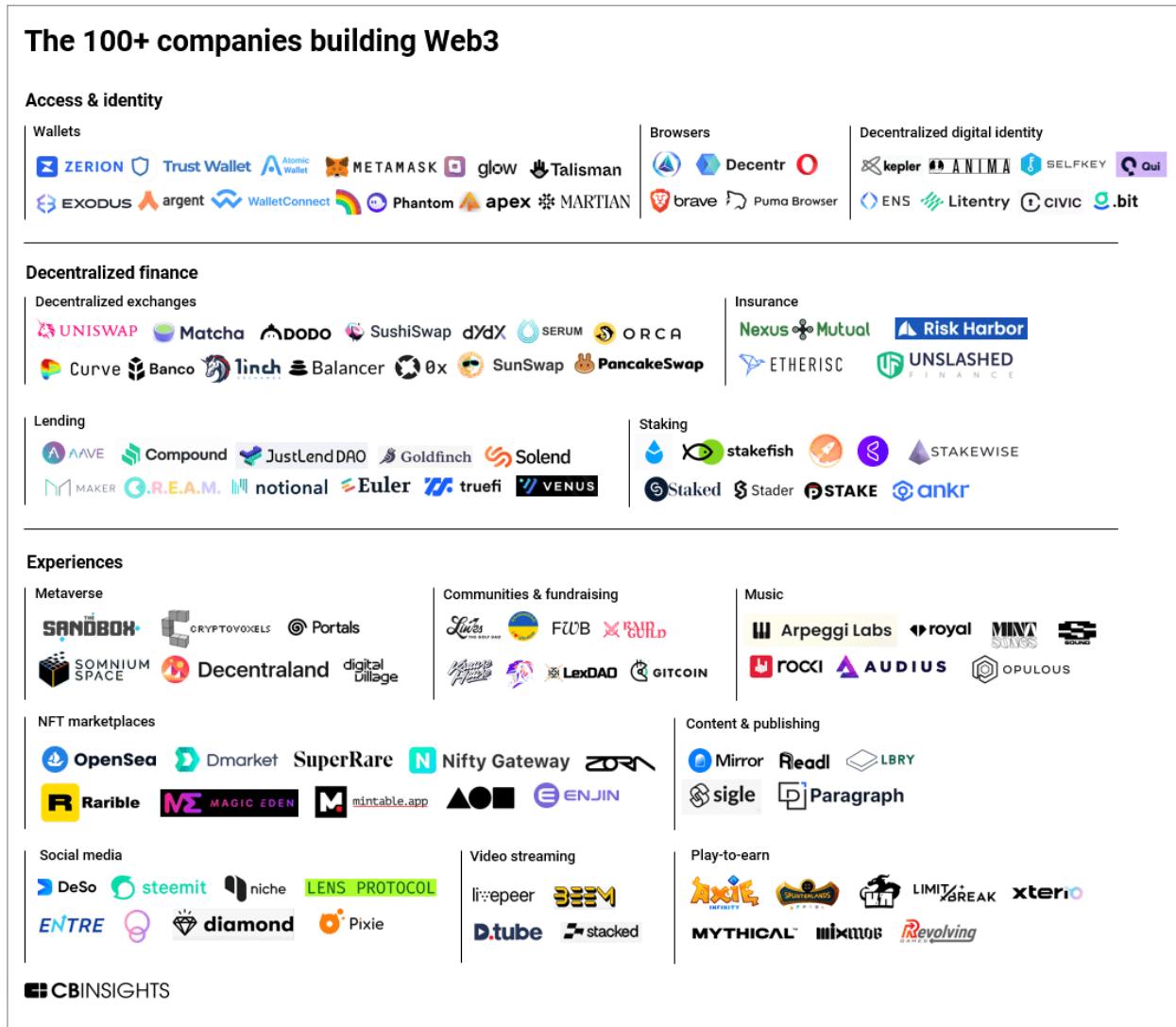
Perché i progetti aperti possono aiutare l'economia di rete?

Business / Informatica

● Basic

Negli anni 2000, con la crescita di internet e la diffusione del Web2, l'**apertura e la libertà sono due condizioni sempre più importanti per gli utenti e le loro esigenze**.

Secondo un rapporto di We Are Social e Hootsuite del 2022, gli **utenti di internet nel mondo hanno superato i 4.9 miliardi**, con una penetrazione globale del 62,5%. Inoltre, il 58,4% della popolazione mondiale utilizza i social media, con una media di 2 ore e 25 minuti spese sui social media ogni giorno.



Questi dati dimostrano l'enorme impatto del Web2 e della scalabilità sociale di internet sulla società e sull'economia globale. La richiesta di servizi e informazioni aperti e condivisi è diventata sempre più importante per gli utenti, e ciò ha portato all'**emergere di nuove aziende e modelli di business basati sull'apertura e sulla condivisione**.

Ad esempio, piattaforme come **Wikipedia, GitHub e Reddit sono diventate molto popolari grazie alla loro natura open source e alla condivisione di conoscenze e informazioni**. Allo stesso tempo, le piattaforme social come Facebook, Twitter e Instagram hanno permesso agli utenti di connettersi con altre persone e di condividere le loro esperienze e idee in modo aperto e condiviso.

La scalabilità sociale di internet si riferisce alla sua capacità di crescere e adattarsi alle esigenze degli utenti senza compromettere l'accesso o la qualità del servizio. Questa caratteristica è stata particolarmente importante per la diffusione del **Web2, che ha introdotto l'idea di un web aperto**.

Questa libertà ha portato alla nascita di una vasta gamma di servizi e applicazioni, nonché alla creazione di comunità online dinamiche e globali.

La richiesta di servizi e informazioni aperti e condivisi è stata quindi una tendenza importante nel mondo digitale degli anni 2000, che ha portato alla creazione di nuove piattaforme e modelli di business basati sull'apertura e sulla condivisione. Ciò ha quasi eliminato il concetto di "internet privato" e ha reso la scalabilità sociale di internet un fattore cruciale per il successo delle aziende e delle piattaforme digitali.

2

Chi gestisce il nodo e le informazioni?

- 2.1 Come viene gestito un full node?
- 2.2 Quali sono le modalità di gestione delle chiavi private?
- 2.3 Che cosa si intende per analisi dei dati sulla blockchain?
- 2.4 Come si possono creare dei business model con i dati?
- 2.5 Neutrino e il caso Coinbase
- 2.6 La gestione dei server per il mining e per lo staking pool
- 2.7 Ethereum Name Service con IPFS

2.1

Teoria dei sistemi distribuiti

• Medium

Come viene gestito un full node?

Ethereum e Bitcoin sono basati su una rete distribuita, dove i nodi della rete condividono e validano le transazioni. **Gestire un nodo sulla rete Ethereum o Bitcoin significa ospitare e mantenere un'istanza del software del nodo che connette il tuo computer alla rete.**



Per i più esperti è possibile creare in casa un full node, scaricando un software come Bitcoin Core e scaricare anche l'intera blockchain, rimanendo collegato al network. In questo caso vediamo un Raspberry che contiene, al suo interno, un nodo Bitcoin, a sua volta contenente un nodo di **Lightning Network** e uno di Tor. Tuttavia, il mantenimento e la gestione di un nodo implicano di avere condizioni sempre favorevoli in termini di banda e di memoria.



Lightning Network

Definizione: Il Lightning Network è una rete di nodi decentralizzata che permette di inviare un numero potenzialmente illimitato di transazioni istantaneamente.

Questa rete è parallela alla blockchain di Bitcoin, ed esegue alcune transazioni sulla blockchain e altre off-chain.

Fonte: <https://academy.youngplatform.com/blockchain/lightning-network-bitcoin/#:~:text=Il%20Lightning%20Network%20%C3%A8%20una,blockchain%20e%20altre%20off%2Dchain>

Un **servizio di gestione del nodo** può aiutare a semplificare questo processo, offrendo funzionalità come un esploratore di blocchi e una query per risorse specifiche. Ecco una tabella concettuale riasuntiva:

Funzionalità	Ethereum	Bitcoin
Esploratore di blocchi	Etherscan, Blockchair	Blockchain.info, Blockcypher
Query per risorse	Infura, Alchemy	Bitcore, Blockstream
Monitoraggio	CoinTracking, Delta	Blockfolio, Bitcoin Ticker Widget

La gestione di un full node permette inoltre di creare dei servizi come:

- **l'esploratore di blocchi, un sito web o un'applicazione che fornisce una visualizzazione delle transazioni e dei blocchi sulla rete.** Consente di accedere a informazioni come il saldo di un indirizzo, le transazioni in sospeso e le conferme di transazioni.
- La **query per risorse, che permette di accedere ai dati sulla blockchain**, come il bilancio di un indirizzo, il contenuto di un blocco e lo stato attuale della rete. Questo può essere fatto utilizzando un'API fornita da un servizio di gestione del nodo.
- Infine, il **monitoraggio può aiutare ad osservare le tendenze di mercato e le attività sulla blockchain**. Esistono diversi servizi di monitoraggio per entrambe le reti, che possono fornire dati come il volume degli scambi, la capitalizzazione di mercato e altro ancora.

Per esempio, Infura è un servizio cloud di infrastruttura blockchain che offre un'API (Application Programming Interface) semplificata per l'accesso alle informazioni contenute all'interno di Ethereum e ad altre piattaforme EVM compatibili. In pratica, **Infura fornisce un'interfaccia semplificata per la connessione alle reti blockchain senza dover gestire l'infrastruttura sottostante**, come i nodi di Ethereum, che richiedono una configurazione e una manutenzione costante. Questo servizio offre anche una soluzione enterprise per la connessione ad Ethereum e ad altre reti blockchain, con funzionalità come il bilanciamento del carico, la ridondanza e la scalabilità automatica.

Infura è stato fondato nel 2016 ed è diventato un servizio molto popolare tra gli sviluppatori di applicazioni decentralizzate (dApps) e le organizzazioni che desiderano interagire con le reti blockchain senza dover gestire l'infrastruttura sottostante.

Dall'altro canto, **la gestione dei nodi rappresenta una sfida in termini di decentralizzazione della rete**. Per esempio, i servizi cloud sono offerti da provider centralizzati, e conseguentemente, l'infrastruttura di rete può essere considerata meno distribuita rispetto ad altre reti peer-to-peer. In questo contesto, la centralizzazione si riferisce al fatto che tutti i nodi della rete non sono distribuiti in modo uniforme ma si concentrano in poche mani, ovvero in quelle delle grandi aziende che offrono i servizi cloud.

Ciò può **creare una serie di problemi, tra cui la possibilità che i nodi siano vulnerabili agli attacchi informatici o che i dati sensibili vengano esposti a rischi di sicurezza**. Inoltre, l'infrastruttura centralizzata può rendere la rete vulnerabile a interruzioni di servizio o a eventuali problemi di manutenzione.

2.2

Crittografia

• Hard

Quali sono le modalità di gestione delle chiavi private?

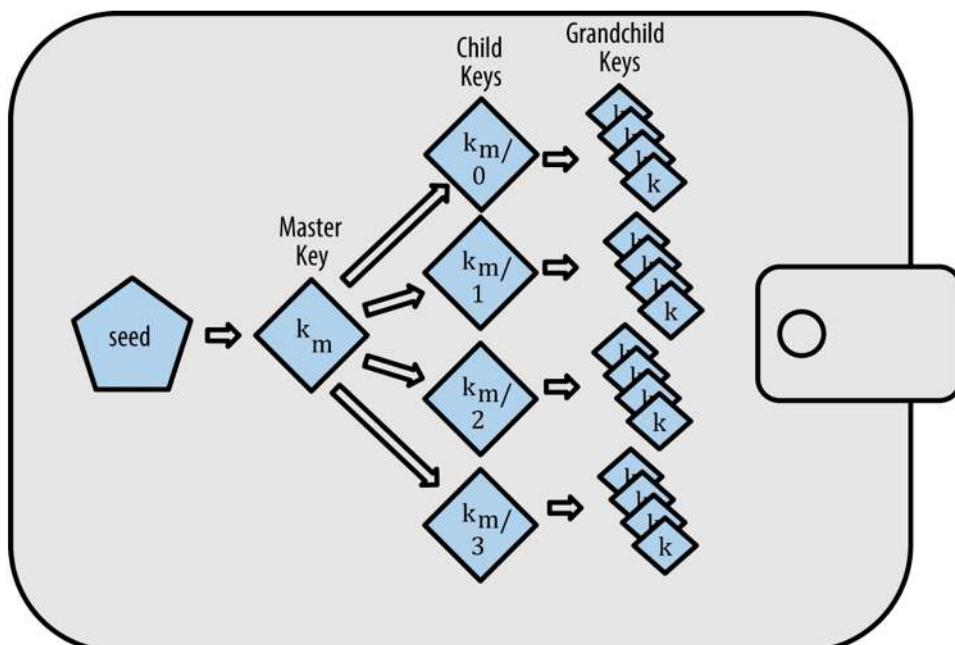
La **gerarchia delle chiavi** è un concetto crittografico fondamentale utilizzato dai **wallet di digital assets** per garantire la sicurezza dei fondi e può essere rappresentata in modo schematico attraverso una tabella concettuale. Qui di seguito ne proponiamo una:

Gerarchia delle chiavi	Descrizione
Seed	Un seed (seme) è una sequenza di parole che viene generata casualmente e viene utilizzata per generare tutte le chiavi del wallet. Il seed è la radice della gerarchia delle chiavi e può essere utilizzato per ripristinare il wallet in caso di perdita o malfunzionamento.
Master key	Il master key (chiave principale) è una chiave privata che viene generata dal seed. Il master key è utilizzato per generare tutte le chiavi figlie del wallet e può essere utilizzato per creare backup del wallet o per importare il wallet in altre applicazioni.
Chiavi figlie	Le chiavi figlie sono le chiavi che vengono generate dal master key. Le chiavi figlie possono essere di diversi tipi, come ad esempio chiavi di pagamento, chiavi di cambio o chiavi di autorizzazione. Le chiavi figlie possono essere utilizzate per firmare transazioni, ricevere pagamenti o effettuare altre operazioni all'interno del wallet. Le chiavi figlie possono anche essere generate in modo gerarchico, creando così una struttura ad albero delle chiavi all'interno del wallet.

Il processo di generazione delle chiavi avviene nel seguente modo:

1. In una gerarchia di chiavi, viene **generato un “seed”** (o seme) casuale, che viene utilizzato come punto di partenza per generare tutte le altre chiavi. Il seed deve essere gestito con cura, poiché rappresenta il punto di accesso a tutti i fondi del wallet.
2. A partire dal seed, viene **generata una “master key”** (o chiave principale), che viene utilizzata per generare tutte le altre chiavi figlie. La master key è una chiave crittografica privata che viene utilizzata per firmare le transazioni e autorizzare l'invio dei fondi.
3. A sua volta, la **master key può essere utilizzata per generare altre chiavi figlie, che possono essere a loro volta utilizzate per gestire diversi aspetti del wallet**. Ad esempio, una custodia di digital assets può utilizzare una chiave figlia per la multi-firma (ovvero la firma di una transazione che richiede l'autorizzazione di più chiavi), o una chiave figlia per la firma di transazioni a basso valore.
4. Ogni chiave privata figlia può essere moltiplicata con funzioni one-way per generare progressivamente chiave pubblico e indirizzo. **Questo collegamento tra chiavi e indirizzo è cruciale per garantire la sicurezza e l'integrità delle transazioni nel processo di approvazione nella rete**. Un indirizzo, per esempio nel wallet di bitcoin, è composto da 160 bit e può variare tra 27 e 34 caratteri alfanumerici.

Ogni chiave figlia può essere utilizzata per generare ulteriori chiavi figlie, creando così una gerarchia di chiavi che si estende in profondità. In questo modo, il wallet di digital assets può generare una grande quantità di chiavi figlie, ciascuna utilizzata per gestire una piccola quantità di digital assets. Questo sistema rende più sicuro il portafoglio dell'utente, in quanto la perdita o il compromesso di una chiave figlia non compromette la sicurezza delle altre.



La gerarchia delle chiavi consente quindi di separare i diversi ruoli e responsabilità all'interno della custodia di digital assets, fornendo un sistema di governance che garantisce la sicurezza dei fondi. In particolare, i ruoli e le responsabilità possono essere assegnati a chiavi figlie specifiche, che possono essere gestite separatamente e autorizzate in modo selettivo.

Ad esempio, una custodia di digital assets può utilizzare una chiave figlia per la gestione delle transazioni di basso valore, che viene utilizzata per autorizzare automaticamente tutte le transazioni inferiori a una certa soglia. Una seconda chiave figlia, gestita separatamente, può essere utilizzata per la gestione delle transazioni di alto valore, che richiedono l'autorizzazione esplicita del proprietario del wallet.

Gli exchange di digital assets utilizzano diverse modalità di gestione delle chiavi private e pubbliche all'interno della loro infrastruttura informatica, in base alle loro esigenze di sicurezza e di accessibilità. Ecco alcune delle modalità più comuni utilizzate dagli exchange:

1. **Modello segregato:** In questo modello, ogni utente ha una coppia di chiavi unica (una chiave privata e una chiave pubblica) per accedere al proprio portafogli. Le chiavi private sono memorizzate in un sistema altamente sicuro e accessibile solo ai proprietari delle chiavi. Questo modello garantisce un alto livello di sicurezza per gli utenti, in quanto le chiavi private sono protette da eventuali attacchi informatici.
2. **Omnibus account:** In questo modello, tutte le chiavi private degli utenti vengono memorizzate in un unico account. Questo modello è meno sicuro rispetto al modello segregato, in quanto in caso di attacco informatico, tutte le chiavi private degli utenti potrebbero essere compromesse. Tuttavia, questo modello semplifica la gestione degli account e riduce i costi operativi.
3. **Multisig:** In questo modello, per effettuare una transazione sono necessarie le firme digitali di più utenti, ognuno dei quali possiede una chiave privata. Questo modello garantisce un alto livello di sicurezza, poiché le chiavi private sono distribuite tra più utenti e le transazioni richiedono l'approvazione di più persone.
4. **Cold storage:** In questo modello, le chiavi private sono memorizzate offline, in un sistema altamente sicuro e protetto da eventuali attacchi informatici. Questo modello è il più sicuro, ma richiede più tempo e costi operativi per accedere alle chiavi private.

In generale, gli exchange di digital assets utilizzano una combinazione di queste modalità per garantire un alto livello di sicurezza per i propri utenti e per proteggere le chiavi private dalle minacce informatiche.

In sintesi, la gerarchia delle chiavi consente alle custodie di digital assets di gestire in modo selettivo i ruoli e le responsabilità all'interno del wallet, fornendo un sistema di governance flessibile e sicuro per la gestione dei fondi.

2.3

Teoria dei sistemi distribuiti

• Basic

Che cosa si intende per analisi dei dati sulla blockchain?

Immagina di avere un grande libro dove vengono scritte tutte le transazioni che vengono fatte con dei soldi magici chiamati digital assets. Questo libro è pubblico, quindi tutti possono leggerlo e vedere le transazioni che vengono fatte. **Uno strumento di analisi on-chain è come una lente d'ingrandimento che ti permette di guardare bene dentro questo libro e vedere tante informazioni interessanti**, come ad esempio chi ha mandato i soldi, a chi sono stati mandati, e quanto ne sono stati mandati. In questo modo, puoi capire meglio come funziona il sistema dei digital assets e fare scelte più intelligenti.

Concetto	Descrizione
Indirizzi	Gli indirizzi sono identificatori univoci utilizzati per identificare le entità all'interno della blockchain, come i wallet o i contratti. Gli indirizzi sono composti da una serie di caratteri alfanumerici e vengono generati tramite funzioni di hash crittografiche.
Montante	Il montante è la quantità di un digital asset che viene inviata o ricevuta in una transazione. Il montante viene registrato all'interno del registro della blockchain e viene utilizzato per calcolare il saldo del wallet o del contratto.
Timestamp	Il timestamp è un valore numerico che indica la data e l'ora in cui una transazione è stata aggiunta alla blockchain. Il timestamp viene utilizzato per garantire che le transazioni siano aggiunte in ordine cronologico alla blockchain.
Hash delle transazioni	L'hash delle transazioni è un valore univoco che viene calcolato mediante una funzione di hash crittografica e viene utilizzato per identificare in modo univoco una transazione all'interno della blockchain. L'hash delle transazioni viene anche utilizzato per garantire l'integrità dei dati all'interno della blockchain.
Token	Un token è un digital asset che viene emesso da un contratto sulla blockchain. I token possono essere utilizzati per rappresentare asset digitali come ad esempio titoli di proprietà, diritti d'autore o punti fedeltà.
Tipo di transazione	Il tipo di transazione indica il tipo di operazione che viene effettuata all'interno della blockchain, come ad esempio l'invio di fondi, la creazione di un contratto o l'aggiornamento di un asset.
Indirizzi del contratto	Gli indirizzi del contratto sono gli indirizzi utilizzati per identificare i contratti all'interno della blockchain. Gli indirizzi del contratto sono simili agli indirizzi del wallet, ma sono utilizzati esclusivamente per interagire con il contratto.
Signature	Il signature è un valore crittografico che viene utilizzato per garantire l'autenticità e l'integrità di una transazione. La signature viene generata utilizzando la chiave privata del mittente e viene verificata utilizzando la chiave pubblica corrispondente.
Blocco	Il blocco è un insieme di transazioni che vengono registrate sulla blockchain in modo sequenziale. Ogni blocco contiene un hash del blocco precedente, garantendo così l'integrità della blockchain. I blocchi vengono creati utilizzando algoritmi di consenso come, ad esempio, il Proof of Work (PoW) o il Proof of Stake (PoS).

I servizi di analisi on-chain sono strumenti che permettono di monitorare e analizzare l'attività che avviene sulla blockchain. Infatti, si basano sull'accesso ai dati contenuti sulla blockchain, grazie alla loro natura pubblica e trasparente. Attraverso l'utilizzo di software specifici, questi servizi raccolgono, elaborano e visualizzano informazioni sulla transazione, come ad esempio la quantità di digital assets trasferite, l'indirizzo mittente e destinatario, le commissioni pagate, e così via.

The Ethereum Blockchain Explorer interface displays various metrics and transaction details. Key information includes:

- ETHER PRICE:** \$1,883.42 @ 0.06746 BTC (-2.72%)
- MARKET CAP:** \$226,794,815,238.00
- TRANSACTIONS:** 1,943.12 M (12.4 TPS)
- MED GAS PRICE:** 34 Gwei (\$1.34)
- LAST FINALIZED BLOCK:** 17096231
- LAST SAFE BLOCK:** 17096262
- TRANSACTION HISTORY IN 14 DAYS:** A line graph showing transaction volume over time.
- Latest Blocks:**
 - Block 17096320 (10 secs ago) - Fee Recipient: 0xe...; 152 txns in 12 secs; 0.02639 Eth
 - Block 17096319 (22 secs ago) - Fee Recipient: 0x32AAA4...; 144 txns in 12 secs; 0.01753 Eth
 - Block 17096318 (34 secs ago) - Fee Recipient: Flashbots: Builder; 196 txns in 12 secs; 0.05644 Eth
 - Block 17096317 (46 secs ago) - Fee Recipient: 0x978071...; 144 txns in 12 secs; 0.01342 Eth
- Latest Transactions:**
 - From 0x2750b... To 0xdAC17F...; 0.00
 - From 0x6A4e4f... To 0xdAC17F...; 0.00
 - From 0x02cf0155147da... To 0x69B250...; 0.00
 - From 0xcdcd946d39c1f4... To 0xc2a832...; 0.01839 Eth

Alcune aziende, infatti, offrono questo servizio agli sviluppatori e ad altre aziende che vogliono sviluppatore una soluzione che fa riferimento alle tecnologie dentro il Web3 come i digital assets, la gestione delle transazioni e la blockchain. Inoltre, esistono anche dei servizi online come Etherscan, o Blockchain.info, che permettono a chiunque di guardare tutti i dati all'interno del registro distribuito.

2.4

Teoria dei sistemi distribuiti

● Medium

Come si possono creare dei business model con i dati?

I servizi di analisi on-chain possono essere utilizzati per diverse finalità, tra cui:

- **Antiriciclaggio:** molte aziende utilizzano questi servizi per monitorare l'attività sulla blockchain e **identificare eventuali transazioni sospette o illecite**, come ad esempio transazioni di grandi quantità di digital assets provenienti da fonti non identificate.
- **Commercio e investimento:** i trader e gli investitori utilizzano questi servizi per **monitorare l'andamento del mercato, analizzare le tendenze e le dinamiche dei prezzi, e identificare eventuali opportunità di investimento**.
- **Governance:** le aziende che gestiscono i digital assets o i token basati sulla blockchain utilizzano questi servizi per **monitorare l'attività sulla propria piattaforma e garantire il corretto funzionamento del sistema**.
- **Audit:** i servizi di analisi on-chain possono essere utilizzati anche per **verificare la correttezza e la trasparenza delle transazioni sulla blockchain**, e garantire la conformità alle normative e agli standard di sicurezza.
- **Momentum, volumi e costo opportunità nel network:** i trader potrebbero utilizzare l'analisi on-chain per **monitorare l'andamento del volume di scambi su Bitcoin, la quantità di Bitcoin detenuta dagli investitori a lungo termine (holder), la quantità trasferita su piattaforme di scambio e così via**. Questi dati possono fornire ai trader una migliore comprensione della domanda e dell'offerta di digital assets sul mercato e quindi aiutarli a prendere decisioni di trading più informate.

Questi dati inoltre possono essere **utilizzati per diverse attività come**, il KYC, l'AML e il trading. Tuttavia, l'utilizzo di questi dati deve essere conforme alla legge sulla privacy e alle normative in vigore nella giurisdizione pertinente. La seguente tabella elenca i dati on-chain che possono essere raccolti per la valutazione normativa, il KYC, l'AML e il trading:

Categoria di dati	Descrizione
KYC	KYC (Know Your Customer) si riferisce ai dati raccolti per identificare i clienti dei digital assets e garantire la conformità alle normative. I dati KYC possono includere il nome, l'indirizzo e l'identità del cliente.
AML	AML (Anti Money Laundering) si riferisce ai dati raccolti per prevenire il riciclaggio di denaro. I dati AML possono includere informazioni sulle transazioni, come il montante, gli indirizzi delle parti coinvolte e il tipo di transazione.
Valutazione normativa	La valutazione normativa si riferisce ai dati raccolti per verificare la conformità alle normative e alle leggi locali. I dati di valutazione normativa possono includere informazioni sulle transazioni, come il montante, gli indirizzi delle parti coinvolte e il tipo di transazione.

Trading	I dati di trading si riferiscono alle informazioni sulle transazioni di digital assets, come il prezzo, il montante e le parti coinvolte. Questi dati possono essere utilizzati per l'analisi del mercato e la valutazione del rischio.
Aziende	I dati aziendali si riferiscono alle informazioni sulle imprese coinvolte nel settore dei digital assets, come il nome, l'indirizzo, la dimensione e le attività. Questi dati possono essere utilizzati per l'analisi di mercato e la valutazione del rischio.
Depositi di garanzia fissi	I dati sui depositi di garanzia fissi si riferiscono alle informazioni sui depositi di digital assets che vengono effettuati come garanzia per una transazione. Questi dati possono essere utilizzati per la valutazione del rischio e per la determinazione del margine di profitto.
Smart contract di regolazione domanda e offerta	I dati degli smart contract di regolazione della domanda e dell'offerta si riferiscono alle informazioni sui contratti intelligenti utilizzati per regolare l'offerta e la domanda di digital assets. Questi dati possono essere utilizzati per l'analisi del mercato e la valutazione del rischio.
Collateralizzazione dei digital assets	I dati sulla collateralizzazione dei digital assets si riferiscono alle informazioni sugli stessi, utilizzate come garanzia per un prestito o una transazione. Questi dati possono essere utilizzati per la valutazione del rischio e per la determinazione del margine di profitto.
Stabilizzazione automatica	I dati sulla stabilizzazione automatica si riferiscono alle informazioni sui meccanismi automatici utilizzati per mantenere il valore di un digital asset stabile. Questi dati possono essere utilizzati per l'analisi del mercato e la valutazione del rischio.
Stabilizzazione tramite pool di garanzie	I dati sulla stabilizzazione tramite pool di garanzie si riferiscono alle informazioni sui pool di digital assets utilizzati per stabilizzarne il valore.

L'analisi on-chain offre diverse aree di applicazioni e diventa un aspetto molto importante per tutte le aziende e le realtà che vogliono offrire a mercato soluzioni di business.

2.5

Legale

● Basic

Neutrino e il caso Coinbase

Neutrino era una **società di analisi blockchain** che **Coinbase** acquista nel febbraio 2019. L'acquisizione ha suscitato polemiche a causa dei precedenti della società, in particolare il fatto che alcuni dei suoi fondatori erano stati coinvolti in un controverso progetto di sorveglianza finanziaria chiamato Hacking Team.

Una volta che la notizia dell'acquisizione è stata diffusa su Twitter, **molti utenti hanno espresso preoccupazione per la scelta di Coinbase** di acquisire una società con legami così controversi, tanto da chiedere a Coinbase stessa di spiegare la propria decisione e di dimostrare che Neutrino non sarebbe stata coinvolta in attività di sorveglianza.

Altri utenti hanno invece difeso Coinbase, sostenendo che l'acquisizione di Neutrino fosse giustificata dalla necessità di migliorare la sicurezza delle transazioni blockchain e di combattere il riciclaggio di denaro.

Molti utenti di Twitter hanno espresso preoccupazione per la **possibilità che Neutrino potesse utilizzare le proprie competenze per sorvegliare le transazioni blockchain e violare la privacy degli utenti di Coinbase**. Altri hanno invece sostenuto che l'acquisizione di Neutrino fosse giustificata dalla necessità di combattere il crimine finanziario e che la società avrebbe lavorato per garantire la privacy degli utenti.

Tale situazione ha quindi creato molti rumors attorno all'acquisizione e questo caso ci spiega quanto sia forte l'attenzione degli utenti nei confronti della privacy.

2.6

Teoria dei sistemi distribuiti

• Medium

La gestione dei server per il mining e per lo staking pool

Le proof-of-work (PoW) e la proof-of-stake (PoS) sono due **algoritmi di consenso** utilizzati in blockchain **per validare le transazioni e mantenere l'integrità della rete**.

L'**analogia tra i due algoritmi può essere fatta in base al concetto di sicurezza e affidabilità della rete**. Entrambi i meccanismi, infatti, cercano di impedire che gli utenti malintenzionati attacchino la rete e compromettano l'integrità delle transazioni.

Tuttavia, ci sono anche differenze significative tra i due algoritmi. Il **PoW richiede ai minatori di risolvere problemi matematici complessi e chi è in grado di produrre più hash, ha maggiore probabilità di essere il primo a risolvere il problema, come se fosse una lotteria dove chi ha più cartelle ha più probabilità**. D'altra parte, il **PoS richiede ai partecipanti di possedere una quantità di token della blockchain per validare le transazioni**. Nella PoS, la competizione dei minatori è sostituita da un sistema proporzionale basato sulla quantità di **ether messi in stake** di un utente rispetto a quella degli altri nodi.

Per il mining di Bitcoin, uno dei software più utilizzati è il famoso **Bitcoin Core**, che consente di effettuare il mining in modalità solitaria. Tuttavia, la maggior parte dei miner preferisce unirsi a un **pool di mining** per aumentare le probabilità di trovare nuovi blocchi e ricevere una ricompensa. In questo caso, i software di mining più noti sono **SlushPool e F2Pool**.

Per lo staking di Ethereum, invece, uno dei software più utilizzati è **Ethereum 2.0 Client**, che consente di partecipare al **processo di staking** sulla blockchain di Ethereum 2.0. Esistono inoltre diverse opzioni di **staking pool**, come ad esempio **Lido o Rocket Pool**, che permettono di delegare il proprio stake ad un pool e ricevere una parte delle ricompense ottenute dallo stesso.

In entrambi i casi, il software di mining o di staking viene scaricato e installato sul proprio computer o su un dispositivo dedicato. Una volta installato, il software si collega al server di mining o di staking pool e inizia ad eseguire le operazioni richieste dal server. Il server riceve le richieste dal software, le elabora ed invia il risultato della computazione. Nel caso del mining, il risultato viene utilizzato per la creazione di un nuovo blocco sulla blockchain, mentre nel caso dello staking la garanzia depositata viene utilizzata per partecipare al processo di staking sulla blockchain.

2.7

Informatica

• Medium

Ethereum Name Service con IPFS

Il **Web3 mira a creare un'esperienza di navigazione più sicura, trasparente e privata, e a garantire la proprietà e il controllo dei propri dati ai propri utenti**.

Le applicazioni decentralizzate non richiedono l'accesso a server centralizzati per funzionare, ma utilizzano invece la potenza di calcolo e la rete distribuita di nodi sulla blockchain per eseguire le operazioni. Un ulteriore strumento chiave per creare un'**esperienza di navigazione Web3 senza censura è l'utilizzo di un l'Ethereum Name Service (ENS)**. Gli ENS forniscono un sistema di nomi di dominio decentralizzato sulla rete Ethereum che consente di assegnare nomi di dominio leggibili dagli utenti alle risorse decentralizzate sulla rete Ethereum, come wallet e contratti intelligenti. Possiamo immaginarli come dei nuovi domini digitali (DNS) per le dApps nel Web3.

Parametro	Descrizione
Estensione del dominio	Indica l'estensione del dominio, come .com, .org, .net, .it, .edu, etc.
Scopo del dominio	Indica lo scopo del dominio, come commerciale, educativo, organizzativo, governativo, etc.
Contenuto del dominio	Indica il contenuto del dominio, come tecnologia, finanza, moda, salute, viaggi, etc.
Paese di registrazione	Indica il paese in cui il dominio è stato registrato, come Italia, Stati Uniti, Regno Unito, etc.
Età del dominio	Indica l'età del dominio, ovvero da quanto tempo il dominio è stato registrato e in uso.
Traffico del sito web	Indica il traffico del sito web associato al dominio, come il numero di visite, pagine viste, tempo medio di permanenza, etc.
Autorità del dominio	Indica l'autorità del dominio, ovvero l'autorevolezza, la popolarità e la reputazione del dominio, misurata ad esempio da metriche come il PageRank di Google o il Domain Authority di Moz.

Per garantire che il contenuto del sito Web associato a un nome di dominio ENS sia immutabile e resistente alla censura, si può utilizzare la tecnologia **IPFS**. IPFS (InterPlanetary File System) è un **sistema di archiviazione distribuito e peer-to-peer che consente di memorizzare e distribuire contenuti in modo decentralizzato**. In questo modo, il contenuto del sito Web associato a un nome di dominio ENS può essere memorizzato su IPFS, rendendolo resistente alla censura e garantendo l'accesso al sito Web senza dipendere da un server centrale.

Dal punto di vista tecnico, gli ENS utilizzano smart contract sulla rete Ethereum per registrare e gestire i nomi di dominio. Gli utenti possono acquistare nomi di dominio utilizzando il digital asset Ether, e possono quindi associare questi nomi di dominio ai propri wallet Ethereum o a qualsiasi altra risorsa decentralizzata sulla rete, come i contratti intelligenti.

Per quanto riguarda la **creazione di un sito web censorship-resistant utilizzando IPFS** (InterPlanetary File System), gli ENS possono essere utilizzati per creare un nome di dominio leggibile dagli utenti per il sito web. L'**utente può quindi associare questo nome di dominio al contenuto del sito web** memorizzato su IPFS. In questo modo, il sito web diventa accessibile tramite il nome di dominio leggibile dagli utenti, e il contenuto del sito web è immutabile e resistente alla censura grazie alla tecnologia IPFS.

In sintesi, gli Ethereum Name Service (ENS) sono un sistema decentralizzato sulla rete Ethereum che consente di assegnare nomi di dominio leggibili dagli utenti alle risorse decentralizzate sulla rete, mentre IPFS è una tecnologia per la memorizzazione e la distribuzione di file in modo decentralizzato e resistente alla censura. L'**uso congiunto di ENS e IPFS consente di creare un sito web censorship-resistant accessibile tramite un nome di dominio leggibile dagli utenti. Tuttavia, rispetto alle altre tecnologie citate, queste sono ancora poco diffuse e il loro utilizzo deve ancora vedere una mass adoption per avere un effetto di rete determinante**.

3

Scalabilità

- 3.1 I problemi della dimensione del blocco e l'introduzione del secondo livello
- 3.2 Il trilemma dei sistemi P2P ed il CAP Theorem
- 3.3 Le soluzioni di secondo livello nel mercato Web3
- 3.4 I modelli di consenso nelle soluzioni di secondo livello
- 3.5 Approfondimento LN su Bitcoin (payment contract)
- 3.6 Approfondimento Abstraction (smart contract wallet e bundle)
- 3.7 Approfondimento Arbitrum (roll up)
- 3.8 Il secondo livello Base dentro l'exchange di Coinbase

3.1

Teoria dei sistemi distribuiti

● Basic

I problemi della dimensione del blocco e l'introduzione del secondo livello

Le reti programmabili che utilizzano la blockchain come database distribuito presentano, a lungo andare, alcuni problemi rispetto alla scalabilità tecnologica del sistema. Ogni blocco ha una dimensione specifica e può contenere solo un certo numero di transazioni. Inoltre, il processo di verifica e validazione delle transazioni richiede tempo ed il **throughput** della blockchain, in alcuni casi, è limitato. Ciò significa che **la blockchain può gestire solo un certo numero di transazioni per unità di tempo, il che limita la sua capacità di scalare verticalmente.**



Throughput

Definizione: Frequenza con cui vengono trasmessi i dati. Può anche essere definito come la quantità di dati spostati con successo da un luogo all'altro in un determinato periodo. La velocità effettiva viene misurata in bit al secondo (BPS). Nei termini di oggi questo sarà espresso in megabit al secondo (Mbps), o Gigabit al secondo (Gbps).

Fonte: <https://www.intel.it/content/www/it/it/support/articles/000026190/wireless.html#:~:text=Throughput%3A%20frequenza%20con%20cui%20vengono,altro%20in%20un%20determinato%20periodo.>

Il vero problema della blockchain è quindi rappresentato dal numero di transazioni al secondo che si riescono a registrare nei nodi. Una bassa scalabilità delle blockchain potrebbe rappresentare quindi un grosso limite, anche per gli sviluppi futuri

In termini generici, come affermato da Banca d'Italia: "Nella teoria dei sistemi distribuiti, la scalabilità di un sistema indica la capacità del sistema di mantenere un adeguato livello di performance all'aumentare della complessità della rete (numero di nodi) o del carico di lavoro (numero di operazioni richieste). Diverse sono le metriche che possono essere utilizzate per misurare le performance di un sistema; tra queste, si considerano il throughput e la latenza."

La **latenza** è quindi un'altra metrica con la stessa funzione del throughput, ma che misura l'intervallo di tempo richiesto dal protocollo per processare e finalizzare le transazioni (c.d. "time to finality") sulla blockchain.

A seguito verrà fornita una tabella che mette a confronto due blockchain in termini di latenza e throughput:

	Latenza	Throughput
Ethereum	La latenza di rete attuale è di circa 15 millisecondi.	- Tx/Sec medio (ultimi 7 giorni): 24.02 TPS - Tempo medio per la generazione di un nuovo blocco TPS: 12,5 secondi.
Algorand	La latenza di rete attuale è di circa 5 millisecondi.	Su Algorand, i blocchi vengono prodotti ogni 3,9 secondi e possono contenere fino a 25.000 transazioni, il che si traduce in un throughput di circa 6.000 transazioni al secondo (6000 TPS).

Come mai vi sono queste **differenze tra Algorand ed Ethereum?**

Il motivo principale è l'algoritmo di consenso, poiché per ethereum parliamo di un PoS, mentre nel caso di Algorand di un PPoS.

Tutto ciò si traduce nel fatto che **Ethereum**, essendo PoS, ha un **fairness elevato** (32 Eth) e l'algoritmo di consenso è più democratico; la scelta del nodo che proporrà il prossimo blocco è determinata sulla quantità di ETH che detiene in stake il nodo, ma per evitare che uno di essi con elevato numero di ETH possa essere selezionato più volte in un breve periodo di tempo sono previsti meccanismi di randomizzazione, rotazione dei validatori, costo d'attacco e dimensioni dello stake. Di conseguenza quando un validatore propone un blocco questo dovrà essere valutato da altri nodi che eseguiranno l'algoritmo sullo stesso blocco per verificare se il nodo proponente abbia operato in modo corretto. Il tempo necessario per finalizzare un blocco è, mediamente, pari a 15 minuti.

Algorand invece non ha un fairness elevato quindi chiunque, anche con pochi Algo in stake, può diventare un nodo validatore. Nel PPoS si utilizza la VRF che funziona in modo simile ad una lotteria e viene utilizzata per scegliere i leader che compongono un blocco e i membri del comitato da una distribuzione binomiale per emulare una chiamata per ogni Algo nell'account dell'utente. Più algo si hanno in stake maggiore è la possibilità che l'account venga selezionato, come se ogni algo nell'account degli utenti partecipasse alla lotteria. Tutto ciò si traduce in una minore democrazia nella scelta del validatore, in quanto se un account detiene molti algo ha elevate probabilità di essere selezionato, anche più volte di seguito, in quanto non sono previsti meccanismi di rotazione dei validatori.

Il secondo problema è la **crescita esponenziale del database distribuito nel lungo periodo**. Poiché ogni transazione viene registrata nella blockchain, l'archivio delle transazioni diventa sempre più grande col passare del tempo. Ciò comporta un aumento del tempo necessario per scaricare e sincronizzare l'intera storia della blockchain, ed un aumento dei costi di storage per i nodi che la conservano. Questo può portare ad un **rischio di centralizzazione dei nodi**, poiché solo i nodi con risorse sufficienti (come storage, banda elettrica e banda) possono continuare a gestire la blockchain, mentre i nodi più piccoli e con meno risorse rischiano di essere esclusi.

Questi problemi hanno fatto sollevare delle critiche attorno ai progetti peer to peer come Bitcoin ed Ethereum, in quanto “disegnati” in maniera poco scalabile nel lungo periodo. Fortunatamente, le rispettive community hanno studiato il problema della scalabilità, proponendo diverse soluzioni **per far “scalare” su un secondo livello (i.e. layer) connesso alla blockchain, garantendo a quest’ultima la sicurezza del primo livello by default tramite la crittografia.**

Alcune di queste soluzioni sono già perfettamente funzionanti, dimostrando solidità tecnica e performance migliore rispetto alla velocità ed ai costi per le transazioni sul network, diminuendo il carico di informazioni all'interno del primo livello.

3.2

Teoria dei sistemi distribuiti

● Hard

Il trilemma dei sistemi P2P ed il CAP Theorem

La **scalabilità di un sistema** è fondamentale per **garantire la sua crescita e per garantire un network effect solido**. In un mondo in cui l'adozione delle tecnologie digitali avviene sempre più rapidamente, la capacità di un sistema di gestire un numero crescente di utenti e di transazioni diventa essenziale per mantenere la sua competitività ed il suo valore.

L'architettura lineare di un database a “catena di blocchi” diventa un problema poiché il database non può crescere in più direzioni, organizzando quindi i dati in maniera meno efficiente rispetto ad altre tipologie di database distribuiti. Per esempio, un database distribuito non lineare come Apache Cassandra può scalare meglio per gestire grandi volumi di dati.

La scalabilità è la capacità di un sistema di gestire un aumento del carico di lavoro. Ci sono **due tipologie principali di scalabilità:**

- La **scalabilità verticale** si riferisce alla **capacità di aumentare le risorse hardware** (ad es. la CPU, la memoria, lo storage) **di una singola macchina per gestire un carico di lavoro maggiore**. In altre parole, una singola macchina può gestire un carico di lavoro più elevato semplicemente aumentando le risorse hardware.
- La **scalabilità orizzontale si riferisce alla capacità di gestire un carico di lavoro maggiore distribuendo il carico su più macchine**. La scalabilità orizzontale significa quindi che un sistema può gestire un carico di lavoro maggiore aggiungendo semplicemente più macchine al sistema.

Scalabilità Verticale	Scalabilità Orizzontale
Aumenta le risorse hardware di una singola macchina	Aggiunge più macchine al sistema
Semplice da implementare	Più complessa da implementare
Può raggiungere un limite di scalabilità in base alle limitazioni hardware	Scalabilità quasi infinita
Più costosa in termini di investimento in hardware	Più costosa in termini di investimento iniziale
Migliore per applicazioni con carichi di lavoro più leggeri	Migliore per applicazioni con carichi di lavoro più pesanti

In particolare, per i digital assets e le blockchain, la **scalabilità è un fattore critico per garantire l'adozione di massa**. Più utenti si uniscono alla rete e più transazioni vengono effettuate, maggiore sarà la pressione sui nodi della rete e sulla capacità del sistema di elaborare e validare le transazioni in modo affidabile e tempestivo.

Attualmente, la dimensione della blockchain di Bitcoin è di circa 380 GB (dato al 22 marzo 2023). I full node di Bitcoin utilizzano il protocollo di rete P2P di Bitcoin per comunicare tra loro e per diffondere le transazioni e i nuovi blocchi della blockchain.

I full node di Ethereum sono eseguiti su macchine con elevate capacità di elaborazione e storage, poiché la blockchain di Ethereum è notevolmente più grande di quella di Bitcoin, occupando circa 1,4 TB di spazio di archiviazione (dato al 22 marzo 2023). I full node di Ethereum utilizzano il protocollo di rete P2P per comunicare tra loro e per diffondere le transazioni e i nuovi blocchi della blockchain.

Alcune **considerazioni rispetto alla scalabilità verticale ed orizzontale di una rete come Bitcoin o Ethereum:**

- Nel lungo periodo, c'è un rischio per la scalabilità verticale del sistema, in quanto la crescita dell'**architettura del database** (lineare e con dimensione dei blocchi limitata) potrebbe obbligare i full node ad utilizzare infrastrutture cloud private, portando ad una minore decentralizzazione dell'infrastruttura delle reti peer to peer.
- Mentre per la scalabilità orizzontale, la rete utilizza un sistema di **consenso decentralizzato** che richiede la verifica di ogni transazione da parte di tutti i nodi della rete, tramite la rete gossip, rendendo **il processo di validazione lento e costoso** in termini di risorse di elaborazione.

Disegnare l'architettura un sistema distribuito come una rete o un database, comporta spesso l'impossibilità di avere le stesse performance di un sistema centralizzato, il quale ha meno problemi a scalare. Alcuni teoremi e considerazioni cercando di affrontare il problema della scalabilità:

- Il **teorema di Brewer**, afferma che in un sistema distribuito non è possibile garantire contemporaneamente le tre proprietà di coerenza (consistency), disponibilità (availability) e tolleranza ai guasti (partition tolerance).
- In "The Limits of Blockchain Scalability and the Trilemma of Decentralization, Security, and Scalability", Larimer ha descritto **il trilemma dei sistemi P2P** come un concetto fondamentale che i progettisti di sistemi distribuiti devono considerare nella progettazione di reti blockchain. Larimer ha sostenuto che la scalabilità, la decentralizzazione e la sicurezza sono tre obiettivi conflittuali che devono essere bilanciati tra loro.

Il trilemma dei sistemi P2P, il teorema CAP e la scalabilità limitata della blockchain sono tutti concetti strettamente correlati. La blockchain rappresenta un esempio di sistema distribuito che sacrifica la

disponibilità a favore della consistenza e del partizionamento tollerante, ma questo **ha un impatto sul la sua scalabilità limitata**, in quanto la verifica di ogni transazione richiede molte risorse di elaborazione. Per questo motivo, molti digital assets e blockchain stanno cercando di migliorare la loro scalabilità attraverso l'implementazione di nuove tecnologie come lo sharding, l'offloading delle transazioni su layer 2, l'ottimizzazione del protocollo di consenso e l'adozione di soluzioni di caching.

3.3

Teoria dei sistemi distribuiti/ Business

● Medium

Le soluzioni di secondo livello nel mercato Web3

Sia su Ethereum che su Bitcoin, ci sono diverse **soluzioni di mercato che cercano di affrontare questo problema**. Di seguito, troverai una tabella riassuntiva:

Protocollo/Progetto	Descrizione
Sidechains	Sidechains sono blockchain parallele connessi alla blockchain principale che consentono di sperimentare nuove funzionalità senza mettere in pericolo la sicurezza della blockchain principale. Sidechains permette la creazione di un'interazione tra blockchain, attraverso lo scambio di valori tra di esse.
Plasma	Plasma è un framework per creare sidechain sulla blockchain di Ethereum. La tecnologia Plasma consente la creazione di una blockchain secondaria che interagisce con la blockchain principale. In pratica, Plasma utilizza la blockchain principale come mezzo per garantire la sicurezza. L'obiettivo principale è quello di migliorare le prestazioni della di Ethereum, consentendo di effettuare un maggior numero di transazioni in modo rapido e sicuro.
Sharding	Sharding è una tecnologia che consente di dividere la blockchain in parti più piccole, chiamate shard, per consentire a più nodi di elaborare le transazioni in parallelo. In pratica ogni nodo viene assegnato ad un diverso shard, per consentire l'elaborazione simultanea di più transazioni. Ethereum 2.0 utilizza la tecnologia di sharding per migliorare le prestazioni della blockchain.
State Channels	State Channels sono canali che consentono a due parti di effettuare transazioni al di fuori della blockchain principale, ma con la sicurezza della blockchain stessa. In pratica, mediante questi canali le parti possono effettuare molte transazioni al suo interno prima di registrare il risultato sulla blockchain principale. L'obiettivo cardine è sempre quello di migliorare le prestazioni della blockchain, consentendo di effettuare un maggior numero di transazioni in modo rapido e sicuro. Un esempio di progetto che utilizza il concetto di State Channels è Lightning Network, il quale permette di effettuare pagamenti Bitcoin off-chain.
Rollups	Rollups sono soluzioni che consentono di elaborare le transazioni fuori dalla blockchain principale, ma di conservare le informazioni di queste transazioni sulla blockchain principale. In pratica, Rollups aggrega molte transazioni in una sola transazione e la registra sulla blockchain principale. Anche i Rollups sono progettati per effettuare un maggior numero di transazioni in modo rapido e sicuro.

Oltre ai casi presenti in tabella va ricordata l'esistenza degli **abstraction account**, di cui se ne parlerà successivamente, e del **builder**, degli strumenti di sviluppo che semplificano la creazione e la gestione di applicazioni decentralizzate (DApp) e di smart contract.

È importante notare che ci sono molte altre soluzioni di mercato in fase di sviluppo e che la lista sopra non è esaustiva e, in aggiunta a ciò, alcune soluzioni possono essere utilizzate sia per Ethereum che per Bitcoin, mentre altre sono specifiche per una delle due blockchain.

3.4

Teoria dei sistemi distribuiti

● Medium

I modelli di consenso nelle soluzioni di secondo livello

I modelli di consenso sono fondamentali per garantire la sicurezza e l'affidabilità delle transazioni dei digital assets. Nei protocolli di secondo livello, i modelli di consenso più utilizzati includono il Proof of Authority (PoA), il Federated Byzantine Agreement (FBA) e il Delegated Proof of Stake (DPoS).

- Il Proof of Authority è un modello di consenso in cui **un gruppo selezionato di nodi autorizzati è responsabile della validazione delle transazioni all'interno della rete**. Questi nodi sono scelti in base alla loro reputazione e affidabilità, e la loro partecipazione viene garantita da un sistema di incentivi e disincentivi.
- Il Federated Byzantine Agreement è un modello di consenso in cui **un gruppo di nodi selezionati si accorda su una serie di regole per la validazione delle transazioni**. Questo modello è particolarmente utile per le applicazioni finanziarie, in cui la velocità e l'affidabilità delle transazioni sono essenziali.
- Il Delegated Proof of Stake è un modello di consenso in cui **i nodi staker eleggono un gruppo di delegati che sono responsabili della validazione delle transazioni all'interno della rete**. Questo modello è particolarmente utile per i digital assets con un alto volume di transazioni, poiché consente di ridurre il tempo necessario per la validazione delle transazioni e aumenta la scalabilità della rete.

I modelli di consenso utilizzati nei protocolli di secondo livello dei digital assets sono quindi progettati per garantire la sicurezza, l'affidabilità e la scalabilità delle transazioni all'interno della rete.

3.5

Approfondimento LN su Bitcoin (payment contract)

Teoria dei sistemi distribuiti / Informatica

● Hard

Il Lightning Network è un protocollo di rete di secondo livello che è stato sviluppato per risolvere i problemi di scalabilità di Bitcoin. Invece di registrare tutte le transazioni sulla blockchain di Bitcoin, Lightning Network consente di effettuare transazioni veloci e a basso costo attraverso canali di pagamento fuori dalla rete.

Gli attori coinvolti in Lightning Network sono i nodi della rete, che sono essenzialmente computer o server che eseguono il software di Lightning Network. Ci sono due tipi di nodi: nodi di routing e nodi finali. I **nodi di routing consentono ai pagamenti di passare attraverso di essi per raggiungere il loro destinatario**, mentre i **nodi finali sono quelli che ricevono e inviano pagamenti**. Ogni nodo ha un identificatore univoco, noto come identità della chiave pubblica.

Le transazioni vengono memorizzate tra i due nodi coinvolti e **solo l'ultima transazione viene registrata sulla blockchain di Bitcoin quando il canale viene chiuso**. Ciò significa che il **numero di transazioni registrate sulla blockchain di Bitcoin viene ridotto**, migliorando la scalabilità della rete.

Per garantire che i pagamenti siano sicuri e non vengano duplicati, Lightning Network utilizza un sistema di smart contract noto come **Hashed Time-Locked Contract (HTLC)**. Gli HTLC permettono ai nodi di impegnarsi in una transazione in cui i **fondi vengono bloccati in un canale di pagamento fino a quando non viene fornita una prova di pagamento valida**. Se il pagamento non viene fornito entro un certo periodo di tempo, i fondi vengono restituiti al mittente.

Per proteggere i fondi dei nodi finali da attacchi informatici o perdite di connessione, Lightning Network prevede l'uso di **watching tower**, ossia nodi specializzati che monitorano il canale di pagamento per conto dei nodi finali e li proteggono da attacchi di frode. Inoltre, il protocollo prevede l'utilizzo di **hub di liquidità, che sono nodi specializzati in grado di fornire liquidità ai canali di pagamento**.

Per implementare Lightning Network, è possibile utilizzare una varietà di software open source come LND, C-Lightning e Eclair. Questi software sono disponibili su GitHub e sono supportati dalla comunità di sviluppatori di Bitcoin.

Fonti

- ▶ Paper originale di Lightning Network: <https://lightning.network/lightning-network-paper.pdf>
- ▶ LND (software di Lightning Network): <https://github.com/lightningnetwork/lnd>
- ▶ Protocollo gRPC: <https://grpc.io/docs/what-is-grpc/>

3.6

Approfondimento Abstraction (smart contract wallet e bundle)

Teoria dei sistemi distribuiti / Informatica

● Hard

L'abstraction account è un concetto tecnico introdotto dallo standard EIP 4337 (Account Abstraction), che permette di separare la gestione dei fondi all'interno della blockchain di Ethereum dalla gestione della sicurezza degli account. In sostanza, l'**abstraction account consente di creare un nuovo tipo di**

account Ethereum che non richiede una chiave privata per accedere ai fondi, ma che può essere controllato tramite uno smart contract.

Lo **standard EIP 4337** è stato proposto per **migliorare la sicurezza e la scalabilità della rete Ethereum, rendendo la gestione degli account più flessibile e decentralizzata**. L'abstraction account consente di creare uno smart contract personalizzato che gestisce l'accesso ai fondi in modo sicuro e trasparente, senza che gli utenti debbano preoccuparsi di mantenere la loro chiave privata in un ambiente sicuro.

Uno dei vantaggi dell'abstraction account è la possibilità di utilizzare una **moltitudine di soluzioni di sicurezza decentralizzate**, come ad esempio hardware wallet o smart contract multisignature, per proteggere i fondi. Ciò rende più difficile per i malintenzionati rubare i fondi, in quanto non possono accedere agli account solo conoscendo la chiave privata.

Per implementare un'abstraction account, è **necessario creare uno smart contract che funga da ponte tra l'account Ethereum e i fondi gestiti dal contratto**. Il contratto deve essere in grado di riconoscere le richieste di prelievo dei fondi e di verificare se la richiesta è valida. Una volta che la richiesta è stata confermata, il contratto esegue la transazione richiesta.

L'utilizzo di un'abstraction account può essere **utile anche per l'implementazione di applicazioni decentralizzate**, come i giochi basati su blockchain. In questi casi, l'abstraction account può rappresentare l'inventario del giocatore, e il contratto può gestire gli scambi di oggetti tra i giocatori in modo sicuro e trasparente.

L'abstraction account è quindi un **concepto tecnico importante per la sicurezza e la scalabilità della rete Ethereum**. Utilizzando uno smart contract per gestire l'accesso ai fondi, gli utenti possono proteggere i loro fondi utilizzando una vasta gamma di soluzioni di sicurezza decentralizzate. Inoltre, l'abstraction account può essere utilizzato per implementare applicazioni decentralizzate più sofisticate, come i giochi basati su blockchain.

3.7

Teoria dei sistemi distribuiti / Informatica

● Hard

Approfondimento Arbitrum (roll up)

Arbitrum è una **piattaforma di smart contract layer 2 per Ethereum** che consente di eseguire contratti intelligenti in modo affidabile, veloce e a basso costo. L'obiettivo principale di Arbitrum è quello di **migliorare l'esperienza degli utenti e degli sviluppatori di Ethereum, riducendo i costi delle transazioni e migliorando la scalabilità della rete**.

In pratica, Arbitrum consente agli utenti di effettuare transazioni su una blockchain parallela, nota come sidechain, che è collegata alla blockchain principale di Ethereum.

Le transazioni su Arbitrum vengono verificate attraverso un sistema di smart contract chiamato *Optimistic Rollup*. Questo sistema **consente di elaborare molte transazioni contemporaneamente, raggruppandole in blocchi e verificandole in modo asincrono rispetto alla blockchain principale**.

Per garantire la sicurezza delle transazioni, Arbitrum utilizza anche un meccanismo di dispute resolution chiamato fraud proof. **Questo sistema consente agli utenti di segnalare eventuali transazioni fraudolente e di ricevere un rimborso dei fondi bloccati nel contratto**. Inoltre, Arbitrum prevede l'utilizzo di nodi specializzati chiamati validators, che sono incaricati di verificare le transazioni sulla sidechain e di assicurarsi che siano conformi alle regole della blockchain. I validators sono selezionati in base al loro **staking di token nativi della sidechain, che garantisce un incentivo economico per mantenere la sicurezza della rete**.

Gli attori coinvolti in Arbitrum includono i nodi della rete che eseguono il software, gli utenti che creano e interagiscono con i contratti intelligenti, e gli operatori del rollup che eseguono e validano le transazioni sulla blockchain di Ethereum.

Fonti

- Sito ufficiale di Arbitrum: <https://developer.offchainlabs.com/>

3.8

Teoria dei sistemi distribuiti/ Business

● Medium

Il secondo livello Base dentro l'exchange di Coinbase

Il progetto **BASE di Coinbase è una soluzione di livello 2** che utilizza la tecnologia di scaling Optimistic Rollups per migliorare le transazioni sulla blockchain di Ethereum. Gli Optimistic Rollups permettono di elaborare i dati delle transazioni in modo off-chain, ovvero al di fuori della blockchain principale, per poi registrare solo il risultato finale. In questo modo, le transazioni possono essere effettuate in modo più veloce e a basso costo, senza compromettere la sicurezza della blockchain.

Il protocollo BASE può essere descritto nel seguente modo:

- **Asset sintetico:** BASE è definito sintetico in quanto il suo andamento dipende da un determinato sottostante, in questo caso individuato in tutti i digital assets.
- **Elastico:** la supply di BASE è elastica e quindi rappresenta un tipo di fornitura che varia in relazione al raggiungimento del prezzo di equilibrio target. Il prezzo target di BASE è un bilionesimo della capitalizzazione di mercato totale di tutti i digital assets.
- **Rebase:** tale termine indica le contrazioni e le espansioni della supply di BASE, in particolare a fronte di un'espansione si genera offerta, diminuendo la scarsità e spingendo il prezzo verso il suo target, la contrazione invece distrugge l'offerta, aumentando la scarsità e spingendo il prezzo verso il suo obiettivo.
- **Cascade:** con questo termine si intende il sistema di remunerazione per lo staking di BASE. La Cascade emette ricompense in base alla durata in cui l'utente mantiene in staking i propri token nella pool (pool liquidity su Uniswap); maggiore è la liquidità fornita e maggiore è il periodo di staking, maggiore sarà la ricompensa.

Fonti

- ▶ <https://www.baseprotocol.org/#definingbase>

4

Privacy

- 4.1 Che valore ha la privacy per gli utenti del Web3?
- 4.2 Che cos'è un protocollo di mixing?
- 4.3 Approfondimento protocollo di mixing su Ethereum: Tornado Cash
- 4.4 Il caso Tornado Cash in USA

4.1

Crittografia
● Basic

Che valore ha la privacy per gli utenti del Web3?

Uno dei temi più controversi rispetto ai digital assets è il **tema dello pseudo-anonimato**. Questo concetto ha a che fare sia con la governance della rete, sia con il livello di crittografia applicato nel sistema per renderlo sempre più vicino al concetto di privacy by design.

Senza considerare la privacy e la protezione dei dati da un punto di vista normativo, che non è oggetto della presente trattazione, ognuno di noi ha una percezione rispetto al concetto di "privacy" ed al suo valore in modalità strettamente individuale e differente. Ci sono utenti che lo considerano un principio cardine per utilizzare una tecnologia, altri invece sono disposti a lasciare parte della privacy in cambio di facilità di uso e servizi. All'interno del mercato dei digital assets, ogni utente ha un livello di privacy differente e conseguentemente ogni utente può aver bisogno di servizi differenti in funzione del segmento di mercato in cui si trovano.

Questo concetto viene spesso messo in **relazione alla possibilità di utilizzare i digital assets per attività criminali, come il riciclaggio**. Tuttavia, non si considera il problema che come database pubblico, se mostrasse i nomi e cognomi dei suoi utenti e i loro saldi, lederebbe il diritto alla privacy. Per prevenire ciò, l'architettura dei wallet tramite PKI garantisce infatti un discreto livello di pseudo-anonimato.

Tra i protocolli peer to peer, ve ne sono alcuni che hanno reso i dati completamente anonimizzati, creando un'architettura privacy by design. Queste reti utilizzano come mezzo di scambio quello che viene definito privacy coin.

I privacy coin sono digital asset progettati per proteggere l'anonimato degli utenti. In sostanza, questi token sono stati creati per garantire che le transazioni che li coinvolgono siano completamente anonieme e non tracciabili.

Le privacy coin utilizzano diverse tecnologie per garantire l'anonimato degli utenti e delle loro transazioni, tra cui:

- **Ring Signatures:** sono utilizzate da Monero e altri digital assets simili per nascondere l'identità del mittente di una transazione all'interno di un gruppo di altre firme.
- **Stealth Addresses:** un indirizzo unico generato per ogni transazione in entrata, in modo che le transazioni precedenti non possano essere associate ad un singolo indirizzo.
- **Zero-knowledge proofs:** sono utilizzati da Zcash per garantire che l'identità del mittente, il destinatario e l'importo della transazione siano completamente anonimi.
- **CoinJoin:** utilizzato da Dash e altri digital assets per unire le transazioni di più utenti in un'unica transazione, in modo da confondere gli eventuali tracciamenti. Questa feature è utilizzata anche da Bitcoin ma non nativamente nelle regole del software attuale.

Di seguito una tabella che riassume le principali caratteristiche di alcune delle principali privacy coin:

Digital Asset	Algoritmo di hash	Algoritmo di consenso	Tecnologia di privacy
Monero	CryptoNight	Proof of Work	Ring Signatures
Zcash	Equihash	Proof of Work	Zero-knowledge proofs
Dash	X11	Proof of Work	CoinJoin

In conclusione, queste tipologie di digital assets possono presentare delle problematiche in termini di riciclaggio ed è quindi necessario dotarsi di processi che permettano di tutelarsi dai rischi derivanti dall'utilizzo di queste pratiche.

4.2

Che cos'è un protocollo di mixing?

Crittografia

● Medium

Per anonimizzare completamente le informazioni all'interno dei network layer 1 come Bitcoin o Ethereum, vengono utilizzati degli aggiunti protocolli informatici definiti come di missaggio (mixing).

I **protocolli di mixing** sono utilizzati per **garantire la privacy e l'anonymato** delle transazioni. Questi protocolli funzionano mescolando i fondi di più utenti, in modo tale da rendere più difficile tracciare le transazioni e identificare gli utenti coinvolti. I due protocolli più utilizzati sono Tornado Cash su Ethereum e CoinJoin su Bitcoin.

Il processo di mixing in Tornado Cash è simile a quello di CoinJoin su Bitcoin. Gli **utenti depositano i loro fondi in un pool di mixing, che rimescola i fondi di tutti gli utenti nel pool e crea transazioni anonime da inviare sulla rete Ethereum**.

Per partecipare ad un pool di mixing, gli **utenti devono prima depositare i loro fondi e ricevere un “impegno” (commitment) in cambio**. L'impegno è un token crittografico che rappresenta la quantità di fondi depositati dall'utente nel pool di mixing.

Dopo aver depositato i fondi, gli utenti devono **attendere un certo periodo** di tempo prima di poter prelevare i fondi dal pool di mixing. Questo periodo di attesa è chiamato **“periodo di abbinamento” (matching period)** e **consente a più utenti di depositare i loro fondi nel pool di mixing prima che vengano rimescolati**.

Dopo il periodo di abbinamento, gli utenti possono prelevare i loro fondi dal pool di mixing. Il prelievo viene effettuato in modo anonimo, senza rivelare l'identità dell'utente o la quantità di fondi prelevati.

I protocolli di mixing, quindi, funzionano mescolando i fondi di più utenti in un'unica transazione, in modo tale da garantire la privacy e l'anonymato delle transazioni.

La seguente tabella riassume le componenti logiche principali di Tornado Cash su Ethereum e di CoinJoin su Bitcoin:

Componente	Tornado Cash su Ethereum	CoinJoin su Bitcoin
Mixing	Tornado Cash utilizza il processo di mixing per mischiare le transazioni con quelle di altri utenti per nascondere la provenienza dei fondi. Il processo di mixing prevede l'utilizzo di smart contract di Ethereum per garantire la sicurezza e l'anonymato delle transazioni.	CoinJoin utilizza il processo di mixing per raggruppare le transazioni di più utenti in un'unica transazione, rendendo difficile tracciare la provenienza dei fondi. Questo processo avviene attraverso l'utilizzo di una transazione con più input e output, in cui tutti i partecipanti versano la stessa quantità di bitcoin.
Anonimato	Tornado Cash utilizza la tecnologia zk-SNARKs per garantire l'anonymato degli utenti. La tecnologia zk-SNARKs permette di verificare che una transazione sia valida senza rivelare i dettagli della transazione stessa.	CoinJoin offre l'anonymato attraverso il mixing di transazioni, rendendo difficile tracciare la provenienza dei fondi. Tuttavia, CoinJoin non garantisce l'anonymato completo, poiché le transazioni possono essere ancora tracciate attraverso l'analisi della blockchain.
Trustlessness	Tornado Cash è una soluzione completamente trustless, il che significa che non è necessario affidarsi a nessuna terza parte per garantire la sicurezza delle transazioni. Gli utenti possono accedere al servizio senza dover fornire informazioni personali o informazioni sulla provenienza dei fondi.	CoinJoin richiede la partecipazione di almeno un'altra persona per effettuare la transazione, il che significa che esiste un certo grado di fiducia nei confronti degli altri partecipanti. Tuttavia, l'utilizzo di CoinJoin è ancora considerato relativamente sicuro perché tutti i partecipanti versano la stessa quantità di bitcoin, il che rende difficile l'identificazione dei singoli partecipanti.

Costi	<i>Tornado Cash prevede il pagamento di una fee per l'utilizzo del servizio. Il costo varia in base alle dimensioni della transazione e alla velocità di elaborazione.</i>	<i>CoinJoin è un'opzione relativamente economica per nascondere la provenienza dei fondi. I costi sono limitati alle commissioni di transazione standard per l'invio di bitcoin sulla rete Bitcoin.</i>
Scalabilità	<i>Tornado Cash su Ethereum è limitato dalla scalabilità di Ethereum stessa. Al momento, Tornado Cash supporta solo un certo numero di transazioni al giorno.</i>	<i>CoinJoin su Bitcoin è una soluzione scalabile perché non richiede l'utilizzo di smart contract e può essere utilizzato in qualsiasi momento senza dover attendere che la rete Bitcoin sia libera da congestimenti.</i>

4.3

Informatica

• Hard

Approfondimento protocollo di mixing su Ethereum: Tornado Cash

Tornado Cash è un **protocollo di privacy decentralizzato che consente agli utenti di effettuare transazioni anonime su Ethereum**. Il protocollo si basa sul concetto di “**pool di mixing**”, in cui gli utenti possono depositare fondi e quindi prelevare la stessa quantità di essi in una transazione separata.

Tornado Cash è solo uno dei molti protocolli di privacy disponibili su Ethereum. Ci sono anche altre soluzioni come **Aztec Protocol**, che utilizza un sistema di criptazione zero-knowledge per garantire la privacy delle transazioni su Ethereum.

In generale, i protocolli di privacy su Ethereum stanno diventando sempre più popolari, poiché sempre più utenti cercano di proteggere la loro privacy online.

Tornando al caso di Tornado Cash, esso è basato sulla crittografia a chiave pubblica e utilizza la crittografia degli zero-knowledge per garantire la privacy delle transazioni. In particolare, il protocollo utilizza lo standard **SNARKS** (Succinct Non-Interactive Argument of Knowledge), un tipo di proof system a bassa latenza e ad alta scalabilità.

Il **codice sorgente di Tornado Cash è open source** ed è disponibile su Github. Il protocollo è scritto in Solidity, il linguaggio di programmazione per smart contract utilizzato su Ethereum. Il contratto intelligente di Tornado Cash è composto da diverse parti, tra cui il generatore di chiavi private e pubbliche, il processo di mixing dei fondi, la generazione di indirizzi anonimi e il meccanismo di prelievo dei fondi. Tornado Cash è stato integrato anche in alcuni wallet, come ad esempio il wallet anonimo **Aztec Protocol**, che utilizza Tornado Cash per garantire la privacy delle transazioni su Ethereum.

Il contratto principale che gestisce il protocollo è il **Tornado.sol**. Questo contratto **definisce tutte le funzioni per il deposito, il ritiro e la gestione degli anonymous tokens**, nonché le funzioni per la configurazione dei parametri del protocollo come la durata del periodo di cooldown, la dimensione delle batch per la creazione di nuovi tokens, ecc.

Il cuore del protocollo è il mixnet, che viene implementato in **Mix.sol**. Questo contratto **gestisce l'intero processo di mescolamento degli ether tra i partecipanti**. Gli utenti che vogliono mescolare i loro ether depositano l'importo desiderato nel contratto Tornado, che crea automaticamente una transazione di mescolamento nel mixnet. La transazione di mescolamento viene creata da una funzione definita nel Mix.sol chiamata mix. Questa funzione accetta una serie di parametri, tra cui l'importo da mescolare, il valore dell'anonymous token, l'indirizzo del destinatario e il tempo di scadenza. La **funzione mix seleziona casualmente altri utenti che hanno depositato denaro in precedenza nel protocollo, e utilizza i loro anonymous token per mescolare gli ether degli utenti in un'unica transazione**.

Per garantire la privacy degli utenti, il mixnet utilizza una tecnologia chiamata **zk-SNARK**, che permette di dimostrare che una transazione è valida senza dover rivelare le informazioni sensibili contenute all'in-

terno della transazione stessa. In questo modo, gli utenti possono mescolare i loro ether senza rivelare l'importo o l'indirizzo del destinatario.

Inoltre, Tornado Cash implementa anche una funzionalità chiamata “**private relayer**”. Questa funzione permette agli utenti di **creare una transazione di mescolamento utilizzando il loro relayer privato**, invece di utilizzare il relayer pubblico fornito dal protocollo. Questo **aumenta ulteriormente la privacy dell'utente**, poiché la transazione non viene pubblicata sulla blockchain principale.

Quanto qui evidenziato ha l'obiettivo di educare sulle potenziali attività di riciclaggio attuabili sulla blockchain. Risulta fondamentale dunque dotarsi di processi che tutelino dai rischi derivanti dall'utilizzo di queste pratiche.

Legale

● Basic

4.4

Il caso Tornado Cash in USA

Nel novembre 2020, l'ufficio del procuratore generale degli Stati Uniti ha presentato un reclamo contro Tornado Cash e la sua società madre, Ethereum Foundation, per **presunte violazioni delle normative antiriciclaggio e delle leggi sulle attività finanziarie illegali (AML – Anti Money Laundering)**.

Secondo il reclamo, Tornado Cash è stata utilizzata per nascondere l'origine di alcuni digital assets utilizzati per attività illegali, come il traffico di droga e la pornografia infantile. Inoltre, gli utenti di Tornado Cash sarebbero stati in grado di eludere le normative AML, che richiedono alle piattaforme di scambio di digital assets di identificare e verificare l'identità dei propri utenti.

Il reclamo ha citato anche la **mancanza di conformità di Tornado Cash con le normative applicabili, come il Bank Secrecy Act (BSA) e le regole sulla custodia delle attività virtuali (VCA)**, che richiedono alle società di digital assets di registrarsi presso il dipartimento del tesoro degli Stati Uniti e di implementare controlli AML.

In risposta al reclamo, **Tornado Cash ha affermato di non avere il controllo sulle transazioni effettuate sulla piattaforma** e di non avere l'obbligo di rivelare le informazioni personali degli utenti. Inoltre, la società ha affermato di non avere una presenza fisica negli Stati Uniti e quindi di non essere soggetta alle leggi statunitensi.

Il caso Tornado Cash evidenzia la **sfida delle autorità regolatorie nell'affrontare l'uso dei digital assets per attività illegali e la necessità di trovare un equilibrio tra la privacy degli utenti e la necessità di conformità con le normative applicabili**. In particolare, il caso ha sollevato dubbi sulla responsabilità delle società di digital assets per le attività dei propri utenti e sulla necessità di regole chiare per garantire la conformità AML.

È importante notare che il caso Tornado Cash ha anche sollevato la **questione del “blacklisting” degli indirizzi di digital assets**, ovvero l'**aggiunta di determinati indirizzi ad una lista nera per impedire loro di partecipare alle transazioni**. Il reclamo presentato dall'ufficio del procuratore generale degli Stati Uniti ha sottolineato la necessità di utilizzare il “blacklisting” degli indirizzi per prevenire il riciclaggio di denaro tramite la piattaforma Tornado Cash.

5

Interoperabilità

- 5.1 Perchè è importante l'interoperabilità tra Web2 e Web3?
- 5.2 Cosa sono i trigger e gli oracoli?
- 5.3 Come possono interagire i protocolli Web3 tra di loro?
- 5.4 Approfondimento libreria WEB3.JS
- 5.5 Cos'è la compatibilità EVM?
- 5.6 Come funziona uno scambio atomico (Atomic Swap) tra due reti?
- 5.7 Perchè gli Atomic swap possono offrire sicurezza nella finanza decentralizzata?
- 5.8 Perchè gli Atomic swap possono essere una vulnerabilità nella finanza decentralizzata?
- 5.9 Approfondimento Atomic Swap su Ethereum
- 5.10 Che cosa si intende per Wrapped Token?

5.1

Informatica

● Basic

Perchè è importante l'interoperabilità tra Web2 e Web3?

Nella scelta di un network vi deve essere un importante requisito da considerare: l'interoperabilità di una rete peer to peer con altre reti aperte e chiuse. Il sistema bancario, per esempio, ha trovato nelle API e nell'open banking la soluzione per far parlare i vari sistemi proprietari.

In particolare, l'Open Banking ha permesso la creazione di API che consentono ai fornitori di servizi finanziari di condividere in modo sicuro e controllato i dati dei loro clienti con altre imprese, come ad esempio quelle nel ramo fintech o con i provider di servizi di pagamento. Ciò ha reso possibile l'interoperabilità tra sistemi chiusi, consentendo ai clienti di accedere a servizi finanziari più personalizzati e convenienti.

Per una crescita organica del Web3, le piattaforme di sviluppo di dApps come Ethereum necessitano di diventare sempre più interoperabili tra di loro e con il Web2.

Per esempio, **molte soluzioni Web 3.0 richiedono ancora l'uso di applicazioni Web 2.0 per alcune funzionalità, come l'autenticazione dell'utente o la fruizione di dati provenienti da fonti terze come il prezzo di un'azione o il pronostico di una partita di calcio.**

Inoltre, l'interoperabilità tra soluzioni Web 3.0 è importante poiché consente a diverse blockchain di comunicare e scambiarsi informazioni tra di loro, creando un ecosistema di reti peer to peer.

L'interoperabilità tra reti peer to peer è importante perché consente di creare un **ecosistema decentralizzato più ampio e robusto**. Invece di avere un singolo punto di controllo o di fallimento, le diverse soluzioni possono lavorare insieme per garantire l'integrità e la sicurezza della rete.

In conclusione, l'interoperabilità rappresenta un concetto importante nel mondo della blockchain e della tecnologia Web 3.0 poiché **consente alle diverse soluzioni di lavorare insieme in modo efficace e sicuro, creando un ecosistema più ampio, interconnesso e decentralizzato.**

5.2

Informatica

● Hard

Cosa sono i trigger e gli oracoli?

I **trigger** sono eventi che, una volta verificati, attivano automaticamente gli **smart contract**. Ad esempio, un trigger potrebbe essere un evento specifico sulla blockchain, come la conferma di una transazione o il raggiungimento di un determinato blocco, o un evento esterno come l'invio di una richiesta HTTP o la ricezione di un messaggio da un altro smart contract. Una volta che un trigger viene attivato, esso causa l'esecuzione automatica di uno o più smart contract.

Inoltre, un evento trigger sulla blockchain può far scattare una chiamata HTTP in una applicazione Web2, come per esempio la notifica di una transazione. In questo modo, il Web3 diventa trigger del Web2.

Gli **oracoli**, d'altra parte, sono fonti di sola informazione esterna che possono essere utilizzate dagli **smart contract** per prendere decisioni o completare operazioni. Gli oracoli forniscono informazioni su eventi esterni alla blockchain, come ad esempio i prezzi delle azioni, le condizioni meteorologiche o il risultato di un evento sportivo. Gli smart contract possono utilizzare queste informazioni per attivare trigger o eseguire altre operazioni.

I trigger e gli oracoli sono quindi **elementi chiave che permettono agli smart contract di interagire con l'ambiente esterno e di svolgere compiti più complessi**. Inserendo questi elementi, gli smart contract

possono diventare molto più flessibili e potenti, rendendoli adatti a molte più applicazioni. Tuttavia, è importante notare che i trigger e gli oracoli **presentano anche alcune sfide, come la sicurezza e l'affidabilità**, che devono essere affrontate per garantire un loro utilizzo più sicuro e affidabile negli smart contract.

Tuttavia, essi possono rappresentare **una fonte di vulnerabilità** per la sicurezza degli smart contract. Se un oracolo fornisce informazioni errate o false, gli smart contract che si basano su queste informazioni potrebbero eseguire operazioni errate o pericolose. Inoltre, i trigger e gli oracoli possono rappresentare una sfida per la scalabilità degli smart contract, poiché la quantità di dati che devono essere elaborati o trasmessi può essere significativa.

In termini di **potenzialità**, i trigger e gli oracoli rendono gli **smart contract molto più flessibili e potenti**, permettendogli di reagire a eventi esterni e di utilizzare informazioni esterne per prendere decisioni o completare operazioni. Ciò significa che gli smart contract possono adattarsi e rispondere alle situazioni in modo autonomo, rendendoli adatti a molte più applicazioni rispetto a quelle possibili senza questi elementi.

In conclusione, è importante sottolineare il fatto che gli **oracoli sono centralizzati e proprio per questo la loro affidabilità dipende dalla fonte di informazioni che utilizzano**. In ogni caso, essi rappresentano un'importante risorsa per lo sviluppo di contratti intelligenti e la creazione di soluzioni decentralizzate per la gestione dei dati.

5.3

Informatica

• Medium

Come possono interagire i protocolli Web3 tra di loro?

Per risolvere la sfida dell'interoperabilità, le community di sviluppatori hanno ideato diverse **soluzioni**. Una delle più comuni è stata la **creazione di standard tecnici nello stack per far sviluppare i contratti intelligenti**. Questi standard consentono di definire un insieme comune di regole e funzionalità che i progetti possono utilizzare per sviluppare i loro smart contract. Alcuni esempi di standard tecnici includono il token standard ERC-20 per Ethereum e il token standard BEP-20 per Binance Smart Chain.

Un'altra soluzione di interoperabilità è la **creazione di ponti digitali tra diverse blockchain**. Questi ponti digitali consentono di trasferire valuta o dati tra diverse blockchain senza la necessità di conversione in valuta fiat. Ad esempio, un ponte digitale tra Ethereum e Binance Smart Chain consente di trasferire token da una blockchain all'altra, attraverso passaggi atomici. Questi ponti digitali sono stati utilizzati per creare una connessione tra diverse blockchain come Ethereum, Bitcoin, Polkadot e Cosmos.

Infine, una soluzione di interoperabilità è la **creazione di token “avvolti” da un token sottostante (wrapped token)**. Questa soluzione consente di creare un token che ne rappresenta un altro, ma su una diversa blockchain. Ad esempio, un token WBTC rappresenta un bitcoin su Ethereum. Questi token avvolti sono utilizzati per connettere diverse blockchain come Ethereum e Bitcoin.

La seguente tabella riassume le soluzioni di interoperabilità discusse sopra:

Soluzione di interoperabilità	Descrizione
Standard tecnici nello stack	Definire un insieme comune di regole e funzionalità per sviluppare gli smart contract
Ponti digitali tra blockchain	Consentire il trasferimento di valuta o dati tra diverse blockchain
Token “avvolti”	Creare un token che ne rappresenta un altro su una diversa blockchain

5.4

Informatica

● Hard

Approfondimento Libreria WEB3.JS

Web3.js è **una collezione di librerie** che ti permette di interagire con un nodo Ethereum locale o remoto utilizzando HTTP, IPC o WebSocket. Questa documentazione ti guiderà attraverso l'installazione e l'esecuzione di Web3.js, oltre a fornire una documentazione di riferimento API con esempi.

Web3.js è fondamentale per la realizzazione del Web3 per vari motivi:

- **Interazione con la blockchain Ethereum:** Web3.js fornisce le funzionalità necessarie per interagire con la blockchain Ethereum. Questo include la possibilità di inviare transazioni, interrogare lo stato della blockchain e accedere ai dati memorizzati su di essa.
- **Comunicazione con i nodi Ethereum:** Web3.js consente alle applicazioni di comunicare con i nodi Ethereum, sia locali che remoti. Questo è fondamentale per le applicazioni che necessitano di interagire con la blockchain stessa.
- **Supporto per vari protocolli di comunicazione:** Web3.js supporta vari protocolli di comunicazione, tra cui HTTP, IPC e WebSocket. Questo lo rende versatile e adatto a una vasta gamma di applicazioni.
- **Integrazione con Metamask:** Web3.js è fondamentale per permettere a Metamask di interagire dal browser con i nodi su Infura. Infura è un servizio che fornisce nodi Ethereum accessibili via HTTP e WebSocket, eliminando la necessità per le applicazioni di eseguire il proprio nodo Ethereum. Metamask utilizza Web3.js per comunicare con questi nodi, permettendo agli utenti di inviare transazioni e interagire con contratti intelligenti direttamente dal loro browser.

Il punto chiave qui è il concetto di “provider”. Un provider in Web3.js è essenzialmente un mezzo di comunicazione tra l'applicazione JavaScript (ad esempio, un'applicazione web come Metamask) e un nodo Ethereum. Ci sono vari tipi di provider disponibili in Web3.js, tra cui HTTP, WebSocket e IPC. Quando si utilizza Metamask, il provider viene impostato su un nodo Ethereum su Infura. Questo permette a Metamask di inviare transazioni, leggere lo stato della blockchain e interagire con i contratti intelligenti, tutto direttamente dal browser dell'utente.

Ecco un esempio di come viene impostato il provider in Web3.js:

```
var Web3 = require('Web3');

// "Web3.givenProvider" sarà impostato se in un browser compatibile con Ethereum.
var Web3 = new Web3(Web3.givenProvider || 'ws://some.local-or-remote.node:8546');
```

In questo esempio, se l'applicazione viene eseguita in un browser compatibile con Ethereum (come Metamask), **Web3.givenProvider** sarà impostato sul provider fornito dal browser. In caso contrario, il provider sarà impostato su un nodo Ethereum locale o remoto specificato dall'URL.

Inoltre, Web3.js fornisce metodi per cambiare il provider dopo che è stato inizialmente impostato, il che può essere utile in alcune situazioni. In sintesi, **Web3.js è una componente chiave dell'ecosistema Web3, in grado di fornire le funzionalità necessarie per interagire con la blockchain Ethereum.**

5.5

Informatica

• Medium

Cos'è la compatibilità EVM?

Il concetto di blockchain EVM compatibili si riferisce alla capacità delle diverse blockchain di essere compatibili con la Ethereum Virtual Machine (EVM) e di poter quindi eseguire gli stessi smart contract sulla piattaforma Ethereum. Ciò significa che le blockchain compatibili con la EVM possono interagire direttamente con la blockchain Ethereum e con tutti i protocolli e le applicazioni che essa supporta. Questa compatibilità è fondamentale per promuovere l'interoperabilità tra le diverse blockchain e per consentire la creazione di ecosistemi decentralizzati ed interconnessi. Tuttavia, è importante notare che la compatibilità con la EVM ha anche i suoi limiti, poiché non tutte le funzionalità e le caratteristiche delle diverse blockchain sono supportate dalla EVM. Inoltre, l'utilizzo di diverse versioni della EVM può creare problemi di compatibilità tra le diverse blockchain.

Nonostante questi limiti, l'idea di blockchain EVM compatibili ha il potenziale per consentire una maggiore interoperabilità tra le diverse blockchain e di favorire lo sviluppo di soluzioni decentralizzate interconnesse e scalabili. Inoltre, oltre ad Ethereum, anche altre piattaforme hanno realizzato altri standard di compatibilità.

Per esempio, **Binance Smart Chain (BSC)** è una blockchain creata per supportare la creazione di applicazioni decentralizzate (dApp) e di contratti intelligenti, che utilizza una versione modificata della Ethereum Virtual Machine (EVM). **Questa versione modificata della EVM supporta gran parte delle funzionalità della EVM di Ethereum, ma è stata ottimizzata per fornire una maggiore scalabilità e velocità di elaborazione.**

Nella pratica, le dApps e i contratti intelligenti scritti per la blockchain Ethereum possono essere facilmente trasferiti e utilizzati sulla Binance Smart Chain, senza la necessità di doverli riscrivere o adattare in modo significativo. Ciò favorisce la creazione di ecosistemi interconnessi e l'interoperabilità tra le diverse blockchain.

Tuttavia, è importante notare che la **Binance Smart Chain non è completamente compatibile con la blockchain Ethereum**, poiché non tutte le funzionalità e le caratteristiche della EVM di Ethereum sono supportate dalla versione modificata utilizzata sulla Binance Smart Chain.

5.6

Informatica

• Medium

Come funziona uno scambio atomico (Atomic Swap) tra due reti?

Gli **Atomic Swap** sono un'ulteriore soluzione per abilitare gli utenti a scambiarsi coppie di digital assets, senza la necessità di intermediari, direttamente sulla blockchain. La peculiarità degli Atomic Swap sta nella loro capacità di promuovere l'interoperabilità tra diverse blockchain, nonostante non sempre i set di regole dei protocolli siano del tutto compatibili l'uno con l'altro.

Gli **Atomic Swap risolvono questo problema consentendo alle diverse blockchain di scambiarsi valute in modo diretto e sicuro**, senza dover passare attraverso terze parti o scambi centralizzati. In sostanza, gli Atomic Swap rappresentano una soluzione innovativa e sicura per il trasferimento diretto di valute tra due parti, promuovendo al contempo l'interoperabilità tra le diverse blockchain.

La logica base del funzionamento di Atomic Swap si basa sulla **creazione di una transazione all'interno di un blocco che avrà successo solo se entrambe le parti coinvolte completeranno tutte le condizioni**

per lo scambio. Ciò significa che **ogni parte coinvolta deve prima bloccare i propri fondi in uno smart contract**, che funge da garante dell'operazione e solo dopo che entrambe le parti hanno compiuto tale operazione il contratto intelligente può rilasciare i fondi alla parte destinataria.

Il processo di Atomic Swap può essere complesso, ma può essere compreso meglio attraverso un esempio: supponiamo che Alice voglia scambiare 1 Bitcoin con Bob per 10 Ether. Alice inizia il processo bloccando 1 Bitcoin in un contratto intelligente, che invia a Bob una chiave privata crittografata. Bob, a sua volta, blocca 10 Ether in un contratto intelligente e invia ad Alice una chiave privata crittografata. In questo modo, entrambe le parti hanno bloccato i propri fondi e hanno accesso alla chiave privata crittografata dell'altra parte. Quando entrambe le parti sono pronte a completare lo scambio, Alice sblocca i 10 Ether di Bob usando la chiave privata di Bob e Bob sblocca il Bitcoin di Alice usando la sua chiave privata. Solo quando entrambi i fondi sono stati sbloccati, il contratto intelligente può rilasciarli alla parte destinataria.

Gli Atomic Swap sono stati **utilizzati con successo per scambiare diverse coppie di valute tra le diverse blockchain**, come ad esempio Bitcoin e Litecoin o Ethereum e Bitcoin. Inoltre, gli Atomic Swap sono stati **utilizzati anche in ambienti di testnet** per dimostrare la loro efficacia e sicurezza. Un esempio è il testnet di Bitcoin, dove gli sviluppatori hanno utilizzato gli Atomic Swap per scambiare Bitcoin e Litecoin senza l'intermediazione di un terzo. Questo ha dimostrato la capacità di Atomic Swap di funzionare anche in ambienti complessi come una blockchain testnet.

5.7

Informatica

● Medium

Perchè gli Atomic swap possono offrire sicurezza nella finanza decentralizzata?

Gli **eventi rappresentano un elemento importante dei contratti intelligenti** e permettono di tracciare le attività all'interno della blockchain. Nel caso degli Atomic Swap, gli eventi sono particolarmente importanti in quanto consentono alle parti coinvolte di monitorare lo stato dell'operazione in tempo reale e di avere la certezza che l'operazione sia stata completata con successo.

Nello specifico di Atomic Swap tra Bitcoin ed Ethereum, gli eventi sono deterministici e pubblici sulle rispettive blockchain, il che rafforza il concetto di interoperabilità tra le due piattaforme. Ciò significa che le parti coinvolte possono verificare in modo autonomo che lo scambio sia stato completato correttamente e che nessuna delle parti abbia tentato di frodare l'altra.

Ad esempio, nel caso di uno scambio tra Bitcoin ed Ethereum, gli eventi associati alla transazione sulla blockchain Bitcoin possono essere tracciati utilizzando un esploratore di blocchi come Blockchain.info, mentre gli eventi associati alla transazione sulla blockchain Ethereum possono essere tracciati utilizzando un esploratore di blocchi come Etherscan.

L'utilizzo degli eventi consente quindi di aumentare la trasparenza e la sicurezza degli scambi tra diverse blockchain, promuovendo così l'interoperabilità tra le piattaforme e **facilitando l'adozione dei digital assets e delle tecnologie blockchain da parte del pubblico**. Questo strumento crittografico è utilizzato in molte applicazioni della finanza decentralizzata come escrow deterministico tra due attori.

5.8

Informatica

• Hard

Perché gli Atomic Swap possono essere una vulnerabilità nella Finanza Decentralizzata?

Il 6 luglio 2023, il protocollo cross-chain Multichain ha subito prelievi insolitamente grandi e non autorizzati, **che sembrano essere il risultato di un attacco hacker o di un “rug pull” da parte degli interni**. Questo exploit ha portato a perdite di oltre 125 milioni di dollari, rendendolo uno dei più grandi attacchi crittografici registrati.



Rug pull

Un rug pull (che letteralmente significa tirare il tappeto da sotto i piedi) sostanzialmente è un furto. Si verifica quando hacker o team che hanno avviato un progetto prelevano i fondi degli investitori, attraverso l'exploit di bugs e/o errori logici di uno smart contract.

I protocolli di bridge cross-chain sono spesso obiettivi lucrativi per gli hacker, principalmente a causa dei loro design sperimentali e del fatto che generalmente hanno grandi depositi centralizzati di asset trasferiti dagli utenti ad altre blockchain. Tuttavia, Multichain ha recentemente riscontrato alcuni problemi notevoli non correlati al suo design del protocollo, suscitando sospetti che questo recente exploit potrebbe essere stato condotto da interni.

Più di 125 milioni di dollari di cripto asset sono stati prelevati da Multichain, con quasi 120 milioni di dollari provenienti dal ponte Fantom di Multichain.

Gli smart contract di Multichain sono protetti da un sistema di calcolo multi-party (MPC), che funziona in modo simile a un sistema di portafoglio multisig. Invece di fare affidamento su chiavi private, i sistemi MPC dividono essenzialmente frammenti di una chiave privata tra molte parti diverse che possono quindi cooperare per eseguire transazioni. Tuttavia, come i portafogli multisig, questi sistemi sono ancora vulnerabili se un attaccante è in grado di ottenere il possesso di un numero sufficiente di chiavi MPC. È possibile che l'attaccante abbia ottenuto il controllo delle chiavi MPC di Multichain per portare a termine questo exploit.

È interessante notare che l'attaccante non ha scambiato asset controllati centralmente come USDC, che possono essere congelati dalla società emittente (Circle, nel caso di USDC), insieme agli indirizzi che detengono tali asset. La maggior parte degli hacker cerca di scambiare rapidamente i fondi per quelli che non sono vulnerabili a tali misure di sicurezza. Infatti, Circle e Tether hanno entrambi congelato diversi indirizzi che detenevano asset prelevati da Multichain, impedendo a questi fondi di essere trasferiti o scambiati per altri asset. In totale, gli indirizzi congelati dai due emittenti di stablecoin detengono circa 65 milioni di dollari in asset rubati da Multichain.

L'exploit di Multichain è potenzialmente il risultato della compromissione delle chiavi dell'amministratore. Mentre è possibile che queste chiavi siano state prese da un hacker esterno, molti esperti di sicurezza e altri analisti pensano che questo exploit potrebbe essere un lavoro interno o un rug pull, in parte a causa dei recenti problemi riscontrati da Multichain.

Questo incidente sottolinea **l'importanza della fiducia nel codice scritto da terzi**. Mentre gli audit del codice possono aiutare a identificare potenziali problemi, la fiducia nel team di sviluppo e nella sicurezza delle chiavi private rimane fondamentale. In questo caso, sembra che le chiavi siano state compromesse, piuttosto che il codice difettoso, sottolineando la necessità di una gestione sicura delle chiavi e della fiducia nei team di sviluppo.

5.9

Informatica

● Hard

Approfondimento Atomic Swap su Ethereum

In un ambiente di testnet, gli Atomic Swap possono essere **utilizzati anche per sperimentare diverse coppie di valute e testare la loro sicurezza**. Ciò può aiutare gli sviluppatori a creare applicazioni basate su Atomic Swap ed inoltre, il loro utilizzo in ambienti di testnet, ha dimostrato la loro sicurezza e capacità di funzionare anche in ambienti complessi.

Abbiamo visto nelle diverse parti del manuale che Solidity è il linguaggio di programmazione utilizzato per creare contratti intelligenti sulla blockchain Ethereum. Implementare Atomic Swap in Solidity richiede l'utilizzo di alcuni concetti fondamentali come le funzioni hash crittografiche e la gestione degli eventi.

Il codice sorgente di un contratto Atomic Swap in Solidity è solitamente suddiviso in tre parti: **lo stato del contratto, le funzioni che definiscono il comportamento del contratto e gli eventi che vengono generati durante l'esecuzione del contratto**. Una volta creato il contratto Atomic Swap, le due parti coinvolte nell'operazione possono inviare i fondi a una transazione di blocco creata dal contratto stesso. La transazione di blocco viene quindi bloccata e l'operazione di scambio diventa “atomic”, ovvero viene eseguita solo se entrambe le parti completano la loro parte dello scambio.

In sostanza, il contratto Atomic Swap permette di scambiare un digital asset per un altro in maniera sicura e senza l'ausilio di intermediari. **Le funzioni del contratto garantiscono la validità dell'operazione, proteggendola mediante l'utilizzo di un codice segreto**. Inoltre, il contratto prevede la possibilità di annullare l'operazione nel caso in cui una delle parti non rispetti le condizioni dell'accordo.

In conclusione, gli Atomic Swap rappresentano uno strumento importante per la promozione dell'interoperabilità tra diverse blockchain, consentendo lo scambio di digital assets in maniera sicura e senza l'ausilio di intermediari.

5.10

Informatica

● Medium

Che cosa si intende per Wrapped Token?

Come accennato in precedenza, i **wrapped token sono digital assets che rappresentano l'equivalente di un altro asset digitale all'interno di una diversa blockchain**. In pratica, un wrapped token è un token “avvolto” attorno ad un altro token, in modo che possa essere **utilizzato all'interno di una blockchain diversa da quella in cui è stato originariamente emesso**.

Ad esempio, un **wrapped Bitcoin (WBTC) è un token basato sulla blockchain Ethereum che rappresenta l'equivalente di un bitcoin “reale”**. I bitcoin vengono depositati presso un custode affidabile, che emette i corrispondenti WBTC sulla blockchain Ethereum. Questi WBTC possono essere utilizzati per partecipare a contratti intelligenti e applicazioni decentralizzate sulla blockchain Ethereum.

In questo modo, i wrapped token **consentono di aumentare l'interoperabilità tra diverse reti, consentendo a utenti e sviluppatori di utilizzare asset provenienti da una blockchain all'interno di un'altra blockchain**.

6

Cosa posso salvare sulla blockchain?

- 6.1 Come funziona la notarizzazione su una rete peer to peer come Bitcoin?
- 6.2 Approfondimento sulla marcatura temporale senza permessi (trustless timestamping)
- 6.3 I paradossi della blockchain nella supply chain
- 6.4 Il caso di IBM Merks
- 6.5 Come si possono scrivere degli Smart Legal Contract?
- 6.6 Decreto semplificazioni e lo stallo dell'Agid

6.1

Come funziona la notarizzazione su una rete peer to peer come Bitcoin?

Il servizio di **trustless timestamping** potrebbe liberalizzare il mercato della marcatura temporale online e di alcuni dei servizi offerti dalle **trust authority**. Questo sistema utilizza la blockchain per associare nuovi metadati (una marca temporale) ad un documento senza il bisogno di affidarsi ad un'autorità centrale o ad un intermediario di fiducia. Ciò significa che l'accuratezza e la validità della marca temporale non dipendono da una singola fonte, ma sono garantite dalla rete blockchain stessa.



Trust authority

Definizione: Operatore autorizzato ad avere un grado di fiducia by default. Per esempio, un notaio è una figura preposta a dare garanzie a favore di terze parti

Il vantaggio del servizio di trustless timestamping è che la marca temporale è registrata in modo decentralizzato e immutabile, rendendolo immune a manipolazioni o cambiamenti da parte di un singolo ente o individuo. Al contrario, i servizi trusted possono essere influenzati da fattori esterni come la mancanza di trasparenza o la compromissione dell'autorità centrale.

Il trustless timestamping funziona registrando la data e l'ora della transazione sulla blockchain. Ogni volta che viene creato un nuovo blocco, viene anche registrato un timestamp che indica l'ora esatta in cui è stato creato.

6.2

Approfondimento sulla marcatura temporale senza permessi (trustless timestamping)

Informatica

● Hard

Un altro esempio riguarda l'utilizzo dello **script di Bitcoin OP_Return per inserire un hash di un documento in una transazione sulla blockchain**. OP_Return è un'opzione di script che consente di inserire una quantità limitata di dati nella blockchain, rendendolo un ottimo strumento per il timestamping di documenti o informazioni.

Il motivo per cui si inserisce un hash del documento invece che il documento stesso all'interno della transazione sulla blockchain è per garantire la protezione e la sicurezza dei dati.

Un hash è una rappresentazione univoca di un insieme di dati che viene generata utilizzando un algoritmo di hash crittografico. Questo algoritmo garantisce che per ogni insieme di dati ci sia un solo hash possibile e che qualsiasi cambiamento nei dati originali produrrà un hash completamente diverso.



Funny Facts

Uno sviluppatore sudcoreano ha fatto storia il 27 aprile 2018 quando ha deciso di registrare i dettagli di un trattato di pace tra Corea del Nord e Corea del Sud sulla blockchain di Ethereum.

Ryu Gi-hyeok ha creato due transazioni ETH con documenti in coreano e inglese della Dichiarazione di Panmunjom, firmata dai leader Moon Jae-in e Kim Jong-un al Summit intercoreano del 2018.

Inserire un hash del documento in una transazione sulla blockchain permette di verificare l'integrità e l'esistenza del documento senza che il documento stesso venga reso pubblico o soggetto a possibili manipolazioni. Ciò significa che gli utenti possono verificare che il documento esiste e che non è stato modificato, senza che il contenuto del documento sia visibile o accessibile a chiunque. Inoltre, poiché i blocchi sulla blockchain sono immutabili e la verifica del timestamp avviene tramite l'hash, **l'utilizzo dell'hash garantisce che la prova di esistenza del documento sia sicura e verificabile anche in futuro.** Questo è importante soprattutto per documenti legali o contratti che devono essere verificabili e immutabili nel tempo.

6.3

Business

• Basic

I paradossi della blockchain nella supply chain

Dal 2016, si è letto su molte testate giornalistiche la nascita di progetti legati al mondo blockchain relativi al **tracciamento di beni all'interno di una filiera**. L'obiettivo comune era **fornire maggiore trasparenza** verso il consumatore e tutti gli attori coinvolti.

Tuttavia, a distanza di anni, molti progetti non hanno trovato abbastanza risonanza, facendo diminuire l'utilizzo di questa tecnologia all'interno delle supply chain.

Oltre al problema dei costi, un ulteriore aspetto che potrebbe aver contribuito al fallimento di molti progetti è il paradosso tra ciò che è considerato vero, autentico e ciò che la blockchain può garantire come strumento di root of trust.

Come abbiamo analizzato in precedenza, ai **dati notarizzati viene attribuito un timestamp ed address di provenienza**. Tuttavia, questi due metadati rappresentano solamente che "il dato x esiste da un tempo t, e che è stato caricato da un attore y". Questo aspetto è molto importante poiché la blockchain non fornisce alcuna garanzia rispetto alla veridicità dei contenuti all'interno del dato. Infatti, all'interno del database distribuito, viene inserito l'hash value del documento, non la versione in chiaro. Quindi, **non vi è alcuna analisi qualitativa del contenuto, confermando questo bias cognitivo che la blockchain non garantisce la veridicità dell'informazione, ma esclusivamente la sua esistenza**.

Certo è, come abbiamo visto in precedenza, la notarizzazione dell'hash garantisce anche una immutabilità del contenuto x al tempo t, ed in alcune situazioni in cui il documento rappresenti due parti contrapposte di interesse, potrebbe essere comodo come prova nel tempo.

6.4

Business

Basic

Il caso di IBM Maersk

La notizia che **Maersk e IBM abbiano deciso di ritirare l'offerta di supply chain basata sulla blockchain, TradeLens**, è stata riportata da diverse fonti di settore, tra cui Reuters e Cointelegraph.

TradeLens è stata lanciata nel 2018 come una piattaforma basata sulla tecnologia blockchain per la gestione delle informazioni sulla catena di fornitura globale, con l'**obiettivo di migliorare la trasparenza e la sicurezza delle transazioni commerciali tra aziende**. La piattaforma è stata sviluppata in collaborazione tra Maersk, la più grande compagnia di navigazione al mondo, e IBM, una delle principali aziende di tecnologia al mondo.

Secondo quanto riportato da Maersk e IBM, il **motivo principale del ritiro dell'offerta** di TradeLens è la mancanza di una piena collaborazione globale del settore. **Nonostante gli sforzi fatti per coinvolgere altre aziende nella piattaforma, sembra che la maggior parte del settore della logistica e della spedizione non abbia aderito in modo significativo alla piattaforma**, compromettendone la redditività commerciale.

La **decisione di ritirare TradeLens rappresenta un colpo per la crescita della tecnologia blockchain** nell'ambito della gestione della catena di fornitura globale. Tuttavia, ci sono ancora molte **altre aziende che stanno investendo in questo settore**, come ad esempio DHL, FedEx e UPS, che stanno sviluppando progetti basati sulla blockchain per migliorare la trasparenza e la sicurezza delle operazioni commerciali.

In ogni caso, l'esperienza di TradeLens offre spunti di riflessione sulle sfide che la tecnologia blockchain deve ancora affrontare per diventare una soluzione affidabile e profittevole per la gestione della catena di fornitura globale.

Fonti

► <https://www.shipmag.it/blockchain-maersk-e-ibm-chiudono-la-piattaforma-tradelens-non-e-risultata-fattibile/>

6.5

Informatica / Legale

Medium

Come si possono scrivere degli Smart Legal Contract?

Il Ricardian Contract è un formato di contratto digitale che incorpora sia il testo del contratto che la sua rappresentazione in formato digitale, fornendo una maggiore automazione nell'esecuzione di transazioni e contratti.

Dal punto di vista informatico, il Ricardian Contract prevede l'**uso di una specifica sintassi di markup per la descrizione del contratto**. In particolare, viene utilizzato un formato **XML**, che consente di definire il testo del contratto e le condizioni che devono essere soddisfatte per la sua esecuzione.

I Ricardian Contract possono avere diverse conseguenze. Innanzitutto, consentono una **maggior automazione nell'esecuzione di transazioni e contratti**, riducendo la necessità di interventi umani e aumentando l'efficienza dei processi. Inoltre, possono fornire **maggior trasparenza e tracciabilità delle transazioni**, grazie alla possibilità di registrare i dettagli del contratto in una blockchain o un registro distribuito.

Tuttavia, l'adozione dei Ricardian Contract potrebbe anche presentare **alcuni problemi, ad esempio la necessità di standardizzare il formato del contratto per consentire l'interoperabilità tra diverse piattaforme e protocolli.** Inoltre, è necessario **garantire la sicurezza e la privacy** dei dati contenuti nei contratti, in particolare quando vengono utilizzati in contesti sensibili come il settore finanziario.

I Ricardian contract sono contratti digitali che **combinano il linguaggio giuridico con quello informatico**, con lo scopo di creare un contratto che sia leggibile sia dalle persone che dai computer. Questo viene reso possibile dall'**inclusione di un documento legale strutturato in un formato standard**, come ad esempio il formato HTML, **all'interno del contratto digitale**.

Per creare un Ricardian contract in Solidity, si può utilizzare una libreria specifica come, ad esempio, la **Ricardian template library** (RTL), che **fornisce gli strumenti necessari per implementare questi contratti**. Una volta che il contratto è stato implementato, viene caricato sulla blockchain e può essere utilizzato come qualsiasi altro contratto.

Le conseguenze dei Ricardian contract sono molteplici e interessano diversi ambiti. Ad esempio, l'utilizzo di questi contratti può **rendere più efficienti e trasparenti i processi di negoziazione e di stipula di contratti**, poiché le parti coinvolte possono accedere facilmente al contenuto del contratto e verificarne l'autenticità. Inoltre, **l'inclusione di un documento legale strutturato all'interno del contratto digitale può rendere più facile l'interpretazione del contratto** da parte delle parti coinvolte e dei tribunali in caso di eventuali dispute.

Tuttavia, l'utilizzo dei Ricardian contract solleva anche **alcune problematiche**, come ad esempio la **necessità di stabilire standard comuni per i documenti legati ai contratti e la necessità di garantire la sicurezza dei contratti digitali**, per evitare eventuali attacchi informatici che potrebbero compromettere l'autenticità del contratto stesso.

6.6

Legal

Basic

Decreto semplificazioni e lo stallo dell'Agid

Il 12 febbraio 2019 è stato pubblicato in Gazzetta Ufficiale il decreto legge 14 dicembre 2018, n. 135, coordinato con la legge di conversione 11 febbraio 2019, n. 12, "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione" ("Decreto Semplificazioni"). Quest'ultimo ha **introdotto diverse modifiche normative per semplificare e snellire la burocrazia, anche nell'ambito della tecnologia blockchain e dei contratti intelligenti** (smart contract).

Il decreto ha previsto all'articolo 8-ter, rubricato "tecnologie basate su registri distribuiti e smart contract", la definizione di "tecnologie basate su registri distribuiti" e di "smart contract". Il vantaggio di questa introduzione nel nostro ordinamento è conferire valore legale anche ad un documento informatico in blockchain. Di fatto questo tipo di memorizzazione produce i medesimi effetti giuridici della validazione temporale elettronica, definita dall'art.4 Regolamento UE n.910/2014: "dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento".

Nella pratica quindi qualsiasi documento concepito con questa tecnologia è a livello giuridico valido, ma solo per quanto riguarda il riconoscimento giuridico temporale e identificativo delle parti. Questa apertura verso la tecnologia blockchain rappresenta sicuramente un grosso passo in avanti nella sua legittimazione e riconoscimento delle sue potenzialità, ma allo stesso modo l'Agenzia per l'Italia Digitale (**Agid**) non ha ancora fornito le linee tecniche per dare concretezza all'attuazione delle nuove norme. Ciò ha creato una certa incertezza nell'ambito delle applicazioni della tecnologia blockchain e degli smart contract, in quanto i soggetti interessati non hanno ancora una guida tecnica precisa e affidabile per poter utilizzare queste tecnologie in modo sicuro e conforme alle norme.

Fonti

- ▶ <https://www.dirittobancario.it/art/distributed-ledger-technology-e-smart-contract-finalmente-e-legge-prime-riflessioni-su-una-rivoluzione/>
- ▶ <https://www.gazzettaufficiale.it/eli/id/2018/12/14/18G00163/sg>
- ▶ <https://www.startmag.it/innovazione/litalia-accelera-su-blockchain-e-dlt-che-cosa-cambia-davvero-con-il-decreto-semplificazioni/>

7

Metaverso

- 7.1 La gamification nel Web3
- 7.2 Dal gaming al metaverso
- 7.3 L'architettura del metaverso
- 7.4 Tokenomics di un metaverso
- 7.5 Come funziona il modello play to earn?
- 7.6 Industrie correlate ed i rischi nella realtà virtuale

7.1

Business

Basic

La gamification nel Web3

Il concetto di **gamification** si riferisce all'uso di elementi di gioco, come le regole, le sfide e le ricompense, in contesti non ludici al fine di aumentare l'**engagement, la motivazione e l'interesse degli utenti**. La gamification è stata applicata con successo in diversi contesti, come l'educazione, la salute, il marketing e il lavoro.

In ambito **Web3**, la gamification può essere utilizzata come **modello di incentivi per aumentare l'adozione e l'utilizzo di piattaforme decentralizzate e di digital assets**. Ad esempio, la creazione di giochi basati su blockchain può incentivare gli utenti a partecipare alle reti blockchain e a completare determinate azioni, come l'estrazione di token o la partecipazione a votazioni. Inoltre, l'uso di ricompense token può essere utilizzato come incentivo per i giocatori e come forma di pagamento per i creatori di giochi. Ci sono **diverse ricerche accademiche** sulla gamification in ambito Web3. Ad esempio, uno studio del 2020 ne ha esplorato l'uso come incentivo per l'adozione di digital assets, suggerendo che la gamification può migliorare la percezione degli utenti sugli asset digitali e aumentare la loro motivazione a partecipare alle reti blockchain. Altri studi invece ne hanno esaminato l'uso come strumento per aumentare la partecipazione alle reti blockchain e per migliorare la sicurezza delle reti tramite l'incentivazione di comportamenti virtuosi.

Fonti

- Giuseppe Littera, Gianni Fenu, Marco Carboni, Andrea Piras. "Blockchain and Gamification: An Empirical Study of Users' Perception and Motivation". International Journal of Human-Computer Interaction, 2020. DOI: 10.1080/10447318.2020.1733755.

7.2

Business

Basic

Dal gaming al metaverso

L'industria del **gaming** è cresciuta in modo esponenziale negli ultimi anni, diventando **una delle industrie più redditizie e innovative del mondo**.

Per comprendere meglio la portata di questo settore, è possibile confrontarlo con altre industrie. Ad esempio, l'industria del cinema, che è stata a lungo una delle principali fonti di intrattenimento, ha raggiunto un valore di mercato di 97,5 miliardi di dollari nel 2019, secondo il report MPAA. L'industria dei videogiochi, invece, ha raggiunto un valore di 372 miliardi di dollari nel 2023, secondo i dati di Statista. Altre metriche interessanti per comprendere l'evoluzione dell'industria del gaming sono le seguenti:

- si prevede che i ricavi mostreranno un tasso di crescita annuale (CAGR 2023-2027) del 7,80%, con un volume di mercato previsto di 502,40 miliardi di dollari entro il 2027.
- Nel segmento dei videogiochi, il numero di utenti dovrebbe raggiungere i 3,04 miliardi entro il 2027.
- La penetrazione di mercato prevista è del 34,5% nel 2023 e dovrebbe raggiungere il 38,3% entro il 2027.
- Il segmento più grande è quello dei giochi per dispositivi mobili, con un volume di mercato di 315,90 miliardi di dollari nel 2023.

- Nel confronto globale, la maggior parte delle entrate sarà generata in Cina (107.300 milioni di dollari USA nel 2023).
- Il ricavo medio per utente (ARPU) nel segmento dei videogiochi dovrebbe raggiungere i 140,20 dollari USA nel 2023.

Inoltre, **l'introduzione di nuove tecnologie come la realtà virtuale e la realtà aumentata sta trasformando l'esperienza di gioco**, creando nuove opportunità per gli sviluppatori. Secondo i dati presi da Statista, si prevede che il mercato globale della realtà virtuale e aumentata raggiungerà un valore di 72,8 miliardi di dollari entro il 2024.

La crescita del settore ha portato anche all'innovazione delle modalità di business, come il modello di gioco **Play-to-Earn**, che **premia i giocatori con digital assets o altri beni virtuali**. Secondo i dati della DappRadar, il volume totale del mercato dei giochi decentralizzati è cresciuto del 26% nel mese di gennaio 2022, raggiungendo i 3,6 miliardi di dollari.

Questo modello è stato ampiamente sposato da progetti di puro gaming all'interno del mondo Web3. Parallelamente, molti progetti hanno creato dei veri e propri mondi virtuali all'interno dei quali i giocatori possono vincere token e scambiarli per altri digital assets e valute tradizionali. **Benvenuti nel metaverso.**

Fonti

- ▶ <https://www.statista.com/outlook/dmo/digital-media/video-games/worldwide#:~:text=Revenue%20in%20the%20Video%20Games.US%24372.00bn%20in%202023>

7.3

Informatica

• Basic

L'architettura del metaverso

Un metaverso è un mondo virtuale, creato da sviluppatori, attraverso il quale gli utenti possono **relazionarsi, fare attività insieme e/o competitive, o semplicemente esplorare**. Rispetto a quest'ultima attività, alcune aziende hanno comprato degli spazi virtuali all'interno di metaversi, definiti come virtual land. Questo è stato principalmente pensato come nuova modalità di fare awareness online all'interno di nuovi "social network tridimensionali".



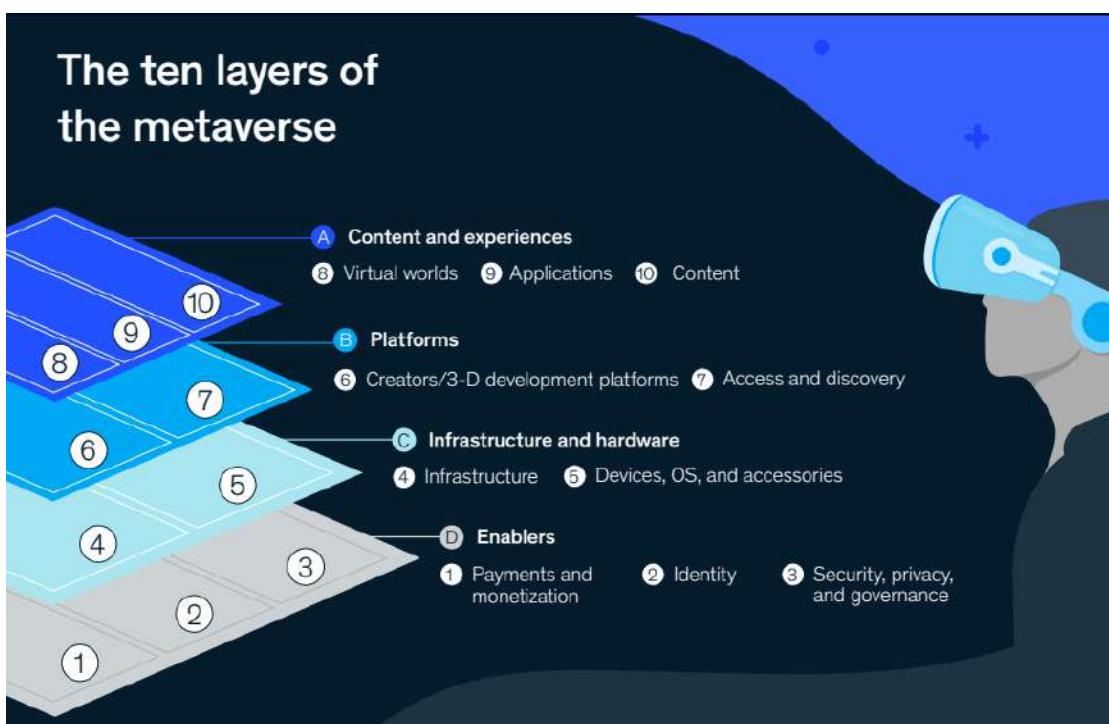
Funny Facts

La land virtuale può essere utilizzata per diverse finalità come la costruzione di edifici digitali o per giochi "play-to-earn". Molte aziende hanno creato dentro la propria land degli edifici virtuali all'interno dei quali un utente può giocare, prendere informazioni e contatti delle aziende o anche comprare dei prodotti e servizi.

A seguito la mappa di The SandBox, all'interno della quale si possono trovare molte aziende Web2 e Web3 che hanno comprato il loro spazio di terra virtuale.



La struttura di un metaverso può essere immaginata come l'unione di più tecnologie (o più livelli), le quali combinate, possono garantire una esperienza immersiva e soddisfacente per l'utente.



Ogni livello contribuisce alla creazione di un'infrastruttura completa per il funzionamento di un **metaverso**, consentendo agli utenti di interagire tra di loro, creare contenuti e persino guadagnare denaro virtuale all'interno del mondo virtuale. Di seguito verrà fornita una descrizione di ogni livello di un'esperienza virtuale nel metaverso, prendendo spunto da un report di McKinsey:

1. **Dispositivi e sensori:** il primo livello è costituito dai dispositivi hardware e dai sensori, come smartphone, occhiali di realtà virtuale e aumentata, e sensori IoT, che consentono agli utenti di accedere nella realtà virtuale dentro il metaverso.
2. **Protocolli e standard:** il secondo livello comprende i protocolli e gli standard tecnologici che regolano l'interazione tra gli utenti, garantendo l'interoperabilità tra gli ambienti virtuali. Questi protocolli includono la tecnologia blockchain, i protocolli di sicurezza e le norme per la creazione di contenuti.
3. **Cloud e infrastruttura:** il terzo livello riguarda la scalabilità, con l'utilizzo di server cloud e altre infrastrutture tecnologiche per garantire un'esperienza fluida agli utenti.
4. **Piattaforme e applicazioni:** il quarto livello comprende le piattaforme e le applicazioni che forniscono l'accesso, come giochi online, piattaforme di realtà virtuale e aumentata oltre ad app per dispositivi mobili.
5. **Contenuti generati dall'utente:** il quinto livello riguarda la creazione di contenuti da parte degli utenti stessi. Questo include la creazione di ambienti virtuali, oggetti e avatar personalizzati.
6. **Esperienza utente:** il sesto livello si concentra sull'esperienza utente all'interno, compresi i meccanismi di interazione, l'audio e la grafica avanzata.
7. **Socializzazione e comunità:** il settimo livello include gli aspetti sociali, come la creazione di comunità, la socializzazione e la collaborazione.
8. **Economia:** l'ottavo livello riguarda l'economia digitale, dove gli utenti possono acquistare, vendere e scambiare beni e servizi virtuali utilizzando digital assets e altri mezzi di pagamento digitali.
9. **Standard etici, governance e sicurezza:** il decimo livello comprende gli standard etici e sociali che guidano l'interazione tra gli utenti. Questi standard includono la privacy, la sicurezza, l'etica e i diritti digitali.
10. **Identità:** l'ultimo livello riguarda la creazione di un'identità digitale che possa essere gestita in maniera autonoma e decentralizzata.

Questi **10 livelli descrivono i vari aspetti di una realtà virtuale in metaverso** e come essi sono interconnessi tra loro. La comprensione di questi livelli è importante per comprendere l'evoluzione e le sue potenziali applicazioni future.

Fonti

- <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse>

7.4

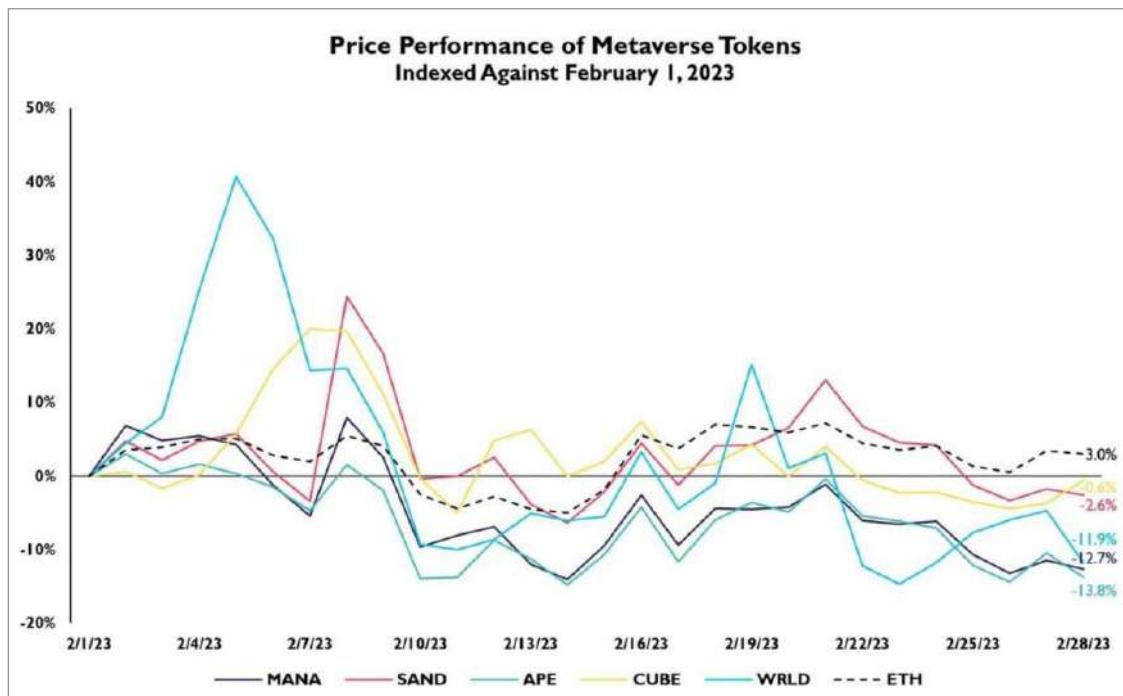
Business

● Basic

Tokenomics di un metaverso

Il metaverso è un **ambiente virtuale in cui le persone possono interagire, comunicare e partecipare a diverse attività in modo immersivo e interattivo**. Le aziende che operano nel metaverso utilizzano spesso modelli di tokenomics per creare e gestire il valore dei loro prodotti e servizi. I **principali modelli di tokenomics utilizzati nel metaverso includono:**

- **Token di utilità:** sono token che offrono accesso ai servizi e alle funzionalità all'interno del metaverso, come l'acquisto di beni virtuali, l'accesso a giochi o servizi di intrattenimento. Questi token sono spesso utilizzati come forma di pagamento all'interno del metaverso.
- **Token di governance:** sono token che offrono diritti di voto e decisione sugli sviluppi futuri del metaverso. Questi token sono spesso utilizzati per coinvolgere la comunità nella gestione e nella governance del metaverso.
- **Token di investimento:** sono token che offrono la possibilità di investire in un progetto nel metaverso come, per esempio, le **land virtuali**. Questi token possono offrire rendimenti in base al successo del progetto e all'adozione del metaverso.
- **Token di creatori di contenuti:** sono token che offrono la possibilità ai creatori di contenuti di monetizzare il proprio lavoro all'interno del metaverso. Questi token possono essere utilizzati come forma di pagamento per il lavoro svolto dai creatori di contenuti.
- **Token di apprezzamento:** sono token che offrono ai partecipanti del metaverso la possibilità di apprezzare il lavoro dei creatori di contenuti, premiandoli con una forma di valuta virtuale che può essere utilizzata all'interno del metaverso.



L'ERC20 e l'ERC721 sono standard di token Ethereum utilizzati per creare token digitali all'interno del metaverso. Qui un elenco dettagliato di alcuni esempi:

Tipo di Token	Descrizione	Esempi ERC20	Esempi ERC721
Token di Governance	I token di governance sono utilizzati per consentire ai titolari di partecipare alle decisioni relative alla gestione della piattaforma o del protocollo, come le decisioni sulle modifiche al codice o sulle politiche di voto.	MKR, GRT, UNI	-
Token di Piattaforma	Questi token sono utilizzati come valuta all'interno della piattaforma, consentendo agli utenti di effettuare transazioni ed accedere ai servizi offerti dalla piattaforma stessa.	BNB, HT, OKB	-

Ricompense	Questi token vengono utilizzati per premiare gli utenti per aver svolto determinate attività all'interno della piattaforma, come la partecipazione alle votazioni o il fornire liquidità per il trading.	SNX, COMP, AAVE	-
Token di Proprietà Immobiliare (Land)	Questi token rappresentano proprietà immobiliari digitali, come terre virtuali o edifici in contesti di realtà virtuale.	Decentraland (LAND), The Sandbox (SAND), Somnium Space (CUBE)	-
Power-Up oggetti unici (ERC721)	Questi token rappresentano oggetti unici, che possono essere utilizzati per potenziare personaggi o oggetti all'interno di giochi online.	Axie Infinity (AXS), Gods Unchained (GODS), ChainGuardian (CGG)	CryptoKitties, CryptoPunks, Bored Ape Yacht Club (BAYC)
Oggetti fungibili (ERC1155)	Questi token rappresentano oggetti fungibili, cioè identici e interscambiabili tra loro. Possono essere utilizzati in giochi online per rappresentare armi, oggetti da collezione e altri beni virtuali.	Enjin Coin (ENJ), The Sandbox (SAND), F1 Delta Time (REV)	-

7.5

Psicologia / Business

● Basic

Come funziona il modello play to earn?

Il **Play-to-Earn (P2E)** è un modello di gioco che premia i giocatori con digital assets o altri beni virtuali per il tempo e l'impegno che dedicano al gioco. Questo modello sta guadagnando sempre più popolarità grazie alla possibilità di guadagnare denaro reale attraverso il gioco online, ma anche grazie alla soddisfazione che i giocatori traggono dalla progressione e dalla gratificazione immediata.

Analizzando il fenomeno sulla base delle **teorie psicologiche cognitive comportamentali**, il Play-to-Earn sfrutta diversi meccanismi per motivare i giocatori ad investire il proprio tempo e la propria energia nel gioco. Uno di questi meccanismi è il **rinforzo positivo**, che consiste nel premiare i comportamenti desiderati dei giocatori con una ricompensa. Ad esempio, quando un giocatore completa una missione o raggiunge un determinato obiettivo nel gioco, viene premiato con un digital asset o con un altro bene virtuale. Questa gratificazione immediata aumenta la motivazione del giocatore a continuare a giocare e a raggiungere nuovi obiettivi.

Un altro meccanismo utilizzato dal P2E è l'effetto di **ancoraggio mentale**, che sfrutta la **tendenza dei giocatori a basare le proprie decisioni sulla prima informazione che ricevono**. Ad esempio, quando un giocatore inizia a giocare ad un gioco P2E e riceve una certa quantità di digital assets come bonus di benvenuto, questo può creare un ancoraggio mentale che lo spinge a continuare a giocare per ottenere ancora più ricompense.

Inoltre, il Play-to-Earn utilizza il **meccanismo della curva dell'esperienza: l'esperienza di gioco diventa sempre più gratificante all'aumentare del tempo e dell'impegno** dedicati. Ciò significa che i giocatori che dedicano più tempo al gioco sono incentivati a continuare a farlo poiché l'esperienza diventa sempre più soddisfacente.

In sintesi, il **Play-to-Earn utilizza diversi meccanismi psicologici per motivare i giocatori a investire tempo ed energia nel gioco**, grazie alla gratificazione immediata, all'effetto di ancoraggio mentale e alla curva dell'esperienza. Questo modello di gioco sta cambiando il modo in cui le persone vedono il gioco online e il potenziale del Metaverse come piattaforma per l'economia virtuale.

7.6

Psicologia / Business

● Basic

Industrie correlate ed i rischi nella realtà virtuale

All'interno dell'industria delle realtà virtuali, come metaversi e mondi di realtà aumentata, troviamo sia aziende che producono software, sia aziende che producono hardware.

Le aziende che producono dispositivi di realtà virtuale **si concentrano sulla creazione di prodotti che offrono esperienze immersive e coinvolgenti**. Questi dispositivi includono occhiali VR, controller, sensori di movimento ed altri accessori. Aziende come Oculus, HTC e Sony hanno creato dispositivi di realtà virtuale avanzati che consentono agli utenti di interagire con il mondo virtuale in modo realistico. Samsung ha sviluppato Gear VR, un dispositivo di realtà virtuale che utilizza uno smartphone come schermo e Google ha creato Google Cardboard, un dispositivo economico che consente a chiunque di sperimentare la realtà virtuale.

Le aziende che sviluppano software per la realtà virtuale **si concentrano sulla creazione di strumenti e applicazioni che consentono agli sviluppatori di creare esperienze di realtà virtuale coinvolgenti**. Unity e Unreal Engine sono due dei principali motori di gioco utilizzati per creare giochi e applicazioni di realtà virtuale. Autodesk e Adobe offrono strumenti di progettazione e animazione che consentono agli artisti di creare contenuti visivi per la realtà virtuale. Altre aziende si concentrano invece sulla creazione di applicazioni specifiche per la realtà virtuale, come applicazioni per l'istruzione, la salute e l'intrattenimento.

Nonostante il progresso della tecnologia, rimanere troppo all'interno di una realtà virtuale può provocare diversi rischi dal punto di vista psicologico e fisico, come:

- **Disturbi dell'equilibrio emotivo:** la realtà virtuale può essere così coinvolgente che i confini tra il mondo reale e quello virtuale diventano sfumati. Ciò può portare ad una sorta di confusione emotiva che può alterare l'equilibrio psicologico.
- **Dipendenza:** la realtà virtuale può essere così coinvolgente che alcune persone possono diventare dipendenti da essa, perdendo il contatto con la realtà e con le relazioni sociali.
- **Disturbi dell'identità:** la realtà virtuale può alterare la percezione della propria identità, poiché le persone possono assumere ruoli diversi da quelli che hanno nella vita reale.
- **Motion sickness:** la realtà virtuale può causare una sorta di mal d'auto (motion sickness), poiché il cervello riceve informazioni contrastanti dal sistema vestibolare e dal sistema visivo.
- **Affaticamento degli occhi:** l'uso prolungato della realtà virtuale può causare affaticamento degli occhi e problemi di visione.
- **Disturbi dell'udito:** l'uso prolungato della realtà virtuale può causare disturbi dell'udito, come ad esempio acufeni e vertigini.

Sarà interessante nei prossimi anni osservare il mercato e capire quali settori saranno quelli più colpiti da queste nuove tecnologie immersive ed esperienziali.

8

Identità digitale

- 8.1 La dematerializzazione del portafoglio
- 8.2 Gli attori e i modelli di gestione dell'identità digitale
- 8.3 La sovranità della propria identità digitale
- 8.4 Il paradigma Self-Sovereign Identity
- 8.5 Singolo wallet o due wallet per identità e denaro?

8.1

Filosofia Digitale

● Basic

La dematerializzazione del portafoglio

Il concetto di dematerializzazione fa riferimento a quei fenomeni in cui vi è in atto una trasformazione di beni materiali in beni immateriali, attraverso l'uso di **informazioni digitali e non tangibili**. Questo processo coinvolge numerosi settori della società, tra cui l'economia.

Vi sono diversi tipi di dematerializzazione che impattano ambito economico, sociale, comportamentale, politico, e culturale.

Ad esempio, i beni culturali come i libri e la musica sono stati dematerializzati attraverso la distribuzione digitale di ebook e file musicali. Allo stesso modo, i documenti cartacei sono stati sostituiti dai documenti digitali, rendendo più facile e veloce l'accesso alle informazioni.

La dematerializzazione ha anche avuto un impatto significativo sulla **cultura e sulla società in generale**. La creazione e la condivisione di informazioni digitali ha reso **più facile per le persone accedere a contenuti culturali, come libri, film e musica, da qualsiasi parte del mondo**. Ciò ha avuto un impatto sulla **diffusione della conoscenza e dell'informazione**, nonché sulla **creazione di comunità online**.

Nel **settore dell'economia**, la dematerializzazione si manifesta nella **sostituzione di prodotti fisici con prodotti digitali e degli strumenti di gestione di essi, come il portafoglio**.

La dematerializzazione del portafoglio si riferisce alla sostituzione dei portafogli fisici con portafogli digitali, conseguenza della progressiva dematerializzazione della identità e del denaro. Questo processo coinvolge la digitalizzazione dei documenti di identità, come i passaporti e le carte d'identità, e la **sostituzione del denaro contante con strumenti di pagamento digitali**, come le carte di credito e i portafogli elettronici.

In particolare, con riguardo a questi ultimi sono nati strumenti di pagamento che includono carte di credito, carte di debito e portafogli elettronici, come Apple Pay e Google Wallet. L'utilizzo di questi strumenti di pagamento digitali consente di effettuare transazioni in modo rapido, sicuro ed efficiente, senza la necessità di utilizzare denaro contante.

La dematerializzazione della identità si basa sulla creazione di identità digitali, ovvero l'insieme di informazioni personali associate ad una persona fisica e memorizzate in formato digitale. Le identità digitali possono essere **utilizzate per accedere a servizi online, effettuare transazioni finanziarie e partecipare a comunità digitali**. La creazione di identità digitali sicure e affidabili richiede la collaborazione tra governi, istituzioni finanziarie e aziende tecnologiche.

Secondo stime della Banca Mondiale, sul nostro pianeta circa **un miliardo di persone non ha un'identità ufficiale**. In termini assoluti a primeggiare in questa classifica negativa è l'India (con 162 milioni di persone senza volto), ma in termini relativi nelle prime posizioni troviamo Somalia, Nigeria, Eritrea ed Etiopia, dove la percentuale di persone «sconosciute» oscilla tra il 77% e il 65%. La diffusione di queste tecnologie e di internet **può aiutare a creare soluzioni più sicure nel tempo, risolvendo alcuni problemi attuali**. Tuttavia, ci sono anche **alcune sfide da affrontare**, come la **protezione dei dati personali e la sicurezza delle transazioni finanziarie**. Per affrontare queste sfide, sono necessari standard di sicurezza rigorosi e tecnologie avanzate per la protezione dei dati.

In conclusione, la dematerializzazione del portafoglio attraverso la dematerializzazione della identità e del denaro rappresenta un importante passo verso una società digitale più sicura, efficiente e sostenibile. Tuttavia, è importante affrontare le sfide che questa trasformazione comporta, per garantire una transizione sicura e senza intoppi verso un futuro digitale.

8.2

Informatica

• Basic

Gli attori e i modelli di gestione dell'identità digitale

Internet ci ha posto di fronte ad una sfida relativa all'identificazione degli utenti online. È proprio in quest'ambito che è stata coniata la definizione di fornitore di identità, o in inglese identity provider (IDP). Questi soggetti si stanno occupando della creazione e gestione delle identità digitali degli utenti per la maggior parte delle risorse che troviamo in rete.

Generalmente, in rete ci sono 2 modelli di gestione dell'identità digitale che utilizzano entrambe un IDP:

- **Modello Centralizzato**
- **Modello Federato**

Il modello centralizzato di identità digitale è anche chiamato “Modello Silos”.

All'interno di questo modello, gli utenti possono crearsi una propria identità digitale (spesso e volentieri sotto forma di “crea un nuovo account”). I dati personali sono **conservati in maniera centralizzata dalle organizzazioni che fungono da identity provider** (che in questo caso è anche il provider del servizio stesso) **e permettono agli utenti di accedere ai servizi**.

Il modello centralizzato è un modello semplice da utilizzare e da implementare per le organizzazioni. Permette alle aziende di detenere i dati dei propri utenti, e in questo modo di tenere una relazione costante con l'utente (fino a che esso userà il servizio offerto).

Il modello centralizzato rende gli **utenti completamente “dipendenti” dalle organizzazioni** che detengono i propri dati, e porta con sé alcuni potenziali rischi e debolezze:

- Poiché la maggior parte dei dati personali vengono detenuti all'interno di database centralizzati, esistono **rischi di sicurezza informatica** dovuti al fatto che un leak del database dell'organizzazione esporrebbe dati sensibili degli utenti
- I sistemi di identità digitale centralizzati hanno creato quello che viene definito come **“fenomeno delle identità multiple”**. In questo modo l'esperienza online dell'utente viene resa più complicata ed egli non ha modo di gestire tutti i suoi dati all'interno della stessa identità digitale.

Per questo motivo, nel tempo, si è osservata una transizione verso il modello che viene definito **federato**. Ovvero la nascita di nuovi **identity provider** (IDP), che **fanno “da ponte” tra l'utente e il servizio a cui l'utente sta accedendo**.



Questi bottoni vengono definiti come social login, sono forniti da Facebook, Google, etc e responsabili della identificazione ed autorizzazione di un utente online nell'accedere all'interno di una risorsa in rete come un sito.

Nel caso del modello federato, **entità come i social network “detengono” effettivamente i dati relativi all’identità digitale dell’utente, limitando la gestione di questi ultimi al sito del servizio (definito anche come service provider), facendosi da garanti delle informazioni fornite.**

Un **esempio di IDP** a livello italiano può essere **SPID**: tramite una singola identità, detenuta da un soggetto tramite uno dei provider che fa parte della “Federazione”, l’utente è in grado di accedere a diversi servizi. Mentre il service provider può essere il sito della regione che offre un servizio online ai propri cittadini.

Allo stesso tempo, anche in questo modello, proprio come in quello Silos, **un utente non è il vero possessore dei propri dati “digitali”, che sono invece sempre detenuti da una terza parte**, ovvero l’identity provider. Per questo motivo un modello di identità digitale federata pesa molto sul provider, che deve “essere presente” in ogni accesso da parte dell’utente ai servizi online.

8.3

Filosofia Digitale

● Basic

La sovranità della propria identità digitale

Cos’è un’identità digitale? Questa è una domanda sempre più attuale, in un mondo che sempre più si digitalizza e trasla i propri servizi dal mondo fisico al mondo informatico. Da un punto di vista tecnico, **un’identità digitale consiste in un insieme di informazioni catalogate all’interno di un sistema informatico e gestite da un ente**.

Andando oltre la semplice definizione di identità digitale, **questa è il modo in cui tutti noi ci identifichiamo all’interno delle nostre interazioni online**, che ormai rappresentano una grande parte delle nostre interazioni giornaliere.

Uno dei primi riferimenti al concetto di “sovranità relativa alla propria identità digitale” si ritrova negli scritti dello sviluppatore Moxie Marlinspike “Sovereign Source Authority” del febbraio 2012. Riprendendo un piccolo frammento, egli affermava che **“gli individui hanno il diritto consolidato della propria identità, ma l’anagrafe (o la registrazione nazionale) ha distrutto la possibilità di avere il controllo su di essa”**.

Dal 2016, il *World Wide Web Consortium*, anche conosciuto come W3C, l’organizzazione non governativa internazionale iniziò a creare dei working group per sviluppatore di framework aperti che permettesseero la standardizzazione di questa nuova infrastruttura digitale. L’obiettivo di questo nuovo framework è quella di **distribuire i dati personali ai singoli proprietari e gestirli grazie ad un borsellino digitale. Ogni singolo utente potrà quindi dimostrare la propria identità digitale in maniera autonoma e custodendo le proprie informazioni in maniera privata**.

Questo nuovo paradigma viene chiamato **Self-Sovereign Identity (SSI)**.

Riprendo le parole di Christopher Allen, la self-sovereign identity si basa sulla **dignità umana e la sua estensione nel mondo digitale**. Questo nuovo framework di gestione dell’identità digitale vuole offrire agli utenti e alle aziende un nuovo modo con cui gestire i propri dati online, senza la necessità di terze parti, che svolgono la funzionalità di identificarsi per accedere a servizi e prodotti digitali e fisici.

8.4

Informatica

● Basic

Il paradigma Self Sovereign Identity

Il **paradigma della Self Sovereign Identity** vuole essere completamente “user centrico”, ovvero l’utente è al centro del controllo ed indipendente nel possesso della propria identità digitale e di tutti i dati ad essa associati. L’obiettivo di questo nuovo framework è quello di decentralizzare la governance dei dati personali, **distribuendo i dati all’interno di ogni dispositivo, aiutando la sicurezza tramite l’eliminazione di un unico punto di vulnerabilità, solito dei modelli Silos e Federato.**

Essa dovrebbe soddisfare alcuni principi per far sì che non abbia gli stessi problemi e le stesse limitazioni dei precedenti modelli come:

1. **Esistenza:** gli utenti devono avere un’entità indipendente;
2. **Controllo:** gli utenti devono controllare le loro identità;
3. **Accesso:** gli utenti devono avere accesso ai loro dati personali;
4. **Trasparenza:** gli algoritmi e i sistemi devono essere trasparenti;
5. **Persistenza:** le identità devono essere durature
6. **Portabilità:** le informazioni e i servizi riguardo alle identità devono essere “trasportabili”;
7. **Interoperabilità:** le identità dovrebbero essere ampiamente utilizzabili;
8. **Consenso:** gli utenti devono consentire l’utilizzo delle loro identità;
9. **Minimizzazione:** la divulgazione delle dichiarazioni degli utenti deve essere minimizzata;
10. **Sicurezza:** protezione dei diritti degli utenti.

Pur essendo una tecnologia innovativa, la Self Sovereign Identity è costruita su strumenti tecnologici testati da anni, la cui combinazione ha permesso la gestione dell’identità digitale direttamente nel proprio client ed in modalità **self-custody**.



Self-Custody

Un portafoglio di autocustodia è un portafoglio digitale in cui solo il detentore possiede e controlla la chiave privata direttamente all’interno del proprio client.

Infatti, tra le tecnologie utilizzate dal modello self-sovereign identity vi sono anche l’**uso della blockchain, per avere un registro pubblico sul quale verificare l’autenticità delle informazioni, e i wallet crittografici, per conservare i dati associati alla nostra identità digitale.**

Rispetto al mondo dei digital assets, i servizi e le tecnologie sul mercato sono ancora in fase di prototipazione e non vi sono grandi progetti di rilievo in termini di adozione, ma l’interesse da parte dei regolatori e di molte industrie tecnologiche è costante.

8.5

Business / Informatica

● Basic

Singolo wallet o due wallet per identità e denaro?

La tecnologia di self-sovereign identity (SSI) utilizza una struttura simile a quella dei digital assets, in quanto entrambe sono basate su crittografia e tecnologie blockchain. Tuttavia, **l'uso di un wallet unico o due wallet differenti dipende dalle specifiche esigenze dell'individuo o dell'organizzazione che utilizza la tecnologia SSI**.

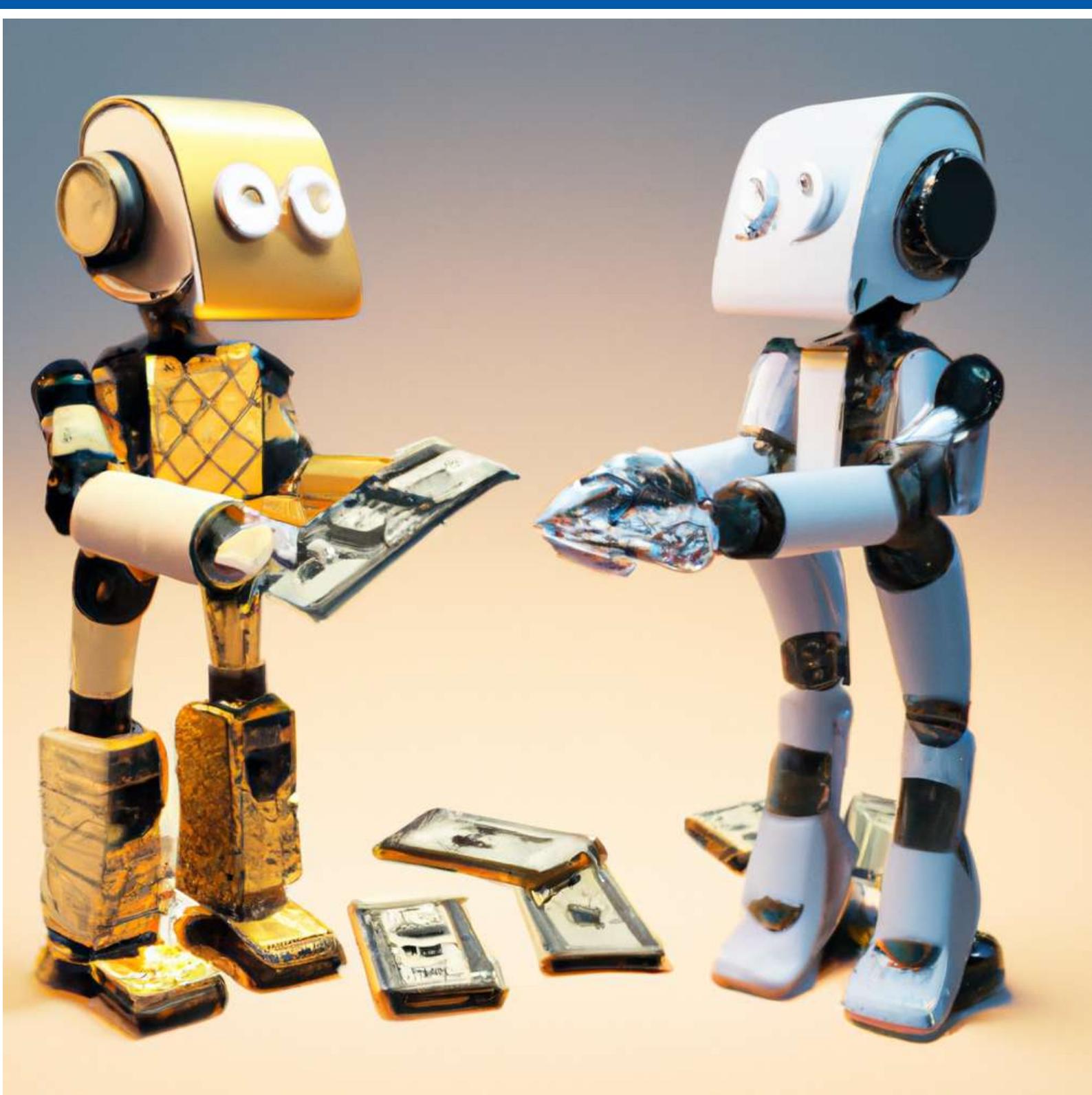
In linea di principio, **un wallet SSI unico potrebbe contenere tutte le informazioni di identità e le credenziali verificate di un individuo**. Ciò potrebbe **semplificare la gestione dell'identità**, rendendola più sicura e trasparente. Tuttavia, ciò potrebbe anche **comportare rischi di sicurezza maggiori**, in quanto un attaccante che accede a un wallet unico potrebbe ottenere accesso a tutte le informazioni di identità e le credenziali di una persona.

D'altra parte, **l'uso di due wallet SSI distinti porterebbe ad una maggiore sicurezza**, poiché le informazioni di identità e le credenziali verificate sarebbero divise tra i due wallet. Tuttavia, ciò **potrebbe anche complicare la gestione dell'identità** e richiedere una maggiore attenzione per garantire che entrambi i wallet siano protetti adeguatamente.

In sintesi, **l'uso di un wallet unico o due wallet differenti dipende dalle esigenze e dalle preferenze individuali o aziendali**. Tuttavia, in entrambi i casi, è fondamentale adottare le misure di sicurezza appropriate per proteggere le informazioni di identità e le credenziali verificate.

Capitolo 5

BANCA E PAGAMENTI NEL WEB3



Introduzione

Il quinto capitolo ha come principale obiettivo formativo quello di analizzare e far comprendere al lettore: le modalità con cui viene creata e gestita la moneta nei tradizionali sistemi monetari, le tecnologie che permettono la creazione di un mercato globale ed interconnesso, e come queste reti informatiche operano e permettono di far interagire tutti gli attori all'interno di un sistema economico (come banca centrale, banca commerciale, cittadino e Stato).

Il secondo obiettivo formativo è quello di analizzare i modelli di governance e le diverse tecnologie informatiche utilizzate oggi nelle principali reti internazionali per le transazioni economiche, per poi fare una comparazione con quelle utilizzate dai digital assets.

Il terzo obiettivo formativo è quello di comprendere che cos'è una stable coin e quali sono i meccanismi attraverso cui il valore di un digital asset può rimanere stabile. Inoltre, verrà approfondito come le stable coin potrebbero interagire con i sistemi informatici delle banche tradizionali, generando nuovi modelli di business grazie alla loro programmabilità. Verrà poi affrontato il cambiamento per una banca commerciale, con l'introduzione delle Central Bank Digital Currencies (CBDC), e come questa dovrà adattarsi ad un cambiamento sostanziale nella gestione della moneta e del credito.

In fine, il capitolo si concluderà offrendo al lettore una riflessione sull'impatto della moneta sulle tensioni geo-politiche e sociali, e di come la dematerializzazione di questa offrirà nuovi terreni di confronto nelle attività economiche e finanziarie di un paese.

In sintesi, il capitolo è composto da 4 macro-blocchi e 33 blocchi formativi, e cerca di far comprendere al lettore la complessità che si genera attorno alla moneta e alla sua gestione tra diversi attori.

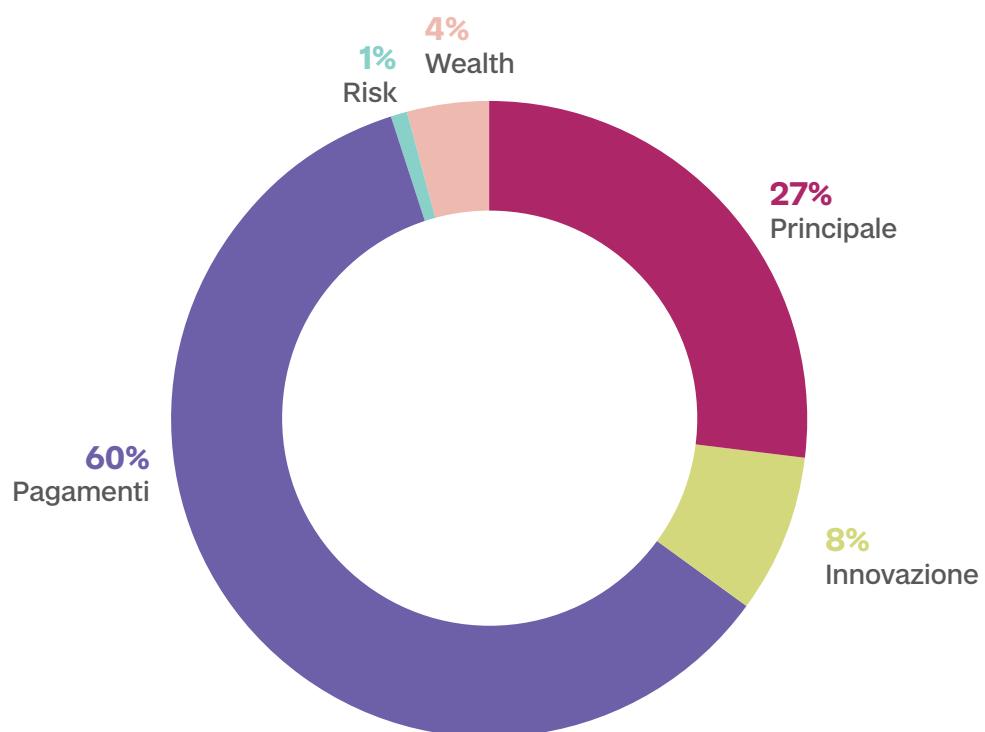
Queste alcune domande a cui cercheremo di rispondere:

- Come il sistema a cambi variabili ha un impatto nella gestione e nella creazione di una moneta all'interno di una comunità economica?
- Qual è il ruolo della banca centrale nella creazione della moneta e come si differenzia dalla creazione di Bitcoin?
- Come funzionano i sistemi di clearing e settlement interbancario?
- Quali sono le principali differenze tra i sistemi di clearing e settlement valutario e retail?
- Come viene gestita la governance nei sistemi di clearing e settlement?
- Quali sono le sfide dell'interoperabilità tra i diversi sistemi di clearing e settlement?
- Come funziona un software payment gateway per i pagamenti online su e-commerce?
- Qual è il ruolo delle stable coin nella finanza decentralizzata e come si differenziano dai digital assets come Bitcoin?

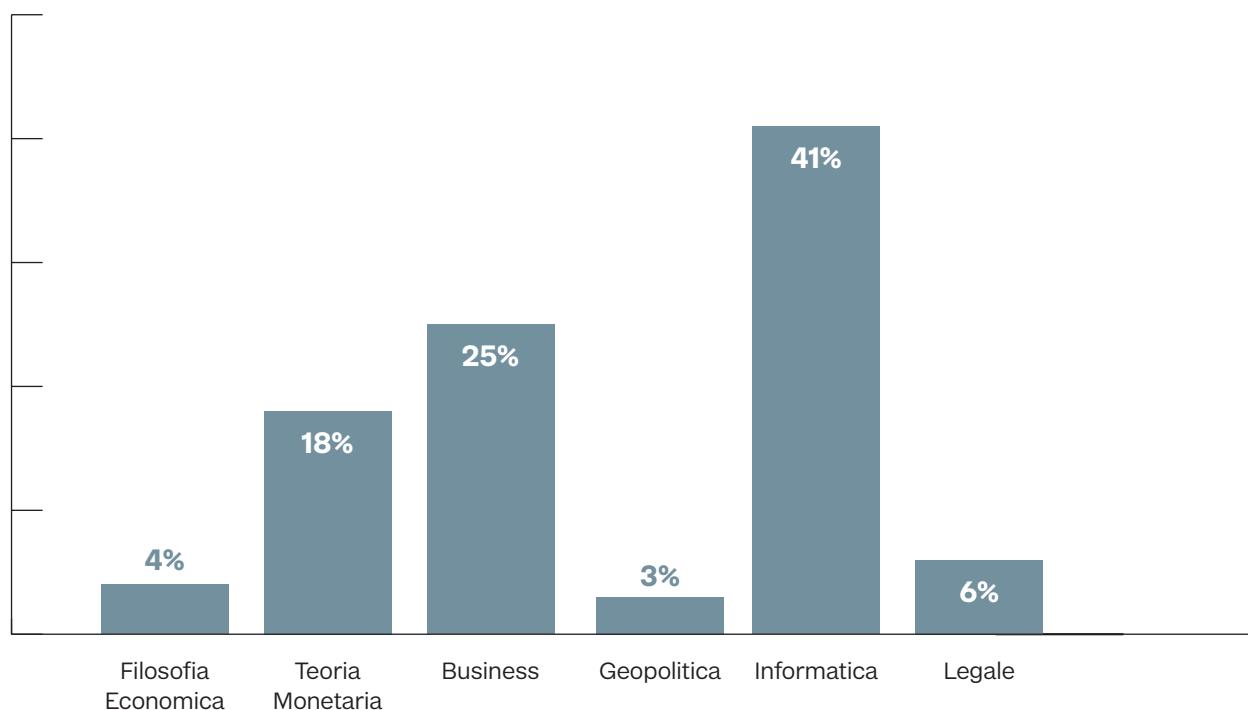
Per poi approfondire con domande più in profondità come:

- Come la programmabilità delle stable coin può influenzare la governance dei sistemi di clearing e settlement?
- Quali implicazioni potrebbero avere le stable coin sul sistema monetario internazionale?
- Quali sono le differenze tra i sistemi peer to peer e quelli non peer to peer nei sistemi di clearing e settlement?
- Come i tokens possono essere utilizzati come forma di pagamento all'interno dei sistemi di clearing e settlement?
- Quali sono le principali sfide nell'implementazione di una CBDC e come potrebbero essere risolte?
- Come una cashless society potrebbe influenzare la creazione della moneta dalla banca centrale alla banca commerciale?
- In che modo i sistemi di pagamento online su e-commerce possono essere integrati nei sistemi di clearing e settlement?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. I sistemi monetari internazionali

- 1.1 Bitcoin come rete di pagamento globale
- 1.2 Il sistema monetario a cambi variabili
- 1.3 Come viene creata la moneta e come entra nell'economia?
- 1.4 Che cosa si intende per base e massa monetaria?
- 1.5 La moneta cattiva caccia la moneta buona?
- 1.6 Come vengono scambiate le monete nell'economia globale?

DIFFICOLTÀ	DISCIPLINA	PERCORSO
● Fil. Econ. / Teoria Mon.	Principale	
● Teoria Monetaria	Principale	
● Teoria Monetaria	Principale	
● Teoria Monetaria	Pagamenti	Wealth
● Filosofia Economica	Principale	
● Informatica	Pagamenti	Wealth

2. I sistemi di clearing e settlement

- 2.1 Quali sono i sistemi di trasferimento nel mercato interbancario?
- 2.2 Quali sono i sistemi di trasferimento nel mercato valutario?
- 2.3 Quali sono i sistemi di trasferimento nel mercato retail?
- 2.4 Come viene gestita l'amministrazione delle reti di clearing e settlement?
- 2.5 Come avviene l'interoperabilità tra le reti interbancarie e retail?
- 2.6 Il fintech e la diffusione di strumenti di pagamento innovativi
- 2.7 Come funziona un pagamento online su e-commerce?
- 2.8 Sistemi peer to peer vs sistemi non peer to peer nei processi di clearing e settlement

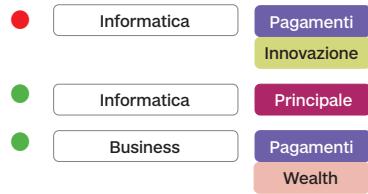
●	Informatica	Pagamenti
●	Business	Pagamenti Wealth
●	Informatica	Principale
●	Informatica	Pagamenti

3. I pagamenti nel Web3

- 3.1 I token come strumenti per i pagamenti
- 3.2 Operazioni con un conto corrente e wallet a confronto
- 3.3 New bank, bonifici istantanei e secondo livello (LN) a confronto
- 3.4 Pagamenti online nel Web3
- 3.5 Pagamenti offline nel Web3
- 3.6 La programmabilità dei payment token
- 3.7 Il ruolo delle stable coin
- 3.8 Come si stabilizza il valore di una stable coin?
- 3.9 Che cos'è la proof of reserve? Il caso Tether
- 3.10 Che cosa si intende per depegging? Il caso Luna e Terra

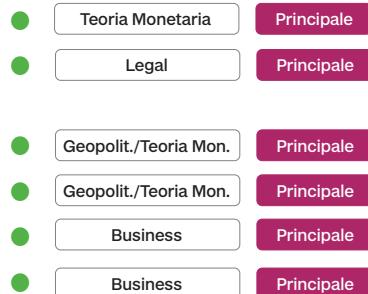
● Business/Informatica	Principale
● Business	Pagamenti
● Informatica	Pagamenti Innovazione
● Informatica	Principale
● Informatica/Finanza	Pagamenti Wealth
● Legal	Pagamenti Risk
● Informatica	Pagamenti Wealth

- 3.11 Approfondimento: gli algoritmi a mercato aperto e riserva in fiat
- 3.12 Il ruolo dell'Open Banking nella interoperabilità
- 3.13 Gli investimenti nella fintech e la contaminazione con digital assets e AI



4. CBDC

- 4.1 Il ruolo delle banche centrali nell'economia contemporanea
- 4.2 Panoramica generale sulle Central Bank Digital Currencies (CBDC)
- 4.3 Moneta dominante e i nuovi assetti geopolitici
- 4.4 La guerra tra le valute internazionali
- 4.5 Verso la cashless society
- 4.6 Bank the unbanked e le opportunità del futuro



1

I sistemi monetari internazionali

- 1.1. Bitcoin come rete di pagamento globale
- 1.2 Il sistema monetario a cambi variabili
- 1.3 Come viene creata la moneta e come entra nell'economia?
- 1.4 Che cosa si intende per base e massa monetaria?
- 1.5 La moneta cattiva caccia la moneta buona?
- 1.6 Come vengono scambiate le monete nell'economia globale?

1.1

Filosofia economica / Teoria Monetaria

● Basic

Bitcoin come rete di pagamento globale

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

“Bitcoin: A Peer-to-Peer Electronic Cash System” è il titolo del white paper pubblicato in rete dallo pseudonimo Satoshi Nakamoto il 31 Ottobre 2008. Bitcoin è una tecnologia che affonda le sue origini nelle prime ricerche sulla crittografia e dei sistemi distribuiti dagli anni 80’, ed è frutto di innumerevoli scoperte nell’informatica. Numerosi sono stati i tentativi prima di bitcoin, che sono falliti.

Questo documento è stato di fondamentale importanza per comprendere l’idea alla base di questa rivoluzionaria valuta digitale, capace di unire e combinare diverse tecnologie esistenti, creandone una nuova.

Durante gli anni, il white paper è stato tradotto in moltissime lingue del mondo, facilitando la diffusione e la comprensione di questa tecnologia in tutto il globo. Bitcoin nasce e cresce come innovazione completamente spinta e guidata dal basso, con un approccio bottom up.

La rete Bitcoin è considerata da milioni di utenti in tutto il mondo come la miglior tecnologia per lo scambio di valore in maniera pseudo-anonima e senza censure.

Tuttavia, **la sua natura deflattiva (non esisteranno mai più di 21 milioni di bitcoin) fa domandare se i bitcoin possono essere una buona moneta nel breve e medio periodo. Se infatti, da un lato la loro quantità finita dovrebbe garantire di non perdere potere d’acquisto nel lungo periodo, dall’altro tanto, questo aspetto non lo rende idoneo ad essere una buona moneta nel breve periodo poiché di valore troppo instabile per essere una unità di conto efficiente.**



Unità di conto

Definizione: Una delle 3 funzioni essenziali della moneta: oltre che riserva di valore e mezzo di scambio, essa rappresenta l’unità di conto, ovvero il metro comune per misurare il valore delle transazioni economiche tramite la fissazione dei prezzi e la contabilizzazione dei debiti e dei crediti, associati al passaggio di proprietà dei beni o delle attività senza un contestuale regolamento in moneta.

Fonte: https://www.treccani.it/enciclopedia/unita-di-conto_%28Dizionario-di-Economia-e-Finanza%29/

Nonostante questo, il concetto di una valuta sempre stabile è un po’ come il sacro Graal dell’economia. **Infatti, nessuna moneta internazionale può essere considerata un perfetto “unit of account” (unità di conto) in quanto tutte le monete nel sistema valutario fluttuano nel tempo e subiscono variazioni di valore, una rispetto all’altra.** Ciò significa che il prezzo dei beni e dei servizi espressi in una valuta può cambiare rapidamente in base alle condizioni di mercato e alle fluttuazioni del tasso di cambio. Tuttavia, nonostante queste fluttuazioni, alcune valute come il dollaro statunitense, l’euro e lo yen giapponese sono comunemente utilizzate come unità di conto a livello globale, ma non sono esenti da variazioni di valore.

Queste considerazioni hanno diviso gli economisti e i teorici, rispetto all’obiettivo originario di bitcoin e la sua percezione oggi.

Un secondo aspetto che divide gli economisti è il fatto che i bitcoin, a differenza di altri sistemi monetari come l’euro o il dollaro, non hanno **corso legale**.



Corso Legale

È quello della moneta legale avente per legge potere liberatorio, cioè la caratteristica di non poter per legge essere rifiutata per l'estinzione delle obbligazioni pecuniarie nello Stato in cui essa è emessa (principio sancito nel nostro diritto dagli artt. 1277 e 1278 c.c.).

Ad oggi, a bitcoin non è riconosciuto corso legale nella maggior parte degli ordinamenti anche in quanto non è emesso da una banca centrale, ma da un codice sorgente pubblico ed immutabile. Per ora, solamente El Salvador e la Repubblica Centro Africana hanno conferito ai bitcoin il valore di corso legale, diventando i primi stati al mondo ad accettare tale digital asset come moneta legale.

1.2

Teoria Monetaria

● Basic

Il sistema monetario a cambi variabili

Il sistema a cambi variabili delle valute internazionali è stato introdotto dopo il cosiddetto **"Nixon Shock"** del 1971, quando gli **Stati Uniti hanno deciso di sospendere la convertibilità del dollaro in oro**, ponendo fine al sistema di Bretton Woods. In questo nuovo sistema, le valute dei diversi paesi sono negoziate sui mercati valutari, e il loro valore relativo è determinato dall'offerta e dalla domanda.

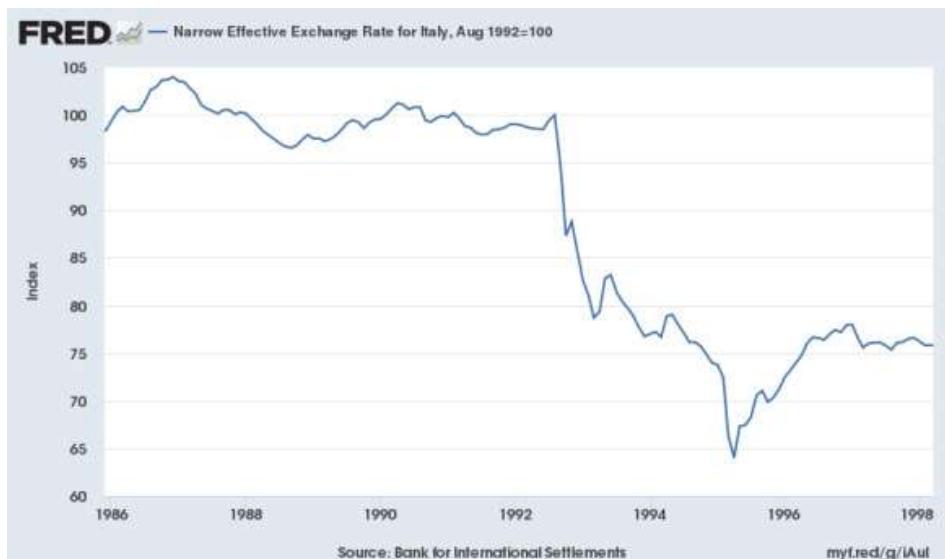
Inoltre, **i tassi di cambio tra le valute sono influenzati da diversi fattori**, tra cui la politica monetaria dei diversi paesi, la situazione economica generale, i tassi di interesse, i flussi di capitale, le notizie e gli eventi geopolitici.

Questo sistema ha portato ad una **maggior volatilità nel mercato valutario**, in quanto il valore delle valute può fluttuare rapidamente in base alle condizioni di mercato e alle notizie in arrivo. Questo può creare sfide per le imprese che operano a livello internazionale, poiché le fluttuazioni dei tassi di cambio possono influenzare il prezzo dei beni e dei servizi e la redditività delle operazioni in valuta estera.

Il mercato forex, anche noto come mercato dei cambi, è il mercato globale in cui vengono scambiate valute di diversi paesi. Il termine "forex" deriva dalla fusione delle parole "foreign exchange", che significa appunto scambio di valute estere.

Il mercato forex nasce nel XVII secolo, quando le valute iniziarono ad essere negoziate in modo regolare ed organizzato. Nel 1971 con l'adozione del sistema di cambio fluttuante, il mercato forex iniziò ad assumere la forma attuale di mercato decentralizzato e globale, aperto 24 ore al giorno, 5 giorni alla settimana.

Tuttavia, il sistema a cambi variabili ha anche portato a **maggiori opportunità di investimento per gli operatori finanziari**, poiché possono cercare di trarre profitto dalle fluttuazioni dei tassi di cambio. Inoltre, questo sistema ha permesso una **maggior flessibilità per le politiche monetarie dei singoli paesi**, poiché possono implementare politiche che si adattano meglio alle loro esigenze economiche specifiche.



Alcuni esempi passati possono essere:

- **Lira italiana:** negli anni '90, la lira italiana ha subito una forte svalutazione rispetto ad altre valute, come il dollaro americano, a causa della crescente inflazione e della difficile situazione economica del paese. Ciò ha avuto un impatto significativo sui prezzi dei beni e dei servizi in Italia, nonché sulle imprese che operano a livello internazionale. Il grafico sopra presentato indica l'andamento della competitività della lira italiana a livello internazionale.
- **Euro:** nel 2010, durante la crisi del debito sovrano europeo, l'euro ha subito un forte calo a causa della preoccupazione degli investitori riguardo alla sostenibilità del debito di alcuni paesi dell'eurozona. Ciò ha portato ad una maggiore volatilità nel mercato valutario e ha influenzato il prezzo dei beni e dei servizi nei paesi dell'eurozona.
- **Dollaro statunitense:** nel 2020, durante la pandemia di COVID-19, il dollaro statunitense ha subito forti fluttuazioni a causa della crescente incertezza economica globale. Ciò ha influenzato il prezzo delle materie prime e ha avuto un impatto sulle imprese che operano a livello internazionale.

In generale, le fluttuazioni del mercato valutario possono essere causate da una serie di fattori, tra cui le decisioni delle banche centrali, le politiche monetarie dei singoli paesi, le fluttuazioni del mercato azionario e delle materie prime, i cambiamenti nella situazione geopolitica e le notizie macroeconomiche. Ciò può rendere difficile prevedere il valore delle valute e creare sfide per le imprese che operano a livello internazionale.

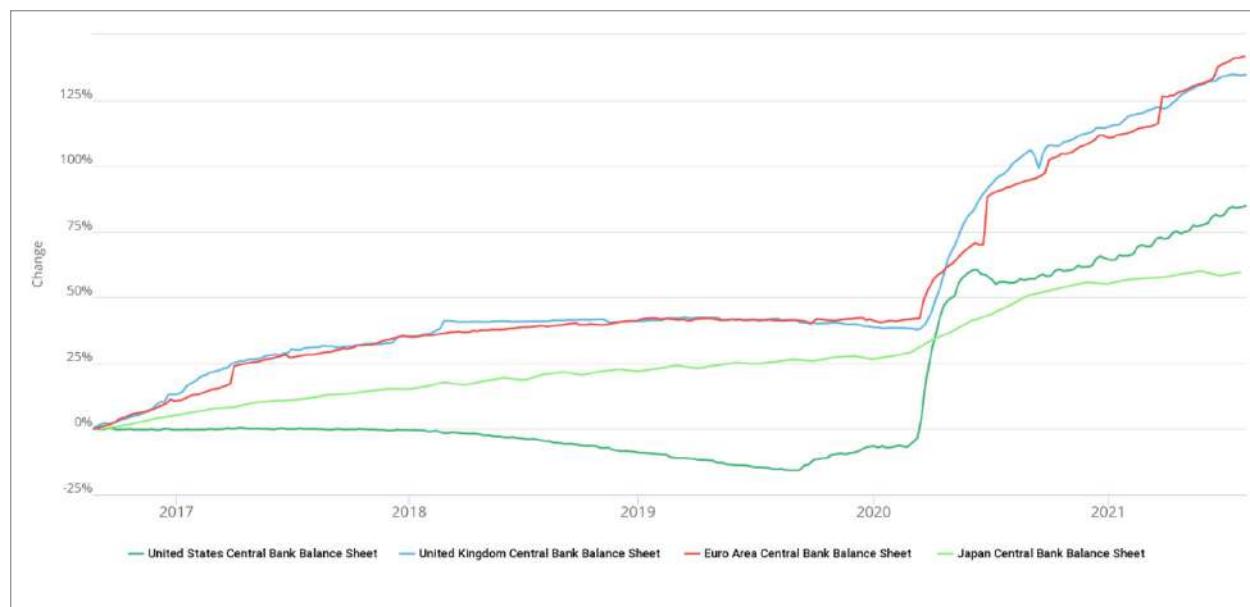
1.3

Teoria Monetaria

• Basic

Come viene creata la moneta e come entra nell'economia?

La moneta di norma viene creata dalla Banca Centrale di ogni singolo Stato o comunità economica (come avviene per l'Unione Europea ad esempio). La quantità di moneta emessa è stabilita in base a diversi fattori quali, tra le varie, la politica monetaria del Paese stesso. Un esempio è il grafico seguente, che mostra un'accelerazione nell'espansione dei bilanci delle banche centrali dati da una politica monetaria espansiva per mitigare la crisi del 2020.



La moneta prima di arrivare al consumatore finale e nell'economia reale, segue dei passaggi intermedi, guidati dalle banche commerciali.

Ecco una descrizione dei passaggi del ciclo della moneta dalla banca centrale al cittadino.

1. La **Banca Centrale emette la moneta** (ad esempio, dollari, euro) e la mette in circolazione nel sistema finanziario. Spesso la richiesta di nuova moneta arriva del Tesoro dei singoli Stati, attraverso la vendita di nuovi titoli di Stato. La Banca Centrale immette liquidità nel mercato attraverso il **Quantitative Easing (QE)** o abbassando il costo del denaro. Quando il costo del denaro si abbassa, solitamente le banche commerciali chiedono in prestito del denaro alla Banca Centrale.
2. Il Tesoro vende i titoli di Stato dentro un mercato primario, dove le banche commerciali comprano i titoli in prima istanza. Successivamente, le banche commerciali vendono, alla Banca Centrale, i titoli di Stato così da ottenere nuova liquidità.
3. Quando la **banca commerciale ha nuova liquidità, può decidere se lasciarla depositata all'interno della Banca Centrale o utilizzarla per concedere prestiti ad imprese e privati**. Ad esempio, una persona potrebbe chiedere un mutuo per comprare una casa, e la banca commerciale concederà il prestito utilizzando parte della moneta che ha ottenuto dalla Banca Centrale.
4. **Quando la banca commerciale concede un prestito, crea un credito per l'importo del prestito**. Ad esempio, se una banca concede un mutuo di 100.000 euro ad un determinato soggetto, crea un credito di 100.000 euro nell'account di quella persona.
5. Tuttavia, quando la banca commerciale crea un credito, **crea anche un debito uguale**. In questo caso, il debito è il prestito stesso. Quindi, se la banca concede un mutuo di 100.000 euro, crea un debito di 100.000 euro che la persona dovrà ripagare nel tempo, insieme agli interessi.
6. **In cambio di questo debito, la banca commerciale guadagna degli interessi**. Ad esempio, se la banca concede un mutuo di 1 anno per l'importo di 100.000 euro ad un tasso di interesse del 5%, guadagnerà 5.000 euro alla fine dell'anno in interessi.
7. Nel frattempo, la Banca Centrale guadagna dal **signoraggio e dalla gestione delle riserve delle banche commerciali**. Il signoraggio è il profitto che la Banca Centrale guadagna emettendo moneta, ovvero la differenza tra il costo di produzione della moneta e il suo valore nominale. Ad esempio, se la Banca centrale produce una banconota da 10 euro che costa 1 euro da produrre, guadagna un signoraggio di 9 euro sulla banconota.
8. Infine, la **Banca Centrale utilizza le politiche monetarie o fiscali per influenzare l'economia**, ad esempio modificando i tassi di interesse o la quantità di moneta in circolazione, al fine di controllare l'inflazione e promuovere la crescita economica.

**QE**

In politica monetaria, con allentamento quantitativo si designa una delle modalità non convenzionali eterodosse e ultra espansive con cui una banca centrale interviene sul sistema finanziario ed economico di uno Stato, per aumentare la moneta a debito in circolazione.

Oltre alle banche centrali, vi sono altri due organismi internazionali che determinano le politiche monetarie:

- Bank of International Settlement (BIS)
- Fondo Monetario Internazionale (FMI)

Fondata nel 1930, la Banca dei regolamenti internazionali è la più antica istituzione finanziaria internazionale. Dal suo inizio fino ai giorni nostri, la BIS ha svolto una serie di ruoli chiave nell'economia globale, dal regolamento dei risarcimenti imposti alla Germania dopo la Prima guerra mondiale, al servizio delle banche centrali nel loro perseguimento della stabilità monetaria e finanziaria.

Il Fondo Monetario Internazionale fu istituito come parte degli accordi di scambio fatti nel 1944 durante la conferenza di Bretton Woods, come ente super partes per garantire stabilità nelle economie ed equità nelle relazioni finanziarie internazionali.

Entrambi questi organismi internazionali hanno avuto un ruolo significativo nel dettare le politiche monetarie internazionali.

Ma dentro una banca commerciale, come viene gestito il sistema di credito e di debito? E quanta liquidità possiede?

In base agli accordi di Basilea, le **banche commerciali sono tenute a mantenere una certa quantità di liquidità interna (il 100% dei prelievi dal deposito)**, ovvero una **riserva minima di denaro** che può essere utilizzata in caso di emergenza. Questa riserva minima è calcolata in base all'ammontare dei depositi raccolti dalla banca.

Infatti, le banche commerciali possono utilizzare la maggior parte dei depositi ricevuti per concedere prestiti ad imprese e cittadini, seguendo il principio della **riserva frazionaria**. Questo significa che la **banca può concedere prestiti per un importo maggiore rispetto alla quantità di denaro effettivamente presente nella riserva**, in quanto si presume che solo una parte dei depositanti richiederà il prelievo del proprio denaro contemporaneamente.

Ad esempio, se una banca ha una riserva minima del 10% e riceve un deposito di 100 euro, può concedere prestiti per un importo massimo di 90 euro, tenendo i restanti 10 euro come riserva.

Inoltre, Il sistema della riserva frazionaria può portare ad un aumento della quantità di denaro in circolazione e quindi all'aumento dell'inflazione, ma può anche **favorire l'attività economica attraverso la concessione di prestiti, migliorando l'effetto della politica monetaria della Banca Centrale**.

1.4

Teoria Monetaria

● Medium

Che cosa si intende per base e massa monetaria?

Le politiche monetarie, adottate dalle banche centrali, possono influenzare la quantità di denaro presente nell'economia, cercando di controllare l'inflazione e stimolare l'attività economica.

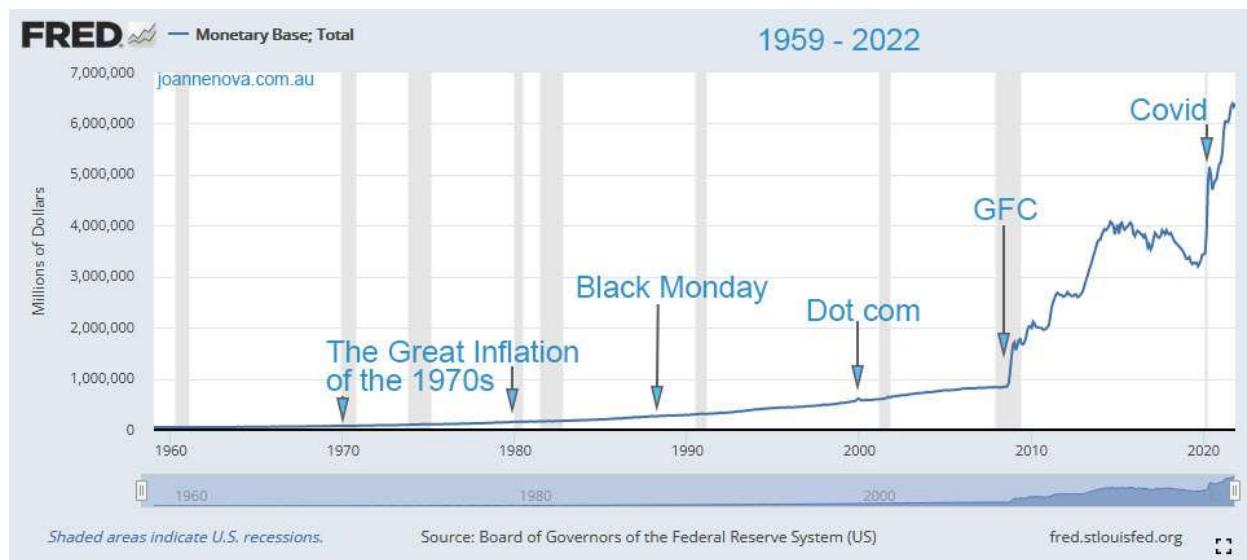
In generale le **masse monetarie rappresentano la quantità di denaro in circolazione in un'economia** e si distinguono in diverse tipologie, ciascuna delle quali si differenzia in base al grado di liquidità del denaro contenuto al suo interno.



Le principali masse monetarie sono:

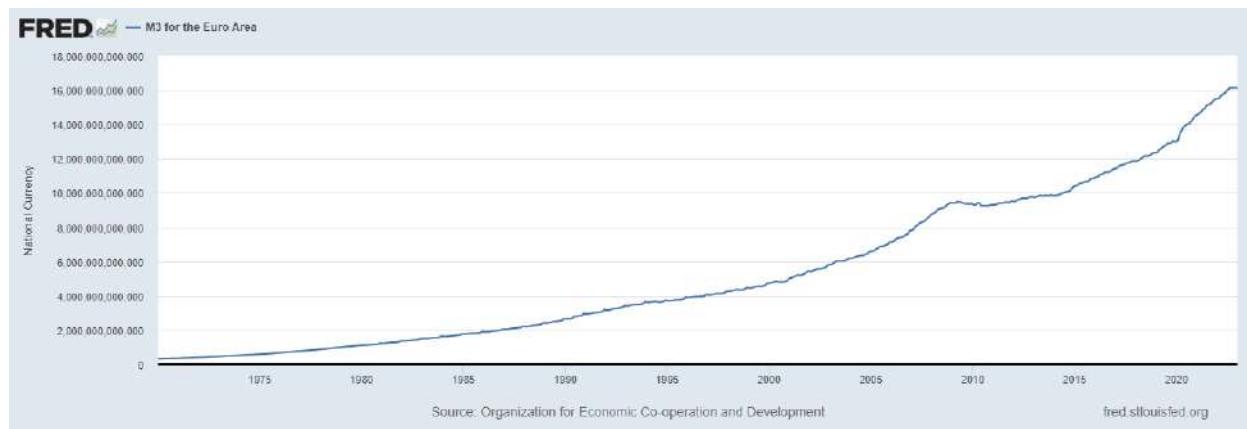
- **M0:** rappresenta la quantità di denaro in circolazione fisicamente **e le riserve di euro di banca centrale delle banche commerciali**. Questa massa monetaria è gestita dalla banca centrale e viene definita anche come base monetaria.
- **M1:** include la quantità di denaro presente in circolazione sotto forma di moneta e banconote, oltre ai **depositi correnti, ai conti correnti postali e alle carte di credito**. Questa massa monetaria è gestita dalle banche commerciali.
- **M2:** rappresenta la **somma di M1 più i depositi a risparmio, i certificati di deposito e altri strumenti finanziari a breve termine**. Questa massa monetaria è gestita dalle banche commerciali.
- **M3:** rappresenta la somma di **M2 più gli strumenti finanziari a lungo termine**, come i fondi comuni di investimento. Questa massa monetaria è gestita dalle banche centrali.

A seguito saranno presentate una serie di grafici che mostrano l'andamento delle masse monetarie nel tempo.



Nel grafico qui sopra riportato si può osservare il progressivo aumento della massa M0 del dollaro, guidata dalle politiche espansive e restrittive della FED. Qui di seguito altri dati rispetto all'incremento di moneta all'interno dei sistemi monetari internazionali come l'euro, il dollaro e dello yen.

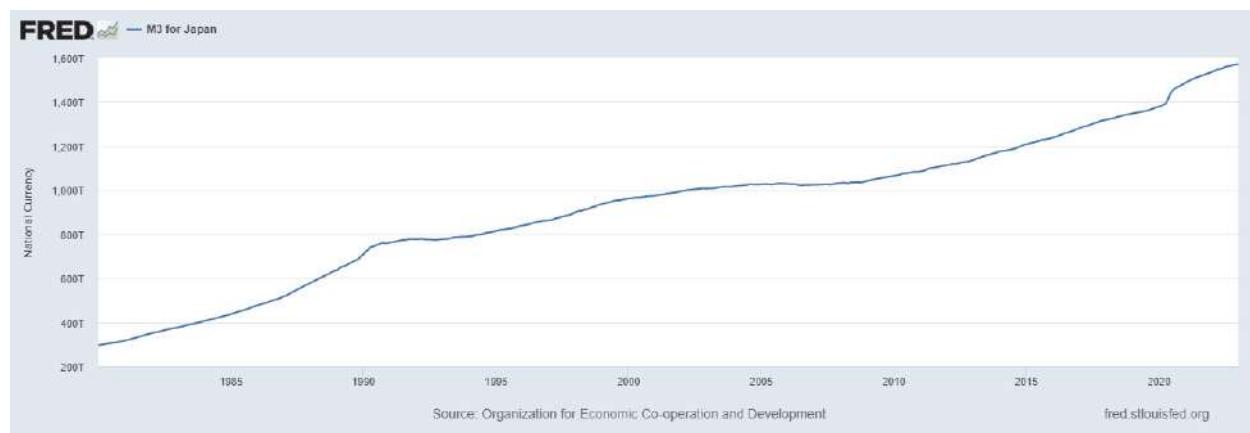
La massa monetaria M3 dell'area dell'euro a gennaio 2022 era di circa 16 trilioni di euro (fonte: Banca Centrale Europea).



La massa monetaria M3 degli Stati Uniti a febbraio 2022 era di circa 22 trilioni di dollari:



La massa monetaria M3 del Giappone a febbraio 2022 era di circa quasi 1,600 triliuni di Yen:



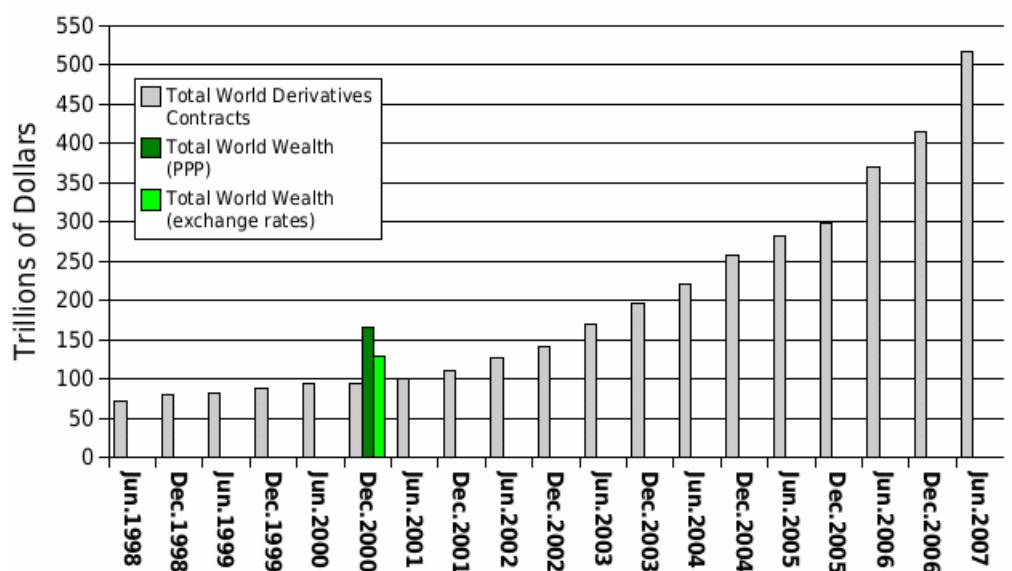
Si noti bene che questo valore non esprime complessivamente il mercato finanziario. Infatti, molti strumenti finanziari più complessi non vengono classificati all'interno delle masse monetarie.

Definizioni degli aggregati monetari dell'area dell'euro

	M1	M2	M3
Banconote e monete in circolazione	X	X	X
Depositi a vista	X	X	X
Depositi con durata prestabilita fino a due anni	X	X	
Depositi rimborsabili con preavviso fino a tre mesi	X	X	
Operazioni pronti contro termine		X	
Quote e partecipazioni in fondi comuni monetari		X	
Titoli di debito con scadenza originaria fino a due anni		X	

Per esempio, gli strumenti derivati e le cartolarizzazioni non appartengono a nessuna tipologia di massa monetaria perché non sono denaro effettivo o depositi bancari, ma **rappresentano invece impegni finanziari**. Gli strumenti derivati sono infatti contratti finanziari che traggono il loro valore da un'attività sottostante, come un'azione o una materia prima, ma non rappresentano denaro effettivo. Allo stesso modo le cartolarizzazioni sono titoli che rappresentano un flusso di pagamenti futuri generati da un gruppo di attività, come ad esempio mutui ipotecari.

World Wealth vs World Derivatives 1998-2007



Questo grafico illustra la ricchezza mondiale totale rispetto al valore nominale totale nei contratti derivati tra il 1998 e il 2007. Possiamo osservare dal grafico presentato che dal 2003 in avanti, il valore dei contratti derivati scambiati all'interno dei mercati di tutto il mondo aveva superato ampiamente il valore delle proprietà e della ricchezza complessiva.

Durante le crisi finanziarie, gli strumenti derivati e le cartolarizzazioni possono avere un impatto significativo sulle masse monetarie, poiché le perdite su questi strumenti possono influire sulla fiducia degli investitori e portare ad un calo dei mercati finanziari. Questo può causare una diminuzione della liquidità ed un aumento del rischio di insolvenza delle banche e delle imprese, con conseguenze negative sull'economia reale.

Inoltre, **la creazione e la diffusione di strumenti derivati e cartolarizzazioni può avere un impatto sulle politiche monetarie, poiché in grado di influenzare la domanda di denaro e la capacità delle banche centrali di controllare l'offerta di moneta**. Pertanto, sebbene non siano inclusi direttamente nelle masse monetarie, gli strumenti derivati e le cartolarizzazioni possono avere un ruolo significativo nel determinare la stabilità del sistema finanziario e dell'economia nel suo complesso.

Riassumendo, attraverso politiche di QE e politiche fiscali espansive, le banche centrali immettono liquidità all'interno della base monetaria M0, la quale viene in parte gestita nelle banche commerciali e fatta entrare nelle altre masse monetarie, nei mercati finanziari e dei derivati, ed in parte gestita dal Tesoro per la spesa pubblica.

Fonti

- ▶ “The Handbook of International Financial Terms” di Peter Moles e Nicholas Terry
- ▶ “Financial Markets and Institutions” di Anthony Saunders e Marcia Millon Cornett

1.5

Filosofia Economica

● Basic

La moneta cattiva caccia la moneta buona?

La teoria della moneta cattiva caccia la moneta buona è stata formulata per la prima volta dall'economista britannico Thomas Gresham nel XVI secolo. Questa teoria sosteneva che, quando due tipi di monete con lo stesso valore nominale ma con diverso contenuto di metallo prezioso sono in circolazione, **le monete di qualità inferiore (moneta cattiva) tendono a sostituire quelle di qualità superiore (moneta buona)** perché **le persone preferiscono tenere le monete di qualità superiore e spendere per quelle di qualità inferiore**. Oggi, questa teoria può essere applicata ai paesi in cui **la moneta nazionale perde valore rapidamente, spingendo le persone a cercare alternative più stabili per conservare il proprio potere d'acquisto**. In questi casi, la teoria della moneta cattiva caccia la moneta buona si verifica quando le persone preferiscono tenere valute estere o metalli preziosi invece della valuta nazionale.

Negli ultimi 100 anni, ci sono stati diversi casi in cui la teoria della moneta cattiva caccia la moneta buona si è verificata.

Uno dei casi più noti è stato quello della Germania negli anni '20, durante l'iperinflazione post-bellica. La moneta nazionale, il marco tedesco, aveva perso valore rapidamente e le persone cercavano alternative più stabili. In questo contesto, molte persone hanno cominciato a preferire **il dollaro americano o l'oro come forma di conservazione del proprio potere d'acquisto**.

Un altro caso interessante è stato quello dell'Argentina negli anni 2000. Durante la crisi economica del 2001, la moneta nazionale, il peso argentino, ha perso valore rapidamente e le persone hanno comincia-

to a cercare alternative più stabili. In questo contesto, **molte persone hanno preferito detenere dollari americani o euro invece dei pesos argentini**. Questo ha portato ad una riduzione della domanda di pesos argentino ed a un aumento del tasso di cambio delle valute estere rispetto alla moneta Argentina. Tuttavia, ci sono anche casi in cui la teoria per cui la moneta cattiva caccia la moneta buona non si è verificata. Ad esempio, durante la Grande Recessione del 2008-2009, molte valute nazionali hanno perso valore rispetto al dollaro americano, come l'euro, la sterlina e lo yen giapponese. Tuttavia, molte persone hanno continuato a utilizzare la propria valuta nazionale.

Anche durante la Grande Recessione, molti beni rifugio hanno registrato un aumento significativo del prezzo, validando il concetto che i risparmiatori hanno preferito sostituire la propria liquidità con asset con maggiore valore intrinseco. Nel settembre 2008, l'oro era quotato a circa 750 dollari per oncia, mentre alla fine del 2010 il prezzo era salito a oltre 1.400 dollari per oncia. **Questo rappresenta un aumento del 87% in due anni**. Allo stesso tempo, il prezzo delle obbligazioni governative è aumentato a causa della maggiore domanda da parte degli investitori in cerca di sicurezza.

Questa teoria ci aiuta a comprendere più nel dettaglio le dinamiche relative al valore delle valute nell'arco del tempo, della loro gestione e della loro relativa stabilità in complesse circostanze sociali e geopolitiche.

1.6

Informatica

● Basic

Come vengono scambiate le monete nell'economia globale?

Quando si dice che un **asset è liquido si intende che è facilmente trasferibile da un punto all'altro del sistema economico ed è facilmente inter-scambiabile con altri asset**. Come abbiamo visto in precedenza, le masse monetarie, gli strumenti finanziari e le valute, sono classificabili in diverso modo e possono essere più o meno liquide in funzione della loro struttura.

Per esempio, i soldi nel nostro conto corrente sono più liquidi dei soldi che abbiamo sotto forma di asset finanziari nel conto titoli, nonostante siano entrambi virtuali: byte all'interno di un database di una banca commerciale. Infatti, il tempo di "prelevare" e/o spostare questi asset da un conto all'altro è differente. Questa differenza è chiaramente legata alla tipologia di regole e reti utilizzate per trasferire gli asset all'interno dell'intero sistema finanziario.

Ma, quindi, come avviene il trasferimento tra banche centrali, banche commerciali, mercati ed individui? Tutto il sistema finanziario si poggia al di sopra di Internet, il quale dagli anni 50 ha creato dei protocolli informatici e delle piattaforme che abilitano facilmente il trasferimento del denaro in maniera sicura e digitale. Queste reti informatiche, in gergo, si occupano di ciò che concerne il "clearing e settlement" dei pagamenti.

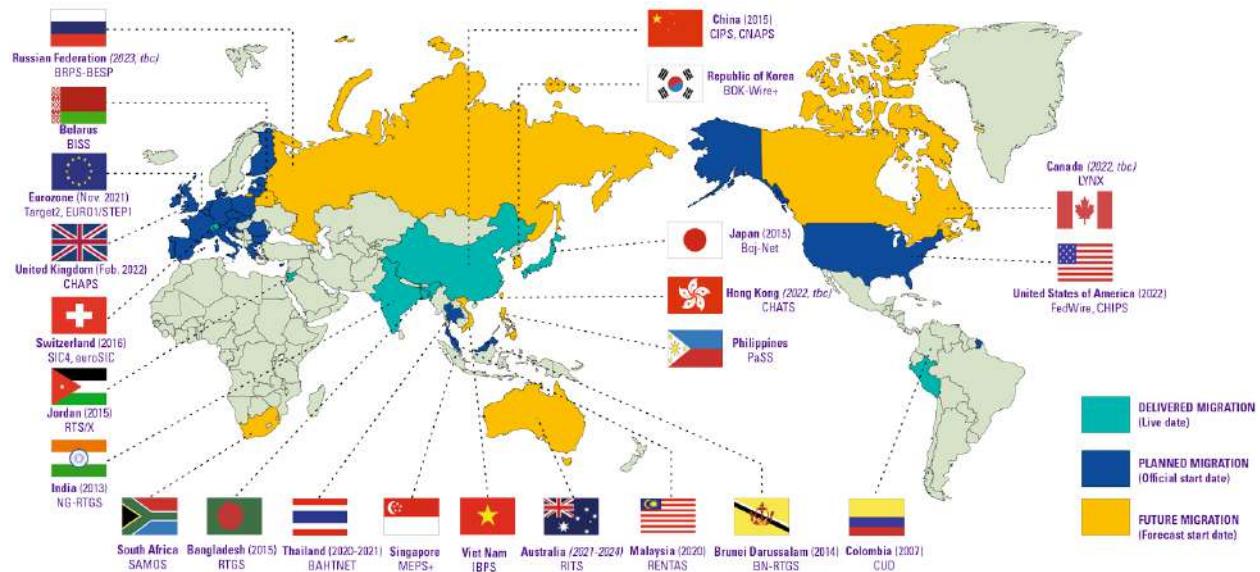
I sistemi di clearing e settlement sono utilizzati dalle masse monetarie per garantire che le transazioni finanziarie siano effettuate in modo sicuro ed efficiente. Il processo di clearing e settlement implica la compensazione e l'elaborazione dei pagamenti tra le parti coinvolte in una transazione finanziaria. Ci sono diversi sistemi di clearing e settlement utilizzati in funzione degli attori coinvolti e degli asset e/o valute utilizzate, tra cui:

- **Sistema di Clearing Interbancario**: questo sistema viene utilizzato per la **compensazione delle transazioni tra le banche commerciali**. Il processo di clearing avviene quando le banche inviano i dati delle transazioni a un'organizzazione centrale, che elabora le informazioni e le invia alle banche coinvolte per la conferma. Una volta confermata la transazione, il sistema di settlement effettua il pagamento. Esempi: Fedwire, TARGET2, CHIPS.
- **Sistema di Clearing e Settlement delle Carte di Pagamento**: questo sistema viene utilizzato per la **compensazione delle transazioni con carte di credito e di debito nel mercato retail**. Il processo di

clearing avviene quando il titolare della carta effettua un acquisto e il sistema di pagamento della carta verifica l'identità dell'acquirente e la disponibilità di fondi. Una volta autorizzata la transazione, il sistema di settlement effettua il pagamento al venditore.

Esempi: VisaNet, Mastercard Payment Transaction Services, American Express Network.

- **Sistema di Clearing e Settlement delle Transazioni su Titoli:** questo sistema viene utilizzato per la compensazione delle transazioni su titoli, come azioni, obbligazioni e altri strumenti finanziari. Il processo di clearing avviene quando gli investitori acquistano o vendono titoli e l'organizzazione centrale raccoglie le informazioni sulle transazioni e le confronta per garantire che siano corrette. Una volta confermata la transazione, il sistema di settlement effettua il pagamento ed il trasferimento dei titoli. Esempi: Depository Trust & Clearing Corporation (DTCC), Euroclear, Clearstream.
- **Sistemi di Clearing e Settlement delle Transazioni su Valute Estere:** questo sistema viene utilizzato per la compensazione delle transazioni su valute estere. Il processo di clearing avviene quando le banche scambiano valute estere e l'organizzazione centrale confronta le informazioni per garantire che le transazioni siano corrette. Una volta confermata la transazione, il sistema di settlement effettua il pagamento. Esempi: CLS Bank International, Global Foreign Exchange Division (GFXD), SWIFT.



Ogni sistema monetario internazionale possiede delle reti proprietarie e private che abilitano uno scambio sicuro ed affidabile per tutte le banche commerciali e d'investimento. Come possiamo osservare dalla mappa, ogni area economica utilizza una o più reti per far comunicare le proprie realtà finanziarie. Altre reti come SWIFT, Visa, Mastercard, invece, non hanno un confinamento preciso ma vengono utilizzate per garantire una standardizzazione nei pagamenti e nei trasferimenti di valore a livello globale. In risposta ad un effettivo oligopolio di alcune aziende private, molti paesi stanno lavorando per creare dei nuovi sistemi di pagamento, completamente proprietari, sia per il mercato dei pagamenti retail, sia per trasferimenti interbancari. La Cina, ad esempio, ha già iniziato ad utilizzare una **Central Bank Digital Currency (CBDC)** in maniera complementare ai sistemi di clearing e settlement utilizzati finora, mentre altri sistemi economici come quello europeo, stanno pianificando la migrazione nei prossimi anni.



Central Bank Digital Currency (CBDC)

Una central bank digital currency, in sigla: CBDC è una tipologia di valuta digitale emessa da una banca centrale anziché da una banca commerciale.

2

I sistemi di clearing e settlement

- 2.1. Quali sono i sistemi di trasferimento nel mercato interbancario?
- 2.2. Quali sono i sistemi di trasferimento nel mercato valutario?
- 2.3. Quali sono i sistemi di trasferimento nel mercato retail?
- 2.4. Come viene gestita l'amministrazione delle reti di clearing e settlement?
- 2.5. Come avviene l'interoperabilità tra le reti interbancarie e retail?
- 2.6. Il fintech e la diffusione di strumenti di pagamento innovativi
- 2.7. Come funziona un pagamento online su e-commerce?
- 2.8. Sistemi peer to peer vs sistemi non peer to peer nei processi di clearing e settlement

2.1

Informatica

• Medium

Quali sono i sistemi di trasferimento nel mercato interbancario?

Le **principal reti di pagamento globali utilizzate dalle banche** commerciali per i meccanismi di clearing e settlement interbancario includono:

1. **SWIFT** (Society for Worldwide Interbank Financial Telecommunication): SWIFT è la rete di pagamento internazionale più grande al mondo. Fornisce servizi di comunicazione e di pagamento, gestendo circa il **90% delle transazioni internazionali tra banche**. La governance di SWIFT è basata su un sistema di voto, dove ogni banca ne ha a disposizione uno, indipendentemente dalla sua dimensione. Per esempio, nella area SEPA, è utilizzato SWIFT come circuito.
2. **CHIPS** (Clearing House Interbank Payments System): CHIPS è una **rete di pagamento interbancaria basata negli Stati Uniti**, che **elabora principalmente transazioni in dollari USA**. CHIPS è gestita dalla Clearing House Payments Company LLC, una filiale di The Clearing House Association. La governance di CHIPS è guidata dai rappresentanti delle banche partecipanti.
3. **Fedwire**: Fedwire è una **rete di pagamento interbancaria negli Stati Uniti**, che gestisce principalmente **transazioni di grandi importi in dollari USA**. La rete è gestita dalla Federal Reserve e offre anche servizi di clearing e settlement per altri servizi di pagamento, tra cui ACH e Check 21.
4. **TARGET2** (Trans-European Automated Real-time Gross Settlement Express Transfer System): TARGET2 è la **rete di pagamento di grossi importi in euro**, che fornisce servizi di clearing e settlement. La rete è gestita dalla Banca centrale europea (BCE) e dalle banche centrali nazionali.
5. **CIPS** (Cross-border Interbank Payment System): CIPS è una **rete di pagamento interbancaria in Cina**, che è stata lanciata nel 2015 per elaborare transazioni transfrontaliere in yuan cinese. La rete è gestita dalla People's Bank of China (PBOC).
6. **ACH** (Automated Clearing House): ACH è una **rete di pagamento negli Stati Uniti che fornisce servizi di clearing e settlement per transazioni di piccoli importi**, come pagamenti salariali, pagamenti con carta di credito e debito e pagamenti alle aziende. La governance di ACH è guidata dall'NACHA (National Automated Clearing House Association), un'organizzazione senza scopo di lucro.

I volumi di queste reti di pagamento variano, ma **SWIFT e TARGET2 gestiscono il maggior numero di transazioni di pagamento di grandi importi**. La governance di queste reti di pagamento varia a seconda della struttura di proprietà e delle regole di voto. Ad esempio, SWIFT è di proprietà delle banche partecipanti, mentre Fedwire è gestita dalla Federal Reserve. La governance di queste reti è importante perché può influire sulla trasparenza e sulla sicurezza delle transazioni, nonché sulla possibilità di inclusione di nuovi partecipanti.

2.2

Informatica

• Medium

Quali sono i sistemi di trasferimento nel mercato valutario?

I sistemi di clearing e settlement per il mercato delle valute estere sono meccanismi utilizzati per il trasferimento di fondi tra banche e altre istituzioni finanziarie che operano con valute estere. **Questi sistemi sono essenziali per garantire l'efficienza e l'affidabilità delle transazioni transfrontaliere, poiché riducono il rischio di insoluti e aumentano la trasparenza e la certezza degli scambi.**

- Il sistema **SWIFT** anche utilizzato per lo scambio di valute estere. Oltre alla messaggistica, SWIFT offre anche una **gamma di servizi di clearing e settlement**, come ad esempio il sistema di pagamento SWIFT MT103, che consente alle banche di effettuare pagamenti in valuta estera.
- Il sistema **CLS**, invece, è un sistema di clearing e settlement specializzato per le transazioni in valuta estera. CLS consente alle banche di effettuare transazioni di valuta estera in modo sicuro e tempestivo, riducendo il rischio di insoluti e aumentando la certezza degli scambi. CLS utilizza un modello di pagamento simultaneo (PvP) che consente di effettuare il pagamento e la liquidazione delle transazioni in modo simultaneo, senza rischio di fallimento di una delle controparti. CLS utilizza anche protocolli informatici avanzati, come ad esempio il protocollo di comunicazione TCP/IP, per garantire la sicurezza delle transazioni e la protezione dei dati sensibili.

Ogni rete di clearing e settlement ha degli indicatori che permettono di comprendere più a fondo le sue peculiarità e le operazioni consentite all'interno della rete. Qui di seguito una tabella con alcune informazioni a riguardo:

Indicatore	Descrizione	Performance/Governance
Volume di transazione	Quantità di transazioni finanziarie elaborate da una rete o sistema di pagamento in un determinato periodo di tempo.	Maggiore volume di transazioni indica una rete di pagamento robusta e in grado di soddisfare la domanda degli utenti. Tuttavia, un volume eccessivamente elevato potrebbe causare problemi di congestione e ritardi nell'elaborazione delle transazioni.
Efficienza operativa	Capacità di una rete o sistema di pagamento di elaborare le transazioni in modo rapido, accurato ed efficiente, riducendo al minimo gli errori e i costi di elaborazione.	Un alto livello di efficienza operativa indica una gestione ottimale delle risorse e un sistema affidabile e performante. La mancanza di efficienza può causare ritardi nell'elaborazione delle transazioni e costi aggiuntivi per gli utenti.
Rischio di controparte	Rischio di perdite finanziarie dovute all'insolvenza o al fallimento di una controparte coinvolta in una transazione.	Una buona governance e la capacità di monitorare e gestire i rischi di controparte sono fondamentali per la stabilità e la sicurezza di una rete o sistema di pagamento. Tuttavia, i rischi di controparte possono essere mitigati solo fino a un certo punto e una gestione inadeguata può causare gravi perdite finanziarie.
Governance	Sistema di regole, politiche e procedure che governano la gestione e il funzionamento di una rete o sistema di pagamento.	Una governance solida è essenziale per garantire l'efficienza, la sicurezza e la stabilità di una rete o sistema di pagamento. Una governance inadeguata può causare problemi di compliance, mancanza di trasparenza e conflitti di interesse.

Sicurezza	Capacità di una rete o sistema di pagamento di proteggere le transazioni finanziarie e i dati degli utenti da frodi, attacchi informatici e altri rischi di sicurezza.	La sicurezza è fondamentale per la fiducia degli utenti e la stabilità del sistema finanziario. Una rete o sistema di pagamento sicuro deve essere in grado di proteggere le informazioni degli utenti e prevenire le frodi e gli attacchi informatici. Tuttavia, i rischi di sicurezza non possono essere completamente eliminati e una gestione inadeguata può causare gravi conseguenze per gli utenti e il sistema finanziario.
-----------	--	---

In generale, sia SWIFT che CLS, sono sistemi di clearing e settlement altamente sofisticati e affidabili, che utilizzano protocolli informatici avanzati per garantire la sicurezza e l'efficienza delle transazioni transfrontaliere.

2.3

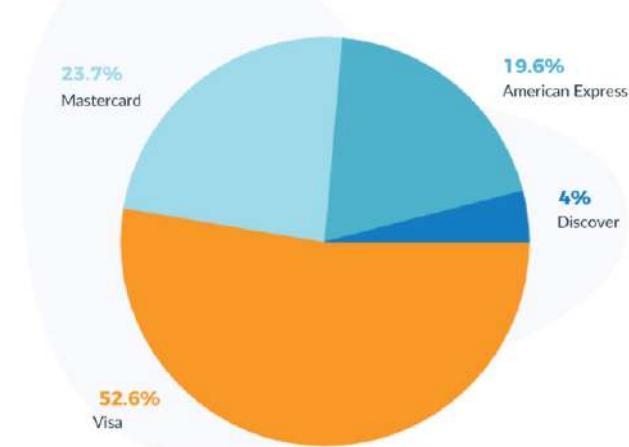
Informatica

● Medium

Quali sono i sistemi di trasferimento nel mercato retail?

Gli strumenti di pagamento retail sono essenziali per **effettuare transazioni di acquisto di beni e servizi sia nei negozi fisici che online**. Questi strumenti includono una vasta gamma di metodi di pagamento, tra cui le carte di credito e di debito, i bonifici bancari, i pagamenti con smartphone, i contanti, gli assegni bancari e i pagamenti online come PayPal.

Top 2021 Credit Card Networks
By Percent of Purchase Volume



Source: SEC filings from Visa, Mastercard, American Express, and Discover

Le reti di clearing e settlement più importanti per i pagamenti retail includono Visa, Mastercard e American Express. Visa è la più grande rete di pagamento al mondo, con una quota di mercato del 53% nel 2021. Elabora pagamenti in oltre 200 paesi e gestisce transazioni per un valore di oltre 11 trilioni di dollari all'anno. Mastercard è la seconda più grande rete di pagamento al mondo, con una quota di mercato del

31% nel 2020. Elabora pagamenti in oltre 210 paesi e gestisce transazioni per un valore di oltre 5 trilioni di dollari all'anno. American Express è una rete di pagamento globale che si concentra principalmente sui consumatori con redditi elevati e sulle imprese. Nel 2020, American Express ha gestito transazioni per un valore di oltre 1 trilione di dollari.

Qui di seguito una tabella riassuntiva con alcune considerazioni su governance, performance, numero di utenti e quota di mercato relativa alla propria tipologia di operatività:

Azienda	Governance	Prestazioni	Numero di utenti	Quota di mercato
Visa	<i>Governance solida, con un sistema di regole rigoroso per la gestione e il funzionamento della rete di pagamento.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno ed una elevata efficienza operativa.</i>	<i>Più di 3,5 miliardi di titolari di carte Visa in tutto il mondo.</i>	<i>Quota di mercato globale del 52,6%.</i>
Mastercard	<i>Governance solida, con un forte impegno per la trasparenza e la compliance.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno e una elevata efficienza operativa.</i>	<i>Più di 2,5 miliardi di titolari di carte Mastercard in tutto il mondo.</i>	<i>Quota di mercato globale del 23,7%.</i>
American Express (AMEX)	<i>Governance solida, con un forte impegno per la trasparenza e la gestione del rischio.</i>	<i>Prestazioni solide, con un elevato volume di transazioni e un'esperienza di servizio clienti di alta qualità.</i>	<i>Circa 114 milioni di titolari di carte AMEX in tutto il mondo.</i>	<i>Quota di mercato globale del 19,6%.</i>
Discover	<i>Governance solida, con un sistema di regole rigoroso per la gestione e il funzionamento della rete di pagamento.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno e una elevata efficienza operativa.</i>	<i>Più di 50 milioni di titolari di carte Discover negli Stati Uniti.</i>	<i>Quota di mercato globale inferiore al 1%.</i>
China Union Payment	<i>Governance guidata dal governo cinese, con un forte impegno per la sicurezza e la stabilità finanziaria.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno e una elevata efficienza operativa.</i>	<i>Sono state emesse 8,4 miliardi di carte China Union Payment in Cina.</i>	<i>Quota di mercato dominante in Cina.</i>
JCB	<i>Governance solida, con un forte impegno per la compliance e la gestione del rischio.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno ed una elevata efficienza operativa.</i>	<i>Più di 130 milioni di titolari di carte JCB in tutto il mondo.</i>	<i>Quota di mercato globale inferiore all'1%.</i>
Diners Club	<i>Governance solida, con un sistema di regole rigoroso per la gestione e il funzionamento della rete di pagamento.</i>	<i>Prestazioni solide, con un alto volume di transazioni elaborate ogni anno e una elevata efficienza operativa.</i>	<i>Circa 10 milioni di titolari di carte Diners Club in tutto il mondo.</i>	<i>Quota di mercato globale inferiore all'1%.</i>

In sintesi, gli strumenti di pagamento retail sono essenziali per effettuare transazioni di acquisto, ma per garantire la sicurezza e l'efficienza dei pagamenti, è necessaria l'infrastruttura fornita dalle reti di clearing e settlement. Visa, Mastercard e American Express sono tra le reti di pagamento più importanti al mondo per i pagamenti retail e continuano ad espandersi a livello internazionale.

2.4

Informatica

● Hard

Come viene gestita l'amministrazione delle reti di clearing e settlement?

La governance delle architetture di clearing e settlement può variare in base alla natura dei pagamenti e all'ambito di utilizzo.

Nelle reti finora elencate, la **governance è spesso gestita da organizzazioni centrali**, come le banche centrali o le associazioni di clearing e settlement. Ad esempio, il sistema di clearing e settlement interbancario degli Stati Uniti, conosciuto come Fedwire, è gestito dalla Federal Reserve. La governance di tali sistemi è spesso definita da standard di settore e da regolamentazioni governative che garantiscono la sicurezza e l'efficienza dei pagamenti.

Analizziamo adesso in maggior dettaglio il funzionamento di SWIFT, Visa e CLS:

Swift (Society for Worldwide Interbank Financial Telecommunication) è una piattaforma di messaggistica interbancaria globale che consente alle banche e alle istituzioni finanziarie di inviare e ricevere pagamenti attraverso una rete sicura standardizzata. La piattaforma utilizza un sistema di messaggistica proprietario chiamato MT (Message Type) per consentire la comunicazione tra le parti. Gli MT sono suddivisi in numerose categorie che rappresentano diversi tipi di transazioni finanziarie, come ad esempio:

- MT103 che rappresenta l'ordine di bonifico;
- MT192 invece corrisponde alla richiesta di cancellazione del pagamento;
- MT199 è un messaggio a testo libero che puoi inviare a banche con cui ha scambio chiave SWIFT attivo.

L'architettura di Swift è composta da diversi componenti, tra cui:

- **SwiftNet:** è la rete di comunicazione che consente alle banche e alle istituzioni finanziarie di scambiarsi messaggi attraverso la piattaforma Swift. SwiftNet utilizza tecnologie di sicurezza avanzate, come la crittografia, per proteggere la trasmissione dei dati.
- **Alliance Messaging Hub (AMH):** è un gateway di messaggistica che consente alle banche e alle istituzioni finanziarie di accedere alla rete SwiftNet. L'AMH è progettato per garantire l'alta disponibilità e l'affidabilità della piattaforma.
- **Swift Interface Pack (SWIFTIP):** è un pacchetto di software che consente alle banche e alle istituzioni finanziarie di integrare la piattaforma Swift nella propria infrastruttura IT.

Questa rete è gestita da SWIFT SCRL, una società cooperativa di diritto belga. L'amministratore di rete di SWIFT è l'organizzazione stessa, ovvero SWIFT SCRL, il quale monitora e gestisce la rete col fine che tutte le informazioni inserite siano corrette.

Per quanto riguarda Visa, la **piattaforma tecnologica è chiamata VisaNet, ed è progettata per gestire milioni di transazioni di pagamento ogni giorno.**

L'architettura di VisaNet è composta da diversi componenti, tra cui:

- **Network Access:** è un sistema di connettività che consente ai partner commerciali di accedere alla rete VisaNet. Il sistema di connettività è progettato per garantire l'alta disponibilità e l'affidabilità della piattaforma.
- **Authorization:** è un sistema di elaborazione che verifica la validità della transazione, autorizza o respinge la stessa sulla base di vari fattori come la disponibilità di fondi e la sicurezza della transazione.
- **Clearing and Settlement:** è un sistema che gestisce il processo di clearing e settlement delle transazioni di pagamento. Il sistema elabora le transazioni e ne calcola l'importo da pagare alle banche e alle istituzioni finanziarie coinvolte.

Anche in questo caso l'amministratore di rete di VISA è l'organizzazione stessa, ovvero la società americana Visa Inc.

Infine, l'**architettura della rete CLS è composta da diversi componenti**, tra cui:

- **Settlement Members:** sono le banche e le istituzioni finanziarie che partecipano alla piattaforma CLS. Le banche e le istituzioni finanziarie devono soddisfare determinati requisiti di liquidità e di credito per diventare membri del sistema.
- **CLS Bank:** è la banca centrale di CLS che gestisce il processo di clearing e settlement delle transazioni di cambio.

Una volta ricevuti i dati dalla rete di pagamento, la banca procede all'elaborazione delle transazioni. Questo processo prevede una serie di attività volte a verificare la validità delle transazioni, addebitare i pagamenti sul conto del cliente e accreditare i fondi sul conto del beneficiario.

In particolare, l'**elaborazione delle transazioni prevede le seguenti fasi:**

- **Verifica della validità della transazione:** la banca verifica che la transazione sia corretta e valida, ad esempio controllando se il conto del cliente ha fondi sufficienti per coprire l'importo del pagamento.
- **Accettazione della transazione:** una volta verificata la validità della transazione, la banca la accetta e procede ad addebitare l'importo sul conto del cliente.
- **Instradamento della transazione:** la banca instrada la transazione verso la banca del beneficiario utilizzando la rete di pagamento. Questo prevede l'invio, alla banca del beneficiario, delle informazioni necessarie per identificare la transazione e accreditare i fondi sul conto del beneficiario.
- **Ricezione della conferma di accredito:** una volta che la banca del beneficiario ha accreditato i fondi sul conto del beneficiario, invia una conferma di accredito alla banca dell'ordinante.
- **Accreditamento dei fondi:** la banca del cliente accreditare i fondi sul conto del beneficiario e la transazione è completata.

Questa rete è gestita da CLS Group Holdings AG, una società svizzera che offre servizi di regolamento per il mercato dei cambi. L'amministratore di rete di CLS è l'organizzazione stessa, ovvero CLS Group Holdings AG.

In generale, i sistemi di pagamento utilizzati dalle banche sono altamente sofisticati e affidabili, in grado di gestire grandi volumi di transazioni in modo rapido ed efficiente. Tuttavia, come per ogni sistema informatico, sono soggetti a rischi di sicurezza informatica e devono essere costantemente monitorati e aggiornati per garantire la sicurezza e l'affidabilità dei pagamenti dagli amministratori della rete.

2.5

Informatica

• Hard

Come avviene l'interoperabilità tra le reti interbancarie e retail?

Dal punto di vista informatico, Visa e Mastercard lavorano in sinergia con le reti di pagamento come SWIFT e SEPA utilizzando standard di messaggistica comuni e protocolli di comunicazione.

In particolare, Visa e Mastercard utilizzano il protocollo **ISO 8583**, che è uno standard di messaggistica per le transazioni di pagamento elettronico. Questo protocollo definisce la struttura dei messaggi, la codifica dei dati e il formato dei campi di dati scambiati tra le parti coinvolte nella transazione. In questo modo, Visa e Mastercard possono comunicare con le banche emittenti e acquirer, nonché con altri sistemi di clearing e settlement interbancari come SWIFT e SEPA, utilizzando un formato comune di messaggi.

Inoltre, Visa e Mastercard utilizzano anche standard di sicurezza comuni come il **protocollo di sicurezza SSL** (Secure Socket Layer) e il **protocollo di sicurezza TLS** (Transport Layer Security) **per garantire che i dati delle transazioni vengano trasmessi in modo sicuro e protetto.**

Per quanto riguarda SWIFT e SEPA, queste reti di pagamento utilizzano standard di messaggistica simili, ma con alcune differenze. **SWIFT utilizza un formato di messaggio chiamato FIN** (Financial Information exchange), che è stato progettato specificamente per il trasferimento di fondi tra banche e istituti finanziari. **SEPA, d'altra parte, utilizza il formato di messaggio XML** (Extensible Markup Language), che è un formato di dati basato su testo e utilizzato per la comunicazione tra le banche nell'area SEPA.

A partire dal 2025 anche lo SWIFT adotterà lo standard ISO 20022 e la messaggistica xml. Tale migrazione è già in corso.

Tuttavia, nonostante queste differenze, Visa e Mastercard possono ancora lavorare in sinergia con SWIFT e SEPA, in quanto queste reti condividono molti dei medesimi standard e protocolli di sicurezza.

In pratica, **quando una transazione viene elaborata tramite una carta di credito o debito di Visa o Mastercard, il messaggio viene trasmesso alla banca emittente attraverso la rete di pagamento di Visa o Mastercard. La banca emittente, a sua volta, potrebbe utilizzare SWIFT o SEPA per elaborare il pagamento.** Il protocollo ISO 8583 viene utilizzato per strutturare il messaggio di transazione, mentre i protocolli di sicurezza SSL e TLS vengono utilizzati per proteggere la trasmissione dei dati. In questo modo, Visa e Mastercard possono lavorare in sinergia con le reti di pagamento come SWIFT e SEPA per elaborare le transazioni in modo rapido, sicuro ed efficiente.

I protocolli di comunicazione giocano un ruolo fondamentale nell'abilitare la relazione tra Visa e Mastercard con SWIFT, SEPA e altre reti di pagamento. Questi protocolli forniscono una base standardizzata per la comunicazione e lo scambio di informazioni tra le parti coinvolte.

In particolare, i **protocolli di comunicazione sono utilizzati per definire le specifiche tecniche relative alla struttura dei messaggi, alla codifica dei dati e al formato dei campi di dati scambiati tra le parti coinvolte nella transazione.** Ciò garantisce che tutte le parti coinvolte siano in grado di comunicare e scambiare informazioni in modo corretto ed efficiente.

Inoltre, Visa, Mastercard, SWIFT e SEPA utilizzano **protocolli di sicurezza** standardizzati come SSL e TLS per proteggere la trasmissione dei dati tra le parti coinvolte. Questi protocolli consentono la **crittografia dei dati in transito, la verifica dell'autenticità delle parti coinvolte e la protezione da eventuali tentativi di intercettazione o manipolazione dei dati.**

Qui di seguito una tabella riassuntiva delle principali reti di clearing e settlement utilizzate tra banche commerciali, istituzioni finanziarie

Rete	Volume giornaliero medio	Governance	Attori coinvolti	Protocolli informatici
SWIFT (Society for Worldwide Interbank Financial Telecommunication)	Circa 5,2 miliardi di messaggi finanziari elaborati ogni anno.	Governance solida, con un comitato di gestione composto da rappresentanti delle istituzioni finanziarie partecipanti.	Banche, istituzioni finanziarie e altre organizzazioni finanziarie in tutto il mondo.	Utilizza protocolli di comunicazione sicuri, come il protocollo di sicurezza delle comunicazioni SWIFT (SWIFTNet) e il protocollo di sicurezza delle transazioni SWIFT (SWIFT MT).
TARGET2 (Trans-European Automated Real-time Gross Settlement Express Transfer System)	Circa 350.000 pagamenti transfrontalieri elaborati ogni giorno, per un valore totale di circa 2,8 trilioni di euro.	Governance solida, con una gestione centralizzata da parte della Banca centrale europea (BCE).	Banche centrali nazionali e istituzioni finanziarie dell'Area unica dei pagamenti in euro (SEPA).	Utilizza il protocollo di comunicazione sicuro SWIFTNet per la trasmissione dei dati.

CHIPS (Clearing House Interbank Payments System)	Circa 250.000 transazioni di pagamento transfrontaliere elaborate ogni giorno, per un valore totale di circa 1,5 trilioni di dollari USA.	Governance solida, con un consiglio di amministrazione composto da rappresentanti delle banche partecipanti.	Banche, istituzioni finanziarie e altre organizzazioni finanziarie negli Stati Uniti e in tutto il mondo.	Utilizza un protocollo di comunicazione sicuro basato su messaggi di dati standardizzati, come il protocollo di messaggistica finanziaria ISO 20022.
Fedwire Funds Service	Circa 830.000 transazioni di pagamento elaborate ogni giorno, per un valore totale di circa 3,5 trilioni di dollari USA.	Governance solida, con una gestione centralizzata da parte della Federal Reserve Bank degli Stati Uniti.	Banche, istituzioni finanziarie e altre organizzazioni finanziarie negli Stati Uniti.	Utilizza il protocollo di comunicazione sicuro SWIFTNet per la trasmissione dei dati.
Bitcoin	Circa 300.000 transazioni elaborate ogni giorno, per un valore totale di circa 1,5 miliardi di dollari USA.	Governance decentralizzata, con una rete di nodi indipendenti che gestiscono la rete.	Individui e organizzazioni che utilizzano bitcoin.	Utilizza un protocollo di comunicazione sicuro basato sulla tecnologia blockchain, chiamato Bitcoin

In sintesi, i **protocolli di comunicazione svolgono un ruolo essenziale nella facilitazione della comunicazione tra Visa, Mastercard, SWIFT, SEPA e altre reti di pagamento**. Questi protocolli forniscono un insieme di regole standardizzate che consentono alle parti coinvolte di comunicare e scambiare informazioni in modo sicuro ed efficiente. In questo modo, i protocolli di comunicazione contribuiscono a **garantire il corretto funzionamento dei sistemi di pagamento elettronico e l'elaborazione sicura ed affidabile delle transazioni finanziarie**.

2.6

Business

Basic

Il fintech e la diffusione di strumenti di pagamento innovativi

I pagamenti digitali rappresentano un'evoluzione tecnologica che ha rivoluzionato il modo in cui le persone effettuano transazioni finanziarie. I **pagamenti digitali consentono di effettuare pagamenti attraverso dispositivi elettronici come smartphone, tablet, computer, smartwatch e altri dispositivi connessi a Internet**.

Servizio di pagamento	Azienda leader	Descrizione	Fatturato
PayPal	PayPal Holdings, Inc.	Servizio di pagamento online che consente di inviare e ricevere pagamenti su internet.	Fatturato di circa 21,5 miliardi di dollari USA nel 2020.
Alipay	Alibaba Group Holding Limited	Servizio di pagamento mobile in Cina, che consente di effettuare transazioni online e offline.	Fatturato di circa 20 miliardi di dollari USA nel 2020.

WeChat Pay	Tencent Holdings Limited	Servizio di pagamento mobile in Cina, che consente di effettuare transazioni online e offline tramite l'app WeChat.	Fatturato di circa 13,5 miliardi di dollari USA nel 2020.
Square	Square, Inc.	Piattaforma che consente di accettare pagamenti con carte di pagamento, ed offre altri servizi, come: gestionale di cassa, finanziamenti, conti e carte per gli esercenti	Fatturato di circa 9,5 miliardi di dollari USA nel 2020.
Stripe	Stripe, Inc.	Servizio di pagamento online per le imprese, che consente di accettare pagamenti con carta di credito e altri metodi di pagamento online. Offrono inoltre altri servizi finanziari come conti, finanziamenti e carte di pagamento.	Fatturato di circa 7,6 miliardi di dollari USA nel 2020.
Adyen	Adyen N.V.	Servizio di pagamento online per le imprese, che consente di accettare pagamenti con carta di credito e altri metodi di pagamento online. Offrono inoltre altri servizi finanziari come conti e carte di pagamento.	Fatturato di circa 2,3 miliardi di dollari USA nel 2020.
Apple Pay	Apple Inc.	Servizio di pagamento mobile che consente di effettuare pagamenti tramite l'iPhone, l'iPad e l'Apple Watch.	Fatturato di circa 1,8 miliardi di dollari USA nel 2020.
Google Pay	Alphabet Inc.	Servizio di pagamento mobile che consente di effettuare pagamenti tramite lo smartphone Android o il browser web.	Fatturato di circa 1,4 miliardi di dollari USA nel 2020.

Esistono diverse **tipologie di pagamenti digitali innovativi nel fintech**, tra cui i seguenti:

1. **Mobile Payments:** i pagamenti mobile consentono agli utenti di effettuare transazioni attraverso un'applicazione mobile. Questo tipo di pagamento è particolarmente utile per i pagamenti in negozi fisici o per inviare denaro ad amici e familiari. Alcuni esempi di app per pagamenti mobili sono PayPal, Venmo, Square Cash, Apple Pay e Google Pay.
2. **Pagamenti con wearable devices:** i dispositivi indossabili come smartwatch e braccialetti intelligenti possono essere utilizzati per effettuare pagamenti in modo semplice e veloce. Alcuni esempi di dispositivi indossabili che supportano i pagamenti includono Apple Watch, Samsung Galaxy Watch, Fitbit e Garmin.
3. **Pagamenti smart:** tutte quelle tipologie di pagamento che permettono all'utente di condividere, dividere o pagare in maniera dilazionata nel tempo.

Dal punto di vista del marketshare, i pagamenti digitali stanno rapidamente acquisendo una fetta sempre maggiore del mercato dei pagamenti globali. Secondo uno studio di Statista, nel 2021 la quota di mercato dei pagamenti digitali è stata del 36,8%, in aumento rispetto al 28,7% del 2019. Questo indica che i pagamenti digitali stanno diventando sempre più popolari tra i consumatori e le aziende.

In particolare, i pagamenti smart hanno acquisito una quota di mercato significativa negli ultimi anni.

Secondo uno studio di eMarketer, nel 2021 hanno rappresentato il 22,6% di tutte le transazioni effettuate negli Stati Uniti, in crescita rispetto al 17,5% del 2019.

Anche i **pagamenti digital commerce stanno guadagnando popolarità, in particolare grazie alla crescita del commercio elettronico**. I pagamenti digitali stanno diventando sempre più importanti per le aziende che operano nel settore del commercio elettronico ed inoltre i consumatori preferiscono sempre di più effettuare acquisti online con le diverse forme di digital payment.

Payment Gateway	Fatturato (2021)	E-commerce Integrati	Fonti
PayPal	\$25,3 miliardi	Magento, Shopify, WooCommerce, BigCommerce, Squarespace, Wix, ed altri.	https://www.evaluation.it/aziende/bilanci-aziende/paypal/
Stripe	\$12 miliardi	Shopify, WooCommerce, BigCommerce, Squarespace, Wix, ed altri.	https://www.theinformation.com/articles/stripes-revenue-growth-slid-last-year-as-firm-burned-through-cash
Adyen	€2,3 miliardi	Magento, Shopify, WooCommerce, BigCommerce, Squarespace, SAP, Salesforce, ed altri.	https://www.adyen.com/dam/jcr:043d4851-a77f-4cac-b872-1d4ef3de846c/Adyen-Annual-Report-2021.pdf

Inoltre, il mercato dei pagamenti sta vedendo l'entrata di colossi tecnologici come Google, Samsung, Apple e Amazon, sfruttando il loro network effect e la loro social scalability.

Per esempio, Apple sta entrando nel mondo bancario, in collaborazione con **Goldman Sachs**, mediante un **conto di deposito** ad alta resa che paga un rendimento annuo del **4,15%**. Si tratta di fatto di uno strumento, per ora disponibile soltanto negli Usa e per clienti residenti in territorio americano, molto simile ad un conto corrente, ma pensato più per il risparmio del denaro che non per il suo uso quotidiano. Disponibile insieme alla **Apple Card**, la carta di credito della big tech di Cupertino, il conto non richiede un deposito minimo ed è protetto dal Federal Deposit Insurance Corporation (**Fdic**).

Il mercato dei pagamenti digitali si sta, anno dopo anno, allargando con l'entrata di player tecnologi, creando delle nuove sfide per tutti gli enti finanziari tradizionali.

2.7

Informatica

● Basic

Come funziona un pagamento online su e-commerce?

Per **payment gateway** si intende un servizio che consente ai negozi online di accettare pagamenti tramite carte di credito e altre forme di pagamento elettronico. Un payment gateway si integra con il sito web del negozio online, permettendo ai clienti di effettuare pagamenti online in modo sicuro e affidabile.

Shopify è una piattaforma di e-commerce che consente agli esercizi commerciali di creare un sito web e di gestire le vendite online. Per consentire a tali esercizi di accettare pagamenti online, Shopify si integra con diversi payment gateway, oltre ad una proposizione diretta definita Shopify payments e realizzata a partire dall'infrastruttura di Stripe.

Dal punto di vista informatico, l'integrazione tra Shopify ed i payment gateway offerti sulla piattaforma avviene attraverso l'utilizzo di API (Application Programming Interface). Le API consentono alle due piattaforme di comunicare tra loro in modo sicuro e affidabile.

Quando un cliente effettua un pagamento sul sito web di un negozio Shopify, il pagamento viene gestito dal payment gateway definito dal commerciante in fase di configurazione del negozio. Il processo di pagamento può variare leggermente a seconda del tipo di carta di credito utilizzata e del paese di provenienza del cliente. In generale, il processo di pagamento avviene in questo modo:

- Il cliente inserisce i dati della carta di credito sul sito web del negozio Shopify.
- Shopify invia i dati della carta di credito al payment gateway tramite API.
- Il payment gateway verifica la validità dei dati della carta di credito e contatta la banca emittente della carta per autorizzare la transazione.
- Una volta autorizzata la transazione, il payment gateway comunica il risultato al sito web di Shopify tramite API.
- Il negozio Shopify conferma l'avvenuto pagamento al cliente.

L'intera transazione di pagamento avviene in pochi secondi e viene gestita attraverso l'utilizzo di protocolli di sicurezza come HTTPS e SSL.

2.8

Informatica

● Basic

Sistemi peer to peer vs sistemi non peer to peer nei processi di clearing e settlement

Le reti peer-to-peer, come Bitcoin e altri digital assets, offrono una serie di vantaggi rispetto alle reti private come SWIFT e Visa nel settore dei pagamenti retail e interbancari. In particolare, le reti peer-to-peer sono aperte, decentralizzate e cross-border, il che significa che possono essere utilizzate da chiunque in qualsiasi parte del mondo senza dover fare affidamento su intermediari centrali come le banche o le società di carte di credito.

Le reti peer-to-peer tendenzialmente offrono anche una maggiore sicurezza e protezione dei dati rispetto alle reti private. Ciò è dovuto alla loro architettura decentralizzata, che rende più difficile per i criminali informatici attaccare la rete e rubare informazioni sensibili.

Tuttavia, le reti peer-to-peer hanno anche alcune limitazioni rispetto alle reti private. In particolare, le transazioni peer-to-peer possono richiedere più tempo per essere confermate e possono essere soggette a fluttuazioni di valore. Inoltre, le reti peer-to-peer non offrono la stessa gamma di funzionalità avanzate che si trovano nelle reti private, come la possibilità di condividere dati tra banche e istituzioni finanziarie.

Di seguito è riportata una tabella che confronta i parametri di alcune reti peer-to-peer come Bitcoin e Tether con le reti private come Visa e SWIFT:

Parametro	Bitcoin	Tether	Visa	Swift
Decentralizzazione	Decentralizzata	Centralizzata	Centralizzata	Centralizzata
Apertura	Open source	Chiuso	Chiuso	Chiuso

Sicurezza	Crittografia robusta	Sicurezza dell'account bancario tradizionale	Sicurezza dell'account bancario tradizionale	Sicurezza dell'account bancario tradizionale
Velocità di transazione	Variabile	Velocità elevata	Velocità elevata	Velocità elevata
Costo di transazione	Variabile	Basso	Variabile	Variabile
Accettazione commerciale	Limitata ma in crescita	Diffusa	Diffusa	Diffusa

In alternativa alle reti pubbliche, altri attori hanno cercato di innovare il mercato dei pagamenti, attraverso la **creazioni di reti consorziali e private che utilizzano la blockchain come database condiviso**. Questi progetti sono stati spesso classificati come reti permissioned, ovvero con permessi. Infatti, differentemente da quelle pubbliche, la blockchain viene aggiornata non attraverso il consenso distribuito ma da un numero di attori prestabilito a priori. Tra le più utilizzate a livello globale possiamo menzionare:

- **Corda:** progettata dall'azienda R3, è utilizzata per ottimizzare alcuni processi finanziari che coinvolgono l'utilizzo di database differenti tra più individui. Uno dei casi di utilizzo in Italia di questa soluzione tecnologica è quello della SIACHain, promosso da SIA.
- **Hyperledger Fabric:** progettata dalla fondazione Linux, è una tra le principali reti private utilizzata per progetti chiusi ad un numero limitato di enti finanziari per condividere le stesse informazioni.
- **Private Ethereum:** progettata utilizzando la stessa architettura di Ethereum, ma con un modello di consenso ristretto per alcuni nodi, questa soluzione è stata adottata internamente da banche internazionali come JP Morgan per integrare servizi di tokenizzazione, pagamenti infragruppo e finanza decentralizzata.

Tendenzialmente, le reti peer-to-peer offrono una maggiore decentralizzazione, apertura, sicurezza e protezione dei dati rispetto alle reti private come Visa, Corda e SWIFT. Tuttavia, le reti peer-to-peer possono essere più lente e soggette a fluttuazioni di valore, e offrono meno funzionalità avanzate rispetto alle reti private.

3

Token di pagamento e stable coin

- 3.1 I token come strumenti per i pagamenti
- 3.2 Operazioni con un conto corrente e wallet a confronto
- 3.3 New bank, bonifici istantanei e secondo livello (LN) a confronto
- 3.4 Pagamenti online nel Web3
- 3.5 Pagamenti offline nel Web3
- 3.6 La programmabilità dei payment token
- 3.7 Il ruolo delle stable coin
- 3.8 Come si stabilizza il valore di una stable coin?
- 3.9 Che cos'è la proof of reserve? Il caso Tether
- 3.10 Che cosa si intende per depegging? Il caso Luna e Terra
- 3.11 Approfondimento: collaterale in valuta fiat e gli algoritmi di mercato aperto come riserva
- 3.12 Il ruolo dell'Open Banking nella interoperabilità
- 3.13 Gli investimenti nella fintech e la contaminazione con digital assets e AI

3.1

I token come strumenti per i pagamenti

Business / informatica

● Basic

Come abbiamo visto nei precedenti capitoli, il Web3 è un insieme di reti informatiche che utilizzano dei digital assets e dei token per creare un'economia di rete. Infatti, non sono solo i bitcoin ad essere utilizzati come mezzo di scambio ma anche altri digital assets. Un digital asset e/o un token può essere considerato un “payment token” se viene utilizzato principalmente come mezzo di pagamento per beni e servizi, anziché come riserva di valore o come strumento di investimento.

Per esempio, la Financial Market Supervisory Authority (FINMA) in Svizzera ha **definito che possiamo considerare un digital asset come “token di pagamento”** se la loro funzione principale è quella di essere utilizzati come mezzo di pagamento per beni o servizi, senza alcun legame diretto con un progetto o una società specifica.

Quindi, un digital asset come Bitcoin può essere considerato un “payment token” o “token di pagamento” se la sua funzione principale è quella di essere utilizzato come mezzo di pagamento e la sua emissione e distribuzione non è direttamente controllata da un'entità centrale o da un progetto specifico.

Digital Asset	Velocità di Transazione	Costo di Transazione	Privacy	Stabilità del Prezzo	Scalabilità	Accettazione Commerciale
BTC	Media-bassa (circa 7 transazioni al secondo)	Variabile, può essere elevato in periodi di congestione della rete	Alcune funzionalità di privacy, ma non completamente anonimo	Volatile	Limitata, il protocollo di BTC può elaborare solo un certo numero di transazioni al secondo	Accettazione commerciale in aumento, ma ancora limitata in molti paesi
BCH	Media-alta (circa 116 transazioni al secondo)	Solitamente basso, ma può aumentare in periodi di congestione della rete	Alcune funzionalità di privacy, ma non completamente anonimo	Volatile	Maggiore rispetto a BTC, ma ancora limitata in confronto a soluzioni di pagamento tradizionali	Accettazione commerciale in aumento, ma ancora limitata in molti paesi
USDT	Variabile a seconda della blockchain. Se ad esempio USDT è trasferito su blockchain Ethereum rispetterà le tempistiche di elaborazione della stessa. Stesso si dica per le altre blockchain	Solitamente basso	Pienamente trasparente, ma non anonimo	Stabile (anch'essa è una stablecoin)	Limitata, ma in costante sviluppo	Accettato in un'ampia gamma di settori, tra cui digital assets, finanza e giochi online

ZEC	Media-bassa (circa 6 transazioni al secondo)	Variabile, può essere elevato in periodi di congestione della rete	Particolare attenzione alla protezione dei dati degli utenti	Volatile	Limitata, ma in costante sviluppo	Accettazione commerciale ancora limitata in confronto a BTC ed altri digital assets popolari
XMR	Media-bassa (circa 15 transazioni al secondo)	Variabile, può essere elevato in periodi di congestione della rete	Particolare attenzione alla protezione dei dati degli utenti	Volatile	Limitata, ma in costante sviluppo	Accettazione commerciale ancora limitata in confronto a BTC ed altri digital assets popolari

Tra i più famosi digital asset utilizzati come mezzo di pagamento ci sono Litecoin, Tether, Bitcoin Gold e Z-Cash e Monero. Nel corso di questo capitolo, andremo ad approfondire quella gamma di payment token che vengono definiti come stable coin: digital asset il cui valore è ancorato ad un sottostante, con l'obiettivo di garantire maggiore stabilità rispetto ai token ed ai digital assets il cui valore è determinato dalle dinamiche di mercato.

3.2

Business
Basic

Operazioni con un conto corrente e wallet a confronto

L'online banking, noto anche come internet banking, web banking o home banking, è un sistema che consente ai clienti di una banca o di un altro istituto finanziario di effettuare una serie di transazioni finanziarie tramite il sito Web o l'app mobile dell'istituto finanziario.

Qui elencate le attività che solitamente sono all'interno di questo servizio digitale:

- **Visualizzazione del saldo e dell'estratto conto**
- **Gestione delle transazioni (bonifici, pagamenti, ricariche, domiciliazioni)**
- **Possibilità di creare e gestire ordini permanenti**
- **Consultazione di tutte le operazioni effettuate**
- **Stampa e salvataggio dell'estratto conto**
- **Possibilità di richiedere carte di credito o prepagate**
- **Gestione dei dati personali e delle preferenze di comunicazione**
- **Assistenza online tramite chat o e-mail**
- **Possibilità di richiedere finanziamenti o mutui**
- **Accesso ai servizi di trading online (se disponibili)**
- **Gestione dei conti deposito e dei fondi d'investimento (se disponibili)**
- **Possibilità di attivare e disattivare funzionalità come i pagamenti contactless o la notifica push.**

Come abbiamo ampiamente descritto in precedenza, per poter operare all'interno del Web3, un utente ha bisogno di scaricare un wallet all'interno del proprio dispositivo. Un wallet può essere equiparato ad un conto corrente per poter operare all'interno delle reti, ricevendo ed inviando i propri digital assets, grazie alle chiavi crittografiche in esso contenute.

Qui di seguito le principali operazioni possibili offerte dai wallet nel mercato dei digital assets:

- **Generazione di indirizzi:** i wallet generano indirizzi univoci per ricevere e inviare digital assets.
- **Saldo:** i wallet visualizzano il saldo attuale dei digital assets in possesso dell'utente.
- **Ricezione:** i wallet consentono agli utenti di ricevere digital assets da altri utenti.
- **Invio:** i wallet consentono agli utenti di inviare digital assets ad altri utenti.
- **Storico delle transazioni:** i wallet tengono traccia delle transazioni effettuate dall'utente.
- **Sicurezza:** i wallet offrono misure di sicurezza come l'autenticazione a due fattori, la crittografia delle chiavi private e la possibilità di impostare password personalizzate.
- **Backup:** i wallet consentono di eseguire il backup delle chiavi private per evitare la perdita di digital assets in caso di smarrimento del dispositivo.
- **Integrabilità:** i wallet possono essere integrati con altre applicazioni e servizi per semplificare l'utilizzo dei digital assets.
- **Conversione valuta:** alcuni wallet offrono la possibilità di convertire i digital assets in altre valute tradizionali o digital assets diversi.
- **Gestione multi-account:** alcuni wallet consentono di gestire più account per diversi digital assets all'interno della stessa applicazione.

Un tra le principali sfide del settore bancario tradizionale sarà quello di integrare all'interno dei loro servizi la possibilità di utilizzare i propri digital assets come strumenti di pagamento.

3.3

Business

• Basic

Newbank, bonifici istantanei e secondo livello (LN) a confronto

Con l'arrivo delle new bank nel mercato, come Revolut o N26, si è introdotto il servizio di bonifici gratuiti ed istantanei. Queste banche non hanno filiali fisiche e operano principalmente online, **il che ha creato maggiore competizione tra gli istituti bancari, rivoluzionando la trasmissione del denaro nel mercato retail**. Ad esempio, Revolut utilizza una rete privata per elaborare i pagamenti in tempo reale tra i propri utenti, eliminando la necessità di intermediazione. N26, invece, ha stretto partnership con altri fornitori di servizi finanziari per offrire bonifici gratuiti ai propri clienti.

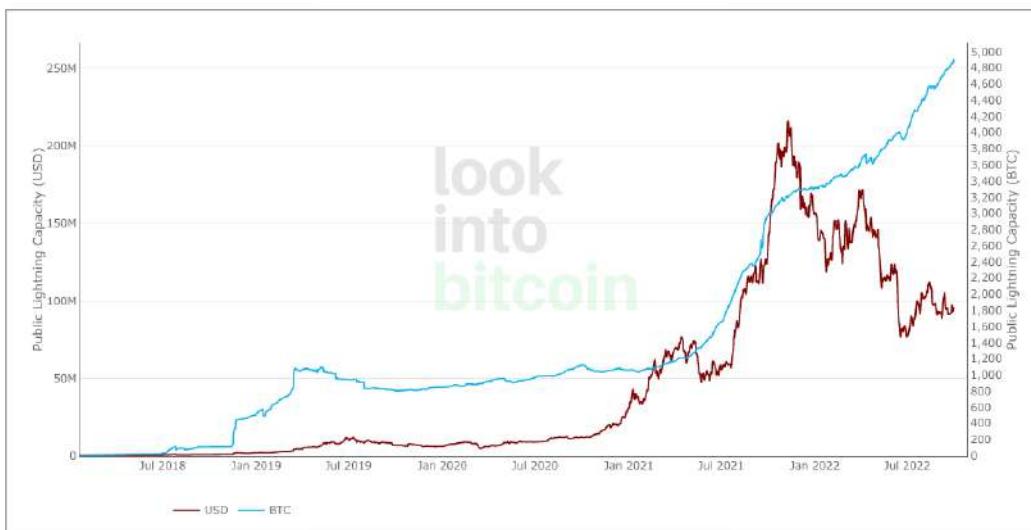
Inoltre, le newbank spesso offrono anche **altre funzionalità innovative** come l'apertura di conti correnti in pochi minuti, l'accesso a valute estere a tassi di cambio vantaggiosi e l'uso di carte di credito virtuali per transazioni online sicure.

Questo ha spinto le realtà finanziarie tradizionali ad innovarsi, per rimanere al passo con l'innovazione e i servizi sul mercato. Per esempio, i bonifici istantanei in Europa sono gestiti attraverso il sistema di pagamenti SEPA Instant Credit Transfer (SCT Inst), che è stato sviluppato dalla European Payments Council (EPC) **per consentire trasferimenti di denaro in tempo reale tra i paesi dell'area SEPA (Single Euro Payments Area)**.

Il processo di esecuzione di **un bonifico istantaneo avviene attraverso la connessione tra le banche del mittente e del destinatario**, che devono essere entrambe aderenti al sistema SCT Inst. Il mittente deve fornire i dati del destinatario, inclusi il suo IBAN (International Bank Account Number) e il BIC (Bank Identifier Code), nonché l'importo da trasferire.

Bitcoin Lightning Capacity

Source: lookintobitcoin.com



Nel web3, **le soluzioni per rimanere competitivi con il mercato dei pagamenti tradizionale, sempre più veloce e senza costi, vengono definite come reti/protocolli di secondo livello**, ovvero meccanismi matematici e crittografici che permettono a due utenti di scambiarsi payment tokens o digital assets, in maniera istantanea a senza costi. Per esempio, nel caso di Bitcoin, la soluzione di secondo livello si chiama Lightning Network (LN). Dal 2020 in avanti c'è stato un'enorme crescita del suo utilizzo, infatti, molti nodi hanno creato un proprio wallet LN per poter trasferire parte della loro liquidità in questo secondo livello del protocollo.

Bitcoin: Lightning Network Number of Channels

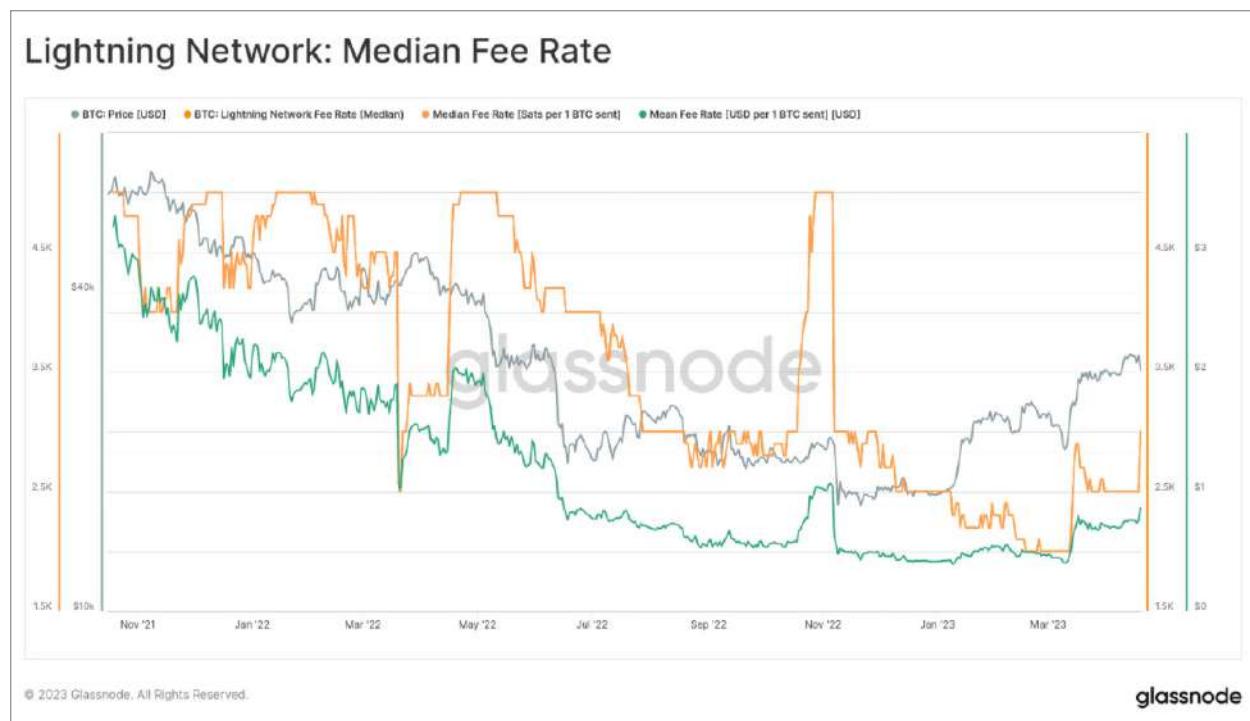


© 2021 Glassnode. All Rights Reserved.

glassnode

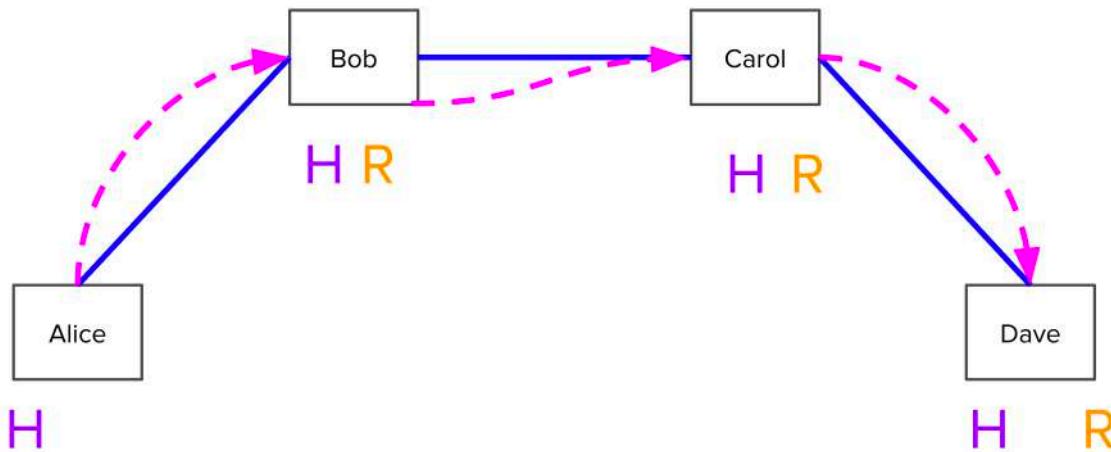
Questa soluzione permette a due o più individui di creare un **canale di pagamento** privato in cui potersi scambiare bitcoin, in maniera istantanea e con costi negli ordini di centesimi di centesimi. In alto possiamo osservare la continua crescita del numero dei canali di pagamento nella rete, dimostrando una buona crescita nell'adozione. Questa crescita potrebbe essere stata spinta dalla netta riduzione dei costi per i pagamenti: grazie ai canali di pagamento, le transazioni salvate sulla blockchain tra due individui, sono solamente due:

- La **prima transazione** verso i canali e i wallet in cui voglio operare sul secondo livello.
- L'**ultima transazione** dai canali verso un wallet che opera sul primo livello.



In questo modo, anche il carico delle transazioni sulla blockchain è ridotto, migliorando la scalabilità del sistema. Ma come potrebbe sfruttare una banca questo secondo livello? **Uno dei possibili servizi che potrebbe offrire è quello di diventare un payment hub.**

Un payment hub nel Lightning Network è un nodo che ha molti canali aperti con altri nodi. Questo significa che molte persone possono inviare pagamenti attraverso questo nodo, senza dover necessariamente aprire un nuovo canale. **La banca diventa un nodo intermedio privilegiato, definito come hops, che aiuta le connessioni tra individui nella rete.**



Gli hops nel Lightning Network di Bitcoin si riferiscono **al numero di nodi intermedi che un pagamento deve attraversare per raggiungere la sua destinazione finale**. Infatti, se il destinatario finale non ha un canale aperto con il mittente, il pagamento dovrà essere instradato attraverso uno o più nodi intermedi, chiamati "hops". Ogni hop rappresenta un passaggio attraverso un canale aperto tra due nodi diversi. Più hops ci sono, maggiore è la complessità e il tempo necessario per completare il pagamento.

In sostanza, un payment hub è come **una grande stazione di rifornimento per i pagamenti nel network, che rende più facile e veloce il trasferimento di denaro tra gli utenti**. Per concludere, le reti di secondo livello rendono competitivi i servizi di pagamento web3, rispetto ai tradizionali, aprendo la strada a nuovi servizi e applicazioni per il mercato dei pagamenti.

3.4

Business

Basic

Pagamenti online nel Web3

Così come offline, anche online, molti digital commerce hanno dato la possibilità ai propri clienti di pagare con i propri digital assets servizi e prodotti.

I principali gateway di pagamento online per i retail con digital assets includono:

- **Coinbase Commerce:** questo servizio di pagamento permette ai commercianti di accettare pagamenti in digital assets come Bitcoin, Bitcoin Cash, Ethereum e Litecoin. I pagamenti possono essere effettuati tramite QR code o indirizzo wallet.
- **BitPay:** questo gateway di pagamento supporta Bitcoin, Bitcoin Cash e Ethereum e permette ai commercianti di accettare pagamenti tramite questi digital assets. BitPay converte automaticamente i pagamenti in valuta fiat per il commerciante.
- **CoinPayments:** questo servizio di pagamento supporta oltre 1.800 digital assets, tra cui Bitcoin, Ethereum e Litecoin e permette ai commercianti di accettare pagamenti in digital assets e di ricevere automaticamente i pagamenti in valuta fiat.
- **GoCoin:** questo gateway di pagamento supporta Bitcoin, Litecoin e Ethereum e permette ai commercianti di accettare pagamenti in questi digital assets, convertendo automaticamente i pagamenti in valuta fiat per il commerciante.
- **Kraken:** questo exchange di digital assets offre un servizio di pagamento che permette ai commercianti di accettare pagamenti in Bitcoin, Bitcoin Cash, Ethereum e USDT, sempre offrendo la possibilità di convertire automaticamente i pagamenti in valuta fiat per il commerciante.
- **CoinGate:** questo gateway di pagamento supporta oltre 50 digital assets, tra cui Bitcoin, Ethereum e Litecoin e permette ai commercianti di accettare pagamenti in digital assets e di ricevere automaticamente i pagamenti in valuta fiat.

Shopify è un altro importante gateway di pagamento che ha aggiunto la possibilità di accettare pagamenti in digital assets. La piattaforma supporta diversi digital assets, tra cui Bitcoin, Bitcoin Cash, Ethereum, Litecoin e USDC, grazie alla partnership con CoinPayments.

Ecco i passaggi che un ecommerce effettua per accettare un digital asset:

- Per accettare pagamenti in digital assets con Shopify, i commercianti devono configurare l'opzione di pagamento tramite CoinPayments. Questo implica la creazione di un account CoinPayments e l'aggiunta di un token di pagamento all'interno dell'account Shopify.
- Una volta configurato il pagamento in digital assets, i clienti possono selezionare l'opzione di pagamento tramite essi durante il processo di checkout. Verrà quindi mostrato un QR code contenente l'indirizzo del portafoglio digitale del commerciante, insieme alla quantità di digital assets richiesta per l'acquisto. Il cliente deve quindi inviare la transazione al portafoglio del commerciante utilizzando un portafoglio digitale compatibile con il digital asset utilizzato.
- Shopify converte automaticamente i pagamenti in digital assets in valuta fiat per il commerciante. I fondi vengono poi depositati sul conto bancario del commerciante come qualsiasi altra transazione di pagamento.

Per effettuare pagamenti in maniera completamente peer-to-peer, senza l'uso di intermediari o gateway di pagamento, un e-commerce può semplicemente esporre la propria chiave pubblica per ricevere pagamenti diretti dai clienti. In questo modo, i clienti possono utilizzare un portafoglio digitale che supporta il digital asset del commerciante e inviare la transazione direttamente all'indirizzo del portafoglio del commerciante.

3.5

Business

● Basic

Pagamenti offline nel Web3

Come online, così come offline, è possibile utilizzare i propri digital assets per comprare beni e servizi, esistono infatti delle carte di credito che permettono all'utente di pagare un negozio fisico con i digital assets.

Queste carte funzionano attraverso una **piattaforma di pagamento che converte il digital asset posseduto dal titolare in valuta tradizionale e poi la utilizza per effettuare il pagamento**.

Inoltre, ci sono anche i **POS virtuali per digital assets, che sono dispositivi hardware o software che consentono ai commercianti di accettare pagamenti in digital assets senza dover possedere una conoscenza tecnica approfondita**. Questi dispositivi utilizzano un **meccanismo di instant exchange** per convertire i digital assets ricevuti in valuta tradizionale, rendendo il processo di pagamento più fluido. Dal punto di vista tecnico, i servizi di carte di credito e POS virtuali per digital assets funzionano attraverso un sistema di conversione istantanea (instant exchange) in cui la piattaforma di pagamento scambia il digital asset posseduto dal titolare con la valuta tradizionale richiesta dal commerciante.

Un servizio di instant exchange che converte digital assets in valute fiat e invia i fondi al commerciante su canali Visa e Mastercard si basa su un'infrastruttura tecnologica complessa e sicura che coinvolge diversi attori e processi.

Il **servizio di instant exchange deve essere integrato con una serie di exchange di digital assets e piattaforme di pagamento fiat**, al fine di accedere a un'ampia gamma di valute digitali e fiat. Questi exchange e piattaforme possono essere connessi attraverso API (Application Programming Interface) che consentono l'accesso e lo scambio di informazioni in modo sicuro e affidabile.

Il procedimento di pagamento può seguire questi passaggi:

- Una volta che un commerciante desidera accettare pagamenti in digital assets, deve registrarsi con il servizio di instant exchange e fornire le informazioni necessarie per ricevere i pagamenti. Il servizio di instant exchange provvederà a generare un indirizzo di pagamento univoco per il commerciante, che gli verrà comunicato e che potrà essere utilizzato dai clienti per inviare digital assets per i loro acquisti.
- Quando un cliente effettua un acquisto utilizzando digital assets, il servizio di instant exchange verifica la transazione e converte immediatamente l'asset digitale in una valuta fiat, come dollari americani o euro. Questo avviene attraverso una serie di scambi e conversioni tra diversi digital assets e valute fiat, che sono gestiti in modo automatico e istantaneo dal servizio di instant exchange.
- Una volta che la conversione è completata, il servizio di instant exchange invia i fondi al commerciante utilizzando i canali Visa o Mastercard. Questo avviene attraverso un sistema di pagamento che è integrato con i network di carte di credito e che consente di inviare fondi in modo sicuro e immediato al commerciante.

Il numero transazioni per beni e servizi è ancora molto ridotto rispetto alle transazioni relative a scambi finanziari; tuttavia, la maggiore facilità d'uso e una migliore *user-experience* aiuterà l'adozione di questi nuovi modi di pagare con digital assets.

3.6

Informatica
● Basic

La programmabilità dei payment token

All'interno del mercato fintech, se dovessimo mappare tutte le tipologie di applicazioni potremmo riasumerle all'interno di questa tabella:

Tipo di Servizio	Descrizione
App di Gestione Finanziaria	<i>App per la gestione del budget, delle spese e del risparmio</i>
Pagamenti Digitali	<i>Piattaforme per l'elaborazione di pagamenti online, mobile e peer-to-peer, split payment, conti aziendali e condivisi</i>
Prestiti e microprestiti Online	<i>Servizi di prestito online che utilizzano algoritmi per valutare la solvibilità creditizia e concedono pagamenti in anticipo di beni e servizi con servizi come Buy Now - Pay Later</i>
Consulenza Finanziaria Online	<i>Servizi di consulenza finanziaria online che utilizzano l'AI e l'apprendimento automatico per offrire consigli personalizzati agli utenti</i>
Servizi di Crowdfunding	<i>Piattaforme online per il finanziamento collaborativo di progetti o imprese</i>
Assicurazioni Digitali	<i>Servizi di assicurazione online che utilizzano l'AI per valutare i rischi e offrire polizze personalizzate</i>
Soluzioni di Sicurezza Finanziaria	<i>Servizi che utilizzano tecnologie di sicurezza come la biometria e l'AI per proteggere le transazioni finanziarie degli utenti</i>
Servizi di Finanza Commerciale	<i>Piattaforme online per la gestione di transazioni commerciali e finanziarie tra aziende</i>

La **programmabilità dei pagamenti si intende l'utilizzo di token e contratti intelligenti per automatizzare i pagamenti, creare delle logiche interne riproponendo modelli off-chain o aggiungendo nuove modalità esclusivamente on-chain**. Questa innovazione potrebbe aprire nuove categorie di servizi all'interno del settore Fintech.

Qui elencate una serie di funzionalità che potrebbero essere offerte da una azienda Fintech nel web3:

- **Granular Payment:** si tratta di una forma di pagamento che permette di suddividere una somma in piccoli importi per effettuare pagamenti parziali in base alle condizioni contrattuali previste. Ad esempio, un contratto di granular payment potrebbe prevedere di pagare un fornitore in base alla quantità di prodotto consegnato e accettato dal cliente.
- **Split Payment:** in questo caso, il pagamento viene suddiviso tra due o più destinatari in proporzione a quanto previsto dal contratto. Ad esempio, un contratto di split payment potrebbe prevedere che il pagamento per un prodotto venga suddiviso tra il produttore, il distributore e il rivenditore in base a una percentuale prestabilita.
- **Decentralized Escrow:** si tratta di una forma di pagamento che prevede un intermediario che trattiene i fondi in modo sicuro fino a quando non viene soddisfatta una determinata condizione contrattuale. Ad esempio, in un contratto di decentralized escrow, i fondi potrebbero essere trattenuti fino a quando il prodotto non viene consegnato al cliente.
- **Payment to Delivery:** in questo caso, il pagamento viene effettuato solo dopo la conferma della corretta ricezione del prodotto o del servizio da parte del cliente. Ad esempio, in un contratto di payment to delivery, il pagamento potrebbe essere effettuato solo dopo che il cliente ha confermato di aver ricevuto il prodotto in buone condizioni.

- **Stable Coin:** la programmabilità viene utilizzata nelle stablecoin per implementare meccanismi di stabilizzazione dei prezzi, che consentono di mantenere il valore della stablecoin ancorato ad un asset sottostante (ad esempio, il dollaro americano) o ad un indice di mercato. Per fare ciò, vengono utilizzati smart contract che regolano l'emissione e la gestione delle stablecoin, prevedendo ad esempio la creazione o il riscatto di monete in base alla domanda e all'offerta sul mercato. Questi smart contract possono anche prevedere la ridistribuzione degli eventuali interessi o dividendi generati dall'asset sottostante, allo scopo di mantenere il valore della stablecoin il più possibile stabile e prevedibile per gli utenti.
- **Burn coin:** in questo caso, quando una transazione viene fatta verso un certo indirizzo la quantità totale dei token a disposizione diminuisce della quantità introdotta nella transazione.

La **programmabilità dei pagamenti retail con gli smart contract consente quindi di creare contratti automatizzati che semplificano e velocizzano le transazioni commerciali**, eliminando gli intermediari e riducendo i rischi associati alle transazioni. Inoltre, questi contratti possono essere **personalizzati per soddisfare le specifiche esigenze delle parti coinvolte**, garantendo maggiore trasparenza e affidabilità nel processo di pagamento.

3.7

Informatica / Business

● Basic

Il ruolo delle stable coin

Le **stablecoin sono diventate uno strumento sempre più importante nell'ecosistema dei digital assets, poiché offrono una soluzione al problema della volatilità dei prezzi dei digital assets stessi**. Ecco alcuni dei principali utilizzi delle stablecoin nel mercato:

- **Scambio tra digital assets:** le stablecoin sono spesso utilizzate come base per lo scambio tra digital assets, poiché consentono di evitare le fluttuazioni dei prezzi delle valute digitali. Ad esempio, è possibile acquistare Bitcoin o Ether utilizzando una stablecoin come Tether o USD Coin.
- **Finanza decentralizzata (DeFi):** le stablecoin sono uno strumento fondamentale per la finanza decentralizzata (DeFi), in particolare, vengono utilizzate come collaterale per l'accesso a prestiti in digital assets e come valuta di riferimento per i protocolli di scambio decentralizzati (DEX).
- **Hedging:** le stablecoin possono essere utilizzate anche come meccanismo di hedging, poiché consentono di proteggere il proprio portafoglio dalle fluttuazioni dei prezzi dei digital assets. Ad esempio, un trader può acquistare una stablecoin quando prevede una discesa dei prezzi dei digital assets, in modo da poter poi acquistarli nuovamente a prezzi più bassi.
- **Pagamenti:** le stablecoin possono essere utilizzate come mezzo di pagamento in digital assets, poiché consentono di effettuare transazioni a basso costo e in tempi rapidi. Alcune stablecoin, come USDC e BUSD, sono state approvate per l'uso commerciale negli Stati Uniti e sono supportate da un crescente numero di esercizi commerciali.

Ecco una lista delle principali stablecoin sul mercato, con alcuni dati relativi alle loro attività on-chain:

1. Tether (USDT)

- Blockchain: Ethereum, Solana, Tron, Binance Smart Chain, Algorand, OMG Network, Liquid Network, Bitcoin Cash, EOS
- Numero di transazioni giornaliere (media 7 giorni): circa 3,5 milioni
- Volume giornaliero (media 7 giorni): oltre 100 miliardi di dollari
- Numero di wallet attivi: circa 10 milioni

2. USD Coin (USDC)

- Blockchain: Ethereum, Algorand, Solana, Stellar, Hedera Hashgraph, Tron, Avalanche, Binance Smart Chain
- Numero di transazioni giornaliere (media 7 giorni): circa 1,3 milioni
- Volume giornaliero (media 7 giorni): circa 4 miliardi di dollari
- Numero di wallet attivi: oltre 7 milioni

3. Binance USD (BUSD)

- Blockchain: Ethereum, Binance Smart Chain
- Numero di transazioni giornaliere (media 7 giorni): circa 500.000
- Volume giornaliero (media 7 giorni): oltre 2 miliardi di dollari
- Numero di wallet attivi: non disponibile

4. Dai (DAI)

- Blockchain: Ethereum
- Numero di transazioni giornaliere (media 7 giorni): circa 35.000
- Volume giornaliero (media 7 giorni): circa 100 milioni di dollari
- Numero di wallet attivi: oltre 2,7 milioni

5. TrueUSD (TUSD)

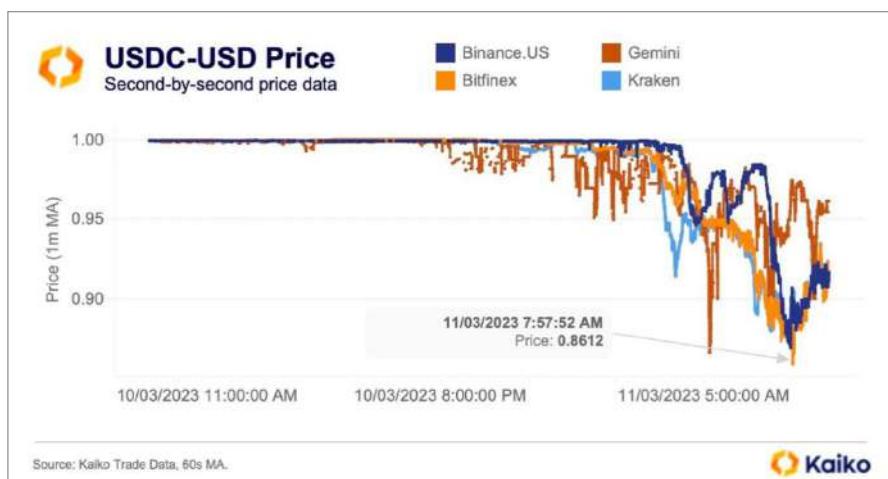
- Blockchain: Ethereum, Binance Smart Chain, Avalanche
- Numero di transazioni giornaliere (media 7 giorni): circa 10.000
- Volume giornaliero (media 7 giorni): circa 40 milioni di dollari
- Numero di wallet attivi: circa 200.000

6. Paxos Standard (PAX)

- Blockchain: Ethereum, Binance Smart Chain, Ontology, Algorand
- Numero di transazioni giornaliere (media 7 giorni): circa 3.000
- Volume giornaliero (media 7 giorni): circa 15 milioni di dollari
- Numero di wallet attivi: non disponibile

I dati riportati potrebbero variare nel tempo in base alle attività degli utenti e alle oscillazioni dei mercati. Nonostante ciò, la **stabilità delle stablecoin non è sempre garantita**, proprio per via di eventi esterni che influenzano il loro andamento. Recentemente, con i problemi legati al caso della **Silicon Valley Bank**, si è assistito al crollo della stablecoin USDC di Coinbase e Circle. In questo caso specifico, nonostante la stablecoin fosse peggiorata al dollaro, i legami tra SVB e Circle hanno creato un senso di sfiducia tale da portare molti investitori a vendere USDC, causando un repentino crollo di valore.

A seguito un grafico che può far comprendere bene la volatilità di USDC a seguito del rilascio delle prime informazioni legate alla crisi di SVB:



In conclusione, però è importante ricordare come anche le singole valute nazionali, nonostante la loro stabilità, in periodi di crisi hanno subito importanti variazioni in termini di tasso di cambio, che hanno comportato problemi in termini di potere d'acquisto.

3.8

Informatica/Finanza

● Medium

Come si stabilizza il valore di una stable coin?

La relazione tra unit of account e stablecoin è di grande interesse per il mondo finanziario in quanto le **stablecoin, essendo digital asset progettate per mantenere un valore stabile, possono fungere da unità di conto alternativa alle valute ufficiali.**

Il **concepto di pegging**, ovvero il collegamento del valore di una stablecoin ad un asset sottostante, rappresenta un **elemento essenziale per garantire la stabilità del valore** della stablecoin stessa. Questo collegamento può essere realizzato attraverso l'utilizzo di meccanismi di stabilizzazione dei prezzi, come ad esempio l'emissione e il riscatto di stablecoin in base alla domanda e all'offerta sul mercato. L'utilizzo delle **stablecoin come unità di conto** alternativa alle valute ufficiali può offrire numerosi vantaggi ai consumatori e alle aziende. Ad esempio, le stablecoin possono offrire un valore stabile e prevedibile, eliminando l'incertezza associata alle fluttuazioni dei tassi di cambio delle valute ufficiali. Inoltre, le stablecoin possono facilitare le transazioni internazionali, eliminando la necessità di convertire continuamente le valute in un mercato in cui si utilizzano valute diverse.

Categoria di Pegging	Meccanismo di Stabilizzazione	Esempi di Stablecoin	Esempi di Aziende di Mercato
Fiat-Collateralized	<i>1:1 backing con valuta fiduciaria</i>	USDT, USDC, TUSD	Tether, Circle, TrueUSD
Digital asset -Collateralized	<i>Backing con altri digital assets</i>	DAI, BitUSD	MakerDAO, BitShares
Algorithmic	<i>Algoritmi di controllo dell'offerta</i>	Basis, Ampleforth	Basis Protocol, Ampleforth
Commodity-Collateralized	<i>Backing con materie prime</i>	Digix Gold Token (DGT), Tiberius Coin	Digix, Tiberius Coin

Il **funzionamento della stabilità delle stable coin dipende dal sistema di peg**, ovvero la meccanica che tiene il valore del digital asset legato a quello di un'altra valuta (ad esempio, il dollaro statunitense). Ci sono diversi modi per implementare questo sistema, come ad esempio depositi di garanzia, algoritmi di mercato aperto o entrambi.

- **Depositi di garanzia fissi:** in questo meccanismo, la quantità di stable coin emessa è fissata e la sua emissione non viene regolamentata da alcun algoritmo. Il prezzo della stable coin viene mantenuto a un valore di peg specifico tramite depositi di garanzia fissi, che coprono il valore nominale della stable coin.
- **Contratti intelligenti di regolazione della domanda e dell'offerta:** in questo meccanismo, il prezzo di una stable coin viene regolato tramite un contratto intelligente che modifica la domanda e l'offerta. Ad esempio, se il prezzo di una stable coin si alza rispetto al suo valore di peg, il contratto intelligente aumenta l'offerta di stable coin sul mercato, riducendo così il prezzo. In caso contrario, il contratto riduce l'offerta di stable coin, aumentando il prezzo.
- **Digital asset-collateralizzazione:** questo meccanismo utilizza un altro digital asset come garanzia per stabilizzare il prezzo di una stable coin. Ad esempio, una stable coin potrebbe essere collateralizzata da Ethereum (ETH). In questo caso, la quantità di ETH mantenuta come garanzia deve essere sufficiente a coprire il valore nominale della stable coin. Se il prezzo della stable coin dovesse deviare dal suo valore di peg, il contratto intelligente agirebbe per regolare la quantità di ETH mantenuta come garanzia.
- **Stabilizzazione automatica:** in questo meccanismo, il prezzo di una stable coin viene regolato automaticamente dal sistema senza l'intervento umano. Ad esempio, potrebbe essere utilizzato un algoritmo di apprendimento automatico che analizza i dati di mercato per determinare se il prezzo della stable coin sta deviando dal suo valore di peg, e agisce di conseguenza per regolarlo.

- **Stabilizzazione tramite pool di garanzie:** in questo meccanismo, il prezzo di una stable coin viene mantenuto a un valore di peg specifico tramite un pool di garanzie, che può includere digital assets, monete fiat o altre risorse. Il pool di garanzie viene gestito da una serie di regole che stabiliscono come la quantità di garanzie deve essere modificata per mantenere il prezzo della stable coin ad un livello specifico.
- **Stabilizzazione tramite prezzatura oracle:** in questo meccanismo, il prezzo di una stable coin viene regolato tramite l'utilizzo di un oracolo che fornisce informazioni sul prezzo di mercato. L'oracolo viene utilizzato per determinare se il prezzo della stable coin sta deviando dal suo valore di peg, e agisce di conseguenza per regolarlo. (synthetic asset)
- **Stabilizzazione tramite pool di prestiti decentralizzati:** in questo meccanismo, il prezzo di una stable coin viene mantenuto a un valore di peg specifico tramite un pool di prestiti decentralizzati, che forniscono liquidità quando il prezzo della stable coin sta deviando dal suo valore di peg. Questi prestiti sono gestiti da un contratto intelligente che regola la quantità di liquidità fornita per mantenere il prezzo della stable coin a un livello specifico.

3.9

Legal

• Medium

Che cos'è la proof of reserve? Il caso Tether

La **Proof of Reserve** è una prova che viene spesso utilizzata nelle stablecoin, come Tether (USDT), per dimostrare che le riserve di digital assets sottostanti alla stablecoin corrispondono effettivamente al numero di token in circolazione, generalmente effettuata da audit terzi. Tether è una delle stablecoin più popolari ed è emessa dalla società Tether Limited.

Per dimostrare la Proof of Reserve, **Tether ha adottato una serie di misure, tra cui la pubblicazione delle proprie riserve di digital assets.** Tether fornisce un aggiornamento quotidiano sulle riserve che sostengono i token in circolazione. Inoltre, la società ha stipulato contratti di servizio con alcune banche e istituti finanziari che le consentono di avere accesso ai prestiti in dollari USA per garantire la stabilità della valuta.

Tether ha inoltre adottato un **sistema di convalida crittografica delle riserve utilizzando la blockchain.** Le transazioni effettuate con Tether possono essere verificate attraverso la blockchain per garantire che la stablecoin sia effettivamente supportata dalle riserve di digital assets sottostanti.

Tuttavia, Tether ha subito alcune critiche riguardo alla trasparenza delle sue riserve, poiché la **società non ha mai pubblicato una verifica esterna indipendente delle riserve.** Inoltre, ci sono state preoccupazioni sulla natura delle riserve sottostanti, poiché Tether ha utilizzato anche altre forme di garanzia oltre ai digital assets, come ad esempio i prestiti in dollari USA.

La Proof of Reserve rappresenta quindi un modo per dimostrare le riserve di stablecoin, dimostrando la presenza di digital assets sottostanti volti a garantirne la stabilità. Tuttavia, è importante che le aziende che emettono stablecoin dimostrino una piena trasparenza delle loro riserve attraverso audit indipendenti e altre misure di verifica per garantire la sicurezza e la fiducia degli utenti.

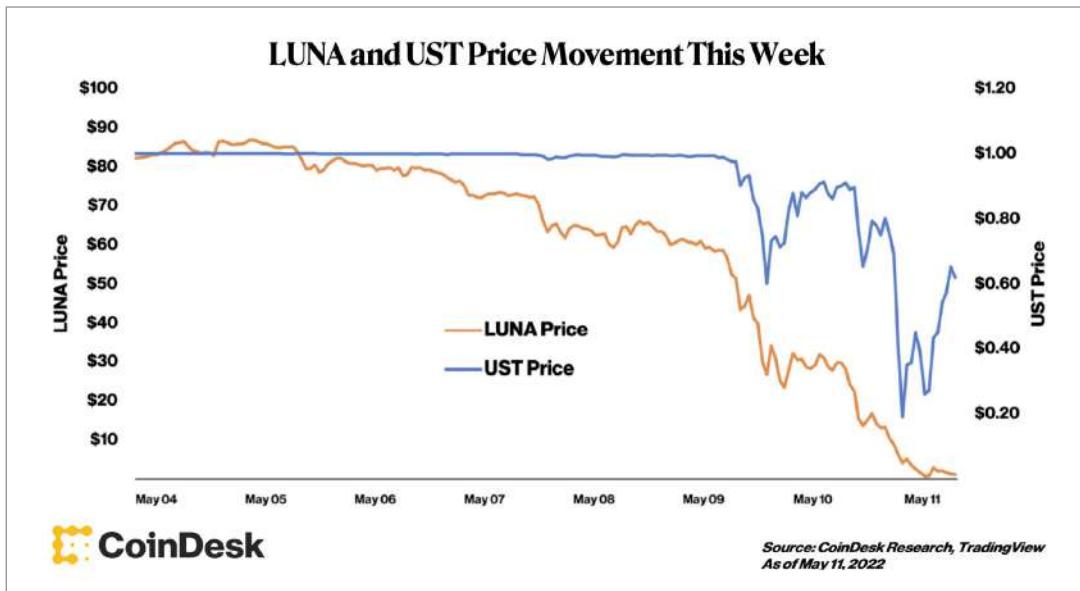
3.10

Informatica

• Hard

Che cosa si intende per depegging? Il caso Luna e Terra

Il **caso di Luna e Terra** è un esempio interessante di come una **stablecoin possa subire un crollo**. Luna e Terra erano stablecoin ancorate al valore dell'oro e degli altri digital assets. La loro **stabilità era garantita da un pool di garanzie** che comprendeva entrambe le valute ancorate.



Come abbiamo citato in precedenza, l'algoritmo di mercato aperto è uno dei meccanismi più comuni utilizzati per stabilizzare le stablecoin. Il suo funzionamento si basa sulla creazione di un pool di garanzie che viene utilizzato per acquistare o vendere la stablecoin al fine di mantenere il peg. In termini di codice, la stabilità di Luna e Terra era garantita da algoritmi di mercato aperto che utilizzavano depositi di garanzia per mantenere il peg. Tuttavia, **a causa della volatilità del mercato e della mancanza di liquidità, questi algoritmi non sono stati in grado di mantenere la stabilità della stablecoin**.

Inoltre, la **mancanza di liquidità nei mercati di Luna e Terra ha reso difficile per l'algoritmo di mercato aperto acquistare o vendere la stablecoin per mantenere il peg**. Questo ha portato ad una carenza di offerta o di domanda di Luna e Terra, che a sua volta ha portato ad una flessione del loro valore.

In termini di formule matematiche, l'algoritmo di mercato aperto funziona in base alla seguente formula:

Supponiamo che il valore attuale della stablecoin sia S , il valore ancorato sia A e la quantità di stablecoin nel pool di garanzie sia G . Allora, l'algoritmo di mercato aperto funziona nel seguente modo:

- Se $S > A$, allora l'algoritmo acquista la stablecoin sul mercato e aumenta la quantità di garanzie nel pool ($G = G + (S - A)$)
- Se $S < A$, allora l'algoritmo vende la stablecoin sul mercato e riduce la quantità di garanzie nel pool ($G = G - (A - S)$)

Tuttavia, come menzionato in precedenza, la volatilità del mercato e la mancanza di liquidità nei mercati di Luna e Terra hanno reso difficile per l'algoritmo di mercato aperto mantenere il peg, rendendo inefficace questa formula.

Il crollo di Luna e Terra dimostra l'**importanza di una solida architettura di stabilizzazione e di trasparenza nella progettazione di una stablecoin**. Inoltre, mostra che le stablecoin sono soggette alle stesse sfide e alle stesse incertezze degli altri digital assets, per questo è necessario che gli investitori e gli utilizzatori comprendano i rischi associati ad esse.

3.11

Informatica

● Hard

Approfondimento: collaterale in valuta fiat e gli algoritmi di mercato aperto come riserva

I **depositi di garanzia sono un modo per mantenere la stabilità delle stablecoin** tramite il legame con un'altra valuta, ad esempio il dollaro statunitense. In questo sistema, una parte del valore di una stablecoin viene detenuta come deposito di garanzia per mantenere il loro valore legato a quello della valuta di riferimento.

Supponiamo di avere una stablecoin chiamata "StableCoin" e che sia peggata al dollaro statunitense. Se vogliamo emettere 100 unità di StableCoin, dovremmo detenere 100 dollari statunitensi come deposito di garanzia. Questo significa che se un utente vuole riscattare 10 unità di StableCoin, deve restituire 10 dollari statunitensi e ricevere 10 unità di StableCoin. In questo modo, il valore della stable coin rimane legato a quello del dollaro statunitense.

Gli algoritmi di mercato aperto sono un'**altra soluzione per mantenere la stabilità delle stablecoin**. Questi algoritmi funzionano tramite l'**acquisto e la vendita automatica di stable coin e altri digital assets per mantenere il prezzo ad un valore specifico**.

Ad esempio, se il prezzo di una stablecoin scende al di sotto del suo tasso di peg, l'algoritmo potrebbe acquistare automaticamente la stablecoin sul mercato per aumentare la domanda e rispristinare la stabilità. Allo stesso modo, se il prezzo di una stablecoin aumenta al di sopra del suo tasso di peg, l'algoritmo potrebbe vendere automaticamente la stable coin per abbassare l'offerta.

Questi algoritmi funzionano sulla base di una serie di equazioni matematiche che determinano il momento in cui acquistare o vendere la stablecoin per mantenere il prezzo a un livello specifico.

I depositi di garanzia e gli algoritmi di mercato aperto sono due componenti chiave che rendono possibile l'utilizzo di stablecoin. I depositi di garanzia garantiscono che ci sia sempre una quantità sufficiente di riserve per coprire la quantità di stablecoin in circolazione, mentre gli algoritmi di mercato aperto mantengono il prezzo della stablecoin ad un valore di peg specifico. Insieme, questi componenti creano un sistema stabile e affidabile che consente l'utilizzo di stablecoin in una vasta gamma di applicazioni.

3.12

Informatica

● Basic

Il ruolo dell'Open Banking nella interoperabilità

Open banking è un **conceitto che si riferisce alla condivisione di dati finanziari tra diverse organizzazioni, consentendo a terze parti di accedere ai dati finanziari dei clienti per offrire servizi migliorati e personalizzati**. Ciò è reso possibile dall'adozione di standard tecnici aperti e di interfacce di programmazione delle applicazioni (API) che consentono ai servizi finanziari di interagire tra loro.

L'open banking ha un **ruolo importante nell'interoperabilità tra i sistemi peer-to-peer e privati** perché consente alle diverse reti di comunicare tra loro e di condividere informazioni finanziarie. Ad esempio, le stable coin come Bitcoin e Tether possono essere integrate con i servizi bancari tradizionali utilizzando

API aperte e standard tecnici comuni, consentendo agli utenti di inviare e ricevere denaro in modo più efficiente e sicuro.

L'open banking può anche **facilitare la transizione verso un sistema finanziario più aperto e decentralizzato**. Ciò è reso possibile dalla creazione di reti di pagamento peer-to-peer che utilizzano le tecnologie blockchain per consentire transazioni sicure e veloci tra utenti in tutto il mondo, senza la necessità di intermediari centrali.

In generale, l'**open banking** può aiutare a creare un ecosistema finanziario più aperto, interoperabile e innovativo, consentendo a diverse reti di comunicare tra loro e di offrire servizi finanziari personalizzati ai clienti.

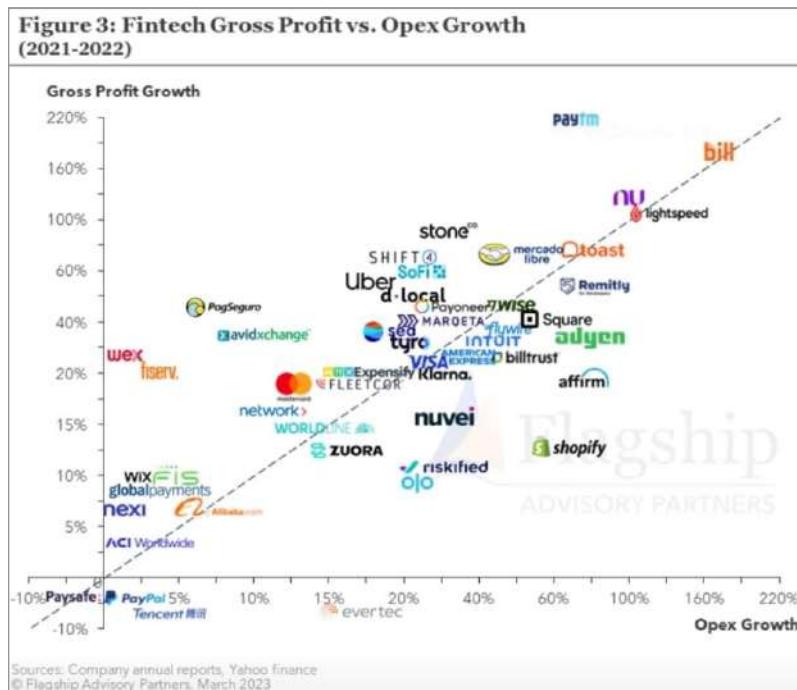
3.13

Business

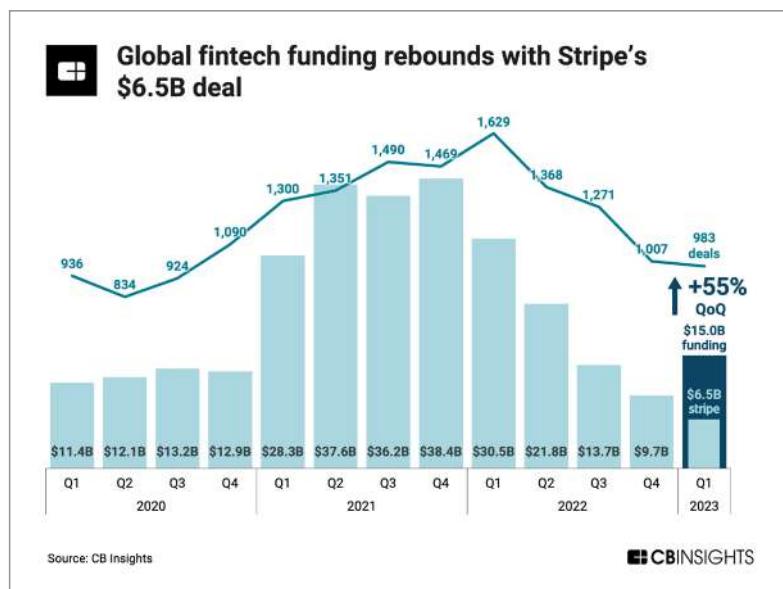
● Basic

Gli investimenti nel fintech e la contaminazione con digital assets e AI

Il mercato degli investimenti nel settore fintech è stato in costante crescita nel 2020 e 2021, con numerose startup fintech che hanno ottenuto finanziamenti significativi e valutazioni a miliardi di dollari. Un esempio di successo è la raccolta di fondi record di \$ 500 milioni da parte di Chime, una società di servizi bancari digitali, nel 2020.

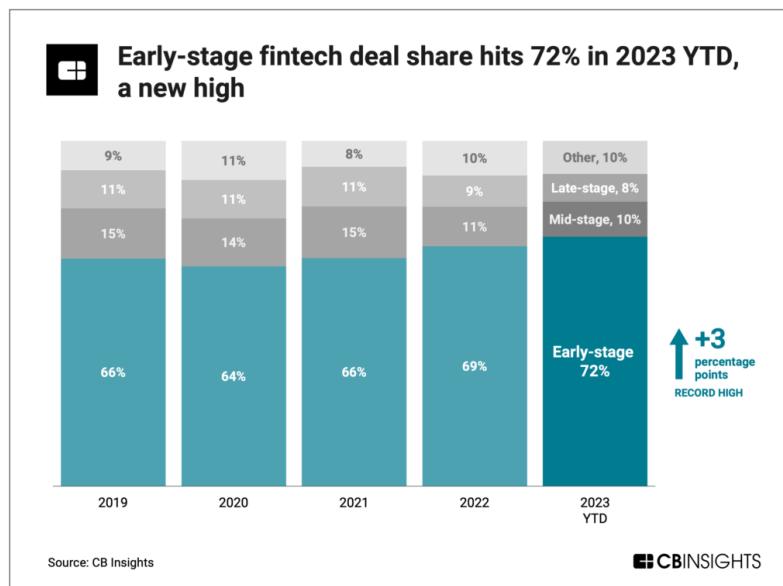


Tuttavia, nel 2022 si è vista una netta contrazione della crescita di molte startups ed **una diminuzione degli investimenti in questo settore**. Utilizzando i dati di CB Insights, mettiamo in evidenza alcuni dei punti salienti del report State of Fintech del primo trimestre 2023.

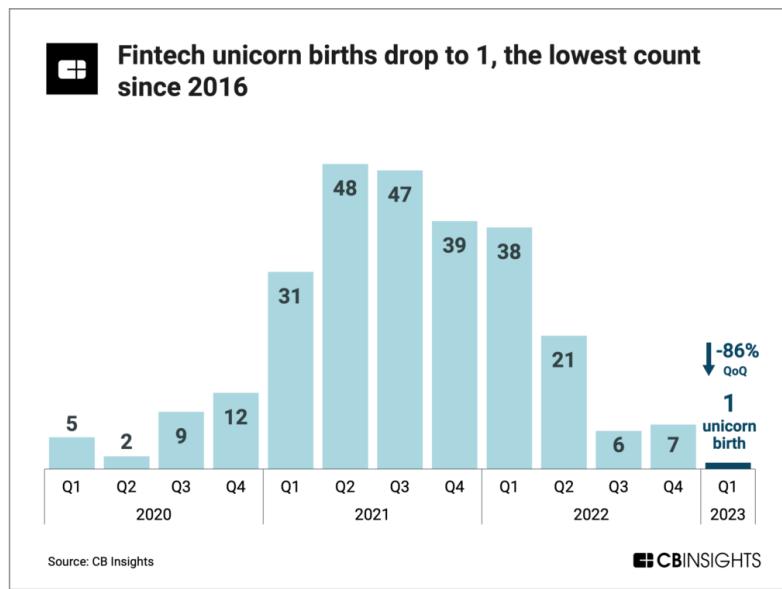


I finanziamenti fintech globali sono rimbalzati nel primo trimestre del 2023, arrivando a 15 miliardi di dollari, un aumento del 55% su base trimestrale.

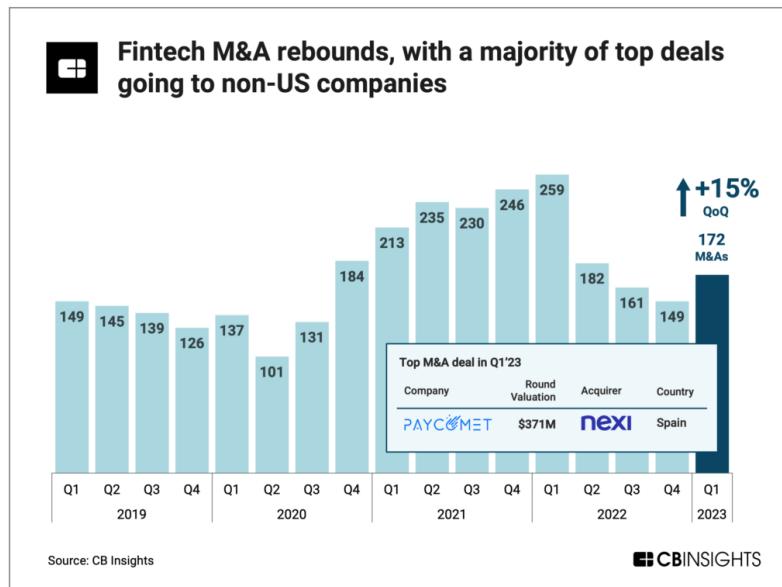
Il conteggio delle operazioni è diminuito del 2% su base trimestrale a 983 offerte, è andato relativamente bene rispetto al più ampio ecosistema di venture capital, in cui il conteggio delle operazioni è diminuito del 12% su base trimestrale. Il solo mega round di Stripe ha impedito ai finanziamenti fintech trimestrali di tornare ai livelli del 2017. Ciò suggerisce che l'attività di investimento fintech, come l'attività complessiva di investimento di rischio, continua a rallentare.



La quota di accordi nella fase iniziale domina regolarmente l'attività complessiva di investimento fintech. In Q1'23, ha raggiunto un nuovo massimo. Il 72% delle operazioni era in fase iniziale, rispetto al 69% dell'intero anno 2022. Ciò è probabilmente dovuto in parte alle preoccupazioni degli investitori per le valutazioni gonfiate del 2021 e i mercati pubblici incerti, che li stanno costringendo a investire in round iniziali più piccoli e meno rischiosi. Tra i primi 10 seed e angel round, il 60% è andato a fintech al di fuori degli Stati Uniti. Il più grande seed round (\$ 45 milioni) nel primo trimestre del 23 è andato alla piattaforma di regolamento dei crediti di carbonio con sede nel Regno Unito, Carbonplace.



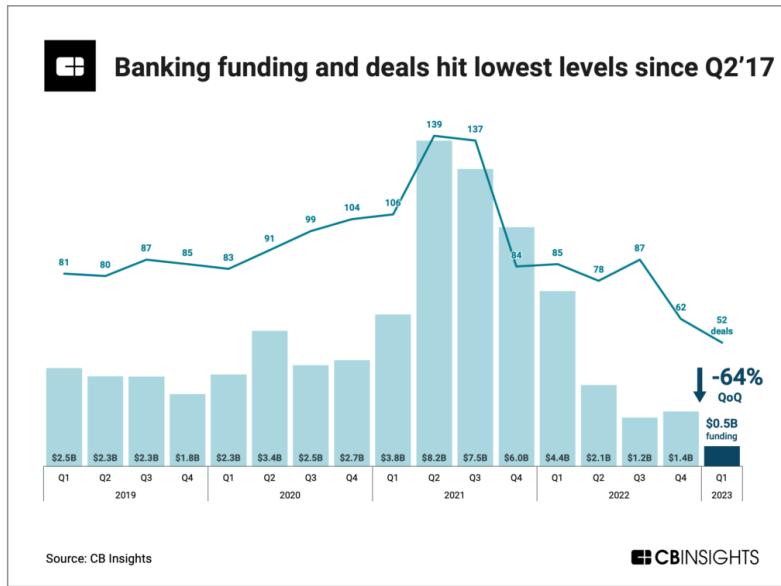
Nell'ultimo anno, le nascite di unicorni fintech sono diventate sempre più rare poiché il fintech e il più ampio spazio VC hanno iniziato a subire correzioni nelle valutazioni. Dal Q1'22 al Q1'23, le nascite di unicorni sono diminuite del 97%. Q1'23 ha visto la nascita di un solo unicornio (società valutata oltre \$ 1 miliardo), un calo dell'86% su base trimestrale e il livello trimestrale più basso dal 2016. Tuttavia, il totale degli unicorni fintech si è attestato ancora a 314 nel primo trimestre del 23, con un aumento dell'11% su base annua.



Dato l'attuale contesto macroeconomico e le valutazioni inferiori, le startup fintech hanno visto ridurre il numero di exit messe a segno. Sebbene le acquisizioni fintech siano rimbalzate del 15% su base trimestrale per raggiungere 172 operazioni nel primo trimestre del 2023, ciò ha comunque segnato un calo del 34% rispetto al massimo record di 259 nel primo trimestre del '22.

La maggior parte delle prime 10 operazioni di fusione e acquisizione del primo trimestre 2023 riguardava fintech con sede al di fuori degli Stati Uniti. Tuttavia, gli Stati Uniti sono risultati ancora in testa nella quota di exit globali nel primo trimestre del '23, rappresentando il 37% del totale. In particolare, la massima valutazione di fusioni e acquisizioni è scesa sotto i 500 milioni di dollari per la prima volta nell'ultimo anno.

Come sono andati gli altri tipi di exit? Le IPO sono leggermente aumentate fino a raggiungere quota 4 nel primo trimestre del 2023, ma le SPAC sono rimaste a 0. L'unica IPO con una valutazione divulgata (\$ 25 milioni) è stata per TAP Global, una piattaforma crittografica con sede a Gibilterra.



I finanziamenti alle fintech focalizzate sul settore bancario sono diminuiti in modo significativo negli ultimi 2 anni. Rispetto ai massimi record del secondo trimestre del 21, i finanziamenti fintech e il conteggio delle operazioni sono diminuiti rispettivamente del 94% e del 63%. Questo è stato il più grande calo di finanziamento trimestrale in tutte le categorie fintech nel primo trimestre del 23. Il finanziamento della tecnologia patrimoniale è diminuito solo del 24% su base trimestrale. Nel frattempo, pagamenti, prestiti digitali, insurtech e mercati dei capitali hanno visto aumentare i finanziamenti su base trimestrale. La maggior parte dei finanziamenti nel primo trimestre del 23 è andata a operatori bancari in fase iniziale. In effetti, le operazioni in fase iniziale nel settore bancario hanno rappresentato il 60% del totale per il primo trimestre del '23, un massimo di 5 anni.

Durante l'inizio del 2023, ci sono stati altri segnali di scricchiolio per la fintech come:

- Il colosso assicurativo tedesco Allianz sta provando a vendere il 5% nella banca digitale tedesca N26 per circa 160 milioni. Questo valore rappresenta meno di un terzo dei multipli valutativi spuntati nel 2021 da un marchio tra i più brillanti della nicchia.
- La casa di investimento Schroders svaluta del 50% la sua quota e implicitamente dimezza il valore della App di Nik Storonsky, Revolut: da 33 a 18 miliardi di dollari.

Il 2023 sarà un anno fondamentale per il settore fintech, per tornare a crescere. Del nuovo carburante per questo settore potrà essere la collaborazione e la contaminazione di altre tecnologie di altri settori vicini come:

- Lo sviluppo del settore dell'intelligenza artificiale, in grado di offrire nuove tipologie di servizi e di ottimizzazione, analizzando i profili di rischio, ottimizzando la gestione di pagamento ed offrendo personal chat per attività di customer care e analisi del mercato.
- Lo sviluppo del settore dei digital assets e dei pagamenti web3, in grado di offrire nuove tipologie di servizio, aprendo a nuove tipologie di asset scambiati, e programmando nuove tipologie di pagamenti intelligenti

La contaminazione di queste tecnologie potrà essere cruciale per tornare a far entrare capitali in questo settore.

Fonti

- ▶ Greco, A. (2023). Continua il momento no del fintech: Allianz mette in vendita il 5% della banca N26 a un terzo del valore 2021. Tratto da: https://www.repubblica.it/economia/finanza/2023/04/20/news/continua_il_momento_no_del_fintech_allianz_mette_in_vendita_il_5_della_banca_n26_a_un_terzo_del_valore_2021-396836077/

4

CBDC

- 4.1 Il ruolo delle banche centrali nell'economia contemporanea
- 4.2 Panoramica generale sulle Central Bank Digital Currencies (CBDC)
- 4.3 Moneta dominante e i nuovi assetti geopolitici
- 4.4 La guerra tra le valute internazionali
- 4.5 Verso la cashless society
- 4.6 Bank the unbanked e le opportunità del futuro

4.1

Teoria Monetaria

● Basic

Il ruolo delle banche centrali nell'economia contemporanea

Il ruolo delle banche centrali nello stampare moneta e custodire oro e argento è cambiato nel tempo. Tuttavia ci sono sempre state delle costanti rispetto all'operato di una banca centrale:

- Creazione di banconote, monete, moneta elettronica o altre forme di valuta
- Presenza o assenza di un collaterale
- Autonomia nella gestione e nella distribuzione della liquidità in una economia e in un territorio

Rispetto al secondo punto, andiamo ad analizzare le banche centrali da fine della seconda guerra mondiale. Dal 1944, gli accordi di Bretton Woods stabilirono **un sistema monetario internazionale basato sul dollaro americano, ma ancora ancorato all'oro (gold standard)**. Le banche centrali dovevano mantenere un tasso di cambio fisso tra la loro valuta e il dollaro, il quale era convertibile in oro al tasso di \$35 per oncia. Inoltre, le banche centrali occidentali utilizzano il dollaro e titoli esteri come riserve interne. Tuttavia, nel 1971, la crescente inflazione, l'embargo dell'OPEC e il costo della guerra del Vietnam spinsero gli Stati Uniti ad abbandonare il sistema aureo, creando una crisi monetaria globale. Nel 1973, i paesi occidentali firmarono l'accordo di Smithsonian, **che prevedeva un sistema di tassi di cambio fluttuanti, consentendo alle valute di fluttuare liberamente**. Da quel momento in avanti, nessuna valuta internazionale dei paesi industrializzati si è basato su un tallone aureo, ovvero delle riserve di oro e argento che garantivano un controvalore e più stabilità.

Le banche centrali continuarono a intervenire nei mercati per stabilizzare i tassi di cambio. In questo periodo, si iniziarono ad utilizzare **le politiche monetarie per controllare l'inflazione, combattere le crisi economiche e stimolare la crescita economica**. Il ruolo delle banche centrali divenne sempre più importante nella gestione delle politiche monetarie dagli anni '70 in poi.

La Banca Centrale Europea (BCE) è stata istituita nel 1998 come parte del Sistema Europeo di Banche Centrali (SEBC) e ha il compito di attuare la politica monetaria per l'area dell'euro. **Essa opera in collaborazione con le banche centrali nazionali (BCN) dei paesi dell'Unione Europea (UE) che hanno adottato l'euro come valuta**. Il SEBC è composto dalla BCE e dalle BCN di tutti i 27 stati membri dell'UE, ad eccezione della Danimarca che ha una clausola di esenzione. Le BCN svolgono un ruolo importante all'interno del SEBC ed eseguono le politiche monetarie stabilite dalla BCE.

La BCE detiene riserve valutarie in diverse valute, come dollari USA, yen giapponesi, renminbi cinesi, oro e SDR. Tecnicamente, le BCN hanno il compito di gestire le riserve valutarie del proprio paese e di garantire la stabilità finanziaria nazionale. Tuttavia, **oggi la scelta di creare nuova moneta non è più determinata dalle riserve, ma da scelte di politica economica mirata ad avere una inflazione programmata (inflation target)**.

4.2

Legal

● Basic

Panoramica generale sulle Central Bank Digital Currencies (CBDC)

Nel 2020, Mark Zuckerberg, insieme a tante altre aziende hi tech, proposero di creare un consorzio digitale, dal quale far emergere un nuovo digital asset privato chiamata “Libra”. L’idea era creare una stable coin proprietaria, con asset finanziari come collaterale per renderla stabile. Questo avvenimento fece allarmare i regolatori e le banche centrali di tutto il mondo, poiché era chiaro che la posta in gioco era alta: queste avrebbero dovuto competere con le aziende tech per quello che riguarda l’emissione di valuta all’interno dell’economia globale.

Da quel momento, molte banche centrali hanno iniziato a lavorare su una loro versione di digital asset privato, definito come CBDC.

Le CBDC, o Central Bank Digital Currencies, sono **valute digitali emesse dalle banche centrali**. Il loro obiettivo principale è quello di modernizzare il sistema finanziario e offrire ai cittadini un mezzo di pagamento digitale sicuro ed efficiente. Alcuni paesi, come la Cina, Inghilterra e la Svezia, hanno già iniziato a sperimentare le loro CBDC, mentre altri stanno ancora valutando se adottarle o meno.

Ancora non è chiaro come entreranno all’interno dei sistemi economici, tuttavia, è sicuramente interessante approfondire l’impatto che potranno avere questi nuovi sistemi informatici all’interno del mercato dei sistemi internazionali di trasferimento del valore.

Per quanto riguarda l’**impatto delle CBDC sui servizi di clearing e settlement**, è importante notare che queste valute digitali **potrebbero ridurre la necessità di intermediari finanziari**. In altre parole, le transazioni potrebbero avvenire direttamente tra i titolari di conti bancari e le banche centrali, senza passare per le banche commerciali o altri intermediari.

Tuttavia, sarà interessante comprendere il loro ruolo rispetto ai sistemi di clearing e settlement utilizzati ad oggi all’interno dei sistemi interbancari e rispetto alle operazioni fatte dai retails nelle operazioni di compra vendita per prodotti e servizi. Dal punto di vista tecnico, infatti, ci si domanda quali saranno le caratteristiche della rete e quali servizi potrà offrire, anche rispetto alle performance delle reti già esistenti.

Servizi offerti	TARGET2	SEPA	CHAPS	Euroclear	Clearstream	SWIFT
Transazioni interbancarie in tempo reale	Sì	Sì	Sì	No	No	Sì
Transazioni internazionali	Sì	Sì	Sì	Sì	Sì	Sì
Compensazione e regolamento di titoli	No	No	No	Sì	Sì	Sì
Gestione dei rischi di controparte	Sì	Sì	Sì	Sì	Sì	Sì
Integrazione con altre reti di pagamento	No	Sì	No	No	No	Sì
Market share	47.54%	39.70%	5.41%	2.98%	2.25%	2.12%

Fonte: Statista (dati relativi al 2020)

TARGET2, SEPA e CHIPS sono servizi di clearing e settlement interbancario che operano in Europa. TARGET2 è il più grande in termini di market share, seguito da SEPA e CHAPS. **Euroclear e Clearstream, invece, offrono servizi di clearing e settlement per transazioni di titoli**, mentre **SWIFT fornisce servizi di messaggistica finanziaria e di clearing e settlement per transazioni interbancarie e internazionali**. Tuttavia, anche se le CBDC sono adottate su larga scala, è probabile che i servizi di clearing e settlement continuino ad essere utilizzati per transazioni tra banche commerciali o per scambi transfrontalieri. Inoltre, **l’implementazione delle CBDC richiederà un’infrastruttura tecnologica sofisticata e sicura**, che potrebbe essere fornita da fornitori di servizi finanziari esistenti o da nuovi operatori specializzati.

Paese	Progetto CBDC	Fonte
Cina	Digital Yuan	https://www.imf.org/en/News/Articles/2022/07/07/sp070722-central-bank-digital-currency-and-the-case-of-china
Svezia	E-krona	https://www.riksbank.se/en-gb/payments--cash/e-krona/
Canada	CAD-COIN	https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/central-bank-digital-currency/
Stati Uniti	Digital Dollar Project	https://www.federalreserve.gov/central-bank-digital-currency.htm
Giappone	Digital Yen	https://www.boj.or.jp/en/paym/digital/index.htm
Europa	Eurocoin	https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
Uk	Digital Pound	https://www.bankofengland.co.uk/the-digital-pound

In sintesi, l'**adozione delle CBDC potrebbe comportare un cambiamento significativo nel panorama dei servizi di clearing e settlement**, ma è difficile prevedere con esattezza l'entità di tale cambiamento e quali operatori ne beneficeranno o ne subiranno le conseguenze.

4.3

Geopolitica / Teoria Monetaria

● Basic

Moneta dominante e i nuovi assetti geopolitici

Secondo Ray Dalio, la moneta dominante è un concetto importante per capire come funziona l'economia globale.

La **moneta dominante è quella valuta che viene utilizzata da molti paesi come riserva di valore e mezzo di scambio**. La moneta dominante può influenzare l'economia globale in vari modi, ad esempio attraverso gli effetti delle fluttuazioni dei tassi di cambio e la capacità di un paese di finanziare il proprio debito.

Attualmente, il dollaro americano è considerato la moneta dominante, ma secondo Dalio questa situazione potrebbe cambiare nel tempo. Ad esempio, potrebbe emergere una nuova valuta come moneta dominante, o potrebbero esserci più valute che condividono lo status di moneta dominante. Inoltre, la crescente digitalizzazione delle finanze potrebbe portare ad una maggiore adozione di valute digitali come riserva di valore e mezzo di scambio.

Dalio sostiene che comprendere il concetto di moneta dominante è importante per gli investitori e per coloro che sono interessati alla politica economica. **La capacità di prevedere i cambiamenti nella moneta dominante può aiutare a prendere decisioni più informate sugli investimenti e sulle strategie di politica economica**.

Ad esempio, il fatto che il dollaro americano sia la moneta dominante ha permesso agli Stati Uniti di finanziare il proprio debito emettendo obbligazioni denominate in dollari. Ciò ha reso gli Stati Uniti meno dipendenti dai prestiti esteri e ha permesso al governo di finanziare programmi di spesa pubblica più ambiziosi. Tuttavia, questa situazione ha anche causato un aumento del debito pubblico degli Stati Uniti, che potrebbe diventare insostenibile nel lungo termine.

Dalio ha anche sottolineato l'**importanza di comprendere le fluttuazioni dei tassi di cambio** tra le valute, **che possono influenzare le esportazioni e le importazioni di un paese, nonché la redditività delle imprese che operano a livello internazionale**. Inoltre, le fluttuazioni dei tassi di cambio possono anche **influenzare la capacità di un paese di pagare il proprio debito**.

In sintesi, la comprensione del concetto di moneta dominante è importante per capire come funziona l'economia globale e per prendere decisioni informate sugli investimenti e sulla politica economica. Da-

lio ha sviluppato un modello economico innovativo che sfida la saggezza convenzionale e ha proposto una serie di riforme per il sistema economico globale, tra cui l'adozione di una politica monetaria più equilibrata e la riforma del sistema fiscale.

4.4

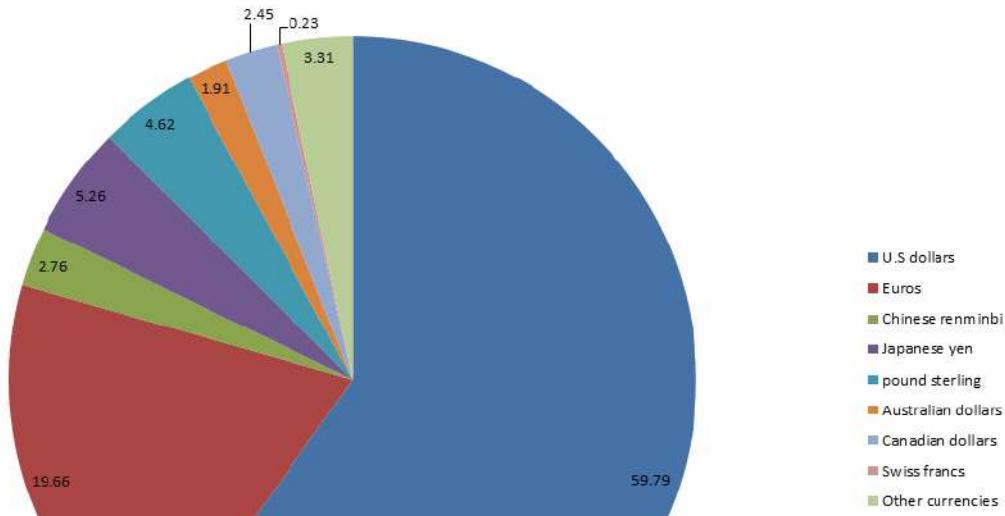
La guerra tra le valute internazionali

Geopolitica / Teoria Monetaria

● Basic

Il predominio del dollaro nei flussi commerciali e di investimento globali sta affrontando una serie di nuove minacce mentre molti paesi promuovono piani per aumentare l'uso di valute alternative.

Share of allocated global foreign-exchange reserves Q32022



GRAPH: ELIAMEP, Source: IMF, (COFER)



Per decenni, il biglietto verde ha regnato supremo come valuta di riserva mondiale ed è ampiamente utilizzato nel commercio transfrontaliero, in particolare per materie prime come il petrolio con oltre il 59% di *market share* rispetto alle altre valute internazionali. Grazie alla relativa stabilità dei prezzi, gli investitori lo considerano un bene rifugio in tempi di maggiore incertezza economica e geopolitica.



How to read this map: The size of the country corresponds to its level of foreign exchange reserves in Q1 2018 according to the IMF. The color corresponds to the continent.

Article & Sources:
<https://howmuch.net/articles/countries-with-the-biggest-forex-reserves>
<http://www.imf.org>

howmuch net

Il dollaro è stato ulteriormente rafforzato lo scorso anno da un aumento dei tassi di interesse statunitensi che lo hanno reso attraente per gli investitori stranieri alla ricerca di rendimenti più elevati. È salito del 17% durante i primi nove mesi del 2022, ma da allora ha perso un po' del suo splendore sulla prospettiva che la Federal Reserve possa presto porre fine ai suoi aumenti dei tassi man mano che l'inflazione si raffredda rapidamente.

In questo contesto arrivano le ultime minacce al regno del biglietto verde: ecco alcuni progetti valutari provenienti da tutto il mondo che mirano in ultima analisi a minare la supremazia del dollaro.

- **Il Brasile e l'Argentina hanno recentemente annunciato che si stanno preparando a lanciare una valuta comune**, denominata "sur" (sud), che potrebbe eventualmente diventare un progetto simile all'euro abbracciato da tutto il Sud America. Una valuta comune potrebbe aiutare a rafforzare il commercio sudamericano, hanno affermato i leader dei paesi in una dichiarazione congiunta, perché elude i costi di conversione e l'incertezza del tasso di cambio. Ciò potrebbe erodere il dominio del dollaro nella regione, dato che dal 1999 al 2019 il biglietto verde ha rappresentato fino al 96% del commercio tra il Nord e il Sud America, secondo la Federal Reserve.
- **Nazioni dalla Cina e Russia all'India e Brasile, stanno spingendo per stabilire più scambi in unità diverse dal dollaro**, con piani che vanno dall'uso di valute locali a una stablecoin sostenuta dall'oro e una nuova valuta di riserva BRICS. La nuova unità di riserva si baserebbe su un paniere di valute dei membri del gruppo: Brasile, Russia, India, Cina e Sudafrica.
- **Russia e Iran stanno lavorando insieme su un digital asset sostenuto dall'oro**, una "stablecoin" che potrebbe sostituire il dollaro per i pagamenti nel commercio internazionale. I due Paesi, entrambi colpiti dalle sanzioni occidentali, vogliono emettere un "token della regione persiana" da utilizzare nelle transazioni transfrontaliere, con l'intenzione di lanciarlo in una speciale enclave economica ad Astrakhan nel sud della Russia, che già gestisce le spedizioni iraniane. Mirando ad aumentare il loro volume di scambi a \$ 10 miliardi all'anno attraverso mosse come lo sviluppo di un sistema di pagamenti internazionali alternativo a SWIFT, da cui sono banditi.

Il regno del dollaro come principale offerta di riserva è già in declino mentre i banchieri centrali diversificano le loro partecipazioni in valute come lo yuan cinese, la corona svedese e il won sudcoreano, secondo il Fondo monetario internazionale.

4.5

Business

● Basic

Verso la cashless society

La direzione che sta seguendo la maggior parte del mondo industrializzato è quella della totale dematerializzazione progressiva della moneta, trasportando l'uomo all'interno di una società completamente digitale e cashless. Il concetto di **cashless society si riferisce ad una società in cui le transazioni finanziarie vengono effettuate esclusivamente con mezzi elettronici**, senza l'utilizzo di contanti. In una società cashless, le persone utilizzano carte di credito, carte di debito, pagamenti mobile e altre forme di pagamento elettronico per acquistare beni e servizi.

Questa tendenza verso una società senza contanti sta diventando sempre più popolare in tutto il mondo. Ad esempio, in Svezia, il governo sta lavorando per eliminare completamente il contante entro il 2023, mentre in Danimarca il 36% delle transazioni avvengono già esclusivamente con mezzi elettronici. Anche in paesi come il Regno Unito, l'Australia e il Canada si sta verificando una transizione verso una società cashless. Secondo un rapporto della Bank of Canada, l'utilizzo del contante in Canada è diminuito del 40% negli ultimi dieci anni, mentre in Australia, il 37% delle transazioni effettuate nel 2019 sono state effettuate senza contanti.

In Cina, l'uso di pagamenti digitali è diventato così diffuso che la maggior parte delle persone non porta più contanti con sé. Le piattaforme di pagamento come Alipay e WeChat Pay, che consentono ai consumatori di effettuare pagamenti mobili tramite smartphone, sono diventate estremamente popolari, con oltre un miliardo di utenti attivi.

In India, il governo ha introdotto la demonetizzazione nel 2016, eliminando le banconote di valore elevato per promuovere l'utilizzo di pagamenti digitali. L'iniziativa ha spinto molti indiani a utilizzare le app di pagamento come Paytm e BHIM per effettuare transazioni quotidiane.

La transizione verso una società senza contanti ha diversi vantaggi, tra cui una maggiore sicurezza e una maggiore efficienza nei pagamenti. Tuttavia, ci sono anche alcune **preoccupazioni riguardanti la privacy e la sicurezza dei dati personali**. In ogni caso, sembra che la tendenza verso una società cashless sia destinata a crescere ulteriormente nel prossimo futuro.

4.6

Business

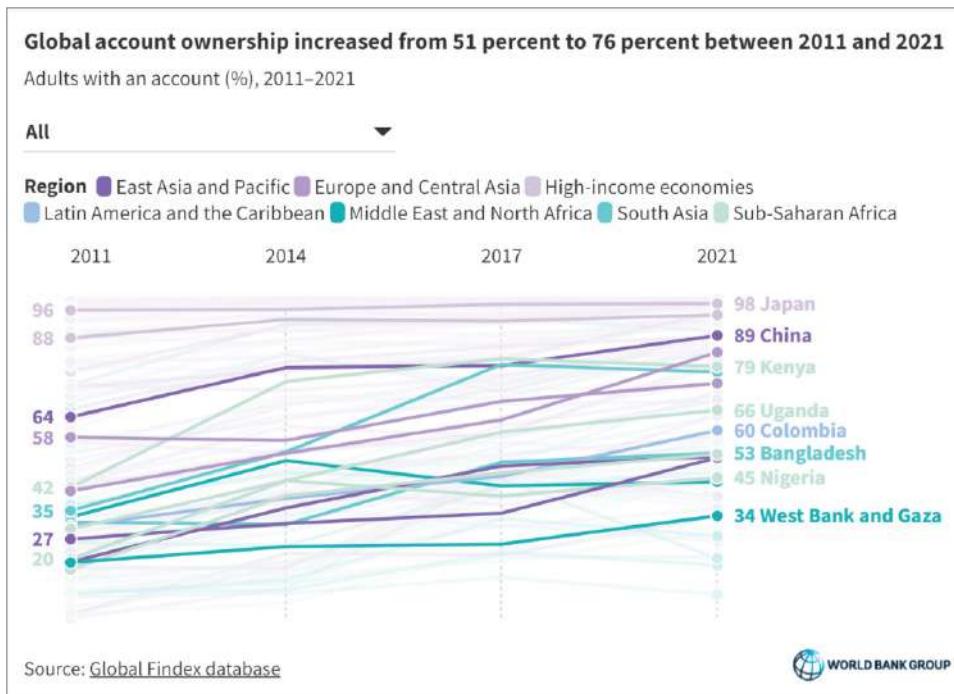
● Basic

Bank the unbanked e le opportunità del futuro

Il concetto di "bank the unbanked" si riferisce all'idea di fornire servizi bancari e finanziari a individui e comunità che altrimenti non avrebbero accesso a tali servizi. Questi individui e comunità, noti come "non bancarizzati", sono spesso esclusi dal sistema finanziario tradizionale a causa di barriere economiche, sociali o geografiche. Fortunatamente, la crescita organica della copertura di Internet **in quasi tutte**

Le parti del globo può facilitare lo sviluppo e la crescita di servizi finanziari completamente digitali, come CBDC e Stable Coin, all'interno di un territorio nuovo e in via di sviluppo.

Il processo di bank the unbanked mira a **promuovere l'inclusione finanziaria e l'accesso ai servizi bancari** per tutti gli individui, indipendentemente dal loro status socioeconomico. Ciò può essere fatto attraverso l'implementazione di soluzioni innovative **come servizi bancari mobili, banche comunitarie e microfinanza**. Questo può avere importanti effetti positivi sulla crescita economica e sullo sviluppo sociale. In particolare, può contribuire a ridurre la povertà, aumentare la sicurezza finanziaria e promuovere l'imprenditorialità nelle comunità sottosviluppate.



Secondo i dati del 2020 del World Bank Global Findex Database, circa il 7% della popolazione adulta europea non ha accesso a un conto bancario. In America, il tasso di non bancarizzati è del 22%. In Africa, il tasso di non bancarizzati è del 57%, con paesi come il Niger e la Repubblica Centrafricana che hanno tassi di non bancarizzati superiori al 70%. In Asia, il tasso di non bancarizzati è del 29%.

Tuttavia, è importante notare che il bank the unbanked non è una soluzione a tutti i problemi finanziari. Ci sono ancora sfide da affrontare, come la scarsa alfabetizzazione finanziaria e la mancanza di regolamentazione adeguata. Tuttavia, l'obiettivo di fornire servizi bancari a coloro che ne hanno bisogno rimane una priorità importante per le istituzioni finanziarie e le organizzazioni internazionali.

Fonti

- Central Bank Balance Sheet. Tratto da: <https://cbonds.it/glossary/central-bank-balance-sheet/>
- World Bank Global Findex Database 2020. Tratto da: <https://globalfindex.worldbank.org/>
- World Gold Council. Tratto da: <https://www.gold.org/goldhub/data/gold-prices>

Capitolo 6

BANCA E INVESTIMENTI NEL WEB3



Introduzione

Il sesto capitolo si pone come principale obiettivo formativo quello di mettere in luce la complessità del processo sociale di misurazione del valore di qualsiasi bene asset, tangibile e/o intangibile. Riprendendo le teorie di filosofia economica e con alcuni esempi, si è cercato di analizzare come, insieme di individui e il “mercato”, non sempre misurano il valore di un bene o di un asset in maniera completamente razionale e non sempre vi è una simmetria informativa durante il processo di analisi individuale e collettiva.

Il secondo obiettivo formativo è quello di aiutare il lettore a comprendere la maturità dell’industria dei digital asset e come questa, con nuove soluzioni tecnologiche, faciliti la nascita di nuovi modelli di business per gli operatori nel mercato, compresi gli istituti finanziari e banche tradizionali.

Il terzo obiettivo formativo è quello di comprendere i potenziali quali sono i principali business model degli operatori nel mercato dei digital asset, riassumendo quali possibili applicazioni e soluzioni possono essere offerte a mercato e come la normativa aiuti a definire dal punto di vista legale i digital asset. Inoltre, si parlerà anche della gamma di strumenti derivati utilizzati nel settore di finanza tradizionale, che hanno come sottostante indici relativi ad aziende web3 e digital asset

Il capitolo finisce con un confronto tra bitcoin, oro e dollaro per comprendere e distinguere le differenze e le analogie di questi asset, con particolare attenzione ai modelli di offerta e la rispettiva relazione con il proprio valore sul lungo periodo, cercando di comprendere la doppia natura di bitcoin, visto da alcuni come oro digitale e da altri come contante peer to peer.

In fine, si analizzeranno alcuni indici e statistiche per comprendere l’evoluzione del mercato dei digital asset nel corso degli ultimi anni, e come poter leggere alcune informazioni che troviamo all’interno dei protocolli, come la tokenomics e altri dati on-chain.

In sintesi, il capitolo è composto da 5 macro-blocchi e 31 blocchi formativi, e cerca di aiutare a comprendere la complessità attorno al mercato finanziario, la definizione di valore e la tipologia dei digital asset nel mercato.

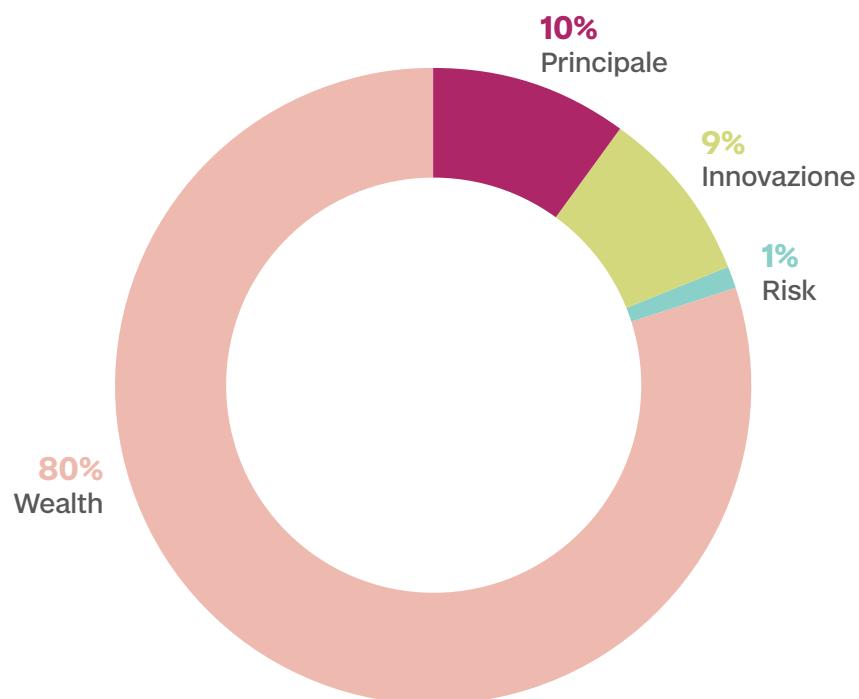
Queste alcune domande a cui cercheremo di rispondere:

- Perché la filosofia e la psicologia sono determinanti per comprendere la misurazione del valore in asset?
- A che punto ci troviamo nel modello di maturità del mercato del web3?
- Come vengono classificati alcuni digital asset dal punto di vista normativo?
- Cosa sta facendo la finanza tradizionale durante questi nuovi trend tecnologici?
- Cosa si intende per tokenizzazione di un asset?
- Come influisce sul valore il costo di produzione di un singolo bitcoin? E dell’oro?
- Quali sono le considerazioni da fare per creare una soluzione di custodia di digital asset?
- Quali sono le differenze nel revenue model dei i servizi CEFI e dei DEFI, e come vengono utilizzati gli utility token per ottenere nuova liquidità dal mercato?
- Quali sono i dati di mercato del web3, dei digital asset e token NFT da analizzare per studiare le tendenze di mercato?
- Come un utente può entrare nel mercato finanziario del web3 e può acquistare un digital asset?

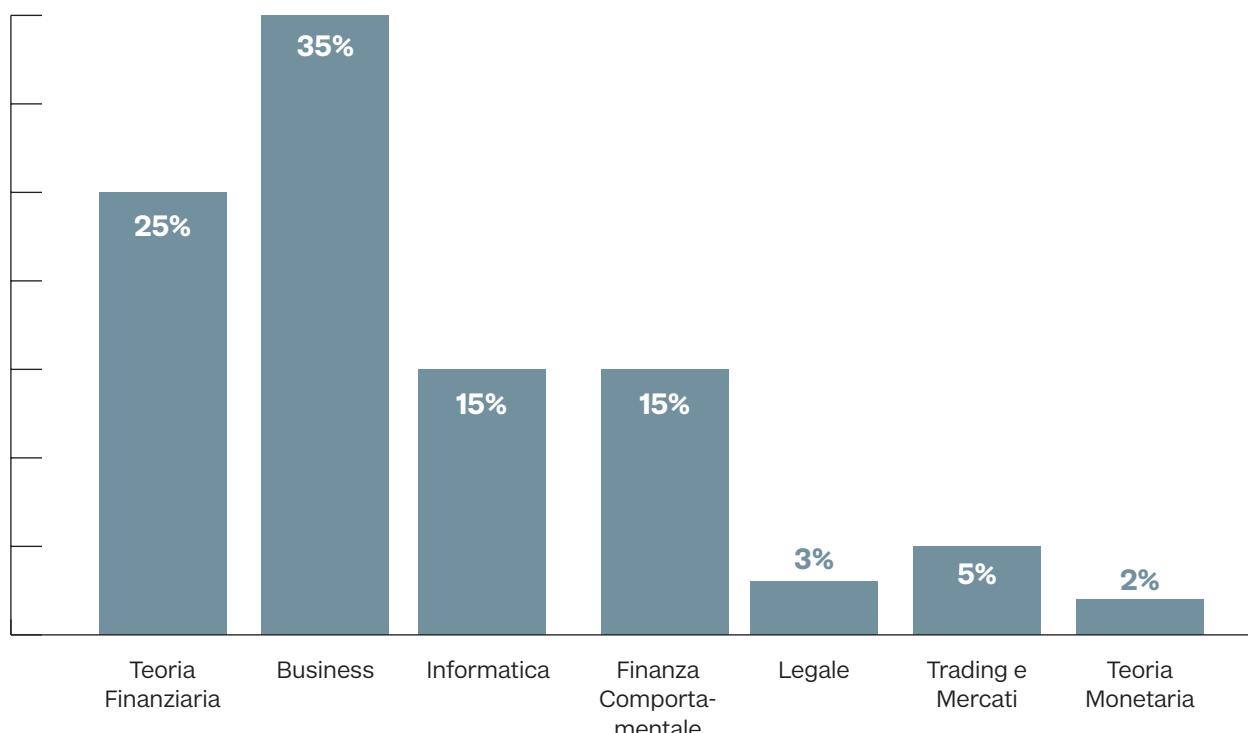
Per poi approfondire con domande più in profondità come:

- Come viene effettuata l’analisi fondamentale dei digital asset, e perché si confronta il modello di stock to flow di Bitcoin con quello dell’oro?
- Quali sono i dati on-chain utili per comprendere più a fondo alcune dinamiche di mercato e come si confrontano con quelli di applicazioni e servizi del web tradizionale?
- Quali sono i mercati DEFI su cui gli utenti comprano e vendono prodotti finanziari derivati?
- Esiste qualche grado di correlazione tra i digital asset e altri strumenti finanziari tradizionali?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. L'uomo e il processo di misurazione del valore

- 1.1 La misurazione del valore degli asset tangibili ed intangibili
- 1.2 Il processo bottom-up nella misurazione dal valore
- 1.3 Simmetria e asimmetria informativa, quanto il mercato è razionale?

DIFFICOLTÀ DISCIPLINA PERCORSO

●	Finanza Comportam.	Principale
●	Theoria Fin./Business	Wealth
●	Finanza Comportam.	Wealth

2. Il modello di maturità del mercato Web3

- 2.1 L'evoluzione del mercato finanziario Web3
- 2.2 Quali sono le asset class nel Web3?
- 2.3 ICO VS IPO: le differenze
- 2.4 IPO di Coinbase
- 2.5 Approfondimento dei servizi della finanza decentralizzata
- 2.6 Come si muovono i player nel mercato Web3 e dei digital assets?

●	Business	Wealth
●	Theoria Finanziaria	Wealth
●	Theoria Finanziaria	Wealth
●	Business	Wealth
●	Informatica/Business	Wealth
●	Business	Wealth

3. I servizi del mondo banking nel mercato Web3

- 3.1 Accesso al mercato dei digital assets e volumi a confronto
- 3.2 Come possono essere classificati i digital assets?
- 3.3 Quali sono i revenue model dei DEX e dei CEX?
- 3.4 Utility token come revenue model: il caso BNB
- 3.5 La tokenizzazione di assets
- 3.6 Tra il Web2 e il Web3: la custodia dei digital assets
- 3.7 Tra il Web2 e il Web3: on-ramp e smart order routing nel Web3
- 3.8 Tra il Web2 e il Web3: come costruire un digital asset backed security?

●	Business	Wealth
●	Legal	Wealth
●	Business	Wealth
●	Business	Wealth
●	Informatica	Wealth
●	Informatica/Business	Wealth
●	Informatica/Business	Innovazione
●	Informatica/Business	Wealth
●	Informatica/Business	Innovazione
●	Informatica/Business	Wealth
●	Informatica/Business	Innovazione

4. Prodotti derivati sul mercato Web3

- 4.1 Quali sono i derivati nel mercato del Web3?
- 4.2 Approfondimento degli ETP
- 4.3 Analisi dei dati degli strumenti derivati su CEX e DEX

●	Theoria Finanziaria	Wealth
●	Theoria Finanziaria	Wealth
●	Theoria Finanziaria	Wealth

5. Bitcoin come digital asset

- | | | | |
|---|--------------------------------------|---|---|
| 5.1 Il processo di price discovery di un digital asset come bitcoin | ● | Finanza Comportam. | Principale |
| 5.2 Che cosa si intende per asset deflattivo ed inflattivo? | ● | Teoria Finanziaria/
Finanza Comportam. | Wealth |
| 5.3 Confronto tra l'offerta di bitcoin e Oro nel tempo | ● | Teoria Finanziaria | Wealth |
| 5.4 Il principio di inflazione e l'invenzione dell'aggiustamento della difficoltà | ● | Teoria Mon./Informat. | Wealth
Innovazione |
| 5.5 La ricerca e sviluppo nel settore del mining di bitcoin | ● | Informatica | Wealth
Innovazione |
| 5.6 Quanta energia consuma davvero Bitcoin? | ● | Business | Principale |
| 5.7 Dove vengono estratti oro e bitcoin? | ● | Business | Principale |
| 5.8 Che cos'è il modello stock to flow? | ● | Teoria Finanziaria | Wealth |
| 5.9 Bitcoin per gli Stati e le imprese | ● | Business | Wealth |
| 5.10 Bitcoin a confronto con altri asset | ● | Trading e mercato | Wealth |
| 5.11 Come utilizzo i dati on-chain per capire il mercato? | ● | Trading e mercato | Wealth |

1

L'uomo e il processo di misurazione del valore

- 1.1 La misurazione del valore degli asset tangibili ed intangibili
- 1.2 Il processo bottom-up nella misurazione dal valore
- 1.3 Simmetria e asimmetria informativa, quanto il mercato è razionale?

1.1

Finanza Comportamentale

● Basic

La misurazione del valore degli asset tangibili ed intangibili

Nell'ambito dell'economia e della finanza, la misurazione del valore di un bene rappresenta un processo complesso che coinvolge una serie di variabili e fattori decisionali. Questa complessità si amplifica ulteriormente quando si tratta di attribuire valore a beni intangibili come idee o innovazioni.

Iniziamo con l'analisi dei beni tangibili. Il valore di un bene tangibile è influenzato **da una serie di fattori, tra cui la sua utilità, la sua rarità, la domanda e l'offerta, e la percezione del suo valore da parte dei consumatori**. Questi fattori sono strettamente legati ai principi fondamentali dell'economia e della filosofia economica. Ad esempio, la teoria del valore-lavoro di Adam Smith sostiene che il valore di un bene è determinato dalla quantità di lavoro necessaria per produrlo. Allo stesso modo, la teoria del valore soggettivo di Carl Menger sostiene che il valore di un bene è determinato dalla sua utilità percepita da parte del consumatore.

Qui di seguito altre teorie che hanno cercato di determinare il processo con cui misuriamo il valore ad un bene:

- **Karl Marx e la teoria del valore del lavoro:** Marx estese la teoria del valore del lavoro di Smith, sostenendo che il valore di un bene è determinato dal "lavoro socialmente necessario" per produrlo. Questo include non solo il lavoro fisico, ma anche il tempo, l'energia e le risorse necessarie per formare il lavoratore.
- **David Ricardo e la teoria del valore del lavoro:** Ricardo, come Smith e Marx, sosteneva che il valore di un bene è legato al lavoro necessario per produrlo. Tuttavia, ha anche introdotto il concetto di vantaggio comparato, sostenendo che i paesi dovrebbero specializzarsi nella produzione di beni per i quali hanno un vantaggio relativo.
- **Alfred Marshall e la teoria del valore soggettivo:** Marshall ha sviluppato ulteriormente la teoria del valore soggettivo, introducendo il concetto di utilità marginale. Secondo questa teoria, il valore di un bene è determinato dalla sua utilità aggiuntiva (o marginale) per il consumatore. In altre parole, quanto un consumatore è disposto a pagare per un bene dipende da quanto quel bene migliora la sua situazione attuale.
- **John Maynard Keynes e la teoria della preferenza per la liquidità:** Keynes ha introdotto l'idea che il valore di un bene può essere influenzato dalla sua liquidità, o dalla facilità con cui può essere convertito in denaro. Questo può spiegare perché le persone sono spesso disposte a pagare di più per beni che possono essere facilmente venduti o scambiati.
- **Friedrich Hayek e la teoria del processo di scoperta:** Hayek ha sostenuto che il valore di un bene è determinato non solo dalla sua utilità o dal lavoro necessario per produrlo, ma anche dalla conoscenza e dalle informazioni disponibili sul bene. Questo può spiegare perché il valore di un bene può cambiare nel tempo man mano che vengono scoperte nuove informazioni.

Queste teorie, insieme a molte altre, contribuiscono a formare un quadro complesso di come viene determinato il valore di un bene tangibile.

Quando si tratta di valutare beni intangibili come idee o innovazioni, la complessità aumenta ulteriormente. **Questi beni non possono essere valutati in base a criteri tangibili come la dimensione o il peso, e il loro valore può variare notevolmente a seconda del contesto.** Ad esempio, un'idea innovativa può avere un valore enorme in un'industria ma essere praticamente inutile in un'altra.

Proviamo ad applicare le teorie precedentemente citate, nel processo di misurazione di valore di una idea:

- **Karl Marx e la teoria del valore del lavoro:** questa teoria si basa sull'idea che il valore di un bene è determinato dal lavoro necessario per produrlo. Tuttavia, nel caso di beni intangibili come le idee, è difficile quantificare il "lavoro socialmente necessario". Ad esempio, quanto "lavoro" è necessario per generare un'idea innovativa? E come si misura questo lavoro?

- **David Ricardo e la teoria del valore del lavoro:** anche questa teoria è di difficile applicabilità per i beni intangibili. Se il valore di un bene è legato al lavoro necessario per produrlo, come si determina il valore di un'idea che può essere generata in un istante, ma che potrebbe avere un impatto enorme?
- **Alfred Marshall e la teoria del valore soggettivo:** Questa teoria può essere applicata ai beni intangibili, ma presenta ancora delle sfide. Ad esempio, come si misura l'utilità marginale di un'idea o di un'innovazione tecnologica? E come si determina quanto un consumatore è disposto a pagare per un bene intangibile?
- **John Maynard Keynes e la teoria della preferenza per la liquidità:** Questa teoria può avere senso per i beni tangibili che possono essere facilmente venduti o scambiati, ma può essere difficile da applicare ai beni intangibili. Ad esempio, come si determina la "liquidità" di un'idea o di un'innovazione tecnologica?
- **Friedrich Hayek e la teoria del processo di scoperta:** Questa teoria può essere particolarmente rilevante per i beni intangibili, dato che il valore di un'idea o di un'innovazione tecnologica può cambiare drasticamente man mano che vengono scoperte nuove informazioni. Tuttavia, può essere difficile prevedere come queste scoperte influenzino il valore di un bene intangibile.

La finanza comportamentale aggiunge un ulteriore livello di complessità a questo processo. Questo campo di studio esamina **come le emozioni e i pregiudizi cognitivi influenzano le decisioni economiche degli individui, spesso in modi che sfidano le previsioni dei modelli economici tradizionali**.

In conclusione, mentre le teorie economiche tradizionali forniscono un quadro utile per comprendere come viene determinato il valore di alcune tipologie di beni, **esse presentano significative sfide quando si tratta di valutare beni intangibili come le idee e le innovazioni tecnologiche**. Questo sottolinea la necessità di sviluppare nuove teorie e modelli che possano affrontare la complessità e l'unicità di questi beni.

1.2

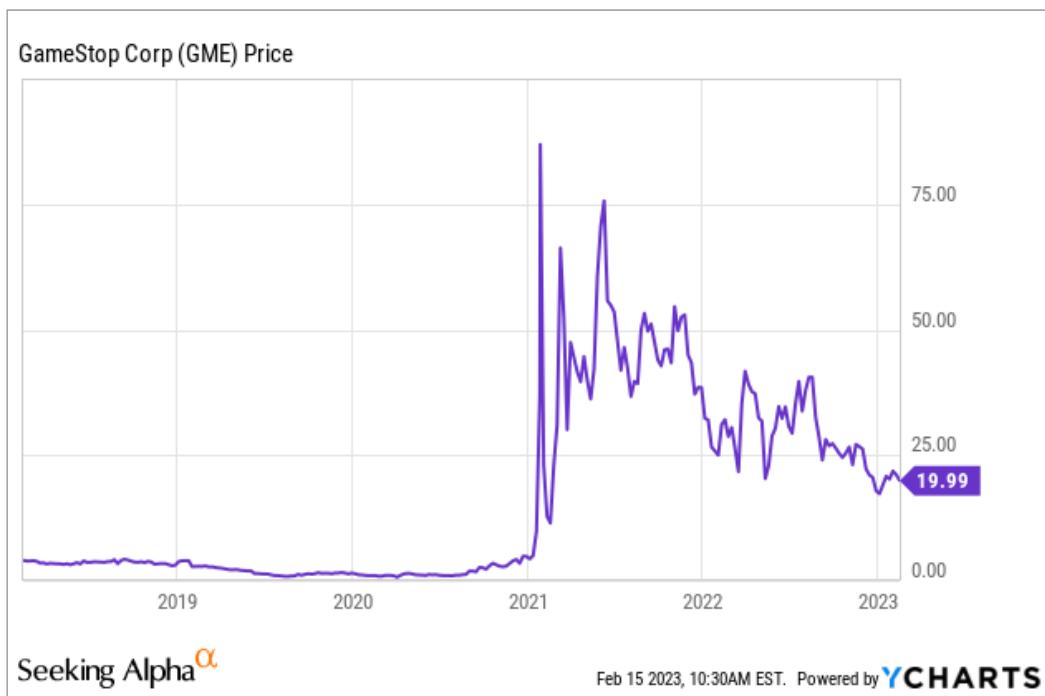
Teoria Finanziaria / Business

• Basic

Il processo bottom up nella misurazione del valore

Il caso GameStop rappresenta un esempio emblematico di come il processo di misurazione e determinazione di valore di un bene come un asset finanziario, sia una serie di conseguenze sociali che provengono dal basso (processo bottom up). Nel 2021, una comunità di investitori retail ha utilizzato i social media e le piattaforme di trading online per coordinare una campagna di acquisto di azioni di una società in difficoltà finanziarie, al fine di sfruttare la situazione e ottenere un profitto.

In particolare, la campagna di acquisto è stata attuata attraverso una **strategia di short squeeze**, ovvero l'**acquisto massiccio di azioni in modo da provocare un aumento del prezzo** e una riduzione del numero di azioni disponibili sul mercato, sfruttando la posizione short dei fondi di investimento che avevano scommesso sulla caduta del prezzo delle azioni di GameStop.



La strategia di **short squeeze**, tuttavia, ha suscitato polemiche e controversie, poiché ha portato ad un'accelerazione dei prezzi delle azioni che ha messo in difficoltà i fondi di investimento che avevano scommesso sulla caduta del prezzo, generando ingenti perdite per questi ultimi.



Short squeeze

Definizione: Uno short squeeze avviene quando i prezzi di un mercato aumentano improvvisamente, superando le aspettative degli analisti e degli investitori. Gli short squeeze possono impattare notevolmente gli investitori che adottano la strategia della vendita allo scoperto, o i trader che operano sulle azioni con gli strumenti derivati, come i CFD o le barrier.

Fonter: <https://www.ig.com/it/strategie-di-trading/cos-e-uno-short-squeeze--200824#:~:text=Uno%20short%20squeeze%20avviene%20quando,degli%20analisti%20e%20degli%20investitori.>

L'episodio ha sollevato diverse questioni etiche e regolatorie, in quanto la campagna di acquisto ha messo in luce **il potere dei social media e delle piattaforme di trading online nell'influenzare i mercati finanziari**, ma ha anche evidenziato la necessità di una maggiore regolamentazione del settore e della trasparenza delle informazioni finanziarie.

Inoltre, il caso GameStop ha messo in evidenza **il potere dei processi bottom-up nel cambiamento delle dinamiche dei mercati finanziari e nella partecipazione attiva dei cittadini alle scelte economiche**. Tuttavia, la loro attuazione senza una regolamentazione adeguata potrebbe comportare rischi significativi per l'integrità dei mercati finanziari e la tutela degli investitori.

Per concludere possiamo quindi affermare che il processo di misurazione del valore di un bene, anche nei mercati finanziari è determinato da dinamiche sociali complesse, a volte contrapposte, **che a seguito di diverse azioni, porta inevitabilmente a vinti e a vincitori, con giustificazioni più o meno razionali**.

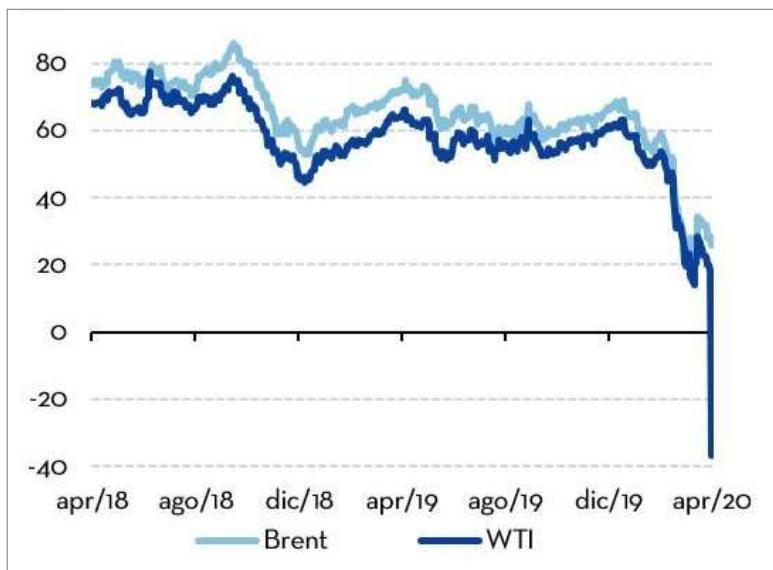
1.3

Finanza Comportamentale

• Basic

Simmetria e asimmetria, quanto il mercato è razionale

Il 20 aprile 2020, il prezzo dei futures del greggio WTI (West Texas Intermediate) è **andato sottozero per la prima volta nella storia**, crollando di oltre il 300% per atterrare in area negativa a -37,63 dollari al barile. Ciò ha significato che i produttori di petrolio erano disposti a pagare agli acquirenti per liberarsi del loro petrolio poiché non c'era spazio sufficiente per stoccare il greggio non venduto a causa della diminuzione della domanda globale dovuta alla pandemia di COVID-19.



Liquidazioni

Nel mondo della finanza, la liquidazione si riferisce a uno scambio che chiude forzatamente la posizione con leva di un trader a seguito della perdita totale o parziale del margine iniziale del trader.

Il prezzo negativo del petrolio non è stato causato solo dalle **liquidazioni** dei trader, ma anche dalla combinazione di una domanda in forte calo a causa della pandemia da coronavirus e di un'eccessiva produzione da parte dei paesi produttori di petrolio, in particolare l'Arabia Saudita e la Russia. Questo ha portato a un eccesso di offerta sul mercato, che **ha fatto diminuire il prezzo del petrolio fino a diventare negativo. Tuttavia, la diffusione notizia e la paura dei mercati ha creato un effetto a cascata verso posizioni corte, facendo crollare il prezzo.**

Questo evento senza precedenti ha avuto un impatto significativo sui mercati finanziari e sull'industria petrolifera globale, e sulla considerazione di avere un mercato finanziario razionale. I prezzi del greggio sono rimasti bassi per diversi mesi dopo l'evento, con il WTI che ha raggiunto un massimo di \$43,06 al barile solo a novembre 2020.

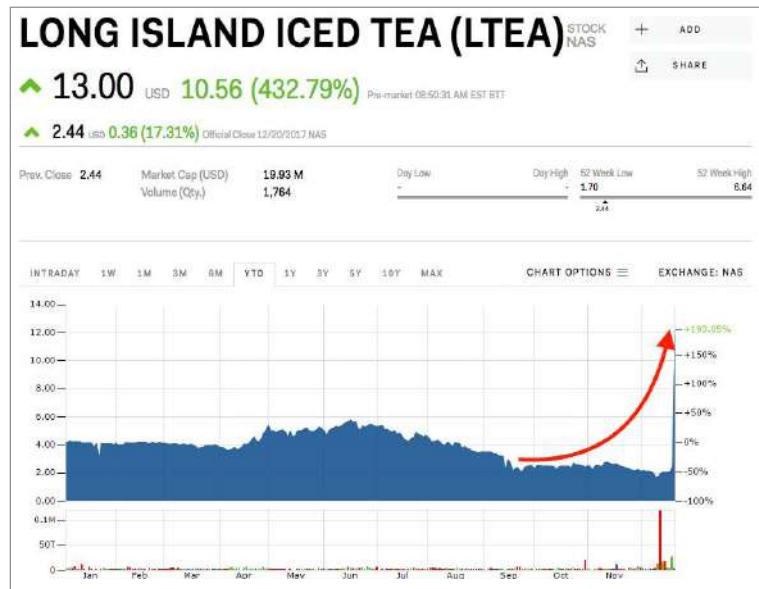
Questo altro esempio, in cui il valore di un bene è stato considerato negativo dal mercato è un ulteriore prova che il processo di misurazione di un bene non è determinato solo dal costo di produzione o dal prezzo di mercato, ma anche **dalle relazioni sociali, culturali e simboliche che si creano intorno ad esso. Spesso, inoltre, guidato da spinte irrazionali e dalle poche informazioni presenti in una determinata circostanza.**

Un ulteriore scenario in cui si è dimostrato che il mercato sia poco razionale e guidato da una forte **asimmetria informativa** è l'episodio di Long Blockchain Corp. Nel 21 Dicembre 2017, Long Island Iced Tea Corp decidere di fare **un rebranding della propria ragione sociale in Long Blockchain Corp.** Secondo un'analisi di Ars Technica, questo avvenimento è simile al modo in cui le aziende alla fine degli anni '90 hanno aumentato i loro prezzi delle azioni semplicemente aggiungendo ".com" ai loro nomi.



Asimmetria informativa

L'asimmetria informativa è una condizione in cui un'informazione non è condivisa integralmente fra gli individui facenti parte dello stesso processo economico: dunque una parte degli agenti interessati dispone di maggiori informazioni rispetto al resto dei partecipanti e può trarre un vantaggio da questa configurazione.



A distanza di anni, il titolo in borsa di Long Blockchain Corp, un picco di + 193%, quando ha annunciato il rebranding, è crollato arrivando ai minimi storici, **dimostrando la completa irrazionalità del mercato al momento del cambio di nome.**



Per riassumere, gli esempi riportati ci fanno intuire come sia complesso la misurazione e la determinazione del valore di un bene tangibile, intangibile, di un asset finanziario al giorno d'oggi e come le masse siano facilmente suscettibili a forti cambiamenti, spesso guidati da poche informazioni e da istinti irrazionali durante questo processo. Per concludere, il **processo di definizione di ciò che ha valore o meno è sempre strettamente legato a dinamiche complesse, emotive e sociali.**

Fonti

- ▶ <https://www.bbc.com/news/business-52350082>
- ▶ https://arstechnica.com/tech-policy/2017/12/iced-tea-company-stock-triples-after-adding-blockchain-to-name/?utm_content=buffer1ae54&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
- ▶ <https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain#xj4y7vzkg>

2

Il modello di maturità del mercato Web3

- 2.1 L'evoluzione del mercato finanziario Web3
- 2.2 Quali sono le asset class nel Web3?
- 2.3 ICO VS IPO: le differenze
- 2.4 IPO di Coinbase
- 2.5 Approfondimento dei servizi della finanza decentralizzata
- 2.6 Come si muovono i player nel mercato Web3 e dei digital assets?

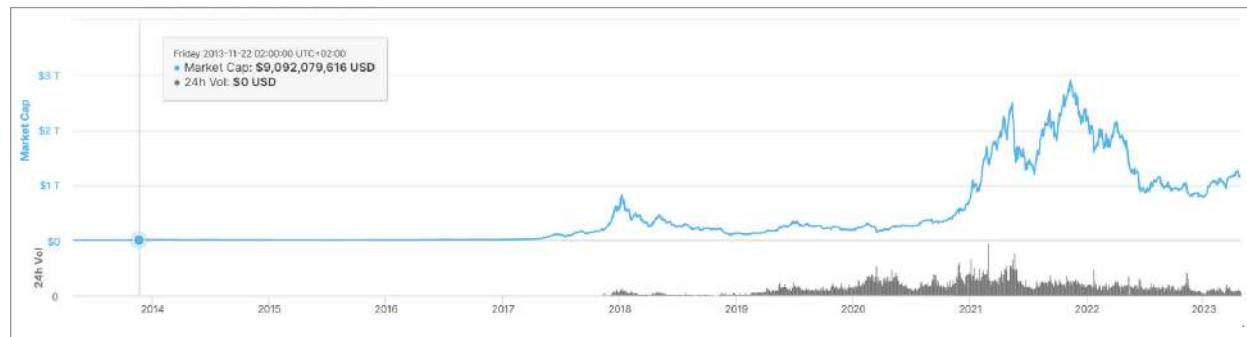
2.1

Business

● Basic

L'evoluzione del mercato finanziario Web3

Dal 2015, il mercato dei digital asset ha visto **un'esplosione di interesse e attenzione da parte di investitori, regolatori, aziende tecnologiche e media finanziari**. In basso, il grafico mostra la capitalizzazione di mercato totale di tutti i digital, inclusi stablecoin e token. Ad oggi (26/04/2023), il numero di digital asset nel mercato sono oltre 23.000, scambiate in oltre 619 exchange centralizzati e decentralizzati.

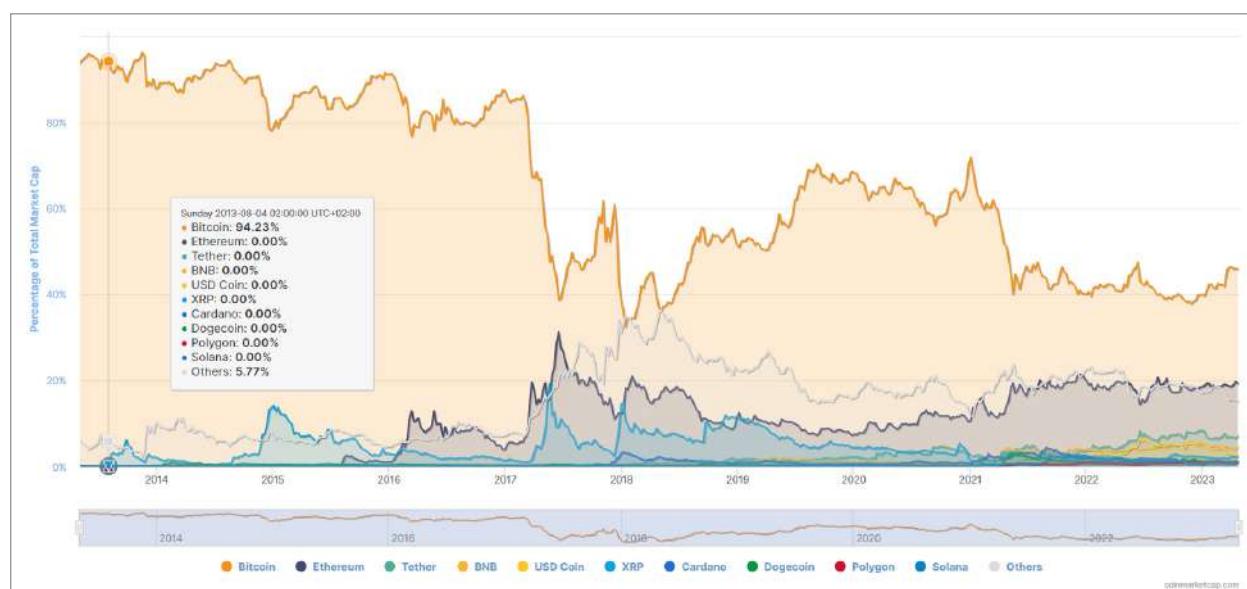


Il grafico sottostante mostra invece la distribuzione di capitali distribuita tra i dieci digital asset più capitalizzati. BTC rimane il primo asset per capitalizzazione, ed è rimasto per tutti questi anni il più grande del mercato, motivo per cui il suo dominio è un parametro seguito da molte persone (ie. Bitcoin Dominance). Inoltre, un ulteriore aspetto per cui è molto seguito, riguarda il susseguirsi degli **halving**.



Halving

Dal verbo inglese “to halve”, ovvero “dividere in due parti di dimensioni uguali o approssimativamente uguali”



Gli halving per Bitcoin sono eventi programmati in cui la ricompensa per i minatori che confermano le transazioni sulla rete Bitcoin viene dimezzata. Questo avviene ogni 10.000 blocchi estratti, ovvero circa ogni quattro anni. L'ultimo halving è avvenuto nel maggio 2020, portando la ricompensa per i minatori da 12,5 a 6,25 Bitcoin per blocco estratto.

Questo meccanismo di riduzione della ricompensa è stato progettato per rendere gli asset digitali come Bitcoin scarsamente programmabili, ovvero limitati nella loro offerta.



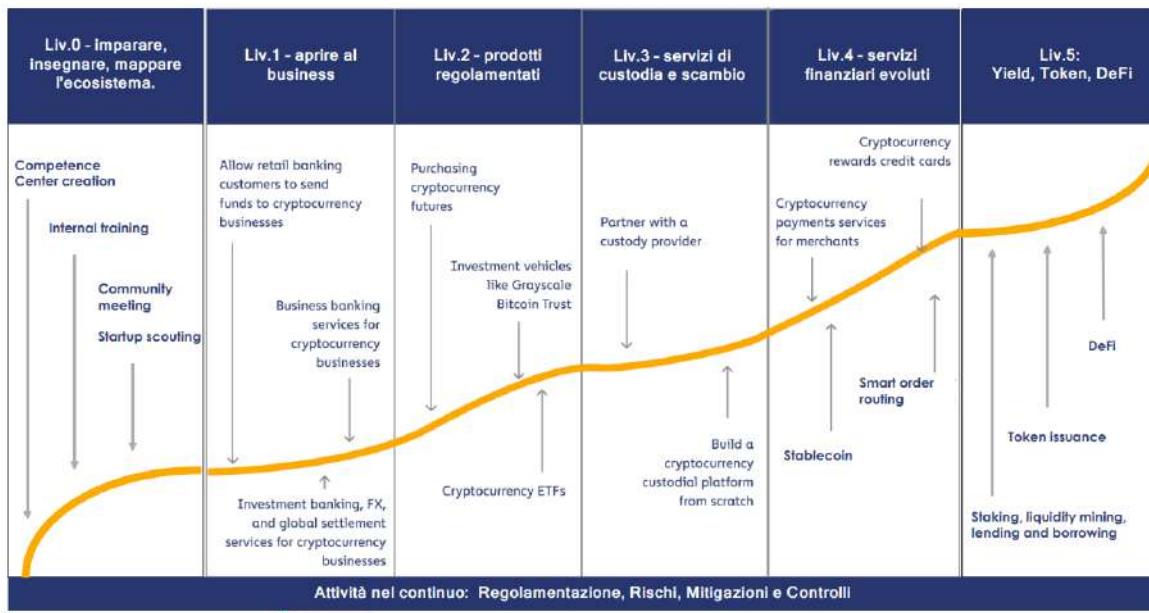
Questi avvenimenti periodici scandiscono ogni era del mercato dei digital asset poiché:

- Rappresenta un cambiamento significativo nella dinamica dell'offerta di Bitcoin, digital asset primo per "dominance"
- C'è una buona correlazione tra la crescita del valore di Bitcoin con quello dell'intera industria dei digital asset

Dalla nascita di Bitcoin nel 2009 ad oggi, diversi trend di mercato si sono verificati nell'industria, come riporta la tabella in basso riportata. La maturità stessa del mercato si sta sedimentando anno dopo anno con l'introduzione di nuove tecnologie e nuovi modelli di business possibili per tutti gli stakeholders all'interno dell'industria e nei diversi settori.



Questa evoluzione dei servizi porta necessariamente un continuo aggiornamento delle tecnologie e delle soluzioni possibili, per tutti quei soggetti che hanno interesse nell'entrare nell'industria con soluzioni tecnologiche e finanziarie.



Per concludere, infatti, il percorso che normalmente gli operatori finanziari tradizionali si trovano ad affrontare quando approcciano l'ecosistema dei digital asset è scandito da diversi livelli, definibili all'interno della tabella in alto riportata.

2.2

Teoria Finanziaria

• Basic

Quali sono le asset class nel Web3?

Il termine **Web 2.0** viene utilizzato per descrivere l'evoluzione del World Wide Web dalla sua fase iniziale di sviluppo statico di pagine web verso una fase più dinamica e interattiva in cui gli utenti sono diventati parte integrante della creazione e condivisione di contenuti online. Le principali asset class all'interno del mondo Web 2.0 includono:

- **Social media:** Le piattaforme di social media sono tra le più diffuse e popolari del Web 2.0. Questi servizi consentono agli utenti di creare e condividere contenuti, connettersi con altre persone, partecipare a discussioni e creare reti sociali.
- **Video sharing:** I siti di video sharing, come YouTube, consentono agli utenti di caricare e condividere video online, offrendo l'opportunità di accedere a contenuti di intrattenimento, educativi o informativi.
- **Blog:** I blog sono siti web in cui gli utenti possono creare e condividere contenuti in modo informale, spesso utilizzando un tono di voce personale e approfondendo specifici argomenti di interesse.
- **E-commerce:** Le piattaforme di e-commerce offrono un'ampia varietà di prodotti e servizi online, consentendo agli utenti di effettuare acquisti da qualsiasi luogo e in qualsiasi momento.
- **Search engine:** I motori di ricerca, come Google, consentono agli utenti di accedere a una vasta gamma di informazioni e contenuti online, rendendoli uno strumento indispensabile per la navigazione e la ricerca di informazioni in rete.
- **Messaging e comunicazione:** I servizi di messaggistica e comunicazione, come WhatsApp e Skype, consentono agli utenti di comunicare in tempo reale tramite messaggi testuali, chiamate vocali o videochiamate, senza limiti geografici.

L'importanza di queste asset class all'interno del mondo Web 2.0 si riflette nel loro impatto sulla società e sulla cultura digitale, oltre che sulle opportunità di business e sulle modalità di interazione tra individui e organizzazioni. La loro evoluzione continua a plasmare la forma e il futuro del Web 2.0 e del mondo digitale nel suo complesso.

Le asset class del Web2 e del Web3 sono diverse a causa delle caratteristiche distintive di queste due fasi di sviluppo delle tecnologie informatiche e digitali.

Il **Web2 è caratterizzato da applicazioni web centralizzate e da una struttura a due livelli**, ovvero un livello client e un livello server, che gestiscono la maggior parte delle funzionalità. Le asset class del Web2 sono pertanto focalizzate su prodotti e servizi che si basano su questa struttura centralizzata, come ad esempio i social network, le applicazioni di messaggistica istantanea, le piattaforme di e-commerce, i motori di ricerca e le piattaforme di video sharing.

Il **Web3, al contrario, è caratterizzato dalla decentralizzazione delle applicazioni web e dall'uso di tecnologie blockchain**, che consentono la creazione di una rete di nodi peer-to-peer per la gestione dei dati e delle transazioni. Le asset class del Web3 sono quindi incentrate sui prodotti e servizi che sfruttano questa struttura decentralizzata, in particolare sulle applicazioni decentralizzate (dApps), i protocolli di blockchain, i token non fungibili, digital asset di varia natura.

Inoltre, nel **Web3 è presente una distinzione tra layer 1 e layer 2**. Il **layer 1 si riferisce alla blockchain di base, come ad esempio Bitcoin o Ethereum, mentre il layer 2 si riferisce alle soluzioni di scaling e di interoperabilità costruite sopra la blockchain di base**. Le asset class del layer 1 sono quindi incentrate sulla creazione e gestione di nuove blockchain, mentre quelle del layer 2 si concentrano sulla creazione di soluzioni di scaling e interoperabilità tra blockchain.

2.3 ICO VS IPO: le differenze

Teoria Finanziaria

● Medium

Ci sono una serie di passi legali e normativi che devono essere seguiti per effettuare un IPO e quotarsi in borsa, che possono variare in base al paese di riferimento. Ecco una **panoramica generale dei passi principali**:

1. **Scelta del mercato di quotazione:** la società deve scegliere il mercato di quotazione in cui intende quotarsi. Ad esempio, in Italia si può scegliere tra la Borsa Italiana o il mercato AIM Italia.
2. **Selezione dei consulenti:** la società dovrà selezionare un team di consulenti per aiutarla a portare a termine l'IPO. In genere, il team comprende una banca d'affari, un avvocato specializzato in diritto societario, un revisore contabile e un'agenzia di comunicazione.
3. **Preparazione della documentazione:** la società deve preparare una serie di documenti, tra cui il prospetto informativo, che descrive l'azienda e il suo business, le sue prospettive future, le azioni offerte e le condizioni dell'offerta.
4. **Valutazione della società:** la società dovrà farsi valutare da una banca d'affari o da un esperto indipendente per determinare il prezzo delle azioni offerte e stabilire la quantità di azioni da offrire.
5. **Approvazione del prospetto informativo:** il prospetto informativo deve essere approvato dall'autorità di vigilanza del mercato di riferimento (in Italia, la CONSOB) prima che l'offerta possa essere lanciata.
6. **Roadshow:** la società dovrà organizzare una serie di incontri con gli investitori per promuovere l'IPO e presentare il business dell'azienda.
7. **Lancio dell'offerta:** la società lancia l'offerta di azioni e aspetta che gli investitori presentino le loro richieste di acquisto.
8. **Allotment:** una volta terminate le richieste di acquisto, la società stabilisce il prezzo delle azioni e l'ammontare delle azioni da allocare ad ogni investitore.

9. **Quotazione in borsa:** le azioni vengono messe in commercio e inizia la negoziazione sul mercato di riferimento.

Questi sono i passi principali per effettuare un IPO. Tuttavia, è importante notare che le regole e i requisiti possono variare in base al paese di riferimento e alla normativa vigente. In ogni caso, l'aiuto di un team di consulenti esperti è fondamentale per portare a termine l'operazione in modo efficace e conforme alle regole. Una **ICO** (Initial Coin Offering) è un tipo di raccolta di fondi che si basa sulla vendita di token digitali emessi da una società o un progetto basato sulla blockchain. Premettendo che alle ICO di digital assets qualificabili come prodotti finanziari si applicano le medesime regole delle IPO, di seguito sono descritti i **passi principali per lanciare una ICO online senza considerarne gli impatti ed i relativi obblighi normativi:**

- **Pianificazione e preparazione:** la società o il progetto dovrebbe avere un piano dettagliato che descrive le finalità dell'ICO, le condizioni dell'offerta, la quantità e il prezzo dei token, la durata dell'ICO e i criteri di distribuzione dei fondi raccolti.
- **Creazione del token:** la società o il progetto deve creare il token digitale, definirne le caratteristiche tecniche (come il tipo di blockchain utilizzato, il protocollo di consenso e le funzioni di utilizzo) e stabilire il suo valore di mercato.
- **Creazione del white paper:** il white paper è un documento che descrive il progetto in dettaglio, illustrando i suoi obiettivi, il team, la tecnologia e il modello di business. Il white paper deve essere chiaro e convincente, al fine di attirare l'attenzione degli investitori.
- **Creazione del sito web dell'ICO:** il sito web dell'ICO deve contenere tutte le informazioni relative all'offerta, tra cui il white paper, le condizioni dell'offerta, le modalità di partecipazione e le informazioni sul team.
- **Marketing e promozione:** la società o il progetto deve promuovere l'ICO attraverso diversi canali di marketing, come annunci sui social media, pubblicità online, eventi e influencer marketing.
- **Lancio dell'ICO:** la società o il progetto lancia l'offerta di token e aspetta che gli investitori presentino le loro richieste di acquisto. A differenza dell'IPO, l'ICO viene solitamente lanciata online, senza l'intermediazione di una banca d'affari.
- **Allotment:** una volta terminate le richieste di acquisto, la società o il progetto stabilisce il prezzo dei token e l'ammontare dei token da allocare ad ogni investitore.
- **Distribuzione dei token:** una volta effettuato il pagamento, i token vengono distribuiti agli investitori.
- **Quotazione dei token:** i token vengono emessi su un exchange di digital assets e inizia la negoziazione sul mercato.

Sia la IPO che la ICO prevedono una fase di marketing e promozione, ma la **ICO tende ad essere più focalizzata sulla creazione di una comunità di sostenitori che possono diffondere la notizia della raccolta di fondi attraverso i social media.**

2.4 IPO di Coinbase

Business

Basic

Coinbase è una delle più grandi piattaforme di scambio di digital assets al mondo e il suo successo ha suscitato un grande interesse tra gli investitori. L'azienda ha avuto il suo Initial Public Offering (IPO) sulla borsa NASDAQ il 14 aprile 2021, con una capitalizzazione di mercato di \$85,8 miliardi al momento dell'apertura delle contrattazioni.

Secondo i dati della SEC (Securities and Exchange Commission), l'offerta pubblica iniziale di Coinbase ha raccolto \$3,7 miliardi, diventando così la più grande IPO di una società tecnologica statunitense degli

ultimi quattro anni. L'offerta pubblica iniziale di Coinbase ha attratto un'ampia base di investitori istituzionali, compresi fondi pensione, hedge fund e banche d'investimento.



Secondo uno studio condotto da Pipsay, una società di ricerche di mercato, il 41% degli americani aveva sentito parlare dell'IPO di Coinbase, mentre solo il 12% degli intervistati aveva mai utilizzato la piattaforma per l'acquisto o la vendita di digital assets. Tuttavia, il 62% degli intervistati ha dichiarato di avere almeno una conoscenza basilare in materia.

Per concludere, l'IPO di Coinbase ha portato alla luce come l'interesse rispetto a questa nuova industria non comprenda soltanto il mercato retail, ma anche parte di investitori istituzionali, che vedono una possibile prospettiva espansiva per aziende operanti con digital asset e DLT.

2.5

Informatica / Business

● Medium

Approfondimento dei servizi della finanza decentralizzata

Il mondo dei digital asset ha offerto nuove modalità di investimento partecipative e del tutto nuove rispetto alla finanza tradizionale e le applicazioni web2. Andiamo ad approfondire dal punto di vista tecnico-finanziario il funzionamento di questi protocolli:

- **Lo staking è un processo in cui un utente blocca una quantità di digital asset come garanzia per verificare le transazioni sulla blockchain e ricevere ricompense sotto forma di interessi o token.** Dal punto di vista finanziario, lo staking può rappresentare una **forma di investimento a basso rischio e a lungo termine**, in cui l'utente guadagna ricompense passive per il suo coinvolgimento nella rete. Tuttavia, l'utente corre il rischio di perdere parte o tutto il suo investimento se il digital asset perde valore o se la rete fallisce.
- **Le liquidity pool sono un meccanismo in cui gli utenti depositano fondi in una cassaforte virtuale, chiamata "pool", per fornire liquidità ai mercati di scambio decentralizzati (DEX).** In cambio, ricevono una quota delle commissioni di transazione generate dai trader che utilizzano il pool. Dal punto di vista finanziario, le liquidity pool rappresentano un'opportunità per gli utenti di guadagnare

- rendimenti passivi sui loro digital asset**, mentre contribuiscono all'efficienza del mercato decentralizzato. Tuttavia, esiste il rischio di perdere parte o tutto il proprio investimento a causa di fluttuazioni del prezzo delle digital asset o di perdite derivanti da hack o errori di codice.
- **Il farming è un processo in cui gli utenti depositano fondi in una liquidity pool o in un protocollo di yield farming per guadagnare ricompense sotto forma di token di governance o altre digital asset.** Dal punto di vista finanziario, il farming rappresenta un'**opportunità per gli utenti di guadagnare rendimenti elevati sulla loro digital asset, ma con un rischio maggiore rispetto allo staking o alle liquidity pool**. I rendimenti elevati possono essere il risultato di una maggiore esposizione al rischio, che può essere causato da una varietà di fattori, tra cui fluttuazioni dei prezzi dei digital assets, perdite di sicurezza o errori di codice.
 - **Il peer-to-peer lending è un processo in cui gli utenti possono prestare o prendere in prestito digital asset da altri utenti su una piattaforma decentralizzata.** Gli utenti che prestano digital asset guadagnano interessi sul prestito, mentre gli utenti che prendono in prestito pagano un tasso di interesse. Dal punto di vista finanziario, il peer-to-peer lending rappresenta un'**opportunità per gli utenti di guadagnare interessi sulla loro digital asset, ma con un rischio maggiore rispetto allo staking o alle liquidity pool**. Il rischio maggiore deriva dalla possibilità che gli **utenti che prendono in prestito non riescano a restituire il prestito**, causando una perdita per gli utenti che prestano. Inoltre, il prestito può essere soggetto a fluttuazioni del prezzo dei digital assets, il che può aumentare ulteriormente il rischio.

Tutti questi servizi di finanza decentralizzata, nonostante siano già ampiamente presenti nel mercato, vedendo moltissimo liquidità “bloccata” all'interno di queste soluzioni, non sono ancora chiaramente regolamentati e questo alimenta la possibilità di applicazioni fraudolente e poco sicure per tutti gli stakeholders coinvolti.

2.6

Business

• Basic

Come si muovono i player nel mercato Web3 e dei digital assets?

I **digital asset sono un fenomeno relativamente nuovo** nel mondo finanziario e, di conseguenza, le **istituzioni finanziarie stanno ancora cercando di capire il loro ruolo in questo nuovo ecosistema**.

In primo luogo, **molte istituzioni finanziarie tradizionali, come banche e società di investimento, stanno iniziando a offrire servizi di trading e di custodia di digital asset ai propri clienti**. Questo è dovuto al crescente interesse da parte dei clienti nel possedere questi nuovi asset digitali e alla necessità di questi clienti di avere un modo sicuro e affidabile per acquistarle e conservarle.

In secondo luogo, **molte istituzioni finanziarie stanno iniziando a esplorare l'uso delle digital asset come forma di investimento**. Ad esempio, diverse società di investimento stanno iniziando a offrire fondi negoziati in borsa (ETF) che seguono l'andamento dei prezzi delle digital asset come bitcoin, consentendo agli investitori di ottenere esposizione al mercato attraverso i propri portafogli di investimento.

Tuttavia, il ruolo delle istituzioni finanziarie nel mondo delle digital asset non è privo di contraddizioni. Ad esempio, nel 2018 il CEO di un primario istituto finanziario internazionale ha affermato che Bitcoin e gli altri asset digital sono “solo una frode” e ha avvertito i propri clienti di non aver nessun nell'investire in esse, sia a titolo personale che come strategia del proprio gruppo finanziario. Tuttavia, qualche anno dopo, sempre Jamie Dimon ha dichiarato di aver maturato dell'interesse rispetto all'evoluzione dell'industria e nell'offerta di servizi finanziari legati a quest'ultima.

Molte istituzioni finanziarie si trovano in una posizione difficile nel tentativo di bilanciare l'adozione con la gestione dei rischi di non conformità derivanti dall'incertezza regolamentare in materia.

In conclusione, le istituzioni finanziarie stanno giocando un ruolo sempre più importante nel mondo dei digital asset, sia come fornitori di servizi ai clienti che come investitori. Tuttavia, l'**adozione da parte delle istituzioni finanziarie rimane ancora in fase di sviluppo** e sarà interessante vedere come evolverà questa tendenza nel corso dei prossimi anni.

3

I servizi del mondo banking nel mercato Web3

- 3.1 Accesso al mercato dei digital assets e volumi a confronto
- 3.2 Come possono essere classificati i digital assets?
- 3.3 Quali sono i revenue model dei DEX e dei CEX?
- 3.4 Utility token come revenue model: il caso BNB
- 3.5 La tokenizzazione di assets
- 3.6 Tra il Web2 e il Web3: la custodia dei digital assets
- 3.7 Tra il Web2 e il Web3: on-ramp e smart order routing nel Web3
- 3.8 Tra il Web2 e il Web3: come costruire un digital asset backed security?

3.1

Business
Basic

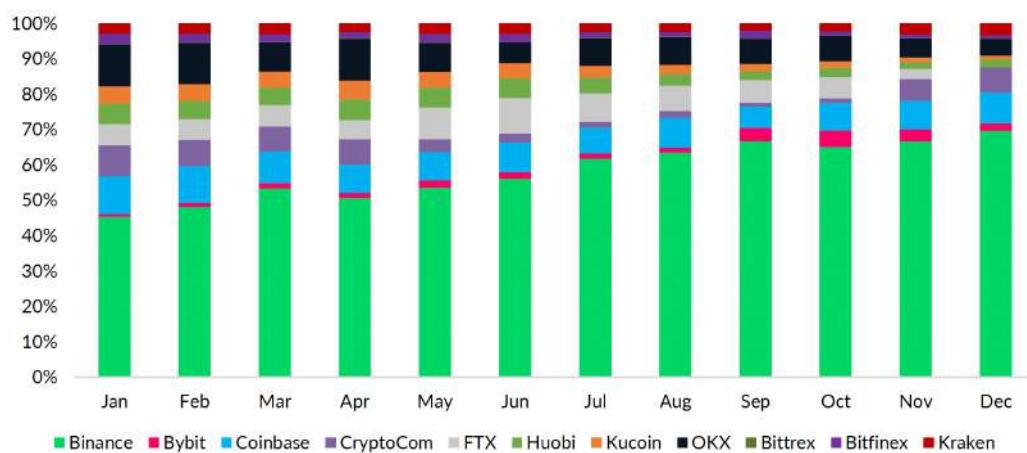
Accesso al mercato dei digital assets e volumi a confronto

Ad oggi, la maggior parte degli stakeholder che sono interessanti ad acquistare dei digital asset si affidano ad exchange, sparsi oggi in tutto il globo. Da un punto di vista non formale, gli exchange di digital asset e le borse valori condividono diverse analogie. Eccene alcune:

- **Entrambi sono mercati dove è possibile comprare e vendere asset attraverso l'incontro tra domanda e offerta:** le borse valori offrono azioni, obbligazioni, fondi comuni di investimento e altri strumenti finanziari, mentre gli exchange di digital asset permettono di comprare e vendere Bitcoin, Ethereum e Litecoin e altri digital asset.
- **Entrambi utilizzano gli ordini di acquisto e vendita:** gli investitori possono inserire ordini di acquisto e vendita per comprare o vendere asset sulla base delle loro analisi di mercato.
- **Entrambi possono essere influenzati dalle notizie di mercato:** come le borse valori, gli exchange di digital asset possono essere influenzati dalle notizie economiche, politiche e di altro tipo.

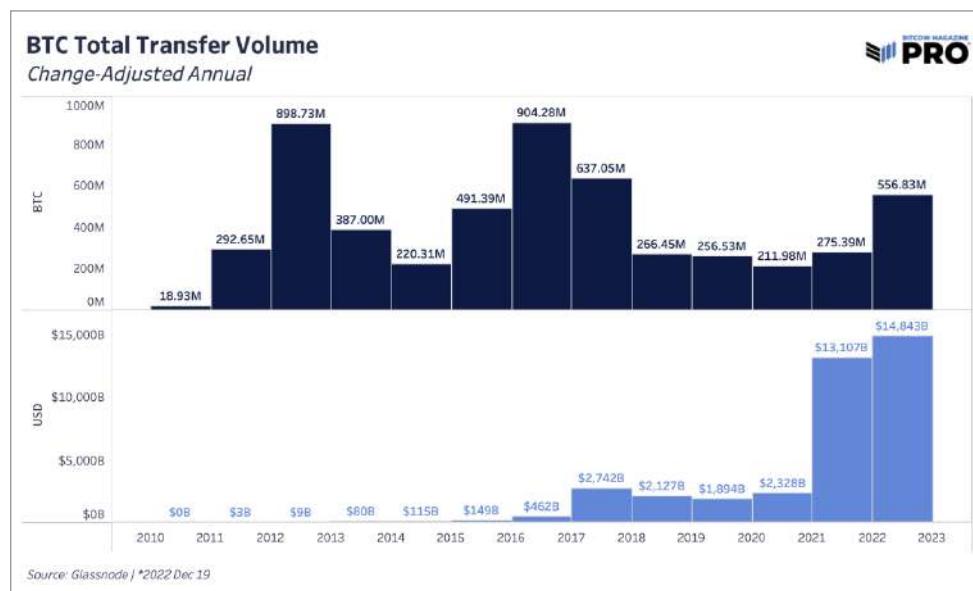
Qui di seguito, una tabella con i market share dei principali exchange di digital asset utilizzati dagli utenti fino al 2022:

Figure 3 – Monthly Market Share of Analysed Exchanges, 2022



Una delle principali differenze con le borse tradizionali, sta nel fatto che gli exchange permettono all'utente di generare un wallet e/o trasferire verso altri wallet i propri digital asset. La gestione delle digital asset rimane quindi discrezionale all'utente rispetto alla modalità di custodia, se direttamente dall'exchange o effettuare solamente la compra vendita e poi traferirli in wallet proprietari.

Ecco una tabella con i volumi dal 2010 al 2022 di bitcoin, rappresentati come unità singole e come controvalore in dollaro, con i dati presi da Glassnode:



Esistono anche ulteriori metodi consentono l'acquisto di digital asset in un modo più tangibile e immediato:

- **Bancomat Bitcoin:** I bancomat bitcoin, noti anche come BTM (Bitcoin Teller Machines), funzionano in modo simile ai tradizionali bancomat. Gli utenti possono acquistare Bitcoin inserendo denaro contante o una carta di credito/debito nel bancomat e ricevendo in cambio bitcoin direttamente nel loro portafoglio digitale. Alcuni dei principali fornitori di BTM includono CoinFlip, General Bytes e Lamassu. Questi bancomat sono distribuiti in tutto il mondo, con una concentrazione particolarmente alta negli Stati Uniti;
- **Voucher Bitcoin:** I voucher bitcoin sono un altro metodo per acquistare questi digital asset. Questi voucher, che possono essere acquistati in negozi fisici o online, contengono un codice che può essere riscattato per Bitcoin su un sito web specifico. Bitnovo e Azteco sono due esempi di servizi che offrono voucher Bitcoin. Questi voucher possono essere un regalo ideale per coloro che sono interessati a entrare nel mondo dei digital assets;
- **Transazioni fisiche:** Infine, è possibile acquistare Bitcoin attraverso transazioni fisiche con un altro individuo, facilitate dalla partecipazione di community online su piattaforme come Facebook, Reddit o Bitcointalk.

Inoltre, la compra-vendita di digital asset può comprendere anche piattaforme OTC o, come abbiamo visto in precedenza, direttamente in protocolli di finanza decentralizzata attraverso l'uso di complessi smart contract.

Alcune delle soluzioni precedentemente citate, in maniera quasi analoga alle borse tradizionali, sono soggetti a diverse normative in materia di antiriciclaggio (AML) e di finanziamento del terrorismo (CFT), sia in Europa che negli Stati Uniti. Alcuni dei **rischi legali e di compliance** che gli exchange devono affrontare includono:

- **Identificazione dell'utente:** gli exchange devono identificare i propri utenti, anche attraverso l'utilizzo di controlli di conoscenza del cliente (KYC) e di controlli di verifica dell'identità (IDV). Questo può comportare la raccolta di una serie di informazioni personali, come il nome, l'indirizzo, la data di nascita e il numero di telefono, che devono essere verificate e mantenute in modo sicuro.
- **Monitoraggio delle transazioni:** gli exchange devono monitorare le transazioni che si verificano sulla loro piattaforma per individuare eventuali attività sospette e segnalare tali attività alle autorità competenti. Questo comporta l'implementazione di sistemi di monitoraggio delle transazioni (TMS) e di altre misure di sicurezza, come l'individuazione dei pattern di comportamento anomalo.
- **Conformità alle normative AML/CFT:** gli exchange devono rispettare le normative AML/CFT sia in Europa che negli Stati Uniti. Ciò significa che devono attuare misure di controllo interne, adottare politiche e procedure adeguate e formare il proprio personale su queste normative.

- **Conformità alle leggi sulla privacy:** gli exchange devono rispettare le leggi sulla privacy e proteggere le informazioni personali dei propri utenti in modo sicuro.
- **Rischio di frode:** gli exchange devono proteggersi contro il rischio di frode e di attività illegali, come il riciclaggio di denaro e il finanziamento del terrorismo.
- **Licenze e autorizzazioni:** in alcuni paesi, gli exchange di digital asset sono soggetti a licenze e autorizzazioni specifiche. Mentre negli Stati Uniti, gli exchange devono ottenere una licenza dallo stato in cui operano.

È importante notare che il mondo dei digital asset è ancora in fase di evoluzione e che molte questioni relative alla regolamentazione e alla normativa dei prestatori di servizi devono ancora essere definite dalle autorità competenti.

3.2

Legal

● Medium

Come possono essere classificati i digital assets?

All'interno degli exchange di digital asset è possibile trovare un'elevata quantità di essi, relativa a differenti progetti e differenti startup. La seguente tabella rappresenta le principali tipologie di token all'interno del mondo dei digital assets, suddivisi in quattro macrocategorie: payment token, utility token, security token e governance token.

La classificazione dei digital asset (o cripto attività), ai sensi MiCAR, è la seguente:

- **Utility token o token di utilità:** “un tipo di cripto-attività destinato unicamente a fornire l'accesso a un bene o a un servizio prestato dal suo emittente”;
- **Asset Reference Token (ART) o Token con riferimento all'attività (cd. Stablecoin):** “un tipo di cripto-attività che non è un token di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali”;
- **E-money Tokens o Token di moneta elettronica:** “un tipo di cripto-attività che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale”.

Non sono disciplinati dalla MiCAR:

- Strumenti finanziari digitali o Token rappresentativi di strumenti finanziari, i quali devono essere a tutti gli effetti ricompresi nella definizione di cui all'articolo 4, paragrafo 1, punto 15, di cui alla Direttiva 2014/65/UE (MiFID II). Sono a tutti gli effetti strumenti finanziari – e soggetti alla normativa in materia - anche quelli emessi in formato digitale ai sensi del D.L. 25 del 17 marzo 2023 (c.d. decreto fintech).

Tuttavia, la definizione di MICA è solo circoscritta al territorio europeo. Senza utilizzare la tassonomia normativa, i digital assets sono stati classificati in maniera differente dal mercato, spesso attraverso questa nomenclatura:

- I **payment token sono progettati per fungere da mezzo di pagamento** in un ecosistema specifico e consentono il trasferimento di valore tra parti senza la necessità di intermediari.
- Gli **utility token sono utilizzati all'interno di un ecosistema specifico per fornire** accesso digitale a un bene o servizio disponibile su una DLT (Distributed Ledger Technology o tecnologia di registro distribuito) e sono accettati solo dall'emittente di quel token (“utility tokens”). Tali “utility tokens” hanno scopi non finanziari, legati al funzionamento di una piattaforma digitale e di servizi digitali e

dovrebbero essere considerati come un tipo specifico di cripto attività. Solitamente, gli utility token sono **emessi inizialmente attraverso una ICO** (cd. Initial Coin Offering) o IEO (cd. Initial Exchange Offering) e possono essere scambiati in exchange. **Ethereum è un esempio di utility token**, in quanto viene utilizzato per sostenere i costi di transazione e la all'interno della piattaforma Ethereum.

- Con il termine **security token si fa generalmente riferimento rappresentazioni su DLT di strumenti finanziari tipizzati dalla normativa in materia.**

Tipo di token	Esempi
<i>Utility Token</i>	<i>Binance Coin (BNB), Filecoin (FIL), Basic Attention Token (BAT)</i>
<i>Security Token</i>	<i>tZero (TZRO), Blockchain Capital (BCAP), SPiCE VC (SPICE)</i>
<i>Stablecoin</i>	<i>Tether (USDT), USD Coin (USDC), Dai (DAI)</i>
<i>Non-Fungible Token (NFT)</i>	<i>CryptoKitties, Axie Infinity, NBA Top Shot</i>
<i>Governance Token</i>	<i>Maker (MKR), Compound (COMP), Uniswap (UNI)</i>
<i>Payment Token</i>	<i>Bitcoin (BTC), Litecoin (LTC), Dash (DASH)</i>

In conclusione, le direttive come la MICA persegono l'obiettivo di fornire maggiore chiarezza in questo settore, cercando di classificare i digital asset in macrocategorie e cercando di definire le responsabilità e gli obblighi di tutti gli operatori nel settore che abilitato gli utenti a acquistare, vendere e gestire i propri asset digitali. Tuttavia, risulta ancora definire la natura di alcuni digital asset in quanto la loro stessa essenza è ibrida, compresa la logica della propria tokenomics.

3.3

Business

• Basic

Quali sono i revenue model dei DEX e dei CEX?

Se dovessimo eviscerare ogni exchange ed estrarre da esso la lista di **servizi offerti ai propri clienti**, inserendo i servizi comuni e/o i servizi individuabili in almeno un exchange, quella di seguito sarebbe la lista:

- **Trading:** tutti gli exchange offrono la possibilità di acquistare e vendere digital assets. Alcuni exchange offrono anche il trading di margini, e l'acquisto di token non fungibili (NFT).
- **Deposito e prelievo di digital asset:** tutti gli exchange permettono di depositare e prelevare digital asset.
- **Wallet:** molti exchange offrono un wallet integrato per conservare i digital assets. Tuttavia, non sempre la gestione dei digital asset da parte di questi operatori è trasparente.
- **Analisi di mercato:** alcuni exchange offrono strumenti di analisi di mercato per aiutare gli utenti a prendere decisioni di trading.
- **Staking:** alcuni exchange offrono il servizio di staking, che consente agli utenti di guadagnare interessi sui propri digital asset.
- **Lending:** alcuni exchange offrono il servizio di prestito, che consente agli utenti di prendere in prestito digital assets a tassi di interesse competitivi.
- **Servizi di pagamento:** alcuni exchange offrono servizi di pagamento in digital assets.

- **Servizi di sicurezza:** tutti gli exchange offrono servizi di sicurezza, come l'autenticazione a due fattori e la verifica dell'identità per proteggere gli account degli utenti.
- **Programmi di affiliazione:** alcuni exchange offrono programmi di affiliazione, che permettono agli utenti di guadagnare una percentuale delle commissioni dei propri referral.
- **Servizi di customer support:** tutti gli exchange offrono servizi di customer support per aiutare gli utenti a risolvere eventuali problemi. Alcuni exchange offrono anche servizi di supporto premium per i propri utenti.
- **OTC trading:** alcuni exchange offrono il servizio di trading OTC (Over-the-counter), che consente di scambiare digital asset al di fuori delle normali piattaforme di trading pubbliche, ad esempio per effettuare scambi di grandi volumi.
- **Servizi di gestione del portafoglio:** alcuni exchange offrono servizi di gestione del portafoglio che consentono agli utenti di delegare la gestione dei propri digital assets.
- **Servizi di tokenizzazione:** alcuni exchange offrono servizi di tokenizzazione, che consentono agli utenti di convertire asset tradizionali in token digitali, rendendoli negoziabili sulla blockchain.
- **Servizi di data analytics:** alcuni exchange offrono servizi di analisi dei dati relativi ai digital assets e al mercato, come l'analisi del volume di trading, l'andamento dei prezzi, le fluttuazioni di mercato e altro.
- **Servizi di prevenzione delle frodi:** alcuni exchange offrono servizi di prevenzione delle frodi, come l'analisi delle transazioni sospette e l'identificazione degli utenti fraudolenti.
- **Servizi di formazione:** alcuni exchange offrono servizi di formazione, come webinar, tutorial, corsi di trading e di analisi tecnica, per aiutare gli utenti a comprendere meglio il funzionamento dei digital assets e del trading.
- **Servizi di custodia istituzionale:** alcuni exchange offrono servizi di custodia per i propri clienti istituzionali.
- **Servizi di investimento automatico:** alcuni exchange offrono servizi di investimento automatico, che consentono agli utenti di creare un portafoglio basato su algoritmi di trading automatizzati.
- **Market making:** alcuni exchange decentralizzati offrono programmi di incentivazione per gli utenti che forniscono liquidità al mercato, attraverso l'uso di smart contract.
- **Yield farming:** alcuni exchange decentralizzati offrono programmi di yield farming che permettono agli utenti di guadagnare interessi sui propri depositi

In generale, gli **exchange guadagnano principalmente attraverso le commissioni di trading e di prelievo**, quindi le attività che generano maggiori profitti sono quelle legate al trading. In particolare, gli exchange possono guadagnare attraverso:

- **Commissioni di trading:** gli exchange applicano spesso una commissione sulla quantità di digital asset scambiate su di essi, generando una fonte di reddito per ogni transazione.
- **Commissioni di prelievo:** gli exchange possono applicare una commissione per il prelievo dal loro sistema, in modo da generare un profitto su ogni transazione di prelievo.
- **Margin trading:** alcuni exchange offrono la possibilità di fare trading con margine, ovvero di aprire posizioni di trading con fondi presi a prestito dall'exchange stesso, in cambio di una tassa di interesse. In questo modo l'exchange può guadagnare sulla differenza tra gli interessi pagati dagli utenti e quelli ricevuti dal prestito.
- **Servizi di listing:** alcuni exchange guadagnano attraverso i servizi di listing, ovvero l'inclusione di nuovi digital asset sulla piattaforma dell'exchange, che genera una commissione per il loro proprietario.
- **Programmi di referral:** alcuni exchange offrono programmi di referral che consentono agli utenti di guadagnare una percentuale delle commissioni generate dalle persone che si iscrivono all'exchange attraverso un loro invito.
- **Servizi premium:** alcuni exchange offrono servizi premium, come account con funzionalità avanzate o servizi di supporto dedicati, che generano una fonte di reddito aggiuntiva.

In generale, come detto precedentemente, le commissioni di trading e di prelievo sono le attività che generano il maggiore profitto per gli exchange; tuttavia, il profitto può variare significativamente in base alla dimensione dell'exchange, al volume di trading e ad altre variabili di mercato.

Per gli **exchange decentralizzati (DEX)**, le modalità con cui vengono generati i profitti sono diversi rispetto agli **exchange centralizzati**. Se gli exchange centralizzati guadagnano principalmente dalle commissioni di trading, i DEX possono guadagnare attraverso diverse fonti di revenue, tra cui:

- **Commissioni di trading:** come gli exchange centralizzati, i DEX guadagnano dalle commissioni di trading sui loro siti web.
- **Liquidità:** alcuni DEX incentivano gli utenti a fornire liquidità al mercato attraverso i loro programmi di incentivazione. Gli utenti che forniscono liquidità ricevono una quota degli interessi generati dagli scambi e dall'utilizzo di quella liquidità.
- **Governance token:** alcuni DEX emettono un token di governance che viene distribuito ai detentori di token che partecipano alla governance dell'exchange. Questo può portare ad un aumento del valore del token nel tempo e generare guadagni per gli utenti.
- **Staking:** alcuni DEX offrono programmi di staking che permettono agli utenti di guadagnare interessi sui propri depositi staccando i propri token. Questo può portare ad un aumento del valore del token e generare guadagni per gli utenti.
- **Token listing:** gli exchange decentralizzati possono richiedere un pagamento in token o in altri digital asset per elencare un nuovo token sul loro sito.

Inoltre, la più grande differenza con gli exchange centralizzati è la gestione dei digital asset. Infatti, all'interno di un DEX, i digital asset sono sempre gestiti e controllati dagli utenti tramite il wallet, il quale si connette al protocollo, senza lasciare in gestione queste ad una parte centralizzata.

3.4

Business

• Basic

Utility token come revenue model: il caso BNB

Un **utility token** ha lo scopo di fornire l'accesso digitale a un bene o servizio, disponibile su DLT, ed è accettato solo dall'emittente di quel token. **Spesso, tuttavia, questa tipologia di digital asset è stato anche utilizzato per raccogliere capitali per trovare nuova liquidità per finanziare lo sviluppo di nuovi servizi e applicazioni.** Nel contesto degli exchange di digital asset, sia per i centralizzati (CEX) che per i decentralizzati (DEX), un utility token fornisce all'utilizzatore della piattaforma diversi funzionalità come:

- **Pagamento di commissioni di trading:** le utility token possono essere utilizzate per pagare le commissioni di trading su un exchange. In questo modo, gli utenti possono utilizzare le loro utility token per effettuare gli scambi, e l'exchange può generare guadagni in utility token invece di denaro fiat.
- **Governance:** alcune utility token possono essere utilizzate per partecipare alla governance dell'exchange. Ad esempio, i detentori di token possono avere il diritto di votare sulle decisioni chiave dell'exchange, come la selezione di nuovi token da elencare.
- **Accesso a servizi premium:** alcune utility token possono essere utilizzate per accedere a servizi premium dell'exchange, come programmi di incentivi per la liquidità o servizi di analisi avanzata.

In un **exchange decentralizzato**, le utility token sono spesso utilizzate come mezzo di scambio primario all'interno dell'exchange stesso, e gli utenti possono guadagnare o perdere utility token in base alle loro attività di trading o di fornitura di liquidità. In un **exchange centralizzato**, le utility token possono essere utilizzate come mezzo di pagamento per le commissioni di trading e per l'accesso a servizi premium, ma la loro utilità può essere limitata in quanto l'exchange può accettare anche altre forme di pagamento, come denaro fiat o altri digital asset.

Un esempio pratico può essere il token di Binance **BNB**, il quale possiede diverse utilità all'interno della piattaforma Binance, tra cui:

1. **Utilizzo come mezzo di pagamento:** BNB può essere utilizzato per pagare le commissioni di trading sulle piattaforme Binance, ottenendo uno sconto del 25% rispetto all'utilizzo di altri digital assets o valute fiat.
2. **Accesso alle vendite di token (IEO):** Binance utilizza BNB per le vendite di token iniziali (IEO), dando priorità ai detentori di BNB per partecipare alle vendite.
3. **Partecipazione al programma di staking:** i detentori di BNB possono partecipare al programma di staking di Binance, che offre rendimenti annuali sui digital assets detenuti.
4. **Utilizzo come collaterale per i prestiti:** Binance consente ai detentori di BNB di utilizzarlo come collaterale per i prestiti in digital asset.
5. **Utilizzo per l'acquisto di beni e servizi:** BNB può essere utilizzato per acquistare beni e servizi su piattaforme che accettano BNB come metodo di pagamento.

Binance ha lanciato la propria ICO (Initial Coin Offering) di Binance Coin (BNB) nel luglio 2017, raccogliendo circa 15 milioni di dollari in digital assets. Inizialmente, sono stati creati 200 milioni di token BNB sulla blockchain di Ethereum, ma nel 2019, con il lancio della loro blockchain nativa Binance Chain, Binance ha avviato un processo di swap per trasferire i token BNB dalla blockchain di Ethereum alla nuova blockchain **Binance Chain**.

In termini di tokenomics, **inizialmente il token BNB è stato creato come utility token**, destinato ad essere utilizzato all'interno dell'ecosistema Binance, in particolare per pagare le commissioni di trading sulle piattaforme Binance. Inoltre, Binance ha implementato un programma di buyback e bruciatura trimestrale di BNB, in cui riacquista una quantità di BNB dal mercato e li distrugge, con l'obiettivo di ridurre l'offerta totale di BNB e aumentare il valore di ogni singolo token.

Con il passare del tempo, **Binance ha ampliato l'utilità di BNB all'interno dell'ecosistema**, aggiungendo funzionalità come l'utilizzo come collaterale per i prestiti, l'accesso prioritario alle vendite di token iniziali (IEO) e il programma di staking per i detentori di BNB. Attualmente, la capitalizzazione di mercato di Binance Coin è tra le più elevate tra tutti i digital assets, attestandosi a 46 miliardi di dollari al momento della scrittura.

In generale, le utility token possono essere utilizzate per incentivare gli utenti ad utilizzare l'exchange, e possono generare entrate per l'exchange stesso in termini di commissioni di trading o altri servizi offerti. Tuttavia, è importante notare che l'utilità delle utility token può variare a seconda dell'exchange e del loro utilizzo all'interno della piattaforma.

3.5

La tokenizzazione di assets

Informatica

● Basic

Il processo di tokenizzazione inizia con l'acquisizione delle azioni della società che si vuole tokenizzare. Queste azioni vengono poi custodite da un custode, in modo da garantirne la sicurezza. A questo punto, l'azienda che ha acquistato le azioni emette dei token che rappresentano le azioni stesse.

La rappresentazione di asset finanziari tramite token (i.e. tokenizzazione) sta emergendo come una forma innovativa di gestione degli asset, che consente di registrare e trasferire la proprietà degli stessi tramite tecnologia blockchain. La **tokenizzazione degli asset finanziari si basa sulla creazione di token digitali che rappresentano l'asset sottostante e che possono essere scambiati e trasferiti in modo rapido e trasparente**.

Un esempio di tokenizzazione di una stock è l'emissione di **“security token” rappresentanti azioni di una società quotata in borsa**. Questi token vengono emessi sulla blockchain e consentono agli investitori di detenere azioni senza dover passare attraverso intermediari, come ad esempio i depositari centrali, che in genere gestiscono il trasferimento delle azioni.

Per esempio, Bitpanda ha emesso all'interno della propria piattaforma di exchange token che rappresentano azioni di alcune società, come ad esempio Amazon, Facebook, Apple e Tesla. Questo servizio è stato offerto tramite Bitpanda Financial Service, società autorizzata alla prestazione di servizi finanziari dalla FMA austriaca.

La tokenizzazione di asset finanziari come gli stock può portare diversi benefici, tra cui una **maggior trasparenza nella gestione degli asset e una maggiore frazionabilità del asset**. La tokenizzazione **consente di dividere l'asset in frazioni più piccole**, aumentando così la sua accessibilità a un pubblico più vasto di investitori.

Inoltre, la tokenizzazione degli asset finanziari **offre la possibilità di creare "smart contract"** che possono regolare automaticamente i flussi di pagamento degli asset. Ad esempio, nel caso di un dividendo, gli smart contract possono distribuire automaticamente il pagamento ai detentori dei token, in base alle loro quote di partecipazione.

La tokenizzazione degli asset finanziari rappresenta una tecnologia in grado di trasformare il modo in cui gli investimenti vengono registrati, trasferiti e gestiti. La tokenizzazione degli asset finanziari come per le azioni di aziende quotate può aumentare la trasparenza, la liquidità e la divisibilità degli asset.

3.6

Business / Informatica

• Basic

Tra il Web2 e Web3: la custodia dei digital assets

Quando un investitore acquista un titolo, il titolo viene trasferito dal conto del venditore al conto dell'investitore attraverso la rete di trasferimento. I servizi di custodia titoli sono spesso forniti dalle stesse organizzazioni che gestiscono i servizi di clearing e settlement. In questo modo, le organizzazioni di clearing e settlement possono offrire un servizio completo ai propri clienti, gestendo sia la compensazione che la custodia dei titoli.

Nel contesto dei digital asset, un operatore finanziario che vuole offrire un servizio di custodia vede diverse differenze rispetto ai servizi tradizionali:

- In primo luogo, un **conto titoli gestito da una banca è generalmente utilizzato per detenere titoli azionari, obbligazionari e altri strumenti finanziari tradizionali**, mentre un **wallet oggi è esclusivamente utilizzato per detenere digital asset come bitcoin**.
- In secondo luogo, i **conti titoli sono di solito gestiti da banche e altre istituzioni finanziarie che sono regolate dalle autorità di controllo finanziario**. I **wallet, invece, possono essere gestiti da chiunque e non ci sono regole o procedure formali che regolano la loro gestione**.
- In terzo luogo, la **gestione di un conto titoli prevede solitamente una serie di attività e di servizi aggiuntivi, come la negoziazione di titoli, la gestione del rischio, la valutazione degli investimenti e la pianificazione fiscale**. Un **wallet, invece, è utilizzato solamente per la detenzione e la gestione delle digital asset**.

Una **piattaforma di custodia digitale è uno strumento importante per le banche che desiderano detenere, gestire e trasferire asset digitali**. Tra le caratteristiche che una custodia per una banca dovrebbe avere, ci sono un sistema di sicurezza multi-firma che richiede la conferma di più utenti per completare una transazione e tecnologie di sicurezza a prova di manomissione per prevenire accessi non autorizzati ai dati sensibili dei clienti.

Risulta infatti cruciale creare un disegno di prodotto e un design tale per cui sia facilmente riconducibile la responsabilità degli attori coinvolti:

1. Istituto finanziario;

2. Technology Provider;
3. Cliente finale.

Inoltre, una **buona custodia dovrebbe utilizzare sistemi di protezione dalle frodi**, come l'analisi comportamentale per rilevare eventuali attività sospette o transazioni anomale, e offrire un sistema di sicurezza adattivo costantemente aggiornato per rimanere al passo con le minacce emergenti.

Aspetto	Custodia dei Titoli	Custodia Digital Asset
<i>Tipi di asset supportati</i>	<i>Azioni, obbligazioni, fondi comuni, opzioni, ETF</i>	<i>Bitcoin, Ethereum, Litecoin, Bitcoin Cash, ERC-20 tokens</i>
<i>Approvazione transazioni</i>	<i>Approvazione manuale da parte della banca</i>	<i>Approvazione automatica tramite tecnologia multi-firma</i>
<i>Livello di sicurezza</i>	<i>Elevato, con processi e controlli rigorosi</i>	<i>Elevato, con tecnologia di sicurezza avanzata come il multi-party computation</i>
<i>Accesso ai fondi</i>	<i>Lento, con tempi di autorizzazione lunghi</i>	<i>Veloce, con accesso istantaneo ai fondi</i>
<i>Controllo del rischio</i>	<i>Elevato, con un'ampia gamma di controlli del rischio</i>	<i>Elevato, con tecnologie avanzate come l'analisi comportamentale per rilevare attività sospette</i>
<i>Costi</i>	<i>Solitamente alti, con commissioni per i servizi di custodia e transazione</i>	<i>Competitivi, con una struttura di commissioni basata sul volume delle transazioni</i>
<i>Scalabilità</i>	<i>Scalabilità limitata, con un numero limitato di asset che possono essere gestiti</i>	<i>Elevata scalabilità, con supporto per una vasta gamma di digital assets e token</i>

Un'altra caratteristica importante di una custodia digitale è la **possibilità di programmare smart contract all'interno della stessa architettura tramite ambienti di test**. Ad esempio, l'integrazione di ambienti di sviluppo dentro la soluzione di custodia potrebbe consentire agli sviluppatori di creare smart contract personalizzati per le loro applicazioni, che possono essere testati all'interno di un ambiente di sviluppo sicuro prima di essere implementati sulla blockchain principale.

In questo modo, le banche possono utilizzare una custodia digitale che offre un ambiente di sviluppo sicuro per la creazione di smart contract personalizzati, insieme ad una sicurezza adattiva costantemente aggiornata e sistemi di protezione dalle frodi.

3.7

Business / Informatica

● Medium

Tra il Web2 e Web3: on-ramp e smart order routing nel Web3

Il concetto di on-ramp si riferisce alla facilitazione dell'accesso da parte di nuovi utenti ad un determinato mercato o sistema finanziario. In particolare, nell'ambito dei digital asset, l'on-ramp rappresenta il processo attraverso il quale un utente acquisisce la capacità di acquistare e vendere un determinato digital asset, di solito attraverso l'utilizzo di una piattaforma di trading.

Per offrire ai propri clienti un'esperienza di trading efficiente e al contempo minimizzare i costi di esecu-

zione degli ordini, le banche possono implementare il concetto di smart order routing (SOR) attraverso un market maker che ha accesso a vari exchange in simultanea.

Il concetto di smart order routing si riferisce alla tecnologia che consente di eseguire gli ordini di trading su più piattaforme di negoziazione (exchange) in modo efficiente e ottimizzato. Questa tecnologia viene utilizzata da molti operatori di mercato, tra cui i market maker, per ottenere il miglior prezzo possibile per i propri clienti. Per implementare una strategia di smart order routing, un market maker deve integrare le API di più exchange sulla propria piattaforma di trading, consentendo di inviare gli ordini di trading direttamente alle diverse piattaforme. Inoltre, deve implementare algoritmi di smart order routing che consentano di ottimizzare l'esecuzione degli ordini, prendendo in considerazione vari fattori come il prezzo, la liquidità del mercato, le commissioni e le condizioni di mercato.

La SOR è una tecnologia che consente di selezionare il miglior prezzo disponibile su diversi mercati e di eseguire l'ordine sulla base di questa scelta, al fine di ottenere il miglior risultato possibile per il cliente. In pratica, la **SOR analizza continuamente il prezzo e la liquidità dei vari exchange e instrada l'ordine del cliente verso il mercato più conveniente in tempo reale.**

L'integrazione del servizio di on-ramp e della SOR rappresenta un'opportunità per le banche di offrire un'esperienza di trading completa e efficiente ai propri clienti interessati alla negoziazione di digital asset, contribuendo al contempo a ridurre i costi di esecuzione degli ordini e aumentare la propria quota di mercato.

In secondo luogo, la banca dovrebbe **integrare una serie di strumenti per la gestione del rischio, al fine di mitigare i rischi associati al trading di digital asset.** Questi strumenti potrebbero includere la verifica dell'identità dell'utente, la sorveglianza del prezzo e della volatilità del mercato, e la gestione dei margini e del leverage.

In terzo luogo, la banca dovrebbe **fornire un'adeguata formazione e supporto ai propri clienti per l'utilizzo della piattaforma di trading e la gestione del rischio associato al trading di digital asset.** Questo potrebbe includere la fornitura di materiali educativi, webinars, e un servizio di assistenza clienti dedicato.

In conclusione, l'implementazione di un servizio di on-ramp per la negoziazione di digital asset da parte di una banca richiede l'integrazione di una serie di tecniche e strumenti, compresa una piattaforma di trading, strumenti di gestione del rischio e supporto educativo e di assistenza clienti. L'implementazione di un servizio di on-ramp può rappresentare un'opportunità per la banca di espandere la propria offerta di prodotti e servizi e di intercettare una nuova clientela interessata al trading di digital asset.

3.8

Business / Informatica

• Medium

Tra il Web2 e il Web3: come costruire un digital asset backed security?

Spesso quando si parla di tokenizzazione di un asset finanziario, come un titolo azionario, ci si riferisce alla trasposizione di un titolo dai canali finanziari tradizionali verso una blockchain pubblica o privata. Ma come si può fare tecnicamente?

Per creare un token che sia agganciato al prezzo delle azioni nel mercato azionario, per esempio di Tesla, **si può utilizzare un oracolo per ottenere il prezzo corrente delle azioni** di Tesla e utilizzare questo valore come base per il prezzo del derivato sulla blockchain.

Di seguito è illustrato una descrizione ad alto livello su come potrebbe essere fatto.

- **Conoscenze di Solidity:** Per creare smart contracts su Ethereum, dovresti conoscere il linguaggio di programmazione Solidity, che è specifico per la creazione di smart contracts sulla blockchain Ethereum.

- **Creazione del Token:** Creare un token ERC-20 o ERC-721 (o qualsiasi altro standard di token compatibile con Ethereum che preferisci) usando Solidity. Questo token rappresenterà il tuo asset tokenizzato.
- **Prezzo Pegging:** Per legare il prezzo del tuo token al valore di un asset finanziario come Tesla, dovrà creare un oracle. Un oracle è un ente che fornisce dati dal mondo esterno alla blockchain. Nel tuo caso, l'oracle fornirà il prezzo corrente delle azioni Tesla. Un esempio di servizio oracle potrebbe essere Chainlink.
- **Implementazione dell'Oracle:** Dovrai implementare nel tuo smart contract una funzione che interagisce con l'oracle per ottenere il prezzo corrente di Tesla e aggiustare di conseguenza il prezzo del tuo token.
- **Funzionalità di Trading:** Dovrai implementare funzionalità nel tuo smart contract che permettano agli utenti di acquistare e vendere il tuo token in cambio di ETH (o qualsiasi altro digital asset che preferisci).
- **Test e distribuzione:** Una volta completato lo sviluppo del tuo smart contract, dovrà testarlo su una rete di prova Ethereum come Ropsten o Rinkeby per assicurarti che funzioni come previsto. Dopo avere eseguito test sufficienti, potrai distribuire il tuo smart contract sulla rete principale Ethereum.
- **Interazione con il Contratto:** Infine, per permettere agli utenti di interagire facilmente con il tuo smart contract, potresti voler creare un'interfaccia utente, che può essere un sito web o un'applicazione.

Il contratto ha una variabile **oracle** che rappresenta l'indirizzo dell'oracolo e una variabile **priceDecimals** che rappresenta il numero di decimali da utilizzare per il prezzo del derivato. Il contratto ha una funzione **getPrice** che restituisce il prezzo corrente del derivato in base al prezzo delle azioni di Tesla fornito dall'oracle.

In questo esempio, l'interfaccia **IOracle** rappresenta l'oracolo che fornisce il prezzo corrente delle azioni di Tesla. La funzione **getTeslaPrice** restituisce il prezzo corrente delle azioni di Tesla in una forma appropriata per il prezzo del derivato.

Il costruttore accetta come argomenti l'indirizzo dell'oracolo e il numero di decimali da utilizzare per il prezzo del derivato.

La funzione **getPrice** restituisce il prezzo corrente del derivato moltiplicando il prezzo corrente delle azioni di Tesla fornito dell'oracolo per 10 elevato alla potenza di **priceDecimals**, che converte il prezzo delle azioni in una forma appropriata per il prezzo del derivato.

Tuttavia, l'implementazione di tali soluzioni richiederebbe un'analisi approfondita dei requisiti tecnici, legali e normativi, nonché la definizione di standard di sicurezza e di interoperabilità tra i diversi protocolli e sistemi coinvolti.

4

Prodotti derivati sul mercato Web3

- 4.1 Quali sono i derivati nel mercato del Web3?
- 4.2 Approfondimento degli ETP
- 4.3 Analisi dei dati degli strumenti derivati su CEX e DEX

4.1

Teoria Finanziaria

• Medium

Quali sono i derivati nel mercato del Web3?

Negli ultimi anni, i mercati di prodotti derivati aventi quale sottostante Bitcoin hanno visto una crescita significativa. Questi mercati offrono agli investitori l'opportunità di negoziare contratti futures e opzioni su Bitcoin, **consentendo loro di sfruttare le fluttuazioni dei prezzi dei digital asset senza dover possedere fisicamente la valuta digitale.**

I derivati sono dei contratti creati su un'attività sottostante (underlying asset) da cui dipende il loro stesso valore. **Il sottostante può essere di varia natura:** un'azione, un digital asset, una materia prima, i tassi d'interesse e il cambio, degli indici. Indipendentemente da questo fattore, il derivato viene costruito al di sopra di qualcosa; esempio:

- bitcoin -> derivato,
- azioni Unicredit -> derivato,
- oro -> derivato.

I derivati si sono diffusi a macchia d'olio dall'inizio di questo secolo. Oggi vengono scambiati in continuazione, ricoprendo un ruolo di primo piano nel panorama finanziario.

Nel dicembre 2017, CME Group ha lanciato il trading di futures su Bitcoin, diventando la prima grande borsa a offrire tale servizio. Ciò ha permesso agli investitori istituzionali di iniziare a negoziare Bitcoin su una sede regolamentata. Diversi exchange propongono questi strumenti, anche di tipo **perpetual** (senza scadenza). Si trovano inoltre dei **prodotti che tokenizzano azioni**, materie prime e indici.

Ecco un elenco di exchange nei quali è possibile acquistare dei futures e altri strumenti derivati:

Competitor	Stage	Total Funding	Location
Deribit	Series A	\$40M	Panama
EthosX	Convertible Note	\$0.5M	India
Xena Exchange	Acquired	\$3M	Ireland
D2X	Seed VC	\$5.7M	Netherlands
Bitpanda	Series C	\$497.43M	Austria

Deribit, uno dei più grandi exchange centralizzati che offre prodotti derivati su Bitcoin. **Deribit offre contratti futures e opzioni su Bitcoin con un'alta leva finanziaria**, il che significa che gli utenti possono ottenere grandi guadagni o perdite in base alle fluttuazioni dei prezzi dei digital assets.

Uno dei più grandi exchange decentralizzati (DEX) che offre prodotti derivati su Bitcoin è Uniswap. Uniswap è un protocollo di scambio automatizzato basato su Ethereum che consente agli utenti di scambiare token senza la necessità di un intermediario centralizzato. Il protocollo di Uniswap include anche una funzione di creazione di mercato **che consente agli utenti di fornire liquidità per i contratti futures e opzioni su Bitcoin**.

In generale, i mercati di prodotti derivati per i prodotti finanziari come Bitcoin stanno diventando sempre più popolari tra gli investitori che cercano di trarre profitto dalle fluttuazioni dei prezzi dei digital asset e **utilizzando strategie di hedging per proteggere i propri investimenti**.

4.2

Teoria Finanziaria

● Medium

Approfondimento degli ETP

Gli ETP sono strumenti finanziari negoziati su mercati regolamentati il cui obiettivo primario è replicare l'andamento di un indice di riferimento o di un determinato attivo sottostante. Le forme più conosciute sono gli **ETF** (Exchange Traded Funds), gli **ETC** (Exchange Traded Commodities) e gli **ETN** (Exchange Traded Notes). Possono essere usati per diversificare i rischi.

Sebbene gli **ETP** possano assumere diverse forme, presentano caratteristiche comuni:

- sono quotati in mercati regolamentati;
- sono facilmente negoziabili come un'azione nel corso degli orari di apertura degli scambi in borsa;
- vi sono soggetti (partecipanti autorizzati e market maker) che forniscono liquidità ai relativi mercati;
- hanno l'obiettivo di replicare fedelmente la performance dell'indice di riferimento o dell'attività sottostante.

L'acquisto di ETP (Exchange Traded Products) che hanno digital asset come sottostante **può influenzare quest'ultimi in base alla domanda e all'offerta di questi prodotti**. Se ci fosse una forte domanda per gli ETP, ciò potrebbe aumentare la domanda di digital assets sottostanti, portando ad un aumento del prezzo. Allo stesso modo, se c'è una forte offerta di ETP, ciò potrebbe portare a una diminuzione della domanda del sottostante e quindi ad una diminuzione del prezzo.



In generale, quando gli investitori acquistano ETP di digital asset, stanno effettivamente acquistando una quota di un portafoglio che detiene digital asset come sottostante.

L'ente finanziario che emette l'ETP deve effettivamente custodire il Bitcoin e gli altri digital assets sottostanti, al fine di garantire che il valore dell'ETP corrisponda al valore del Bitcoin. **Questo può essere fatto attraverso una società di custodia che detiene fisicamente il capitale in digital asset per conto dell'ente emittente.**

Il processo burocratico negli USA per emettere un ETF comporta diverse fasi. Un gestore ETF, noto anche come sponsor, progetta, sviluppa e lancia il fondo. Il gestore dell'ETF deve presentare un piano dettagliato per il fondo alla Securities and Exchange Commission (SEC) per la sua approvazione. Questo processo può essere impegnativo a causa delle normative che sono state aggiornate per riflettere l'esistenza degli ETF.

Una volta che l'ETF è approvato, il gestore deve acquistare e depositare tutti gli attivi elencati nell'ETF. In cambio, il gestore riceverà un numero di azioni nell'ETF che equivale al valore delle azioni depositate, che sono chiamate "unità di creazione"¹.

Specificamente, nel caso dell'**ETF Bitcoin di BlackRock**, BlackRock ha presentato domanda per un ETF Bitcoin che permetterebbe agli investitori di ottenere esposizione al Bitcoin senza comprarlo direttamente. Questo tipo di ETF è noto come ETF Bitcoin spot, che traccia il prezzo di mercato sottostante del Bitcoin². Per questo ETF, BlackRock ha scelto Coinbase Custody come suo custode. Va notato che la SEC non ha ancora approvato alcuna domanda per ETF Bitcoin spot². Se approvato, l'ETF sarebbe negoziato sul NASDAQ³. A causa delle restrizioni alla presentazione di documenti normativi, BlackRock non ha potuto fornire ulteriori commenti oltre la dichiarazione di registrazione che hanno presentato alla SEC³.

È importante notare che la SEC ha respinto altre domande per ETF Bitcoin spot, comprese quelle di Grayscale Investment LLC e di aziende, tra cui Fidelity, Cboe Global Markets e NYDIG. I rifiuti della SEC hanno sollevato accuse di azione arbitraria, in particolare dato che in precedenza aveva approvato gli ETF su futures Bitcoin².

Al momento della scrittura, ci sono diversi ETP sui digital asset disponibili nei mercati finanziari americani, europei ed asiatici.

4.3

Teoria Finanziaria

● Medium

Analisi dei dati degli strumenti derivati su CEX e DEX

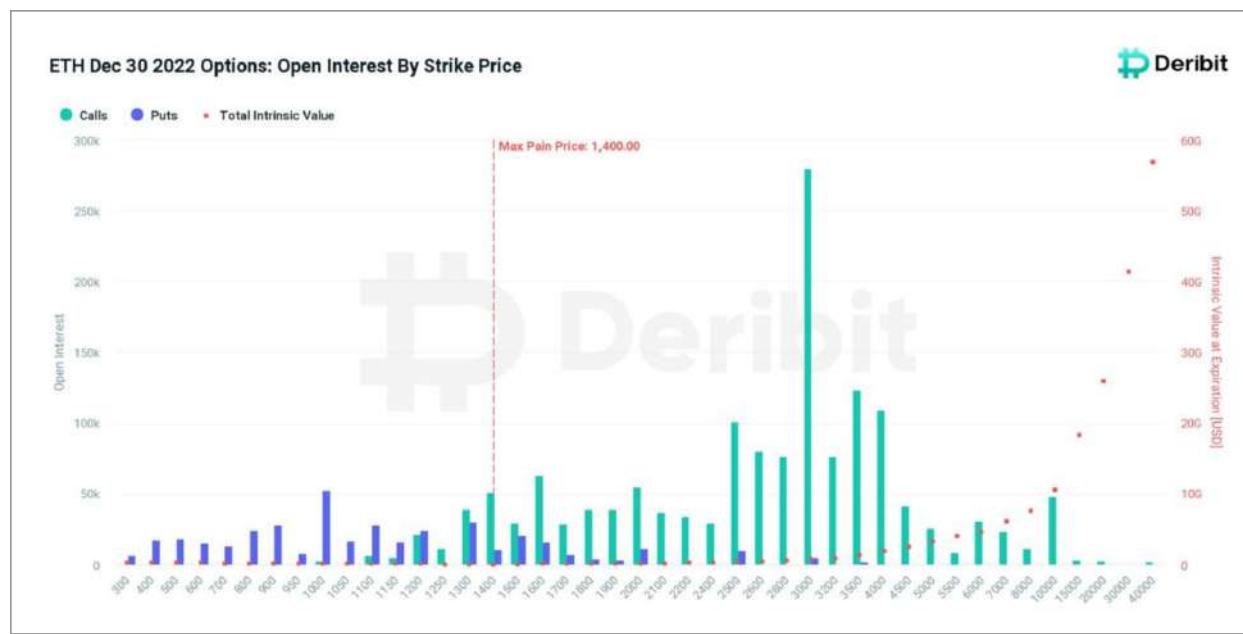
Nel corso degli ultimi anni, il mercato degli strumenti derivati nel settore dei digital asset ha visto un crescente interesse, avvicinando gli investitori tradizionali a questo settore. Qui riportato alcune informazioni che possono aiutare a comprendere tale fenomeno e la continua crescita:

- **Il mercato delle opzioni e la proporzione tra call e put nel breve periodo**
- **La quantità di liquidazioni nel mercato**

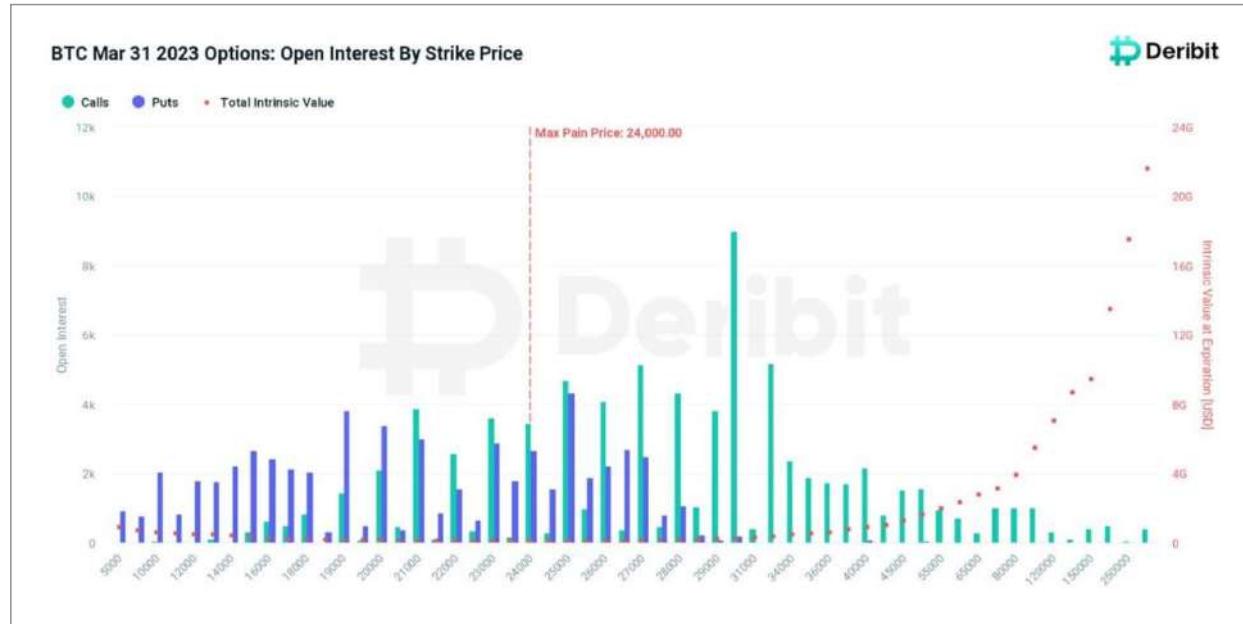
PREZZO DELLE OPZIONI

L'analisi delle opzioni può fornire importanti informazioni sui movimenti futuri dei prezzi di Bitcoin. In particolare, gli investitori possono utilizzare le opzioni come un indicatore della direzione futura dei prezzi di Bitcoin, in quanto i prezzi delle opzioni riflettono le aspettative dei trader per quanto riguarda il prezzo futuro di Bitcoin.

Ad esempio, se il prezzo delle opzioni call (che consentono l'acquisto di Bitcoin ad un prezzo predeterminato) aumenta rispetto alle opzioni put (che consentono la vendita di Bitcoin ad un prezzo predeterminato), questo può indicare una crescente ottimismo tra i trader per quanto riguarda il prezzo di Bitcoin. Al contrario, se il prezzo delle opzioni put aumenta rispetto alle opzioni call, ciò può indicare una crescente preoccupazione tra i trader per quanto riguarda il prezzo di Bitcoin.



Sugli exchange come Deribit, gli investitori possono utilizzare i dati sulle opzioni per monitorare le aspettative del mercato per quanto riguarda il prezzo futuro di Bitcoin e le possibili fluttuazioni di prezzo. Ad esempio, gli investitori possono utilizzare la “volatilità implicita” delle opzioni come un indicatore della volatilità futura del prezzo di Bitcoin. Inoltre, gli investitori possono utilizzare gli strumenti di analisi tecnica disponibili sui mercati di opzioni per identificare tendenze di prezzo e potenziali punti di inversione di tendenza.



Anche sui mercati tradizionali dei futures, i prezzi delle opzioni possono essere utilizzati per prevedere l’andamento dei prezzi di Bitcoin nel breve periodo. Ad esempio, i futures su Bitcoin offerti da CME Group e altri mercati possono fornire agli investitori una visione sulle aspettative del mercato per quanto riguarda il prezzo futuro di Bitcoin. Inoltre, gli investitori possono utilizzare gli strumenti di analisi tecnica disponibili sui mercati di futures per identificare trend di prezzo e punti di inversione di tendenza.

GRAFICO DELLE LIQUIDAZIONI

Il processo di liquidazione si riferisce alla vendita forzata di un'attività finanziaria al fine di coprire un debito o di garantire una posizione marginale. Nel contesto dei digital asset, la liquidazione avviene quando un trader ha effettuato un trade utilizzando leva finanziaria e la sua posizione inizia a perdere valore al punto in cui la sua garanzia marginale è insufficiente per coprire le perdite. In questo caso, lo scambio può liquidare la posizione del trader e utilizzare la garanzia marginale per coprire le perdite.



La distribuzione della liquidità durante le fasi di mercato può avere un impatto significativo sull'andamento del prezzo di bitcoin nel breve periodo. Ad esempio, se c'è una grande quantità di liquidità sul mercato, ciò può spingere il prezzo di bitcoin al rialzo. D'altra parte, se c'è una mancanza di liquidità, il prezzo potrebbe subire una correzione al ribasso.

Ci sono stati diversi esempi storici di grandi liquidazioni che hanno fatto scattare gli stop loss sul mercato di bitcoin. Un esempio recente è avvenuto il 19 maggio 2021, quando il prezzo di bitcoin è sceso di oltre il 30% in poche ore. Ciò è stato causato da una serie di vendite di massa sul mercato, che hanno portato alla liquidazione di posizioni marginate e allo scattare degli stop loss. In totale, sono stati liquidati circa 9 miliardi di dollari di posizioni lunghe su bitcoin in un solo giorno.

Un altro esempio è avvenuto nell'aprile 2020, quando il prezzo di bitcoin è sceso di circa il 50% in un solo giorno. Anche in questo caso, la causa è stata una serie di vendite di massa sul mercato, che hanno portato alla liquidazione di posizioni marginate e allo scattare degli stop loss. In totale, sono stati liquidati circa 1,2 miliardi di dollari di posizioni lunghe su bitcoin in un solo giorno.

In sintesi, la comprensione del processo di liquidazione è importante per comprendere l'andamento del prezzo di bitcoin nel breve periodo, poiché le grandi liquidazioni possono portare a un'impennata della volatilità e possono innescare una correzione al ribasso dei prezzi. Gli investitori e i trader devono considerare attentamente il rischio di liquidazione quando effettuano operazioni con leva finanziaria su bitcoin e altri digital assets.

5

Bitcoin come digital asset

- 5.1 Il processo di price discovery di un digital asset come bitcoin
- 5.2 Che cosa si intende per asset deflattivo ed inflattivo?
- 5.3 Confronto tra l'offerta di bitcoin e Oro nel tempo
- 5.4 Il principio di inflazione e l'invenzione dell'aggiustamento della difficoltà
- 5.5 La ricerca e sviluppo nel settore del mining di bitcoin
- 5.6 Quanta energia consuma davvero Bitcoin?
- 5.7 Dove vengono estratti oro e bitcoin?
- 5.8 Che cos'è il modello stock to flow?
- 5.9 Bitcoin per gli Stati e le imprese
- 5.10 Bitcoin a confronto con altri asset
- 5.11 Come utilizzo i dati on-chain per capire il mercato?

5.1

Finanza Comportamentale

● Basic

Il processo di price discovery di bitcoin

Una tra le domande più comuni che le persone si pongono è: ma ha valore davvero un digital asset come bitcoin e cosa posso fare per misurarlo? Rispondere a questo quesito non è facile, poiché:

- La natura del protocollo Bitcoin è complessa e spesso non viene compresa in quanto necessita di diverse competenze in aree differenti;
- I bitcoins sono digital asset giovani che devono ancora dimostrare nel lungo periodo la propria resilienza come bene rifugio
- Ad oggi, i bitcoins non sono ancora chiaramente inquadrati dal punto di vista regolamentare e questo porta ad incertezze nel mercato;

Possiamo quindi affermare che il valore dei digital asset sta affrontando un processo chiamato price discovering. Il concetto di “**price discovering**” o scoperta del prezzo si riferisce al **processo attraverso cui gli investitori e i trader determinano il valore di un asset nel lungo periodo**. Questo processo avviene tramite il confronto delle informazioni disponibili nel mercato, al fine di determinare il prezzo corretto dell’asset.

Qui riportata la crescita del valore di bitcoin dal 2010 al 2022, in scala logaritmica:



In altre parole, la **scoperta del prezzo è il risultato dell’offerta e della domanda del mercato, che si basa sulle aspettative degli investitori riguardo al futuro dell’asset**. In funzione di ciò, comprendiamo che la percezione delle masse rispetto al valore di un asset intangibile come i bitcoins è determinante rispetto all’evoluzione del valore stesso.



Funny Facts

Il Pizza Day di Bitcoin è una celebrazione iconica della storia dei digital asset. Tutto è iniziato il 22 maggio 2010, quando un utente di Bitcointalk.org di nome Laszlo Hanyecz ha offerto 10.000 Bitcoin a chiunque gli avesse consegnato due pizze. All'epoca, i Bitcoin erano praticamente senza valore, ma Hanyecz ha voluto dimostrare che i digital assets hanno un valore reale e potevano essere utilizzati per effettuare transazioni reali. L'offerta è stata accettata da un altro utente, che ha ordinato le pizze per Hanyecz utilizzando una carta di credito.

Generalmente, il valore di un digital-asset può essere compreso attraverso un processo dinamico che **si origina dall'interazione tra domanda ed offerta**. All'interno degli exchange, gli utenti interagiscono tra loro in processi di acquisto e vendita, andando a determinare il valore tale per cui il mercato diventa efficiente, ovvero c'è una doppia coincidenza di bisogni.

La domanda e l'offerta di digital asset sono influenzate da diversi fattori, tra cui **la fiducia degli investitori per il purpose dei digital asset e dei token, una chiara regolamentazione, la percezione del rischio del progetto, la liquidità e i volumi dei singoli exchange e l'andamento dei mercati finanziari globali**.



Il processo dinamico di domanda ed offerta può causare **una differenza di prezzo tra i diversi exchange**. Questa differenza di prezzo può essere sfruttata dagli investitori attraverso una strategia nota come arbitraggio. In alcuni casi, la differenza di prezzo tra gli exchange può essere talmente elevata da generare un fenomeno noto come "premium price". **Il premium price si verifica quando il prezzo di un digital asset su un exchange è significativamente più alto rispetto al prezzo di mercato**. Questo può essere causato da una serie di fattori, tra cui la domanda elevata sulla piattaforma, la scarsità di offerta o anche situazioni in cui la popolazione ha comprato digital asset per proteggersi da fenomeni di iperinflazione.



FOMO

Definizione: Sigla dell'ingl. *Fear of missing out* ("paura di rimanere escluso"), che si riferisce alla sensazione d'ansia provata da chi teme di essere privato di qualcosa di importante se non manifesta assiduamente la sua presenza tramite i mezzi di comunicazione e di partecipazione sociale elettronici interattivi.

Fonte: https://www.treccani.it/vocabolario/fomo_%28Neologismi%29/

Per concludere, il valore di un digital asset è ancora molto soggetto da momenti euforici di hype nel Bull Market, guidati dal **FOMO**, e seguiti da momenti di estrema paura nei momenti di Bear Market, in maniera molto analoga alle glamour stocks. In questo capitolo, cercheremo di analizzare l'evoluzione del prezzo e del suo valore in maniera più dettagliata.

5.2

Teoria Finanziaria / Finanza comportamentale

● Medium

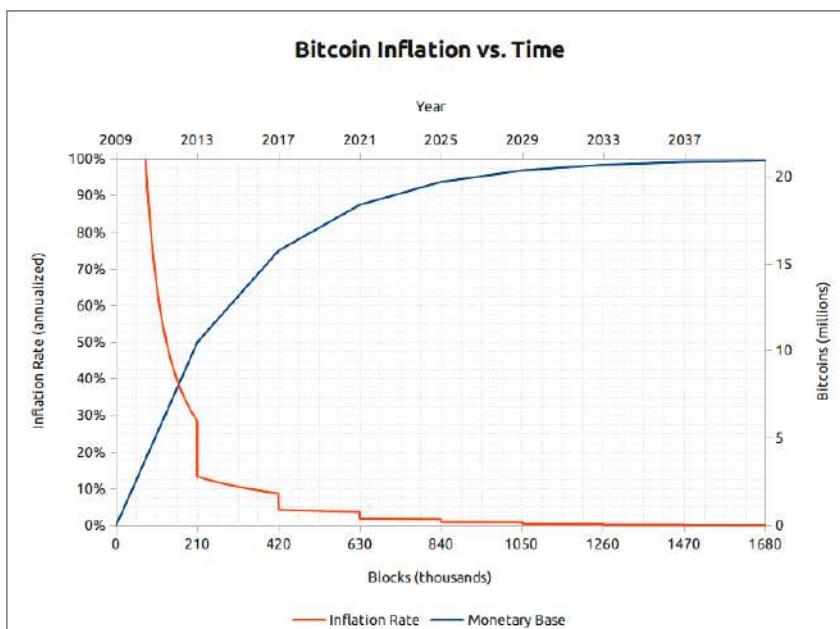
Che cosa si intende per asset deflattivo e inflattivo?

Come abbiamo analizzato in precedenza Bitcoin è un'innovativa forma di asset digitale che presenta caratteristiche simili a quelle del contante, in quanto gestito in maniera autonoma e privo di una controparte centrale. Infatti, **Bitcoin può essere considerato un asset al portatore, in quanto la proprietà e il controllo di ciascun bitcoin sono direttamente correlati al possesso delle chiavi private specifiche**. Ciò significa che la titolarità e la proprietà di un bitcoin possono essere trasferiti autonomamente e direttamente da un utente a un altro, senza la necessità di intermediari centralizzati o di una controparte di fiducia.

La seconda caratteristica di Bitcoin è quella di non essere duplicabile, e conseguentemente essere un **asset digitale “scarso”** all'interno del web.

Gli **asset finanziari deflattivi** sono quell'**insieme di attività finanziarie il cui valore può aumentare nel tempo grazie alla loro scarsità o alla limitata offerta sul mercato**. Differentemente, una valuta fiat come il dollaro o l'euro è per natura un asset inflattivo, poiché vengono create periodicamente per stimolare l'inflazione. L'**oro è un esempio di asset finanziario deflattivo** molto conosciuto. La sua limitata offerta sulla Terra lo rende un bene molto prezioso e il suo valore è stato riconosciuto da secoli come un bene di scambio e riserva di valore. Secondo alcune teorie economiche, la **scarsità è uno dei fattori principali che determinano il valore degli asset finanziari deflattivi**, infatti, la domanda di beni e servizi supera l'offerta, portando ad un aumento del prezzo.

L'**offerta di Bitcoin è limitata**, con una **quantità massima di 21 milioni di unità**. Inoltre, ogni 210.000 blocchi, la quantità prodotta di bitcoin per ogni blocco risolto viene dimezzata, fino ad arrivare a 0.

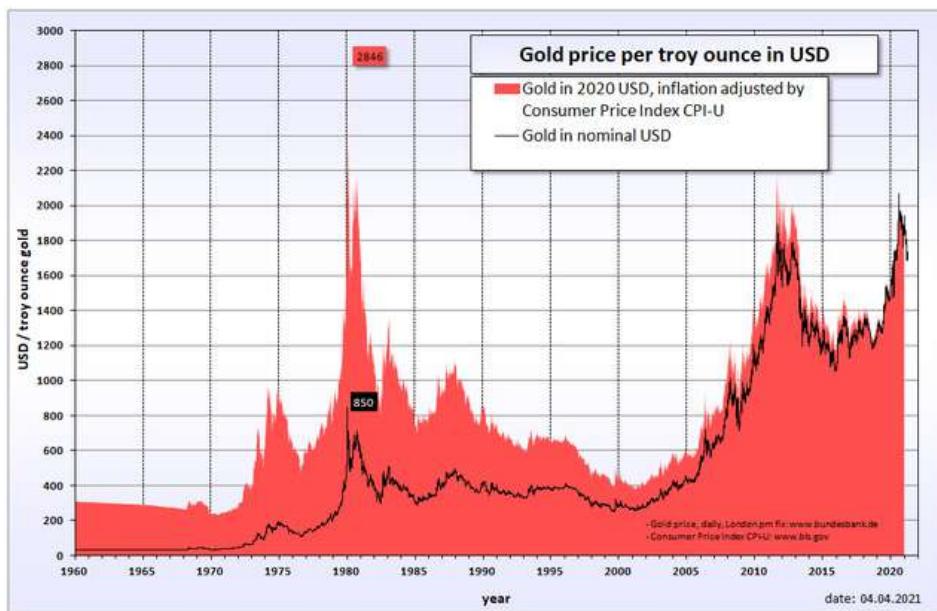


Bitcoin ha quindi una politica monetaria definita come **deterministica** ed **inelastica**. Come abbiamo visto nel primo capitolo e nel sesto capitolo, i bitcoins si posizionano storicamente come una nuova tipologia di hard money.

Facciamo tuttavia un passo indietro per comprendere l'evoluzione del dollaro, ed il passaggio da hard money a soft money del sistema valutario internazionale e del sistema monetario americano.

Dal 1944 con gli accordi di Bretton Woods, il dollaro è stato valuta di riserva per tutti gli Stati Occidentali, in quanto unica valuta **il cui valore era sostenuto da un collaterale**: l'oro. Inoltre, l'incremento di oro nelle casse della Federal Reserve (Fed) fu significativo, permettendo a quest'ultima di creare nuova liquidità nel sistema. Secondo dati del World Gold Council, alla fine della Seconda guerra mondiale nel 1945, la Fed aveva circa 20.000 tonnellate di oro. Durante questo periodo, la Fed aveva fissato il prezzo dell'oro a 35 dollari l'oncia e **garantiva di scambiare dollari per oro a questo prezzo**. Di conseguenza, gli Stati Uniti avevano accumulato riserve auree enormi, poiché gli altri paesi usavano il dollaro come riserva internazionale e chiedevano spesso l'oro in cambio.

È importante sottolineare che l'aumento delle riserve auree della Fed non era l'unico fattore che determinava la solidità del sistema monetario internazionale basato sul dollaro. **La fiducia nella capacità degli Stati Uniti** di garantire mantenere la stabilità monetaria internazionale era altrettanto importante. Fino a quel momento tutte le valute internazionali erano convertibili in dollaro, il dollaro in oro e quindi sostanzialmente **il sistema monetario internazionale era considerevole come un hard money system, basato su un bene deflattivo**.



Nel 1971, gli Stati Uniti sospesero la convertibilità del dollaro in oro. La quantità di dollari creati nella massa monetaria M0 dagli anni '70 ad oggi dipende da molti fattori, tra cui la politica monetaria della Federal Reserve e la domanda di denaro nell'economia degli Stati Uniti.

Secondo i dati della Federal Reserve Bank of St. Louis, alla fine del 1971 la massa monetaria M0 era di circa 48 miliardi di dollari. Alla fine del 2021, la massa monetaria M0 era di circa 9,9 trilioni di dollari. Ciò rappresenta **un incremento di circa 206 volte rispetto ai livelli del 1971**.

Tuttavia, è importante notare che l'espansione della massa monetaria M0 non è stata lineare nel tempo e **non ha avuto un tasso di crescita costante**. Ad esempio, la massa monetaria M0 è aumentata significativamente durante la crisi finanziaria del 2008 e durante la pandemia COVID-19 del 2020, quando la Federal Reserve ha implementato politiche di stimolo monetario per sostenere l'economia.

Se un risparmiatore avesse tenuto i suoi risparmi in dollari dal 1971 fino ad oggi, **il potere di acquisto dei suoi risparmi sarebbe diminuito significativamente**. Ciò è dovuto all'inflazione, ovvero all'aumento generale dei prezzi dei beni e dei servizi nel tempo. Ad esempio, secondo il Consumer Price Index (CPI) del governo degli Stati Uniti, il prezzo medio di un'automobile nel 1971 era di circa \$3.500, mentre nel 2021 è di circa \$38.000. Ciò significa che il potere d'acquisto del dollaro è diminuito drasticamente nel corso degli anni, e il risparmiatore che ha mantenuto i suoi risparmi in dollari avrebbe visto il valore dei suoi risparmi eroso dall'inflazione.

Per concludere esistono asset deflattivi ed inflattivi, i quali nel tempo, possono perdere valore o guadagnarlo in funzione della loro produzione, della loro scarsità e dalla fiducia rispetto ad alcune caratteristiche che lo identificano. Dopo il 71, il sistema valutario internazionale è basato monete con logiche espansive, che inevitabilmente, portano ad una perdita di potere d'acquisto nel lungo periodo.

5.3

Teoria Finanziaria

● Basic

Confronto tra l'offerta di bitcoin e Oro nel tempo

La domanda che ci poniamo è quindi: bitcoin può essere più paragonato ad oro digitale o ad una valuta virtuale peer to peer? Oro e Bitcoin vengono spesso comparati in quanto asset deflattivi. **Analizziamo più nel dettaglio il modello di offerta dei due asset.**

La quantità di oro in circolazione oggi è stimata intorno a circa 197.000 tonnellate metriche, con una variazione di circa l'1% all'anno. Tuttavia, va notato che la **quantità di oro in circolazione è un dato difficile da stimare con precisione**, poiché gran parte dell'oro estratto nel corso della storia è stato fuso, riciclati e raffinato in nuovi prodotti, rendendolo difficile da tracciare e quantificare con precisione.

Secondo il rapporto del World Gold Council, al Q3 2021, la distribuzione dell'oro in circolazione è la seguente:

- Gioielli: 40%
- Riserve dei governi: 18%
- Investimento privato: 16%
- Altre applicazioni industriali: 26%

L'oro viene detenuto in tutto il mondo, ma i paesi con le riserve d'oro più significative includono gli Stati Uniti, la Germania, l'Italia e la Francia. Nel complesso, la quantità di oro detenuta dai paesi del mondo è stimata intorno a circa 35.000 tonnellate metriche.

Di seguito è riportata una tabella che mostra la **quantità di estrazione di oro nel mondo**, divisa per periodi di 25 anni, dal 1900 ad oggi. Le quantità sono espresse in tonnellate metriche (t) e sono state ricavate dal World Gold Council.

Anno	Quantità di oro estratta (tonnellate)
1900	445
1925	1,541
1950	2,525
1975	1,520
2000	2,620
2025	3,280*

Per quanto riguarda l'estrazione dell'oro, esistono diversi metodi per estrarre l'oro dalle miniere. Uno dei metodi più comuni è la tecnica dell'estrazione a cielo aperto, che comporta la rimozione del terreno sovrastante per raggiungere il minerale. Un altro metodo è l'estrazione sotterranea, in cui i minatori scavano gallerie per raggiungere il minerale.

Una volta estratto, l'oro viene raffinato per rimuovere eventuali impurità e trasformarlo in oro puro. Ci sono diverse tecniche di raffinazione, ma in genere coinvolgono il trattamento del metallo con agenti

chimici come l'acido nitrico o il cloro per rimuovere gli elementi indesiderati. L'oro raffinato viene poi fuso in lingotti o monete e utilizzato per scopi finanziari, industriali o decorativi. Chiaramente, il costo dell'oro è direttamente proporzionale al costo di estrazione, raffinazione e messa in commercio.

La prima analogia tra oro e Bitcoin da considerare è che entrambi gli asset vengono estratti utilizzando l'energia. Il ruolo dell'energia elettrica è infatti importante nella definizione del valore di Bitcoin in quanto la **creazione e il mantenimento della rete Bitcoin richiede una notevole quantità di energia elettrica**.



Funny Facts

Il 5 ottobre 2009, il primo prezzo del Bitcoin è stato calcolato nove mesi dopo la creazione della rete Bitcoin, dal sito New Liberty Standard. Il prezzo è stato calcolato utilizzando una formula matematica basata sul lavoro richiesto per generare un Bitcoin.

La formula ha preso in considerazione il costo dell'energia elettrica negli Stati Uniti, l'energia media utilizzata da un computer per generare un Bitcoin e altri fattori. Il risultato finale è stato di 1.309 BTC per 1\$.

Il costo dell'energia elettrica necessaria per il mining di Bitcoin influenza quindi direttamente il costo del mining stesso e, di conseguenza, il valore di Bitcoin. Quando il costo dell'energia elettrica aumenta, il mining di Bitcoin diventa più costoso e questo può portare a un aumento del valore di Bitcoin per compensare il costo aggiuntivo.

Inoltre, la scarsità programmabile di Bitcoin, **unita alla grande quantità di energia elettrica necessaria per il mining, rende Bitcoin un asset molto scarso e difficile da produrre.**

Tuttavia, la relazione tra il costo di produzione e il prezzo dell'oro e Bitcoin non sono sempre così lineari, poiché ci sono molti altri fattori che possono influire sul prezzo, come la quantità in circolazione in quel momento e la domanda, la volatilità dei mercati finanziari, i tassi di interesse, le crisi economiche e l'inflazione.

Fonti

- ▶ World Gold Council. "Goldhub: Gold supply and demand statistics." Aggiornato a febbraio 2022. Disponibile all'indirizzo: <https://www.gold.org/goldhub/data/gold-supply-and-demand-statistics>
- ▶ USGS Mineral Commodity Summaries 2021: <https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-gold.pdf>
- ▶ World Gold Council: <https://www.gold.org/goldhub/data/historical-mine-production>

5.4

Teoria Monetaria / Informatica

● Medium

Il principio di inflazione e l'invenzione dell'aggiustamento della difficoltà

Il principio di inflazione è il processo attraverso il quale il valore di una valuta diminuisce nel tempo, causando un aumento generale dei prezzi dei beni e dei servizi. Questo avviene quando la quantità di denaro in circolazione aumenta più velocemente della produzione di beni e servizi dell'economia, diminuendo così il potere d'acquisto della valuta stessa.

Il funzionamento dell'aggiustamento della difficoltà di Bitcoin è strettamente correlato al principio di inflazione. In particolare, la difficoltà di mining di Bitcoin rappresenta la quantità di lavoro computazionale richiesto per risolvere un blocco nella blockchain. Tale difficoltà viene regolata automaticamente ogni 2016 blocchi estratti, in modo tale da mantenere il tempo medio di generazione dei blocchi attorno ai 10 minuti. **Questo meccanismo di aggiustamento della difficoltà è fondamentale per garantire la stabilità del sistema Bitcoin e prevenire la creazione eccessiva di nuovi bitcoin.** Infatti, se la difficoltà rimanesse costante, l'aumento della potenza di calcolo dei miner porterebbe ad una maggiore velocità di estrazione dei blocchi, con conseguente aumento del numero di bitcoin generati e quindi dell'inflazione.

Dunque, l'aggiustamento della difficoltà di Bitcoin **rappresenta un meccanismo di controllo dell'inflazione, poiché consente di mantenere il tasso di generazione dei bitcoin costante e prevenire il rischio di una creazione eccessiva di nuova moneta.**

L'aggiustamento della difficoltà di Bitcoin è basato su una formula che tiene conto della potenza di calcolo complessiva della rete, espressa in hash al secondo. In particolare, la formula utilizzata per calcolare la nuova difficoltà dopo ogni 2016 blocchi estratti è la seguente

Difficoltà nuova = Difficoltà attuale (**Tempo stimato per 2016 blocchi / Tempo effettivo impiegato per estrarre 2016 blocchi**) dove:

- **Difficoltà attuale è il valore della difficoltà al momento dell'aggiustamento**
- **Tempo stimato per 2016 blocchi è pari a 2016** 10 minuti, ovvero il tempo medio di generazione dei blocchi
- Tempo effettivo impiegato per estrarre 2016 blocchi è il tempo effettivo trascorso per l'estrazione dei 2016 blocchi precedenti

In pratica, la formula tiene conto del tempo effettivo impiegato per estrarre i blocchi precedenti rispetto al tempo stimato, in modo tale da adeguare la difficoltà alla potenza di calcolo della rete. Se il tempo effettivo è inferiore al tempo stimato, significa che la potenza di calcolo della rete è maggiore di quanto previsto e quindi la difficoltà viene aumentata per mantenere il tempo medio di generazione dei blocchi attorno ai 10 minuti. Viceversa, se il tempo effettivo è superiore al tempo stimato, significa che la potenza di calcolo della rete è inferiore di quanto previsto e quindi la difficoltà viene ridotta per mantenere il tempo medio di generazione dei blocchi attorno ai 10 minuti.

5.5

Informatica

● Medium

La ricerca e sviluppo nel settore del mining di bitcoin

La competizione dei miner ha portato ad un forte efficientamento e ad una ricerca costante nello sviluppo di macchine dedicate alla produzione di hash. Qui di seguito alcune considerazioni.

Le **ASIC** (Application Specific Integrated Circuit) sono dei **chip progettati specificatamente per l'estrazione di digital assets**, mentre le **GPU** (Graphics Processing Unit) **sono dispositivi general purpose che sono stati utilizzati anche per l'estrazione di digital asset.**

Negli ultimi anni, il **settore dell'estrazione di digital assets ha subito un'evoluzione significativa** grazie alla ricerca e allo sviluppo delle ASIC e delle GPU. Le **ASIC sono state sviluppate con l'obiettivo di ottenere prestazioni superiori rispetto alle GPU**, in termini di hash rate (cioè la velocità di elaborazione delle transazioni) e di efficienza energetica. Le **ASIC hanno inoltre la capacità di eseguire solo specifici algoritmi di mining, riducendo il rischio di hacking e di attacchi da parte di miner malevoli.**

Secondo un rapporto di CoinShares del 2020, le **ASIC hanno rappresentato il 67,7% della potenza di hash complessiva della rete Bitcoin, mentre le GPU solo il 25,4%**. Questo indica un aumento significativo delle ASIC rispetto al 2014, quando rappresentavano solo il 4,7% della potenza di hash.

Inoltre, le **performance delle ASIC e delle GPU sono migliorate notevolmente negli ultimi anni**. Ad esempio, nel 2013, la migliore ASIC disponibile sul mercato aveva un hash rate di circa 60 GH/s (gigaHash al secondo), mentre nel 2022, le migliori ASIC hanno un hash rate di oltre 100 TH/s (terahash al secondo), ovvero una crescita di oltre 1600 volte in meno di 10 anni. Anche le GPU sono migliorate in modo significativo: ad esempio, la NVIDIA GeForce GTX 680, che era una delle migliori GPU per il mining di digital asset nel 2013, aveva un hash rate di circa 300 MH/s (megahash al secondo), mentre la NVIDIA GeForce RTX 3090, rilasciata nel 2020, ha un hash rate di oltre 120 MH/s, ovvero una crescita di oltre 400 volte in meno di 10 anni.

La ricerca e lo sviluppo delle ASIC e delle GPU hanno quindi permesso un notevole miglioramento delle performance delle attrezzi di mining, sia in termini di hash rate che di efficienza energetica, portando ad una maggiore competitività del settore e ad una crescita dell'adozione dei digital assets.

5.6

Business

Basic

Quanto consuma davvero Bitcoin?



©VonWong - #SkullOfSatoshi

Tra le **principali critiche che vengono mosse verso Bitcoin troviamo quella relativa all'inquinamento e l'utilizzo di energia elettrica**. Tuttavia, l'energia elettrica è utilizzata per garantire sicurezza all'interno del network ed inoltre è un parametro molto importante per i modelli di competizione tra i miner.

Infatti, ogni miner per essere più profittevole cercherà:

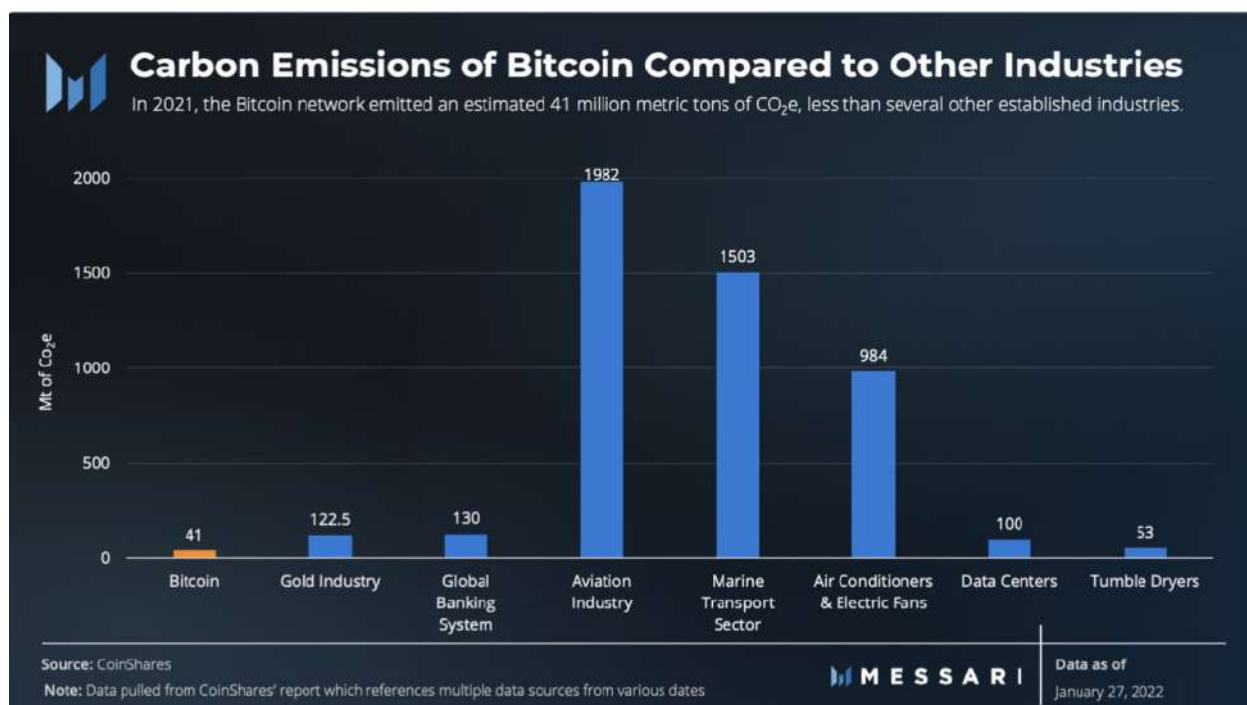
- Di far diminuire la quantità di energia necessaria per estrarre ogni bitcoin
- Di far diminuire il costo dell'energia necessaria per estrarre ogni bitcoin

Queste due condizioni hanno portato l'industria del mining a rivalutare la tipologia di energia utilizzata, cercando di spostarsi verso quelle più rinnovabili, in quanto meno costose rispetto a quelle legate al fossile. Ci sono alcuni studi che ci forniscono alcune stime ed indicazioni rispetto al tasso di penetrazione dell'utilizzo di energie rinnovabili all'interno del mercato del mining dei digital asset.

Secondo un rapporto pubblicato da CoinShares nel 2019, il **74,1% del mining di bitcoin utilizzava energia rinnovabile**, principalmente idroelettrica e geotermica. Tuttavia, questa stima si basa principalmente sui dati relativi alla Cina, che rappresentava il principale paese produttore di bitcoin nel mondo.

Altri studi, come quello condotto da Cambridge Bitcoin Electricity Consumption Index, suggeriscono che il tasso di utilizzo di energia rinnovabile nel mining di digital asset a livello globale potrebbe essere inferiore. Secondo i dati pubblicati nel 2021, il 39% del mining di bitcoin utilizzava energia rinnovabile, mentre per gli altri digital asset l'energia rinnovabile utilizzata è ancora più bassa.

Tuttavia, va considerato che il **settore del mining di digital asset è in continua evoluzione e sono in corso numerosi progetti e iniziative per aumentare l'utilizzo di energia rinnovabile** nel settore. Ad esempio, alcune società stanno investendo in progetti di energia solare e eolica per alimentare i propri impianti di mining, mentre altri stanno sviluppando tecnologie per il recupero dai gas di scarto delle miniere di carbone.



Infine, tutti i sistemi dinamici richiedono energia per funzionare costantemente nel tempo. Per mantenere un sistema dinamico funzionante, quindi, è necessario fornire energia e ridurre l'entropia il più possibile. L'entropia è una misura del caos in un sistema e tende a crescere nel tempo, causando una riduzione dell'efficienza del sistema. La comprensione della dinamica e dell'entropia dei sistemi complessi risulta di fondamentale importanza per la progettazione e il funzionamento di molte tecnologie e dispositivi odierni.

5.7

Business

● Basic

Dove vengono estratti oro e bitcoin?

L'estrazione dell'oro avviene in tutto il mondo, con alcune aree che si distinguono per l'abbondanza di giacimenti e la produzione. Secondo il World Gold Council, i paesi con la più alta produzione di oro nel 2021 sono stati:

1. **Cina: 368,1 tonnellate**
2. **Australia: 328,8 tonnellate**
3. **Russia: 306,4 tonnellate**
4. **Stati Uniti: 198,3 tonnellate**
5. **Canada: 143,6 tonnellate**

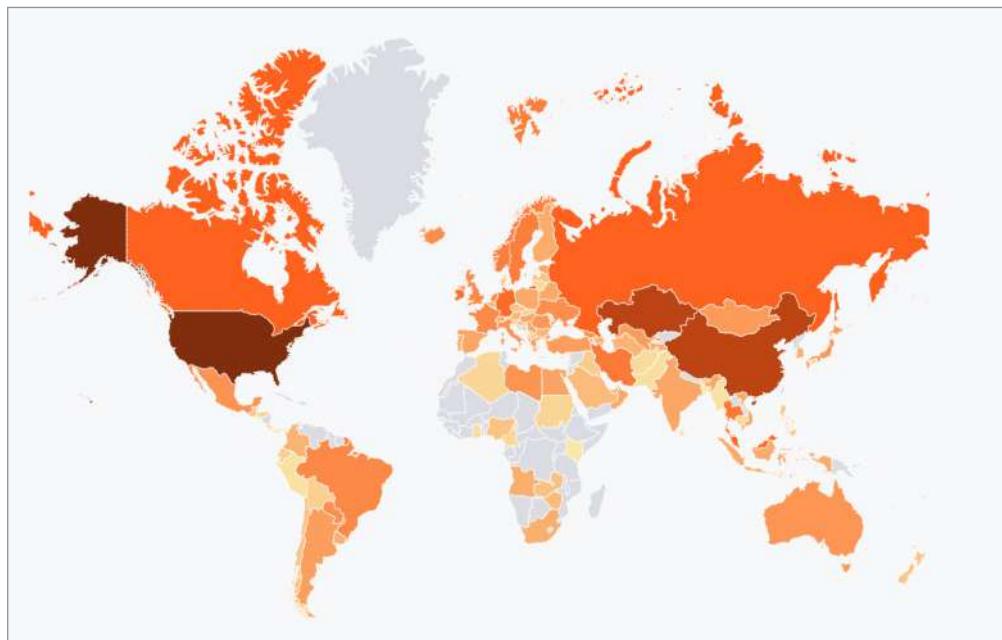
Altre nazioni che hanno una produzione significativa di oro includono il Perù, il Ghana e il Sudafrica.

Le aziende che producono la maggior parte dell'oro sono quelle che operano in modo intensivo nelle attività di estrazione e lavorazione del metallo. Secondo un rapporto del 2021 di Mining Technology, le principali aziende produttrici di oro sono:

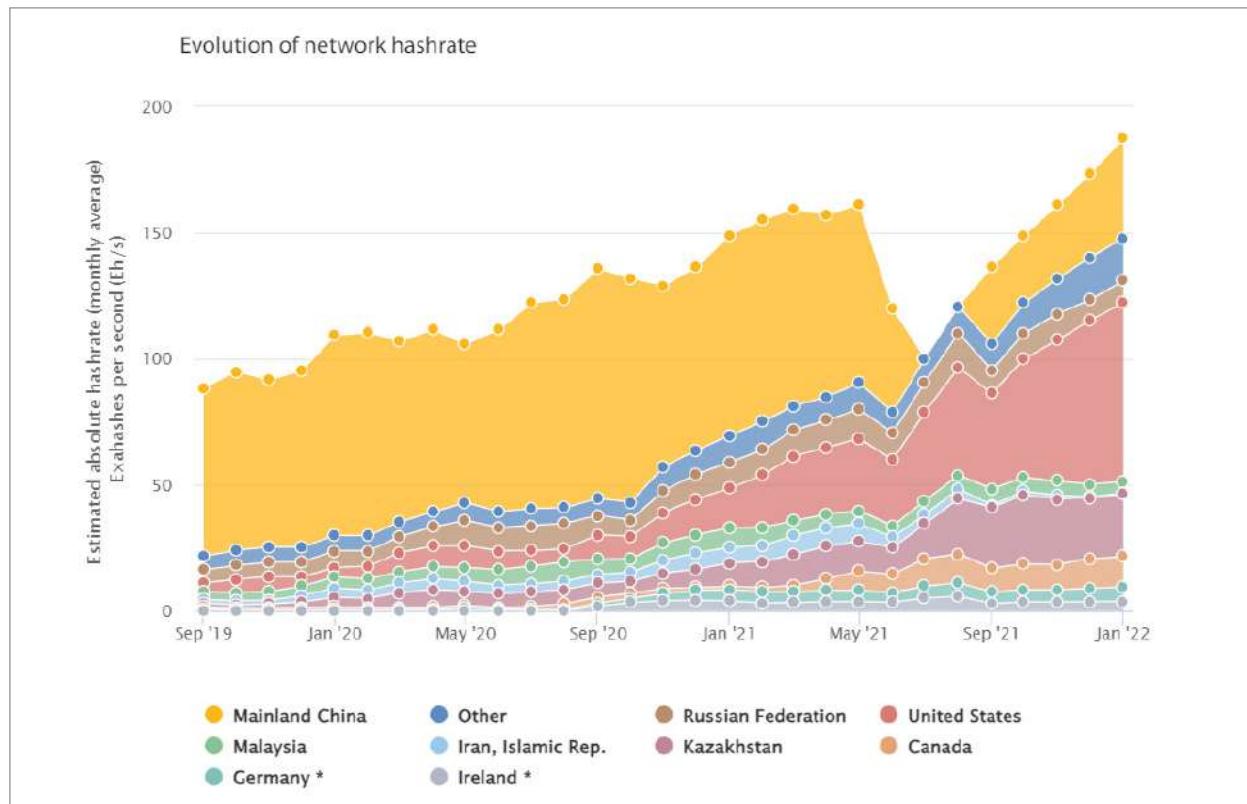
- **Newmont (Stati Uniti)**
- **Barrick Gold (Canada)**
- **AngloGold Ashanti (Sudafrica)**
- **Kinross Gold (Canada)**
- **Polyus (Russia)**

L'oro è stato estratto per millenni, ma ci si aspetta che la disponibilità di giacimenti diminuisca con il tempo a causa della sempre maggiore difficoltà nell'estrazione dell'oro dalle miniere. Tuttavia, le analisi geologiche sono ancora in grado di identificare potenziali nuovi giacimenti. Secondo un rapporto del 2021 di Gold.org, la quantità di oro che rimane da estrarre dipende dalla tecnologia, dall'innovazione e dall'aumento dei prezzi, ma si stima che ci siano ancora circa 54.000 tonnellate di oro economicamente recuperabili in tutto il mondo.

Per quanto riguarda Bitcoin, la **distribuzione di hashing power all'interno della rete cambia continuamente**, ma in generale il potere di hashing è concentrato in paesi con accesso a energia elettrica a basso costo e con una regolamentazione favorevole ai digital asset.



Dopo il ban della Cina sul mining di bitcoin nel 2021, l'hashing power si è distribuito in modo diverso rispetto al passato. In particolare, molte delle attività di mining che prima si concentravano in Cina sono state spostate in altre parti del mondo, come Nord America, Kazakistan e Russia. Questa redistribuzione dell'hashing power ha avuto un impatto significativo sulla distribuzione geografica della potenza di mining di bitcoin, con una riduzione del dominio cinese. Alcuni analisti ritengono che questo potrebbe portare a una maggiore decentralizzazione del mining di bitcoin e a una maggiore sicurezza della rete, poiché non ci sarebbe una concentrazione eccessiva di potere di mining in una sola regione.



Tuttavia, come si può notare dai grafici presi dal sito del Cambridge Centre for Alternative Finance, poco dopo il ban, l'hash rate proveniente dal territorio cinese è tornato a crescere.

Qui di seguito una lista di aziende internazionali che hanno come principale business model il mining di digital asset:

- **Bitmain (Cina)**
- **Riot Blockchain (USA)**
- **Marathon Digital Holdings (USA)**
- **Hut 8 Mining (Canada)**
- **Argo Blockchain (UK)**
- **Hive Blockchain (Canada)**
- **Northern Bitcoin AG: (Germania)**

Ad ogni modo, i **parametri considerati dai miner nello scegliere un paese all'interno di un business model possono variare in base a molteplici fattori, tra cui la regolamentazione governativa, la disponibilità di energia elettrica a basso costo, l'accesso a tecnologia avanzata e la stabilità politica ed economica.**

Fonti

- "Bitcoin Mining Difficulty", Bitcoin Wiki, <https://en.bitcoin.it/wiki/Difficulty>
- <https://ccaf.io/cbeci/index>

5.8

Teoria finanziaria
● Medium

Che cos'è il modello stock to flow?

Il rapporto Stock to Flow (S2F) è un indicatore utilizzato in finanza per valutare la rarezza di un asset. S2F rappresenta la **quantità di un asset che viene prodotto ogni anno in rapporto alla quantità totale esistente. Più elevato è il rapporto, più raro è l'asset e quindi più elevato è il suo valore potenziale.**

Ad esempio, l'oro ha un alto rapporto S2F perché viene prodotto solo una quantità limitata ogni anno. Al contrario, la produzione di petrolio è molto più elevata, il che significa che ha un rapporto S2F più basso. Esso si basa sul rapporto tra l'offerta circolante di un digital asset (stock) e la quantità di nuova offerta introdotta nel mercato (flow) in un determinato periodo di tempo. In particolare, il rapporto tra stock e flow è espresso in termini di anni, ovvero si confronta l'offerta esistente con l'offerta di nuovo rilascio in un anno.

Per quanto riguarda Bitcoin, il suo **rapporto S2F è considerato molto elevato a causa della limitata quantità di nuovi bitcoin che vengono prodotti ogni anno** attraverso il processo di mining. Questo rende Bitcoin un asset molto raro. Tuttavia, poiché il valore di Bitcoin è altamente volatile, non esiste una formula precisa per calcolarne il valore. Molti fattori, come la domanda e l'adozione, influenzano il prezzo di Bitcoin e possono causare fluttuazioni significative.

Il concetto di stock-to-flow (S2F) si riferisce quindi alla **quantità di una determinata risorsa (stock) che è disponibile rispetto alla quantità che viene prodotta ogni anno (flow)**. In altre parole, lo S2F è una **misura che indica quanto una risorsa è disponibile rispetto alla quantità che viene prodotta ogni anno**. Di seguito trovate la tabella con i valori Stock-to-Flow (S2F) di Oro dal 2010 al 2019:

Anno	Valore S2F dell'oro
2010	66.6
2011	65.1
2012	65.3
2013	63.8
2014	60.7
2015	59.6
2016	60.4
2017	59.1
2018	58.9
2019	59.9

Fonte: <https://seekingalpha.com/article/4357409-golds-stock-to-flow-ratio-and-why-matters>

Lo S2F di Oro è particolarmente importante in quanto l'oro è stato tradizionalmente considerato un bene rifugio e una riserva di valore per gli investitori. Infatti, la quantità di oro prodotta nel corso degli anni diminuisce progressivamente fino a quando non si troveranno nuovi luoghi in cui si può cercare questo metallo o si studieranno nuove modalità di estrazione.

Per quanto riguarda Bitcoin, la produzione è deterministica in quanto ogni 210.000, circa 4 anni, la quantità prodotta viene dimezzata, contraendo l'offerta del 50% rispetto ai 4 anni precedenti e con chiare ripercussioni rispetto al modello stock to flow.

Data inizio	Data fine	Block rew	Annual blocchi	Tot block	Annual BTC (FLOW)	Tot BTC (STOCK)	STOCK / FLOW
03-1-2009	03-1-2010	50 BTC	52560		2.680.000	2680000	1
03-1-10	03-1-11	50 BTC	52560		2.680.000	5.360.000	2
03-1-11	03-1-12	50 BTC	52560		2.680.000	8.040.000	3
03-1-12	28-11-12	50 BTC	52320	210.000	2.460.000	10500000	4,2
28-11-12	28-11-2013	25 BTC	52560		1.314.000	11.814.000	8,9
28-11-13	28-11-14	25 BTC	52560		1.314.000	13.128.000	9,9
28-11-14	28-11-15	25 BTC	52560		1.314.000	14.442.000	10,9
28-11-15	09-07-2016	25 BTC	52320	420.000	1.308.000	15.750.000	12,04
09-07-16	09-07-2017	12,5 BTC	52560		657.000	16.407.000	24,9
09-07-17	09-07-18	12,5 BTC	52560		657.000	17.064.000	25,9
09-07-18	09-07-19	12,5 BTC	52560		657.000	17.721.000	26,9
09-07-19	11-05-2020	12,5 BTC	52320	630.000	679.000	18400000	28,2
11-05-20	11-05-21	6,5 BTC	52560		341.640	18.741.640	54,8
11-05-21	11-05-22	6,5 BTC	52560		341.640	19.083.280	55,8
11-05-22	11-05-23	6,5 BTC	52560		341.640	19.424.920	56,8
11-05-23	04-03-24	6,5 BTC	52320	840.000	340.080	19.765.000	58,1
04-03-24	04-03-25	3,25 BTC	52560		170.820	19.935.820	116,7

Possiamo quindi osservare da questa tabella che il rapporto di stock to flow di Bitcoin, dopo il 2024 con il quarto halving che porta la quantità di bitcoin prodotta ogni 10 minuti a 3,25, un valore di stock to flow più alto rispetto a quello dell'oro.

Per concludere, il modello stock to flow cerca di rappresentare in maniera numerica la scarsità di un qualsiasi bene tramite un rapporto. Tuttavia, come abbiamo analizzato in precedenza, questo non rappresenta di per sé l'unico elemento da utilizzare per valutare il valore di un bene, ed inoltre, non tiene conto di tante altre variabili sociali che possono influire sul processo di misurazione di un asset digitale come bitcoin. Tuttavia, può aiutarci a mettere a confronto asset differenti rispetto alla loro produzione nel tempo.

5.9

Business

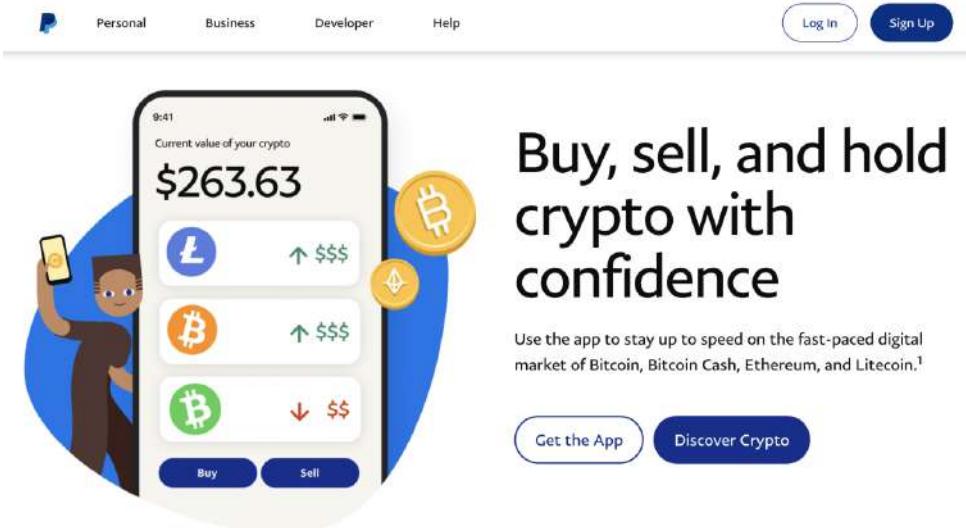
Basic

Bitcoin per gli Stati e le imprese

Negli ultimi anni, molti Stati e aziende tech si sono esposti a Bitcoin in diversi modi. Ad esempio, alcuni Stati hanno iniziato ad accettare Bitcoin come mezzo di pagamento, mentre alcune aziende tech hanno iniziato ad investire in Bitcoin o ad accettarlo come forma di pagamento per i propri prodotti e servizi. **Tra i Paesi che hanno mostrato un interesse nei confronti di Bitcoin, ci sono El Salvador, che nel 2021 è diventato il primo Stato al mondo ad adottare il Bitcoin come valuta legale, e l'Ucraina, che ha recentemente legalizzato il mining di digital asset e la registrazione delle transazioni blockchain.** La Svizzera, invece, è sede di una serie di start-up e progetti legati al Bitcoin ed ai digital assets, il progetto "Crypto Valley" di Zug, una città svizzera, si è guadagnato la reputazione di hub per le aziende legate al Bitcoin e ai digital assets.

Inoltre, il governo del **El Salvador ha emesso dei Bond su Bitcoin**. Si tratta di obbligazioni che pagano interessi in Bitcoin invece di valuta tradizionale. In pratica, gli investitori acquistano i bond in dollari e ricevono gli interessi e il capitale in Bitcoin. Questa iniziativa è stata lanciata nel 2021 come parte degli sforzi del governo di El Salvador per promuovere l'uso del Bitcoin come valuta legale nel paese.

Anche molte aziende tech hanno iniziato ad esplorare le potenzialità di Bitcoin. Ad esempio, **Tesla** ha investito 1,5 miliardi di dollari in Bitcoin nel 2021 e ha iniziato ad accettare i digital assets come forma di pagamento per i propri veicoli. Inoltre, **PayPal** ha annunciato di aver aggiunto Bitcoin alla lista dei metodi di pagamento accettati dai propri merchant negli Stati Uniti.



Nel mondo delle aziende, una delle **società più esposte a Bitcoin è MicroStrategy**, un'azienda di business intelligence con sede nella Silicon Valley. Nel 2020, MicroStrategy ha annunciato di aver investito 425 milioni di dollari in Bitcoin come parte della sua strategia di tesoreria. Successivamente, l'azienda ha aumentato ulteriormente il proprio investimento in Bitcoin e al momento detiene più di 100.000 Bitcoin, che rappresentano una parte significativa del suo valore di mercato.

Anche altre aziende americane della Silicon Valley si sono esposte a Bitcoin. Ad esempio, Square, la società di pagamenti fondata dal CEO di Twitter Jack Dorsey, ha investito 50 milioni di dollari in Bitcoin nel 2020 e ha successivamente aumentato il proprio investimento in digital assets.

Infine, molta ricerca e sviluppo è stata fatta da diverse aziende sparse in tutto il globo per migliorare i problemi di scalabilità e velocità dei layer 1, portando ad un incredibile entusiasmo attorno alle possibilità di questi protocolli peer to peer all'interno di contesti istituzionali come la tokenizzazione di asset.

5.10

Bitcoin a confronto con altri asset

Trading e mercato

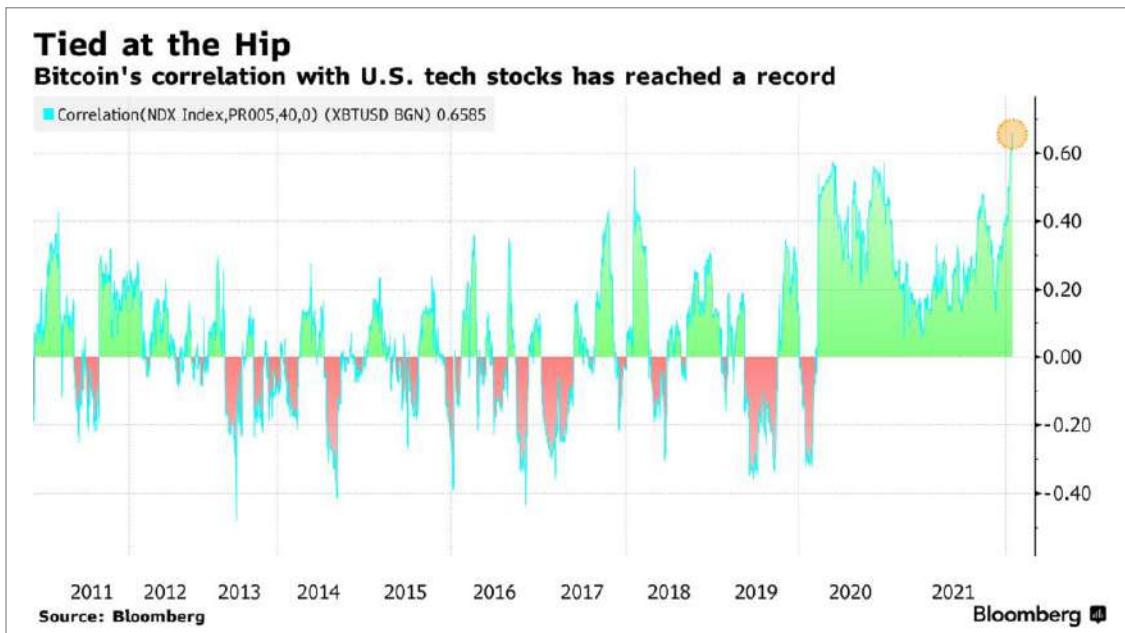
• Hard

Dopo la bolla del 2001, il mercato tecnologico ha subito un **periodo di volatilità durante il 2021 e il 2022**, con alcune delle principali aziende tech che hanno subito perdite significative nel valore delle loro azioni. Ad esempio, Meta (ex Facebook), TSMC, Nvidia, Tesla e Alibaba hanno visto ridursi il valore delle loro azioni rispettivamente del 56%, del 52%, del 50%, del 38% e del 36% (CNBC, 2022). Queste perdite hanno avuto un impatto significativo sul mercato azionario, con la riduzione del valore di alcune delle principali aziende tech che hanno portato ad una diminuzione del valore complessivo del mercato.

Azienda	Riduzione percentuale del valore delle azioni
Meta (ex Facebook)	-56%
TSMC	-52%
Nvidia	-50%
Tesla	-38%
Alibaba	-36%

Le ragioni alla base di questa volatilità del mercato sono complesse e variegate. Tra i fattori principali, vi è il **crescente timore di un aumento dell'inflazione e della stretta monetaria da parte delle banche centrali**, che ha portato ad una **riduzione dell'appetito per il rischio da parte degli investitori**. Inoltre, la **pandemia di COVID-19 ha avuto un impatto significativo sul mercato tech, con alcune aziende che hanno visto un calo della domanda dei loro prodotti e servizi**.

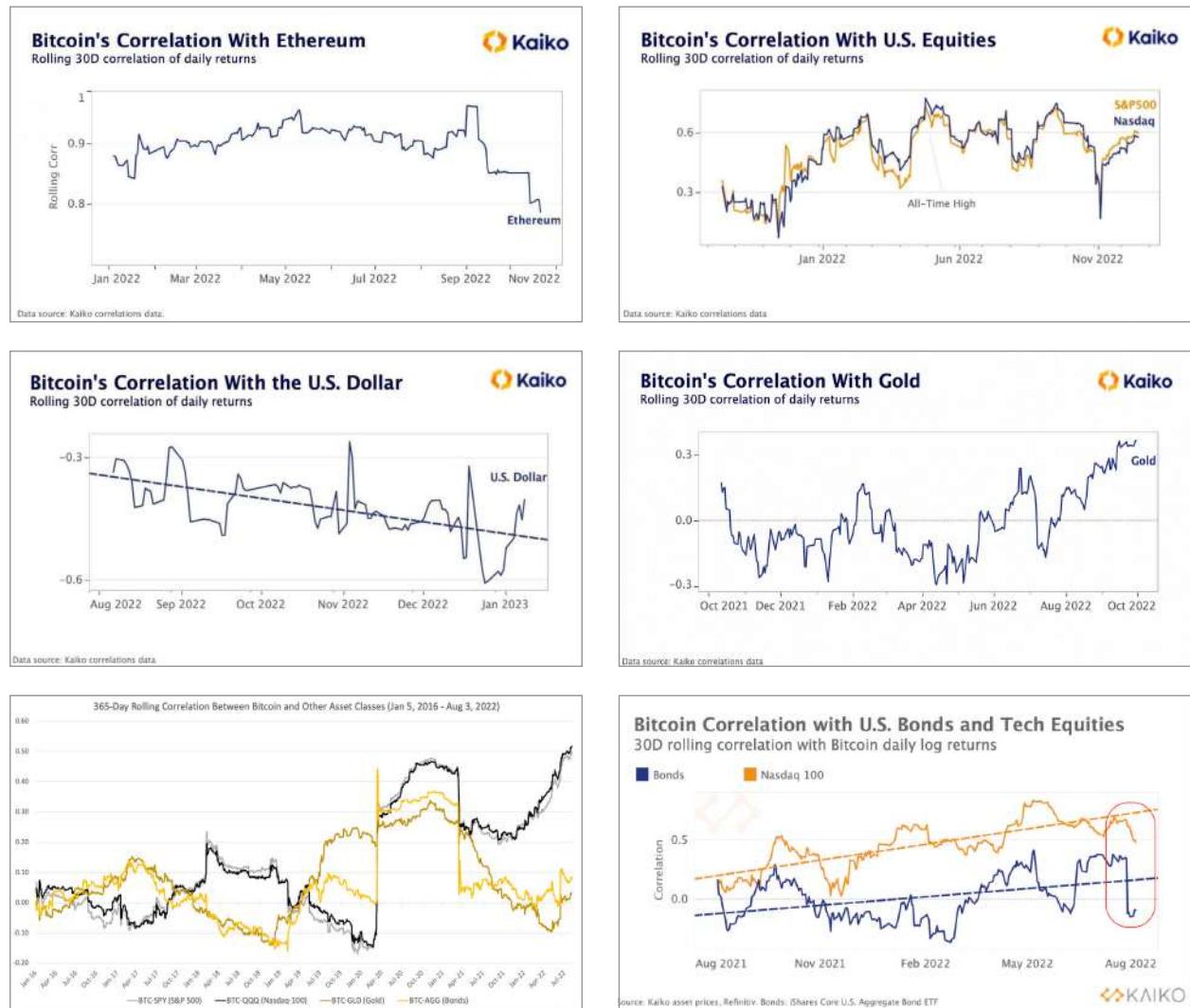
Le conseguenze di questo periodo di volatilità sulle aziende tech sono state molteplici, tra cui una riduzione delle entrate e una diminuzione della capacità di investimento. Inoltre, molte aziende hanno risposto alle difficoltà del mercato attraverso una riduzione dei costi, che spesso si è tradotta in licenziamenti. Ad esempio, nel settembre 2021, Uber ha annunciato un piano di riduzione dei costi che prevedeva il licenziamento di circa il 15% dei suoi dipendenti (CNBC, 2021). Analogamente, Intel ha annunciato nel marzo 2022 che avrebbe eliminato circa il 5% dei suoi dipendenti in tutto il mondo, come parte del suo piano di riorganizzazione aziendale (Reuters, 2022).



Questa crisi del mondo tech ha influito anche sul mercato dei digital assets, il quale si è dimostrato abbastanza correlato, perdendo anch'esso quasi il 60% della capitalizzazione totale del mercato. Nel corso di questa ultima parte, andremo ad analizzare come poter analizzare il valore nel token attraverso una serie di analisi ed indici.

I valori rappresentano la correlazione tra Bitcoin e gli altri asset per ogni anno. La correlazione può variare da -1 a 1, dove -1 indica una correlazione negativa perfetta, 1 indica una correlazione positiva perfetta e 0 indica nessuna correlazione.

Di seguito è presentata una tabella in cui figura la **correlazione tra Bitcoin, Ethereum, S&P, NASDAQ, e i US Bond:**



Per concludere, bitcoin ed in generale i digital asset stanno man mano entrando nel radar di clienti istituzionali e retail, poiché, per alcuni momenti di mercato, esso si comporta in maniera non correlata ad avvenimenti globali. Ad ogni modo, si è potuto osservare anche momenti di stretta correlazione con il mercato tech, durante periodi come il COVID.

Fonte

► <https://www.coindesk.com/markets/2022/10/06/bitcoins-correlation-with-gold-hits-highest-level-in-over-a-year/>

5.11

Trading e mercato

● Hard

Come utilizzo i dati on-chain per capire il mercato?

Per poter analizzare la diffusione dei nodi, la sicurezza della rete e la distribuzione della ricchezza vengono effettuate delle **l'analisi dei dati on-chain**, ovvero i dati pubblici sulla blockchain.

Questi dati includono informazioni sulle transazioni, i volumi di trading, il numero di indirizzi attivi e la distribuzione della ricchezza. L'analisi di questi dati può fornire una comprensione più approfondita delle dinamiche del mercato di Bitcoin e dei flussi di liquidità, che possono essere utili per prendere decisioni di investimento informate.

Di seguito alcuni parametri utili per analizzare la salute del progetto e la possibile evoluzione del mercato:

- Concentration index:
- Hashing power:
- Wallet Age / Number:

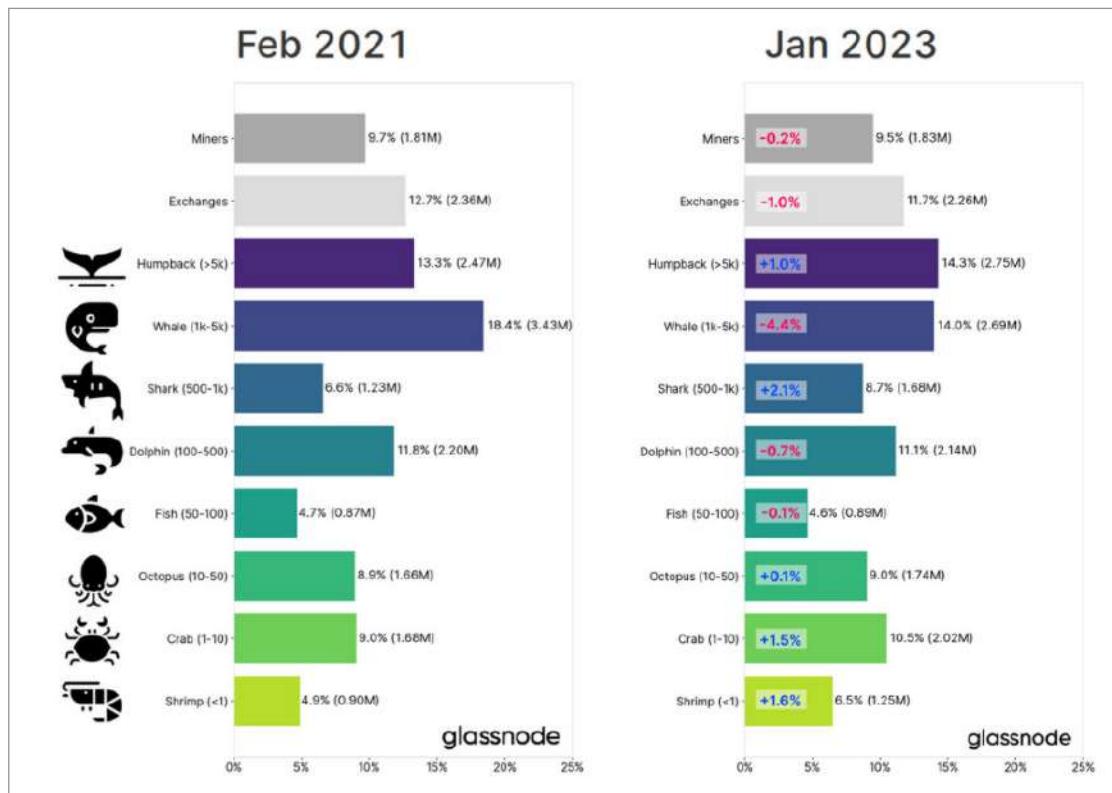
- In&out flow dagli exchange:
- Institutional investment:
- Stock to flow:

CONCENTRATION INDEX

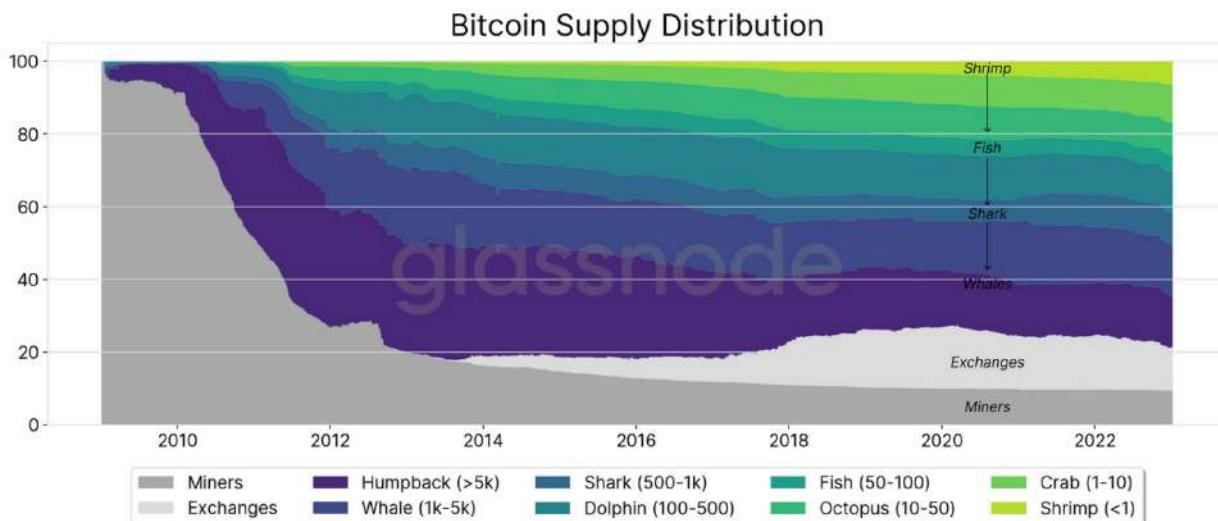
La distribuzione dei bitcoin all'interno della rete può essere uno dei primi dati da analizzare, rispetto alla “salute” del prezzo, e il potenziale rischio di grandi oscillazioni e manipolazione del prezzo nel lungo periodo, da parte di investitori marginali con forte potere sul prezzo.

Dividiamo le entità di rete in base alla loro quantità di Bitcoin posseduti nelle seguenti specie marine:

- | | |
|-----------------------|----------------------------|
| ● Gamberetti (<1 BTC) | ● Delfini (100-500 BTC) |
| ● Granchi (1-10 BTC) | ● Squali (500-1,000 BTC) |
| ● Polpi (10-50 BTC) | ● Balene (1,000-5,000 BTC) |
| ● Pesci (50-100 BTC) | ● Megattere (>5,000 BTC). |



Come possiamo osservare dai dati presentati da Glassnode, dal 2021 al 2023, **la distribuzione di Bitcoin è ancora abbastanza omogenea**. I dati sono stati calcolati analizzando la quantità di bitcoins in circolazione e come sono distribuiti i bitcoins all'interno dei wallet all'interno della rete che hanno fatto almeno una transazione.



L'analisi mostra la **differenza di distribuzione dal 2021 al 2023**, e questi dati supportano ulteriormente la tesi che **l'offerta di BTC sia continuata a distribuirsi nel tempo**, con la distribuzione incessante dei miner che ne è un esempio indicativo. Qui di seguito alcune considerazioni rispetto ai grafici presentati:

- Una proporzione sempre maggiore dell'offerta è detenuta da entità più piccole rappresentative dei detentori al dettaglio, con i Shrimp (<1 BTC) e i Crab (<10 BTC) che assorbono una quantità notevolmente superiore di monete rispetto a quelle estratte nel 2022.
- L'adozione istituzionale successiva al marzo 2020 è visibile on-chain in diverse dimensioni di portafoglio, con i saldi che mostrano segni di essere sempre più guidati dal mercato (ovvero che aumentano/diminuiscono al variare del prezzo).
- Le entità con un saldo compreso tra 10 e 1.000 BTC stanno assorbendo volumi di monete equivalenti al 100% delle monete emesse nel 2022.
- Le riserve degli exchange continuano a diminuire in modo aggregato, soprattutto a seguito del crollo di FTX. Questo è una combinazione sia di una domanda rinnovata per la self-custody, ma anche dell'espansione di soluzioni di custodia istituzionale e collaborativa e di prodotti negoziati in borsa come **GBTC**.



GBTC

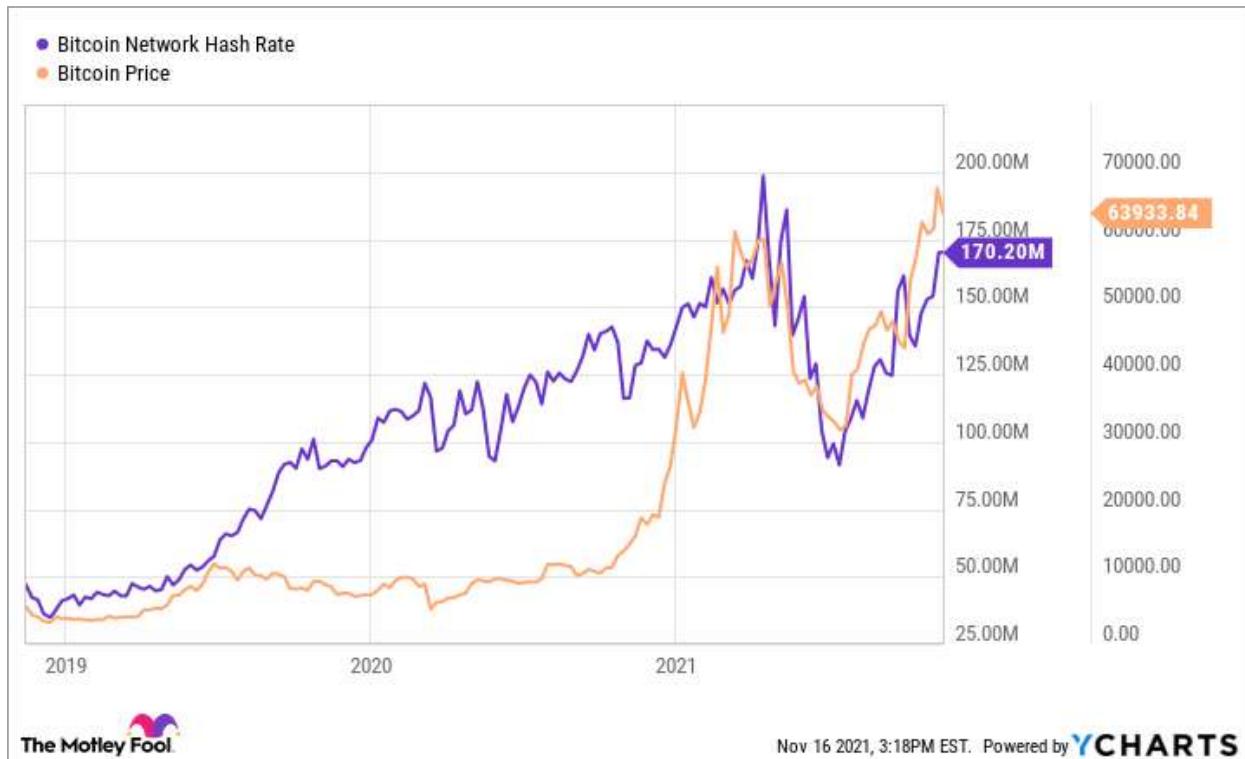
Definizione: Titolo quotato pubblicamente sul mercato over-the-counter OTCQX che offre agli investitori istituzionali la possibilità di ottenere un'esposizione passiva a Bitcoin senza dover acquistare, conservare e custodire direttamente i digital assets.

Fonente: <https://borsaefinanza.it/gbtc-di-grayscale-cos-e-come-funziona/#:~:text=GBTC%20%C3%A8%20un%20titolo%20quotato,e%20custodire%20direttamente%20la%20cripto%20attività>

HASHING POWER

L'hash rate rappresenta la potenza di calcolo della rete Bitcoin, ovvero la quantità di lavoro che i miner dedicano alla risoluzione dei problemi crittografici necessari per validare le transazioni e produrre nuovi blocchi di transazioni.

Il livello di hash rate della rete viene regolato automaticamente dal protocollo di Bitcoin ogni 2016 blocchi, circa ogni 2 settimane. Questo processo, noto come “aggiustamento della difficoltà di mining”, si basa su un algoritmo che valuta il tempo medio necessario per risolvere un blocco (in media, circa 10 minuti) e aggiorna la difficoltà di calcolo necessaria per risolvere il problema crittografico in modo da mantenere costante il tempo di generazione di un blocco.



In pratica, se l'hash rate della rete aumenta, il tempo medio di generazione dei blocchi diminuisce e quindi la difficoltà di calcolo viene aumentata. **Se l'hash rate diminuisce, il tempo di generazione dei blocchi aumenta e la difficoltà viene abbassata.** In questo modo, il protocollo di Bitcoin cerca di **mantenere costante il tempo di generazione dei blocchi a circa 10 minuti**, indipendentemente dal livello di potenza di calcolo dedicato alla rete.

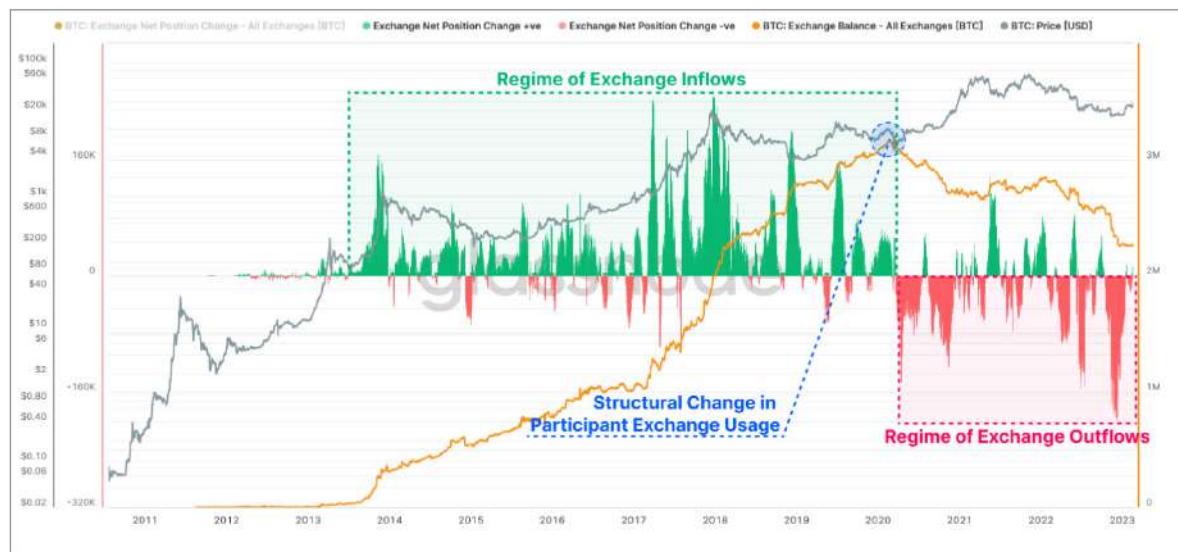
Il livello di hash rate della rete Bitcoin può fornire informazioni utili sul mercato finanziario. Infatti, l'hash rate è una **metrica importante per i miner che partecipano alla rete, poiché determina la loro capacità di guadagnare Bitcoin**. Maggiore è l'hash rate, maggiore è la concorrenza tra i miner e minore è la quantità di Bitcoin che ciascun miner può guadagnare.

Quando l'hash rate della rete Bitcoin aumenta, si può interpretare come un segnale di interesse crescente per i digital assets e, quindi, come un possibile indicatore di una tendenza al rialzo dei prezzi. Tuttavia, un **aumento dell'hash rate potrebbe anche portare a un aumento della difficoltà di mining, rendendo meno profittevole** per i miner dedicare potenza di calcolo alla rete Bitcoin. Al contrario, una diminuzione dell'hash rate potrebbe indicare un calo dell'interesse per i digital assets come un possibile segnale di una tendenza al ribasso dei prezzi.

In sintesi, l'**aggiustamento dell'hash rate nella rete Bitcoin è una tecnologia importante che garantisce la stabilità della rete e fornisce ai miner una metrica chiave per monitorare la loro attività di mining**. Tuttavia, l'hash rate non può essere considerato l'unico indicatore della tendenza dei prezzi del Bitcoin e va sempre valutato insieme ad altre metriche e dati del mercato finanziario.

OUTFLOW E INFLOW INDEX

L'analisi del flusso in entrata (on flow) e in uscita (out flow) di Bitcoin on-chain può essere utilizzata per aiutare a comprendere l'evoluzione del mercato finanziario in termini di momentum. L'**on-chain analytics** è una tecnica utilizzata per analizzare la blockchain di Bitcoin per estrarre informazioni sul flusso di transazioni, la distribuzione delle monete e altre metriche. L'on flow e l'out flow di Bitcoin sono due di queste metriche.



© 2023 Glassnode. All Rights Reserved.

glassnode

L'on flow di Bitcoin rappresenta la quantità di Bitcoin che si muove in un indirizzo wallet specifico, mentre **l'out flow rappresenta la quantità di Bitcoin che esce da un indirizzo wallet specifico**. Solitamente, questo modello viene utilizzato per calcolare l'ingresso e l'uscita dei bitcoins dagli exchange di digital asset.

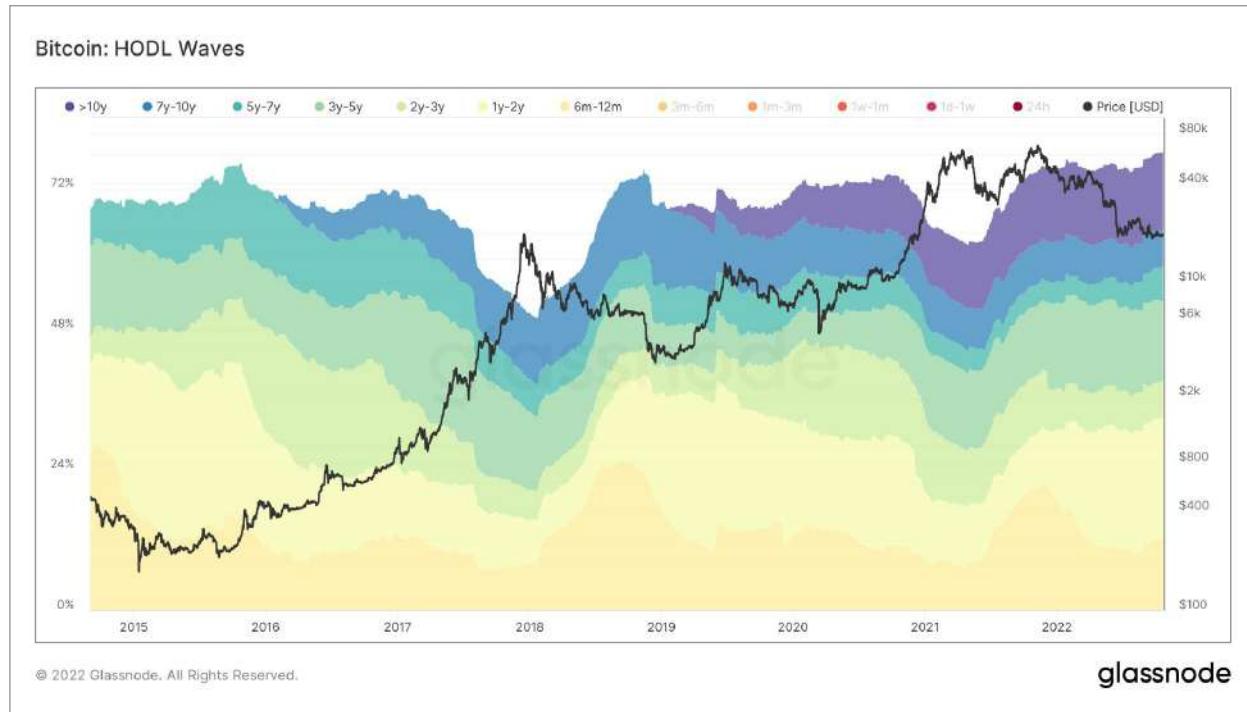
Analizzando questi dati, gli investitori possono capire se i grandi players del mercato stanno accumulando o vendendo Bitcoin. Ad esempio, se l'on flow di Bitcoin verso gli exchange è elevato, potrebbe significare che gli investitori stanno cercando di vendere la loro posizione in Bitcoin. Al contrario, se l'on flow è basso, potrebbe indicare che gli investitori stanno accumulando Bitcoin.

L'analisi dell'on flow e dell'out flow di Bitcoin on-chain può aiutare a capire l'evoluzione del mercato finanziario in termini di momentum. Se **l'on flow di Bitcoin è elevato e l'out flow è basso, potrebbe indicare un aumento della domanda di Bitcoin da parte degli investitori**, il che **potrebbe portare ad un aumento del prezzo**. Al contrario, se l'on flow è basso e l'out flow è elevato, potrebbe indicare che gli investitori stanno vendendo la loro posizione in Bitcoin, il che potrebbe portare ad un calo del prezzo.

WALLET AGE

Il concetto di "wallet age" si riferisce alla durata di tempo per cui un determinato portafoglio di digital assets è rimasto inattivo. Questo parametro è spesso utilizzato nell'analisi fondamentale dei digital assets per comprendere il comportamento dei titolari di portafogli di Bitcoin e per stimare lo spostamento dei flussi di valuta all'interno della rete. Il wallet age è utile per identificare i movimenti di vendita o di accumulo di Bitcoin da parte dei detentori di portafogli inattivi.

L'analisi del wallet age può fornire importanti indicazioni sulle dinamiche di mercato e sulla volatilità dei prezzi dei digital assets. In particolare, quando i wallet più vecchi iniziano a trasferire digital assets si ha un aumento della pressione di vendita, poiché i titolari di questi portafogli possono decidere di monetizzare i loro investimenti. Al contrario, quando i wallet più giovani si attivano con un aumento dei trasferimenti, ciò può indicare un aumento dell'attività commerciale e un possibile aumento della domanda.



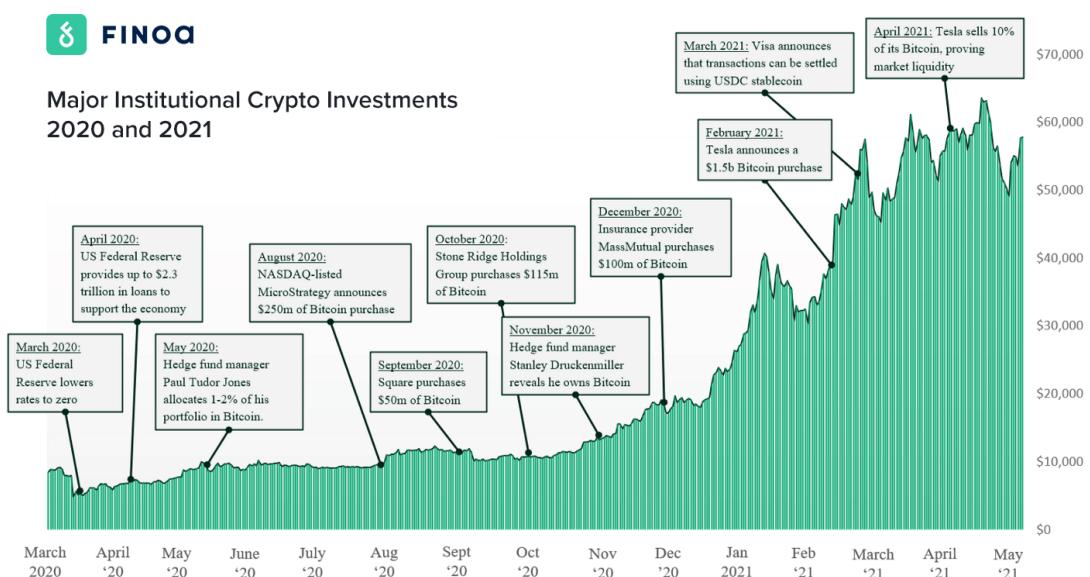
Il grafico mostra infatti come gran parte dei wallet all'interno della rete, tengono bitcoins nel lungo periodo, dimostrando che per molti è un asset da tesaurizzare nel tempo.

Il wallet age è quindi un importante indicatore della distribuzione di Bitcoin tra i partecipanti alla rete. L'analisi di questo parametro può essere **utilizzata per stimare la quantità di Bitcoin detenuta da determinati gruppi**, come i detentori a lungo termine o gli speculatori a breve termine. Ciò può fornire una **migliore comprensione della dinamica di domanda e offerta sul mercato**, il che può aiutare gli investitori a prendere decisioni informate in merito all'acquisto o alla vendita di digital assets.

In sintesi, l'analisi del wallet age è un importante strumento per comprendere il comportamento dei detentori di digital assets e le dinamiche di mercato della rete Bitcoin. Questo parametro può essere utilizzato per prevedere l'attività commerciale futura e identificare i movimenti di vendita o di accumulo di Bitcoin da parte dei partecipanti alla rete.

INSTITUTIONAL INVESTOR

L'ingresso degli investitori istituzionali è un fattore fondamentale da considerare nella valutazione di lungo periodo del mercato dei digital asset. La partecipazione di questi investitori ha rappresentato una svolta significativa per il mercato dei digital asset, poiché ha portato ad un **aumento della liquidità e dell'affidabilità**, e ha **contribuito ad accrescere la credibilità dei digital assets stessi**.



Gli investitori istituzionali sono solitamente società di gestione patrimoniale, fondi pensione, hedge fund e altri investitori di grandi dimensioni, che dispongono di ingenti risorse finanziarie da investire. **Questi investitori hanno un'influenza significativa sul mercato, in quanto possono generare volumi di trading significativi e stabilizzare il prezzo di un asset.** La loro partecipazione inizia ad essere rilevante per il mercato dei digital asset a partire dal 2017, quando sono stati introdotti i primi futures di bitcoin sulla Chicago Mercantile Exchange.

L'ingresso degli investitori istituzionali è un segnale importante della maturità del mercato dei digital asset, poiché indica che il mercato sta diventando sempre più regolamentato e riconosciuto dalle autorità finanziarie. Inoltre, la partecipazione di questi investitori ha spinto molte aziende nel settore a fornire prodotti e servizi mirati a soddisfare le esigenze degli investitori istituzionali, come i fondi di digital asset e i servizi di custodia sicura.

In sintesi, l'ingresso degli investitori istituzionali è un parametro importante da considerare nell'analisi fondamentale di lungo periodo del mercato dei digital asset, poiché indica una crescente accettazione e adozione dei digital assets come asset investibile e una maggiore stabilità del mercato.

Capitolo 7

LA GESTIONE DEL RISCHIO NEL WEB3



Introduzione

Il settimo capitolo ha come principale obiettivo quello di analizzare alcuni riferimenti normativi ed esaminare alcuni ipotetici scenari di rischio, sia informatici che operativi, applicabili ai servizi e agli strumenti del Web3, dei digital assets e delle tecnologie a registro distribuito (cd. DLT).

In particolare, quest'ultimo capitolo tenterà di aiutare il lettore a comprendere:

- le possibili implicazioni legali e di compliance relative alle dApps e Wallet;
- il ruolo e le attività regolatorie, laddove previste, delle Autorità;
- le principali normative a cui adeguarsi per creare un prodotto che possa essere compliant con le norme vigenti.

Il secondo obiettivo è quello di offrire un insieme di best practices ed una iniziale bozza di framework utile nella valutazione e nella misurazione del rischio informatico per i prodotti Web3, per poter disegnare e proporre sul mercato una soluzione che rispetti alcune delle condizioni di sicurezza per il cliente finale.

Il capitolo è strutturato con una prima parte dedicata al rischio informatico, sia per area pagamenti, sia per area investimenti, analizzando prima gli aspetti legati ai wallet e alle stablecoin, attraverso alcuni esempi di eventi negativi accaduti nel mercato, per poi introdurre alcuni rischi di cybersicurezza rispetto a soluzioni di finanza decentralizzata e non sul Web3.

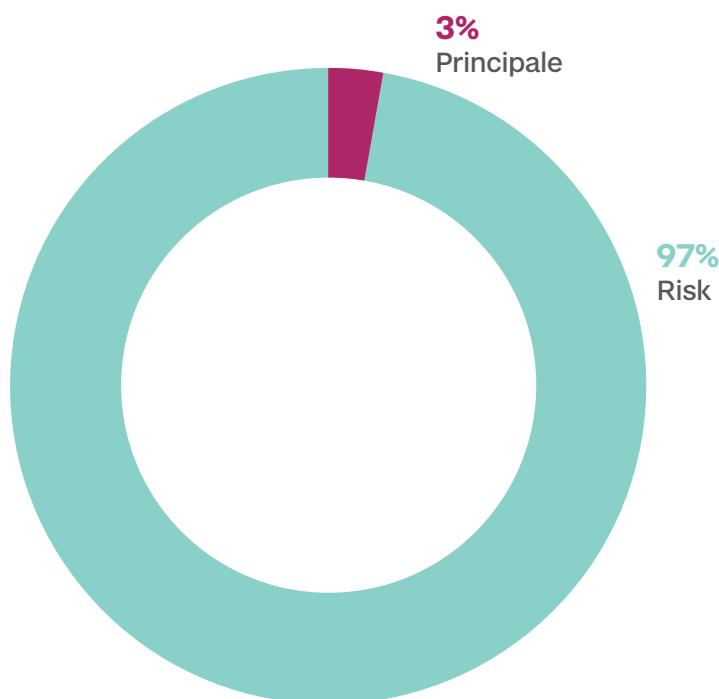
La seconda parte del capitolo invece è dedicata all'analisi del rischio legale e compliance, introducendo le principali normative applicabili ai digital assets classificabili come "strumenti finanziari e di pagamento".

In sintesi, il capitolo è composto da 6 macro-blocchi e 34 blocchi formativi, e cerca di fornire tutti gli strumenti concettuali necessari per affrontare il rischio relativo allo sviluppo di una soluzione sul Web3.

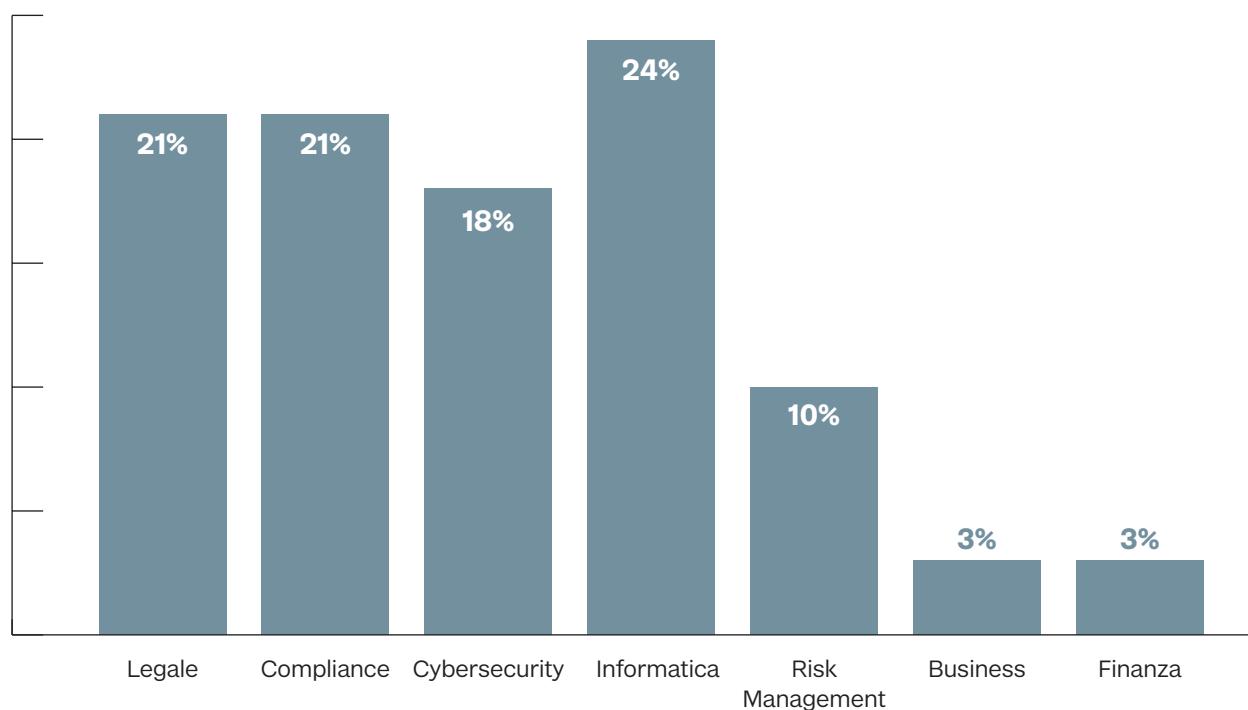
Queste alcune domande a cui cercheremo di rispondere:

- Com'è possibile garantire la sicurezza delle transazioni all'interno di un wallet e quali possono essere i rischi?
- Cosa ha causato l'hack di Parity dal punto di vista informatico?
- Cosa significa "Proof of reserve" in relazione alle stable coin e ai prestatori di servizio di custodia e compra-vendita? Come si può verificare e perché è importante ai fini del risk management?
- In che modo l'audit del codice sorgente e di una pool possono aiutare a prevenire rischi e vulnerabilità nei servizi di finanza decentralizzata?
- Come si può gestire il rischio di liquidità nella gestione di un liquidity pool?
- Quali sono le principali sfide in materia di cybersecurity che affrontano gli exchange nell'operare con nuovi prodotti sul Web3?
- Quali sono state le principali cause del fallimento di alcuni exchange?
- Come si gestiscono le chiavi di crittografia in un servizio di custodia e quali rischi sono associati alla loro gestione?
- Quali sono i rischi reputazionali legati al listing di un Digital Asset?
- Quali possono essere i principali rischi legali e di conformità che devono essere affrontati nel contesto dei protocolli permissionless come quelli utilizzati nei servizi digital asset?

Percentuale Percorsi



Percentuale Aree disciplinari



Indice

1. Introduzione al rischio

- 1.1 Come creare un framework di misurazione del rischio per un progetto Web3

DIFFICOLTÀ DISCIPLINA PERCORSO

● Risk Management Principale

2. Analisi rischio tecnologico per area pagamenti

- 2.1 Quali sono i rischi di connettere un wallet ad un protocollo peer to peer? ●
- 2.2 Attacco informatico ai wallet: il caso Parity ●
- 2.3 Proof of reserve di un servizio di custodia ●
- 2.4 Proof of reserve di una stablecoin proprietaria ●
- 2.5 Come dimostrare la proof of reserve? ●
- 2.6 Gestione di una liquidity pool ●



3. Analisi rischio tecnologico per area investimenti (CEX)

- 3.1 Gli exchange come vulnerabilità dell'ecosistema Web3 ●
- 3.2 Come analizzare la cybersicurezza di un exchange? ●
- 3.3 Key Management per un servizio di custodia proprietario ●
- 3.4 Quali sono i rischi reputazionali nel Web3? ●
- 3.5 Come gestire la tesoreria in un exchange ●



4. Analisi rischio tecnologico per area investimenti (DEX)

- 4.1 Il problema della liquidità nella finanza decentralizzata ●
- 4.2 Truffe nel mercato del Web3 ●
- 4.3 L'importanza della tokenomics in un progetto Web3 ●
- 4.4 Che cos'è lo slippage e l'Impairment Loss Scenario? ●
- 4.5 Che cos'è una rugpull? ●
- 4.6 Flash Loans e le vulnerabilità dei protocolli DEFI ●
- 4.7 Exploit e vulnerabilità: Il caso THE DAO ●



5. Analisi rischio legal e compliance per area investimenti e pagamenti

5.1 Data Act	● Legale	Risk
5.2 Basilea	● Compliance	Risk
5.3 GDPR	● Compliance	Risk
5.4 PSD2	● Legale	Risk
5.5 SLA e OLA nei protocolli permissionless	● Compliance	Risk
5.6 Digital Finance Package e MiCA	● Compliance	Risk
5.7 Gestione Fiscale dei Digital Assets	● Legale	Risk
5.8 MiFID II	● Compliance	Risk
5.9 Definizione normativa degli NFT	● Compliance	Risk Innovazione
5.10 DORA	● Legale	Risk
5.11 EMD2	● Legale	Risk
5.12 AML Act	● Compliance	Risk

6. Overview normativa su identità digitale

6.1 Regolamento eIDAS per l'identità digitale	● Legale	Risk Innovazione
6.2 EU Digital Identity Wallet con l'aggiornamento eIDAS	● Legale	Risk Innovazione
6.3 Che cosa sono gli SSI eIDAS Bridge?	● Informatica / Legale	Risk Innovazione

I TERMINI INSERITI NEL GLOSSARIO SONO EVIDENZIATI NEL TESTO CON IL COLORE ROSSO

1

Introduzione al rischio

1.1 Come creare un framework di misurazione del rischio per un progetto Web3

1.1

Risk Management

● Basic

Come creare un framework di misurazione del rischio per un progetto Web3

Creare un framework di misurazione del rischio è fondamentale per gestire i rischi associati a progetti Web3 come stablecoin, servizi di custodia e prodotti di finanza decentralizzata. Un framework ben strutturato deve affrontare **sia le esigenze normative che quelle di cybersecurity**.

Dal punto di vista normativo, il framework di rischio deve misurare il rischio specifico ed indicare se ci sono degli sforamenti alle soglie che ogni società si è data. La PSD2 richiede ai fornitori di servizi di pagamento di implementare misure di sicurezza adeguate a proteggere i dati dei clienti ed a prevenire le frodi. Il GDPR richiede ai titolari dei trattamenti di adottare misure di sicurezza adeguate a proteggere i dati personali degli interessati.

Nel caso in cui il digital assets sia riconducibile alla classe degli “strumenti finanziari” sarà importante garantire il rispetto della normativa MiFID II, la quale regola la prestazione di servizi di investimento, che potrebbero essere offerti anche tramite prodotti di finanza decentralizzata.

Inoltre, qualora il digital asset non sia classificabile come “strumento finanziario” (o altrimenti riconducibile ad ulteriori classi già ad oggi regolamentate) un’altra fonte da considerare sarà il regolamento MiCA, che impone ai Digital Asset Service Provider di implementare adeguati sistemi di gestione del rischio per prevenire potenziali minacce per la gestione di servizi legati al digital asset.

La cybersecurity è un’area di grande importanza per la gestione di progetti Web3 come stablecoin, servizi di custodia e prodotti di finanza decentralizzata. Ci sono diverse minacce che possono compromettere la sicurezza di questi progetti, tra cui:

- la generazione e la gestione delle chiavi,
- gli attacchi al codice della propria DApp o di un wallet
- il rischio reputazionale associato all’integrazione di protocolli DeFi che possono contenere bug e attacchi da hacker

La gestione delle chiavi è un aspetto fondamentale della sicurezza dei progetti Web3. Le chiavi private sono utilizzate per accedere al wallet, firmare trasferimenti e confermare l’identità degli utenti finali con cui si interagisce. La perdita o il furto di una chiave privata comporta l’impossibilità di accedere al relativo wallet e alla conseguente perdita di digital assets o al furto di dati personali.

Gli attacchi al codice sono un’altra minaccia importante per i progetti Web3. I bug del codice possono essere sfruttati dagli hacker per sottrarre digital assets o compromettere i dati degli utenti.

L’integrazione di protocolli DeFi che possono contenere bug può portare a gravi danni reputazionali. La perdita di digital assets o la compromissione dei dati degli utenti può avere un impatto significativo sulla reputazione del progetto e sulla fiducia degli utenti.

Un ulteriore aspetto da considerare sono le differenze riscontrabili nella regolamentazione e nelle prassi e orientamenti di vigilanza di ogni paese e area economica. Al fine di comprendere correttamente l’ecosistema, è necessario monitorare anche l’andamento delle prassi regolamentari e gli orientamenti di vigilanza di ogni paese ed area economica.

Qui una tabella per quello che riguarda il panorama **dell'Unione Europea**, a cui si aggiungono le normative di riferimento e le relative Autorità di Vigilanza nazionali degli Stati membri della Svizzera e degli Stati Uniti, con un esempio delle rispettive regolamentazioni e degli organi di vigilanza competenti.

Area Geografica	Regolamentazione	Organismo di vigilanza competente
Europa	MiFID II	Autorità europea degli strumenti finanziari e dei mercati (ESMA)
Europa	GDPR	Autorità europea per la protezione dei dati (EDPB)
Europa	SAMLD	Autorità europea di vigilanza bancaria (EBA)
Europa	Crypto-Asset Regulation (MiCa)	Autorità bancaria europea (EBA) ed Autorità europea degli strumenti finanziari e dei mercati (ESMA)
Svizzera	FINMA Guidance for Cryptoassets	Autorità di vigilanza dei mercati finanziari (FINMA)
Svizzera	AMLA	Autorità di vigilanza dei mercati finanziari (FINMA)
Stati Uniti	SEC Regulation D	Security Exchange Commision (SEC)
Stati Uniti	SEC Regulation A+	Security Exchange Commision (SEC)
Stati Uniti	SEC Regulation Crowdfunding	Security Exchange Commision (SEC)
Stati Uniti	FinCEN Guidance	Financial Crimes Enforcement Network (FinCEN)
Stati Uniti	IRS Notice 2014-21	Internal Revenue Service (IRS)
Europa	DORA	Autorità bancaria europea (EBA), Banca d'Italia e AGCOM
Europa	PSD2	Autorità bancaria europea (EBA), Banca d'Italia e AGCOM
Europa	AML Act	Le competenze dell'Autorità bancaria europea (EBA) nel settore AML/CFT sono rimosse e trasferite alla neo-istituita Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (AMLA), la cui attività di supervisione comincerà dal 2026.

In Europa, esistono diverse sandbox per i progetti su Distributed Ledger Technology (DLT) e Digital Asset. Una sandbox è un ambiente di test isolato in cui gli sviluppatori possono sperimentare e testare le loro soluzioni senza dover affrontare le conseguenze di eventuali errori o problemi.

Tra le sandbox più note vi è la Sandbox dell'Autorità di Vigilanza Finanziaria del Regno Unito (FCA), che consente alle aziende di testare le loro soluzioni fintech in un ambiente regolamentato e controllato. Inoltre, la Commissione Europea ha avviato una sandbox per le soluzioni DLT e blockchain, al fine di sperimentare nuove soluzioni nell'ambito della gestione dei pagamenti e della sicurezza finanziaria. Tra le sandbox europee troviamo la Sandbox dell'Autorità di Vigilanza Finanziaria francese (ACPR), la Sandbox dell'Autorità di Vigilanza Finanziaria tedesca (BaFin) e la Sandbox dell'Autorità di Vigilanza Finanziaria svizzera (FINMA).

Per concludere, un altro ente molto importante da monitorare, per le sue iniziative di stimolo e attività relative all'implementazione di politiche per la digitalizzazione europea, è DG Connect, ovvero la Direzione Generale della Commissione Europea responsabile delle politiche e delle attività relative alle tecnologie dell'informazione e della comunicazione (ICT) e alla digitalizzazione. Ad esempio, questo organismo ha sviluppato e coordinato progetti quali:

- **EBSI:** l'infrastruttura di servizi blockchain europea consiste in una rete di nodi interconnessi che gestiscono un'infrastruttura di servizi basata su blockchain, in cui, ogni membro della European Blockchain Partnership (EBP) - i 27 paesi dell'UE, la Norvegia, il Liechtenstein e la Commissione europea - gestirà almeno un nodo.
- **ESSIF-Lab:** Il progetto, finanziato dall'UE, che mira a rafforzare l'affidabilità di Internet con identità elettroniche attraverso lo sviluppo e l'adozione delle tecnologie come i DLT.

All'interno di questo capitolo andremo ad approfondire i temi trattati, sia per quello che riguarda il tema pagamenti, sia quello investimenti. Per finire, abbiamo riportato alcune considerazioni generali per la gestione del rischio di un progetto web3:

- Generare in ambienti offline le chiavi private, definite come masterkey.
- Implementare misure di sicurezza forti per proteggere le chiavi private, come l'utilizzo di crittografia a più fattori e l'archiviazione offline.
- Sottoporre il codice a verifiche continue per identificare e correggere eventuali vulnerabilità.
- Selezionare protocolli DeFi stabili e sicuri e condurre analisi dettagliate dei rischi associati.
- Implementare un sistema di monitoraggio costante per identificare tempestivamente eventuali minacce informatiche.
- Sottoporre il progetto a test di sicurezza e audit regolari.
- Formare adeguatamente il personale sulle best practice di sicurezza e sulle normative applicabili.
- Implementare un piano di risposta alle emergenze per gestire eventuali violazioni dei dati o altre minacce.
- Offrire il servizio ed un prodotto dopo un'attenta analisi normativa in funzione dell'area di mercato di riferimento.

Una chiara regolamentazione ed una forte attenzione rispetto alla sicurezza dei servizi potranno aiutare la diffusione di questa nuova tecnologia, aiutando il processo di dematerializzazione, semplificazione della finanza e della gestione delle moneta.

2

Analisi rischio tecnologico per area pagamenti

- 2.1 Quali sono i rischi di connettere un wallet ad un protocollo peer to peer?
- 2.2 Attacco informatico ai wallet: il caso Parity
- 2.3 Proof of reserve di un servizio di custodia
- 2.4 Proof of reserve di una stablecoin proprietaria
- 2.5 Come dimostrare la proof of reserve?
- 2.6 Gestione di una liquidity pool

2.1

Cybersecurity

● Medium

Quali sono i rischi di connettere un wallet ad un protocollo peer to peer?

Quando un wallet di digital asset viene collegato ad una **DApp (Decentralized Application)** che contiene del codice malevolo, ci sono diverse minacce di sicurezza a cui l'utente potrebbe essere esposto. Innanzitutto, lo **sniffing** (o il “fiutaggio”), una tecnica di attacco che permette ad un attaccante di intercettare e leggere il traffico di rete tra due dispositivi. Nel caso di un wallet di digital asset, se l'utente utilizza una DApp con una connessione di rete non sicura, un attaccante potrebbe utilizzare lo sniffing per intercettare le informazioni sensibili trasmesse tra il wallet e la DApp, come ad esempio la chiave privata del wallet, e utilizzarle per rubare i digital asset dell'utente.

Inoltre, un'altra minaccia a cui l'utente potrebbe essere esposto è un **attacco DDoS** (Distributed Denial of Service), in cui un attaccante, tramite del codice malevolo, invia una serie di transazioni e input verso il wallet che lo rendono inutilizzabile. In questo modo l'attaccante, rendendo inutilizzabile il wallet, tenta in contemporanea di entrare nella sicurezza perimetrale, per poi provare ad attaccare le informazioni all'interno.

Come approfondimenti a queste tematiche di seguito sono riportati tre paper:

“**Security Analysis of Ethereum Smart Contracts**” si concentra sulla sicurezza degli smart contracts, analizzando i meccanismi di sicurezza incorporati nella piattaforma Ethereum e valutando le vulnerabilità che possono essere sfruttate dagli attaccanti per compromettere i contratti. Gli autori discutono anche di tecniche di analisi statica e dinamica per identificare potenziali vulnerabilità nei contratti e forniscono linee guida per la scrittura di smart contract sicuri.

“**Blockchain Security: Risks, Threats, and Countermeasures**” fornisce una panoramica più ampia della sicurezza nella blockchain, analizzando le minacce potenziali e le contromisure disponibili per mitigare. Il libro fornisce una valutazione delle vulnerabilità e delle minacce che possono influenzare il funzionamento della blockchain, come gli attacchi DDoS, le vulnerabilità di rete e le minacce alla sicurezza delle transazioni.

“**A Survey on Security Issues and Challenges in Ethereum Smart Contracts**” fornisce un’analisi delle minacce più comuni ai contratti intelligenti e delle tecniche di sicurezza utilizzate per mitigare. Gli autori esaminano le vulnerabilità dei contratti intelligenti, come i bug di codice, gli attacchi di overflow, le falle nella sicurezza delle transazioni e le vulnerabilità della blockchain, e discutono delle tecniche per mitigare tali vulnerabilità.

Infine, “**Security Considerations for Smart Contracts in Decentralized Applications**” esamina le minacce alla sicurezza delle applicazioni decentralizzate che utilizzano gli smart contract di Ethereum. Gli autori analizzano le possibili vulnerabilità che le DApp possono presentare, come gli attacchi di tipo replay, le vulnerabilità nel codice dei contratti intelligenti e gli attacchi DDoS, e discutono delle tecniche di mitigazione disponibili.

Fonti

- ▶ “Security Analysis of Ethereum Smart Contracts” di Nicola Atzei, Massimiliano Bartoletti e Tiziana Cimoli (2017)
- ▶ “Blockchain Security: Risks, Threats, and Countermeasures” di Jun Wang, Yan Wang, Honggang Wang e Kui Ren (2019)
- ▶ “A Survey on Security Issues and Challenges in Ethereum Smart Contracts” di Shahbaz Ahmed Bhatti, Saif Ur Rehman, Fahad Islam e Hafiz Farooq Ahmad (2020)
- ▶ “Security Considerations for Smart Contracts in Decentralized Applications” di Gopika Premsankar e Abdulhadi Shoufan (2021)

2.2

Cybersecurity

● Hard

Attacco informatico ai wallet: il caso Parity

Nel 2017, la compagnia **Parity ha subito una vulnerabilità nella loro piattaforma di portafogli digitali Ethereum**. Il bug, inizialmente identificato da un utente del forum Ethereum, ha **permesso ad un hacker di congelare circa 153,037 Ether** all'interno dei portafogli Parity. Il bug è stato causato dall'implementazione di una funzione di biblioteca in un contratto intelligente che ha permesso agli utenti di creare contratti con la stessa libreria in modo da condividere il codice. Tuttavia, il codice di questo contratto è stato pubblicato come "pubblico" invece di "interno", il che ha permesso a chiunque di chiamare la funzione di congelamento e bloccare gli ether all'interno dei portafogli Parity.

L'aggressore ha inviato due transazioni a ciascuno dei contratti interessati: la prima per ottenere la proprietà esclusiva del MultiSig e la seconda per spostare tutti i suoi fondi.

Possiamo vedere che la prima transazione è una chiamata a initWallet (linea 216 di WalletLibrary):

```
// constructor - just pass on the owner array to the multiowned and // the limit to daylimit
function initWallet(address[ ] _owners, uint _required, uint _daylimit){
    initDaylimit(_daylimit);
    initMultiowned( owners, required); }
```

Questa funzione è stata probabilmente creata come un modo per estrarre la logica del costruttore del portafoglio in una libreria separata. Questo utilizza un'idea simile al modello delle librerie proxy di cui abbiamo parlato in passato. Il contratto del portafoglio inoltra tutte le chiamate di funzione senza corrispondenza alla libreria utilizzando `delegatecall`, nella riga 424 di Wallet:

```
function() payable {
    // just being sent some cash?
    if (msg.value > 0)
        Deposit(msg.sender, msg.value);
    else if (msg.data.length > 0)
        walletLibrary.delegatecall(msg.data);
}
```

Ciò fa sì che tutte le funzioni pubbliche della libreria siano richiamabili da chiunque, incluso initWallet, che può modificare i proprietari del contratto. Sfortunatamente, initWallet non ha controlli per impedire ad un utente malintenzionato di chiamarlo dopo che il contratto è stato inizializzato. L'attaccante ha sfruttato questo e ha semplicemente cambiato la variabile di stato m_owners del contratto in un elenco contenente solo il loro indirizzo e che richiede solo una conferma per eseguire qualsiasi transazione:

Successivamente, si trattava solo di invocare la funzione `execute` per inviare tutti i fondi a un conto controllato dall'attaccante:

Function: execute(address to, uint256 value, bytes data) ***

MethodID: 0xb61d27f6

Questa esecuzione è stata autorizzata automaticamente, poiché l'attaccante era allora l'unico proprietario del multisig, prosciugando di fatto il contratto di tutti i suoi fondi.

L'attacco avrebbe potuto essere prevenuto non estraendo del tutto la logica del costruttore nel contratto della libreria, o meglio non usando delegatecall come meccanismo di inoltro catch-all. Il modello consigliato definisce in modo esplicito quali funzioni di libreria possono essere richiamate esternamente sul contratto del portafoglio.

È importante notare che la tecnica di astrarre la logica in una libreria condivisa può essere molto utile poiché aiuta a migliorare la riusabilità del codice e riduce i costi di implementazione del gas. Questo attacco, tuttavia, chiarisce che è necessario un insieme di best practice e standard nell'ecosistema Ethereum per garantire che questi modelli di codifica siano implementati in modo efficace e sicuro. Altrimenti, il bug dall'aspetto più innocente può avere conseguenze disastrose.

Fonti

- ▶ The Parity Wallet Hack Explained, Open Zeppelin
 - ▶ <https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7>

2.3

Finanza / Risk Management

● Basic

La proof of reserve di un servizio di custodia

Il concetto di **Proof of Reserve (PoR)** è un **metodo utilizzato dalle aziende che offrono servizi di custodia di digital asset per dimostrare che detengono le risorse crittografiche che sostengono le obbligazioni verso i propri clienti**. In pratica, il Proof of Reserve è una dimostrazione crittografica che le risorse custodite sono effettivamente presenti e che sono accessibili solo al proprietario legittimo o al custode. Le aziende che offrono servizi di custodia di digital asset utilizzano diversi metodi per dimostrare il Proof of Reserve.

Di seguito sono elencate alcune delle **principali aziende legate ai digital asset che offrono servizi di custodia o servizi e soluzioni IT strumentali** rispetto alla fornitura di servizi di custodia da parte di terzi e che hanno dichiarato il proprio AUM (Assets Under Management) e la percentuale del capitale detenuto come Proof of Reserve:

1. **BitGo**: è un'azienda di custodia di digital asset che ha dichiarato di gestire oltre **\$40 miliardi di attività in digital asset** e che il 100% delle risorse è verificabile attraverso il Proof of Reserve.
 2. **Anchorage**: è un'azienda di custodia di digital asset istituzionale che ha dichiarato di gestire oltre **\$10 miliardi di attività in digital asset** e che utilizza un metodo di Proof of Reserve basato su firme crittografiche multi-firma.
 3. **Coinbase Custody**: è una divisione di Coinbase che offre servizi di custodia di digital asset istituzionali. La società ha dichiarato di gestire oltre **\$120 miliardi di attività in digital asset** e utilizza un metodo di Proof of Reserve basato su registri hash verificabili.
 4. **Gemini Custody**: è un'azienda di custodia di digital asset che ha dichiarato di gestire oltre **\$30 mi-**

liardi di attività in digital asset e che utilizza un metodo di Proof of Reserve basato su registri hash verificabili.

5. **Fireblocks:** piattaforma di gestione e custodia di asset digitali che fornisce soluzioni sicure per le istituzioni finanziarie e le imprese che desiderano gestire in modo efficiente i loro asset crittografici. Fondata nel 2018, Fireblocks si è rapidamente affermata come uno dei principali fornitori di servizi strumentali alla custodia e gestione degli asset digitali.

Queste sono solo alcune delle principali aziende che offrono servizi di custodia di digital asset e che utilizzano il Proof of Reserve per dimostrare la propria trasparenza e affidabilità nella gestione delle risorse dei clienti.

Secondo l'insider della blockchain Nick Carter, diversi scambi e istituti di credito hanno fornito volontariamente un PoR a partire da novembre 2022:

- Kraken (assistito dall'auditor, convalida dell'utente con approccio merkle, punto nel tempo) (11/2022)
- BitMex (autovalutazione, convalida dell'utente con approccio merkle, in corso) (11/2022)
- Coinfloor (autovalutazione, validazione utente con approccio merkle) (08/2021)
- Gate.io (assistito dal revisore, convalida dell'utente con approccio merkle, punto nel tempo) (05/2020)
- HBTC (autovalutazione, convalida dell'utente con approccio merkle, point in time) (05/2021)
- CakeDeFi (attestazioni trimestrali con prova patrimoniale) (11/2022)
- Nexo (assistita da auditor, in corso) (attestato giornaliero)
- Ledn (convalida utente con approccio merkle, in corso [semestralmente]) (08/2021)

Un'altra serie di scambi ha fornito una prova di attività senza passività corrispondenti:

- Binance, istantanea 10/11/22 (dashboard Nansen)
- Bitfinex, istantanea 11/11/22 (dashboard Nansen)
- Crypto.com, (segnalato per la prima volta l'11/11/22, Nansen)
- OKX (Nansen)
- KuCoin (Nansen)
- Deribit (Nansen)
- Huobi (Nansen)

Un'attestazione PoR segnala la vigilanza sulla solvibilità di una borsa. Aumenta la fiducia dell'utente in un custode e testimonia un certo grado di trasparenza che il custode garantisce.

Il PoR è uno strumento di autoregolamentazione. Anche se alcuni scambi non sono regolamentati negli Stati Uniti, il PoR può comportare un trattamento più favorevole da parte delle autorità di regolamentazione statunitensi e una maggiore fiducia da parte della loro base di utenti. Il PoR rende più difficile oscurare pratiche commerciali illegali e non etiche come il rehypothecating dei depositi degli utenti.

Tuttavia, PoR non è affidabile. Si basa sull'impegno volontario e non garantisce la piena trasparenza della situazione finanziaria di un custode. Tuttavia, dato lo scarso livello di trasparenza del settore riguardo ai fondi dei clienti, è considerato da molti un inizio per stabilire uno standard minimo di autoregolamentazione. Inoltre, gli scambi e gli istituti di credito sono incoraggiati e liberi di cercare una regolamentazione aggiuntiva per aumentare la propria reputazione sul mercato e, così facendo, guadagnare la fiducia dei propri clienti.

2.4

Informatica

● Basic

La proof of reserve di una stablecoin proprietaria

Per quanto riguarda la **gestione del rischio**, la **prova di valore è un concetto importante per la stabilità di una stablecoin**. La stabilità del valore è solitamente **garantita da una riserva di attività sottostanti o di valuta fiat**, attraverso un insieme di smart contract.

La prova di valore è il processo di dimostrazione che la riserva di attività sottostanti o di valuta fiat è adeguata a garantire la stabilità del valore della stablecoin. Ciò richiede una **verifica regolare delle riserve e una garanzia che il valore delle attività sottostanti sia sufficiente a sostenere il valore della stablecoin**.

Per approfondire il codice di una stablecoin, il processo di audit del codice sorgente su un protocollo come Ethereum è un processo critico che richiede una revisione accurata del codice per identificare eventuali problemi di sicurezza e garantire che il codice sia conforme alle specifiche del protocollo.

La prima fase di questo processo è l'**analisi del codice sorgente**, in cui il team di audit esamina il codice per garantire che sia conforme alle specifiche del protocollo e alle best practices per la scrittura di codice sicuro e robusto. Ciò può includere la revisione della struttura del codice, la verifica della coerenza delle variabili e delle funzioni, nonché la valutazione del codice per identificare eventuali problemi di sicurezza.

Successivamente, il **team di audit dovrebbe eseguire verifiche di sicurezza**, come la valutazione della vulnerabilità dei contratti intelligenti. I contratti intelligenti sono programmi autonomi che eseguono codice sulla blockchain e sono spesso utilizzati per implementare le transazioni in Ethereum. Ciò significa che è fondamentale valutare la sicurezza dei contratti intelligenti per garantire che non siano vulnerabili ad attacchi esterni.

Inoltre, il **team di audit dovrebbe verificare che il codice implementi le procedure di sicurezza standard, come l'autenticazione degli utenti e la gestione degli errori**. Ciò aiuta a garantire che il codice sia resistente agli attacchi esterni e che sia in grado di gestire eventuali errori o situazioni di emergenza.

Infine, il **team di audit dovrebbe eseguire una revisione del codice per identificare eventuali aree di debolezza potenziale**. Ciò può includere la valutazione del codice per la presenza di vulnerabilità note, l'analisi della coerenza dei dati e il controllo delle dipendenze del codice.

2.5

Cybersecurity

● Basic

Come dimostrare la proof of reserve?

Esistono diversi modi in cui le aziende che offrono servizi di custodia di digital asset possono **dimostrare il Proof of Reserve**. Ecco alcune delle modalità più comuni:

1. **Registri hash**: una modalità comune di Proof of Reserve consiste nel **pubblicare un registro hash delle risorse detenute in un determinato momento**. Questo registro hash viene quindi confrontato con la quantità di digital asset che i clienti dicono di possedere, dimostrando che le risorse sono presenti e che sono accessibili solo al proprietario legittimo. Questo metodo di Proof of Reserve è relativamente semplice e può essere eseguito da qualsiasi azienda di custodia di digital asset.

2. **Firme crittografiche multi-firma:** un'altra modalità di Proof of Reserve consiste nell'**utilizzo di firme crittografiche multi-firma**, in cui **più parti devono fornire la loro firma per confermare l'accesso alle risorse detenute**. In questo modo, le risorse possono essere dimostrate come autentiche e accessibili solo dal proprietario legittimo. Questo metodo è spesso utilizzato da aziende di custodia di digital asset istituzionali.
3. **Audit esterni:** alcune aziende di custodia di digital asset possono scegliere di effettuare un **audit esterno per dimostrare il Proof of Reserve**. In questo caso, un'agenzia di audit indipendente esamina i conti dell'azienda e conferma che le risorse detenute sono effettivamente presenti e accessibili solo al proprietario legittimo. Questo metodo può essere **costoso, ma può fornire un alto grado di affidabilità** nella verifica delle risorse detenute.
4. **Tecnologie blockchain:** infine, alcune aziende di custodia di digital asset possono utilizzare la **tecnologia blockchain per dimostrare il Proof of Reserve**. Ad esempio, alcune aziende possono **pubblicare un registro hash delle transazioni di digital asset che conferma l'esistenza delle risorse detenute**. Inoltre, alcune piattaforme blockchain offrono funzionalità di smart contract per consentire la convalida crittografica delle risorse detenute.

In generale, il Proof of Reserve è un **metodo crittografico che fornisce una maggiore trasparenza e affidabilità nella gestione delle risorse dei clienti da parte delle aziende di custodia di digital asset**. L'utilizzo di diverse modalità di Proof of Reserve può offrire un ulteriore livello di sicurezza e garanzia per i clienti che utilizzano questi servizi.

2.6

Informatica

● Medium

Gestione di una liquidity pool

Una liquidity pool nella finanza decentralizzata (DeFi) è un **insieme di fondi bloccati in una smart contract che permette agli utenti di scambiare tra loro diversi digital asset o token senza la necessità di un intermediario**. I partecipanti a una liquidity pool, noti come **liquidity provider**, depositano una quantità di due diversi **digital asset o token** nella proporzione richiesta dal protocollo e **in cambio ricevono un certo numero di token LP (liquidity pool tokens)** che rappresentano la loro **quota di partecipazione alla pool**. Gli utenti possono in seguito scambiare questi token LP con altri digital asset o token oppure venderli a altri utenti interessati.

La creazione di un liquidity pool è un **processo critico per la fornitura di liquidità nei mercati decentralizzati**, in cui i trader possono acquistare e vendere digital asset e token. Esistono diverse modalità per creare un liquidity pool, in cui i partecipanti possono fornire liquidità utilizzando digital asset o token.

Una delle **modalità più comuni per creare un liquidity pool è l'utilizzo di una piattaforma di exchange decentralizzata (DEX), come Uniswap o SushiSwap**. In questi casi, i partecipanti possono fornire liquidità attraverso una coppia di digital asset o token, in cui la quantità di ogni asset viene determinata dal rapporto di scambio tra i due asset. La piattaforma DEX utilizza quindi un algoritmo di scambio automatico per calcolare il prezzo di scambio in tempo reale, utilizzando il volume di liquidità disponibile nel pool.

Un altro approccio per la creazione di un liquidity pool è l'**utilizzo di un protocollo di sintesi, come Synthetix o Mirror**. In questo caso, i partecipanti possono fornire liquidità attraverso l'emissione di un token sintetico, che rappresenta un bene o una risorsa esterna alla blockchain. Questo token sintetico è poi utilizzato come base per il trading di altri token sulla piattaforma.

Infine, un **terzo approccio per la creazione di un liquidity pool è l'utilizzo di un protocollo di prestito, come Compound o Aave**. In questo caso, i partecipanti possono fornire liquidità attraverso il prestito di digital asset o token ad altri utenti della piattaforma. I prestiti sono garantiti da un sistema di collaterale, che consente di ridurre il rischio di default.

Il ruolo dei liquidity pool nella stabilizzazione di una stablecoin consiste quindi nel fornire liquidità sul mercato e garantire un prezzo stabile e prevedibile per la stessa. Inoltre, i liquidity pool consentono di **creare un mercato per la stablecoin**, in cui gli utenti possono acquistarle e venderle in modo rapido ed efficiente, senza incorrere in costi eccessivi.

In conclusione, i liquidity pool rappresentano un elemento fondamentale per la stabilizzazione di una stablecoin, garantendone la disponibilità di liquidità e un prezzo stabile e prevedibile.

3

Analisi rischio tecnologico per area investimenti (CEX)

- 3.1 Gli exchange come vulnerabilità dell'ecosistema Web3
- 3.2 Come analizzare la cybersicurezza di un exchange?
- 3.3 Key Management per un servizio di custodia proprietario
- 3.4 Quali sono i rischi reputazionali nel Web3?
- 3.5 Come gestire la tesoreria in un exchange

3.1

Cybersecurity

● Medium

Gli exchange come vulnerabilità dell'ecosistema Web3

Dal 2009 ad oggi, la lista degli exchange che sono falliti è molto lunga. Molti di questi sono falliti per cause endogene, come un pessimo management, pessima gestione finanziaria e della tesoreria, e una bassa valutazione del rischio, altri invece per cause esogene come attacchi hacker e “bear” market che non ha permesso di sopravvivere ai costi.

Il **fallimento di Mt. Gox**, una volta il **più grande exchange di bitcoin al mondo**, è stato uno dei **più grandi scandali della storia dei digital asset**. Analizzando la situazione in maniera schematica, ecco alcuni dei principali punti da considerare:

Aspetti del mercato:

- Mt. Gox aveva la maggior parte delle quote di mercato dell'exchange di bitcoin nel mondo, con una quota superiore al 70% nel 2013.
- Tuttavia, **l'exchange ha subito molte interruzioni nel trading e problemi tecnici che hanno causato problemi di liquidità e ritardi nei prelievi**.
- Inoltre, i **problematiche di sicurezza dell'exchange**, con numerosi hacking e furti di bitcoin, hanno causato la perdita di oltre 850.000 bitcoin per i clienti dell'exchange.

Aspetti normativi:

- Inizialmente, Mt. Gox **non aveva alcuna regolamentazione ufficiale come exchange** di bitcoin, poiché il governo giapponese non ha regolamentato i digital asset fino al 2017.
- Tuttavia, la **mancanza di una chiara regolamentazione ha permesso a Mt. Gox di operare senza controlli adeguati e ha contribuito alla mancanza di sicurezza dell'exchange**.

Aspetti di cybersecurity:

- Gli **hacker hanno rubato circa 850.000 bitcoin da Mt. Gox**, il che rappresenta circa il 7% di tutti i bitcoin in circolazione al momento del furto.
- Secondo i rapporti, il **furto è stato causato da una vulnerabilità nella sicurezza dell'exchange** e da una gestione negligente delle chiavi private di criptaggio.

Aspetti legali e di responsabilità:

- In seguito al fallimento di Mt. Gox, sono state **avviate numerose cause legali contro l'exchange** e il suo fondatore Mark Karpeles, che ha negato di aver fatto nulla di sbagliato.
- In giugno 2018, **Karpeles è stato condannato a due anni e mezzo di prigione per falsificazione di documenti ma non per il fallimento dell'exchange**.
- Tuttavia, **molti utenti di Mt. Gox non hanno ancora recuperato i loro bitcoin rubati** e il destino dei fondi rimanenti dell'exchange è ancora incerto.

Il fallimento di Mt. Gox è stato quindi causato da una serie di fattori, tra cui problemi di mercato, mancanza di regolamentazione adeguata, vulnerabilità della sicurezza dell'exchange e problemi di gestione aziendale. Il **caso di Mt. Gox è stato un avvertimento per l'industria dei digital asset, evidenziando la necessità di una maggiore sicurezza, regolamentazione e responsabilità nell'ambito delle transazioni**. Un altro caso simile degno di nota è quello di **BitGrail**, un **exchange di digital asset italiano che ha subito un grave fallimento nel 2018**, perdendo circa 170 milioni di euro di digital asset. L'exchange ha dichiarato di essere stato **vittima di un hacker**, ma sono state sollevate alcune **preoccupazioni riguardo alla gestione dell'exchange** e alla sua capacità di gestire i fondi degli utenti.

L'incidente ha portato alla chiusura dell'exchange e ha causato una serie di cause legali. Il fondatore di BitGrail, **Francesco Firano**, è stato accusato di frode e appropriazione indebita dai suoi utenti, ed è stato costretto a dichiarare bancarotta personale.

Sul fronte normativo, il fallimento di BitGrail ha evidenziato la **necessità di una maggiore regolamentazione** del settore dei digital asset in Italia.

Infine, a fine 2022, il fallimento dell'exchange americano FTX, operante in 250 giurisdizioni attraverso 56 entità giuridiche, è stato l'ennesimo episodio di gestione poco trasparenza dei fondi dei clienti e di una superficiale gestione del rischio da parte di questi operatori poco regolamentati.

Di seguito elencati alcuni aspetti che sono emersi dal report dell'agenzia delle Liquidazioni americane:

- Problemi di governance interna.
- Mancanza di personale per le funzioni di controllo rispetto alle attività finanziarie e di accounting.
- Mancanza di standard per le funzioni di controllo e di accounting per tutte le entità all'interno del gruppo.
- Gestione documentale inadeguata.
- Gestione dei digital asset inadeguata (gran parte dei fondi erano in wallet online, vulnerabili a cyber-attacchi).
- Mancanza di best practises rispetto ai set-up ed altri aspetti relativi alla cybersecurity.
- Conflitto di interessi con il fondo Alameda.

Tutti questi eventi hanno portato molti utenti a rivalutare la gestione dei propri digital asset. Infatti, si è notato come a seguito dell'accaduto molti utenti **hanno deciso di trasferire i propri capitali verso soluzioni più sicure** come servizi di custodia istituzionali e servizi di "self-custody" come hardware wallet o software wallet.

Fonti

- ▶ "FTX sues liquidators of its Bahamian affiliate over crypto exchange ownership" Reuters, 20 marzo 2023
- ▶ "Italy to Regulate Cryptocurrency: Presentation of the Draft Law to the Italian Parliament," Forbes, 23 maggio 2019.
- ▶ "BitGrail Owner Ordered to Declare Bankruptcy After Crypto Hack," Coindesk, 16 marzo 2018

3.2

Cybersecurity

● Hard

Come analizzare la cybersicurezza di un exchange

La sicurezza informatica degli exchange di digital asset è di fondamentale importanza per la protezione degli utenti e dei loro fondi. Un framework di cyber security per un exchange di digital asset dovrebbe basarsi su una serie di principi e best practices per garantire la sicurezza dell'architettura complessiva.

In primo luogo, l'**architettura dell'exchange dovrebbe essere progettata per garantire la sicurezza dei dati e delle transazioni**. Gli utenti dovrebbero essere in grado di effettuare transazioni in modo sicuro e affidabile, senza il rischio di perdere i propri fondi o subire furti o frodi.

Il book order e lo smart routing sono due funzionalità crittografiche che richiedono particolare attenzione nella progettazione del sistema di sicurezza informatica di un exchange di digital asset.

Il book order è un registro elettronico che elenca tutti gli ordini di acquisto e vendita di un determinato digital asset, consentendo agli utenti di visualizzare l'andamento del mercato e di effettuare operazioni di trading. Questa funzionalità richiede una particolare attenzione alla sicurezza, poiché **qualsiasi vulnerabilità nel sistema potrebbe consentire ad un attaccante di manipolare il mercato o di accedere alle informazioni riservate degli utenti.**

Per proteggere il book order, l'exchange dovrebbe **adottare una serie di misure di sicurezza avanzate**, tra cui la crittografia dei dati, l'autenticazione degli utenti, la gestione degli accessi, il monitoraggio delle attività, la rilevazione delle intrusioni e la prevenzione degli attacchi.

Lo smart routing è una funzionalità che consente di effettuare transazioni su diversi mercati o scambi contemporaneamente, in modo da **ottenere il miglior prezzo possibile** per un determinato digital asset. Questa funzionalità richiede una particolare attenzione alla sicurezza, poiché **qualsiasi vulnerabilità nel sistema potrebbe consentire a un attaccante di manipolare i prezzi o di accedere alle informazioni riservate degli utenti.**

Componenti	Funzionalità	Considerazioni di Cybersecurity
Book Order	Gestione ordini libri	<ul style="list-style-type: none"> - Utilizzo di crittografia per proteggere i dati personali dei clienti durante la transazione. - Controllo degli accessi per evitare l'accesso non autorizzato alle informazioni sensibili. - Monitoraggio costante delle attività per rilevare eventuali attività sospette.
Smart Routing	Instradamento intelligente dei dati	<ul style="list-style-type: none"> - Utilizzo di crittografia per proteggere i dati sensibili che vengono instradati. - Protezione della connessione e del protocollo di instradamento per evitare attacchi man-in-the-middle e altre minacce. - Controllo degli accessi per garantire che solo i dipendenti autorizzati possano accedere alle informazioni sensibili.
Architettura	Struttura del sistema	<ul style="list-style-type: none"> - Implementazione di procedure di sicurezza per garantire l'integrità, la riservatezza e la disponibilità dei dati. - Utilizzo di tecnologie di sicurezza avanzate come firewall, antivirus, crittografia e rilevamento delle intrusioni. - Protezione dell'architettura stessa da attacchi mirati come i DDoS.
Sicurezza dei dati	Crittografia dei dati, Backup regolari dei dati	<ul style="list-style-type: none"> - La crittografia dei dati è fondamentale per la sicurezza dei dati sensibili. Garantisce che i dati siano protetti durante il trasferimento e quando vengono memorizzati. - I backup regolari dei dati sono importanti per garantire che i dati non vengano persi in caso di attacchi informatici, errori umani o guasti hardware.
Protezione API	Autenticazione forte, limitazione delle autorizzazioni delle API	<ul style="list-style-type: none"> - L'autenticazione forte è fondamentale per proteggere le API. Deve essere richiesto l'utilizzo di una combinazione di credenziali per accedere alle API. - Le autorizzazioni delle API devono essere limitate per prevenire accessi non autorizzati.
Controllo degli accessi	Gestione degli account utente e delle autorizzazioni	<p>La gestione degli account utente e delle autorizzazioni è fondamentale per prevenire accessi non autorizzati. È necessario limitare l'accesso ai dati solo a utenti autorizzati.</p>
Monitoraggio della sicurezza	Analisi dei log	<p>L'analisi dei log è importante per identificare attività sospette. I log devono essere monitorati regolarmente per prevenire attacchi informatici.</p>

Per proteggere lo smart routing, l'exchange dovrebbe **adottare una serie di misure di sicurezza avanzate**, tra cui la crittografia dei dati, l'autenticazione degli utenti, la gestione degli accessi, il monitoraggio delle attività, la rilevazione delle intrusioni e la prevenzione degli attacchi. Inoltre, l'exchange dovrebbe adottare politiche di sicurezza rigorose per garantire la protezione dei fondi degli utenti, la riduzione del rischio di frodi, e la garanzia della trasparenza e dell'integrità dei sistemi di pagamento.

In secondo luogo, l'**exchange dovrebbe adottare misure di sicurezza avanzate per proteggere i propri sistemi e i propri dati**. Questo include la crittografia dei dati, l'autenticazione degli utenti, il monitoraggio dei sistemi, la protezione delle comunicazioni, e l'utilizzo di tecniche di rilevamento delle intrusioni e prevenzione degli attacchi.

In terzo luogo, l'**exchange dovrebbe adottare politiche di sicurezza rigorose per proteggere gli utenti da potenziali minacce**, come il phishing, i malware, gli attacchi DDoS e gli attacchi alla sicurezza dei sistemi. Questo include la formazione degli utenti, la protezione degli account, la gestione delle password, e l'utilizzo di sistemi di sicurezza avanzati.

3.3

Cybersecurity

● Basic

Key Management di un servizio di custodia proprietario

Ecco alcune **best practices** di key management che possono essere utilizzate anche in un exchange di digital asset:

1. **Creare chiavi in ambienti offline:** le chiavi private dovrebbero essere generate in un ambiente offline sicuro, che non sia connesso a Internet, per minimizzare il rischio di compromissione.
2. **Usare hardware wallet:** i wallet hardware, come il Ledger Nano S, sono dispositivi sicuri progettati specificamente per la gestione di digital asset e la creazione di chiavi private.
3. **Usare password complesse:** le password dovrebbero essere lunghe, complesse e utilizzare una combinazione di caratteri maiuscoli e minuscoli, numeri e simboli.
4. **Usare la crittografia:** le chiavi private dovrebbero essere crittografate con algoritmi di crittografia sicuri per impedirne l'accesso non autorizzato.
5. **Fare il backup delle chiavi:** le chiavi private dovrebbero essere regolarmente copiate e conservate in ambienti sicuri, come un deposito a prova di fuoco o una cassetta di sicurezza bancaria.
6. **Usare la multi-firma:** la multi-firma richiede l'approvazione di più utenti per l'elaborazione di transazioni, aumentando la sicurezza e impedendo eventuali manipolazioni.
7. **Limitare l'accesso alle chiavi:** solo personale autorizzato dovrebbe avere accesso alle chiavi private e alle informazioni sensibili dell'exchange.
8. **Monitorare le attività:** i registri delle attività dovrebbero essere monitorati regolarmente per identificare eventuali attività sospette o anomalie.
9. **Aggiornare regolarmente i sistemi:** i sistemi dell'exchange, inclusi i software, dovrebbero essere aggiornati regolarmente per correggere eventuali vulnerabilità.
10. **Eseguire test di sicurezza regolari:** il sistema dell'exchange dovrebbe essere sottoposto regolarmente a test di sicurezza e valutazioni di vulnerabilità per identificare eventuali punti deboli e risolverli tempestivamente.

Tuttavia, non tutti gli exchange nel mercato hanno dimostrato nel tempo di praticare queste best practices, portando alla perdita totale o parziale dei digital asset in gestione. Risulta quindi essenziale analisi di questi *single point of failure* all'interno dell'industria.

3.4

Risk Management

● Basic

Quali sono i rischi reputazionali nel Web3?

Il rischio reputazionale è il rischio che un'entità incorre in perdite derivanti da danni alla reputazione come conseguenza diretta o indiretta di un'azione o di un evento. Nel caso di una banca che presta il servizio di custodia di digital assets per conto della clientela e questa venga hackerata, la perdita di fondi dei clienti potrebbe causare gravi danni alla reputazione dell'istituto finanziario. Ciò potrebbe portare alla perdita di fiducia dei clienti e dei partner commerciali, e alla riduzione della quota di mercato dell'istituzione. In aggiunta a questo la banca potrebbe subire anche una perdita operativa derivante dal rimborso ai propri clienti di quanto gli è stato sottratto dagli hacker.

Per mitigare il rischio reputazionale in questo contesto, la banca dovrebbe adottare misure di sicurezza robuste per proteggere i fondi dei clienti. Ciò potrebbe includere l'utilizzo di pratiche di key management sicure, la creazione di politiche di sicurezza rigide e la gestione attenta dei rischi associati alla custodia di digital assets. Inoltre, **la banca dovrebbe essere trasparente con i propri clienti e comunicare tempestivamente qualsiasi violazione della sicurezza o perdita di fondi.** In questo modo dimostrerebbe la propria responsabilità e il proprio impegno per la sicurezza dei fondi dei clienti, mitigando così il rischio reputazionale e garantendo privacy verso i propri stakeholder in modo analogo.

Il rischio reputazionale è un'**importante preoccupazione per gli exchange di digital asset** e può essere **amplificato dal rischio di listare token fraudolenti o scam token.** La lista di token fraudolenti può influire negativamente sull'immagine dell'exchange, aumentare il rischio di azioni legali e causare la perdita di fiducia dei clienti e degli investitori.

Per evitare la lista di token fraudolenti, gli **exchange dovrebbero adottare una rigorosa procedura di due diligence sui token che vogliono quotare.** Ciò potrebbe includere la verifica della documentazione legale, l'analisi del team di sviluppo e delle loro competenze, l'analisi della tecnologia e della blockchain su cui il token è basato e l'analisi del modello economico del token.

Inoltre, gli **exchange dovrebbero tenere sempre presente la natura dinamica del mercato dei digital asset e dei token.** Ciò significa che dovrebbero **aggiornare regolarmente le loro procedure di due diligence** per rispondere alle nuove minacce e ai nuovi rischi. Inoltre, gli exchange dovrebbero rimanere vigili e **monitorare costantemente i token elencati per rilevare eventuali anomalie o segnali di frode.**

3.5

Risk Management

● Basic

Come gestire la tesoreria di un exchange

La **gestione della tesoreria di un exchange di digital asset** è un aspetto critico per il successo e la sostenibilità dell'attività di scambio di asset digitali. La gestione della tesoreria si occupa di gestire il flusso di denaro all'interno dell'exchange, compresi i depositi, i prelievi, gli acquisti e le vendite di digital asset e le attività di trading. In questo contesto, la gestione della tesoreria deve garantire l'efficienza, la sicurezza e la liquidità delle risorse finanziarie dell'exchange.

Per gestire efficacemente la tesoreria di un exchange di questo tipo, è importante adottare alcune best practice. In primo luogo, l'exchange dovrebbe **mantenere una forte governance della tesoreria, con**

un'adeguata separazione delle funzioni tra le attività di tesoreria e le attività di trading. Questo può essere fatto adottando un sistema di controllo interno adeguato e garantendo una completa trasparenza delle transazioni finanziarie.

In secondo luogo, l'exchange dovrebbe **adottare una politica di gestione del rischio finanziario per mitigare gli effetti di fluttuazioni del mercato.** Ciò può includere l'utilizzo di coperture finanziarie per ridurre il rischio di cambio e il rischio di tasso d'interesse. Inoltre, l'exchange dovrebbe mantenere un adeguato livello di riserve di liquidità per far fronte alle esigenze immediate di prelievo dei clienti e per garantire la stabilità finanziaria dell'exchange.

In terzo luogo, l'exchange dovrebbe adottare una **politica di gestione del rischio di sicurezza informatica per proteggere i fondi dei clienti da eventuali attacchi informatici.** Ciò può essere fatto mediante l'adozione di procedure di sicurezza informatica efficaci, come la crittografia delle transazioni finanziarie e l'adozione di protocolli di autenticazione sicuri.

Di seguito sono riportate alcune best practice per la gestione della tesoreria di un exchange di digital asset:

Best Practice	Descrizione
Governance della tesoreria	<i>Garantire una separazione adeguata delle funzioni tra le attività di tesoreria e le attività di trading</i>
Politica di gestione del rischio finanziario	<i>Utilizzo di coperture finanziarie per mitigare il rischio di fluttuazioni di mercato e mantenere un adeguato livello di riserve di liquidità</i>
Politica di gestione del rischio di sicurezza informatica	<i>Adozione di procedure di sicurezza informatica efficaci per proteggere i fondi dei clienti da attacchi informatici</i>

Infine, va da sé che l'exchange debba **garantire la conformità alle normative locali e internazionali.**

4

Analisi rischio tecnologico per area investimenti (DEX)

- 4.1 Il problema della liquidità nella finanza decentralizzata
- 4.2 Truffe nel mercato del Web3
- 4.3 L'importanza della tokenomics in un progetto Web3
- 4.4 Che cos'è lo slippage e l'Impairment Loss Scenario?
- 4.5 Che cos'è una rugpull?
- 4.6 Flash Loans e le vulnerabilità dei protocolli DEFI
- 4.7 Exploit e vulnerabilità: Il caso The DAO

4.1

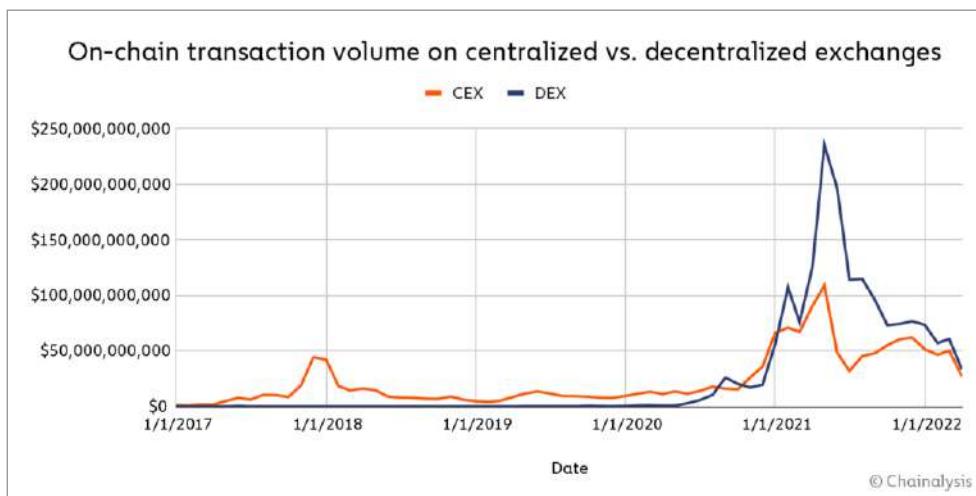
Informatica

● Basic

Il problema della liquidità nella finanza decentralizzata

Il mercato delle **DEX** (decentralized exchange) è un **settore emergente all'interno del mondo dei digital asset**. DEX si differenziano dai CEX (centralized exchange) perché non richiedono un'autorità centrale per gestire le transazioni. Invece, le transazioni vengono eseguite attraverso contratti intelligenti su blockchain.

Uno dei principali problemi delle DEX è la liquidità. Poiché le transazioni sono eseguite attraverso contratti intelligenti, la **liquidità dipende dal numero di partecipanti alla piattaforma**. La liquidità limitata può comportare un rallentamento delle transazioni e un aumento degli spread di prezzo.



Tuttavia, come dal grafico presentato si può notare un incremento di numero di transazioni all'interno di exchange decentralizzati, questo per un aumento di consapevolezza della comunità, miglioramenti in termini di UX e UI, e la paura di affidarsi a exchange centralizzati che possono fallire per mala gestione finanziaria.

4.2

Business

● Basic

Truffe nel mercato del Web3

Il mondo dei digital asset è caratterizzato da una grande volatilità e incertezza, e molti asset digitali hanno fallito nel corso degli anni. Secondo un rapporto dell'agosto 2021 dell'azienda di analisi di mercato Coinopsy, il 69% di tutti i digital asset introdotti dal 2013 è fallito.

Ci sono diverse ragioni per cui molti digital asset falliscono, tra cui:

- Mancanza di adozione:** molti digital asset non sono stati adottati dal pubblico o dalle aziende, rendendoli essenzialmente inutili.
- Scarsa liquidità:** alcuni digital asset hanno una bassa liquidità, il che significa che è difficile per gli utenti comprare o vendere le monete.

3. **Problemi tecnici:** alcuni digital asset possono avere problemi tecnici o di sicurezza che le rendono vulnerabili ad attacchi informatici o altre minacce.
4. **Regolamentazione:** i digital asset possono essere soggetti ad una regolamentazione sfavorevole, il che può limitare la loro utilità e adozione.

Inoltre, un fenomeno comune nel mondo dei digital asset è l'**ICO exit scam**. Un ICO (Initial Coin Offering) è un modo per i nuovi digital asset di raccogliere fondi vendendo le loro monete in cambio di digital asset più stabili come il Bitcoin o l'Ethereum. Tuttavia, **alcune ICO sono in realtà truffe**, in cui i fondatori raccolgono denaro dagli investitori e poi scompaiono con i soldi.

Secondo un rapporto dell'agosto 2021 dell'azienda di analisi di mercato ICO Rating, il **78% di tutti gli ICO del 2017 è stato identificato come truffa**. Molti di questi ICO exit scam hanno causato perdite significative per gli investitori. Secondo uno studio del **2018** condotto da Satis Group, l'**81% di tutte le ICO era stato identificato come truffa, mentre solo il 4% dei progetti era stato identificato come un'offerta di successo**. Questo indica che la maggior parte dei digital asset fallisce a causa di problemi di truffa e mancanza di valore reale.

In sintesi, il mondo dei digital asset è caratterizzato da una grande incertezza e molti di questi asset hanno fallito nel corso degli anni. Gli investitori devono fare attenzione e condurre una rigorosa analisi dei rischi prima di investire in qualsiasi digital asset o ICO.

4.3

Informatica

● Medium

L'importanza della tokenomics in un progetto Web3

La **logica degli smart contract è un elemento cruciale per garantire una tokenomics corretta e gli incentivi giusti**. Ciò significa che gli smart contract sono in grado di garantire l'esecuzione automatica di tutte le regole e le procedure relative all'emissione, alla distribuzione e alla gestione di un digital asset, senza la necessità di un'autorità centrale che ne regoli il funzionamento.

La **dipendenza degli smart contract da una vasta gamma di componenti tecnologici** come il sistema operativo, le librerie e le interfacce di programmazione delle applicazioni (API) rappresenta un **ulteriore elemento di criticità**. Una qualsiasi vulnerabilità presente in uno di questi componenti può infatti compromettere l'intera struttura degli smart contract e il corretto funzionamento della tokenomics.

Le librerie per Ethereum e Bitcoin rappresentano una parte fondamentale della tecnologia blockchain su cui si basano gli smart contract. Tuttavia, **come ogni altra libreria, anche quelle utilizzate nei sistemi blockchain possono presentare vulnerabilità** che potrebbero compromettere la sicurezza degli smart contract e della tokenomics.

Ecco una lista di alcune delle principali librerie su Ethereum utilizzate per la creazione di DApp (applicazioni decentralizzate):

1. **Web3.js:** principale libreria utilizzata per l'interfacciamento con il protocollo Ethereum. Essa consente di interagire con il nodo Ethereum, inviare transazioni e interrogare lo stato della blockchain.
2. **Truffle:** un framework di sviluppo per Ethereum che semplifica la creazione e il testing di smart contract e DApp. Truffle offre una serie di strumenti per la compilazione, il testing ed il deployment degli smart contract.
3. **OpenZeppelin:** libreria di smart contract open source che offre una serie di funzionalità avanzate come controlli di accesso, gestione degli asset, token standard e molto altro. La libreria è stata sviluppata per semplificare la creazione di smart contract sicuri e affidabili.
4. **Embark:** un altro framework di sviluppo per Ethereum che semplifica la creazione di DApp. Embark offre una serie di funzionalità per il testing, il deployment e la gestione degli smart contract e delle interfacce utente.

- PERCORSO RISK**
- PERCORSO INNOVAZIONE**
5. **Drizzle**: libreria per la gestione dello stato dell'applicazione in Ethereum. Essa semplifica l'accesso ai dati della blockchain e la gestione dello stato dell'applicazione utilizzando Redux.
 6. **Infura**: libreria che offre un'infrastruttura API per Ethereum. Essa semplifica l'interfacciamento con il protocollo Ethereum senza la necessità di eseguire un nodo locale.

4.4

Finanza / Informatica

● Hard

Che cos'è lo slippage e l'Impairment Loss Scenario?

Le liquidity pool vengono utilizzate in vari protocolli DeFi per consentire agli utenti di scambiare tra loro digital asset o token in modo più veloce e con costi più bassi rispetto a quelli delle piattaforme centralizzate. Qui di seguito una tabella che riassume alcune piattaforme DEFI all'interno delle quali possono essere creati dei liquidity:

Protocolli DeFi	Descrizione
Uniswap	Uniswap è un protocollo di scambio decentralizzato basato su Ethereum che consente a chiunque di fornire liquidità e scambiare digital asset. Uniswap utilizza un meccanismo di market maker automatizzato (AMM) che permette agli utenti di scambiare digital asset senza bisogno di un intermediario centralizzato. Uniswap utilizza una formula matematica per determinare il prezzo dei digital asset in base all'offerta e alla domanda all'interno del pool di liquidità.
Curve	Curve è un protocollo di scambio decentralizzato che si concentra su scambi di stablecoin. Il protocollo utilizza un meccanismo di market maker automatizzato (AMM) per fornire liquidità e scambiare stablecoin con una bassa slippage. Curve è stato progettato per ridurre al minimo le perdite di slippage e le commissioni di scambio, ed è noto per la sua efficienza nel fornire liquidità a diverse stablecoin come USDT, USDC e DAI. Curve è anche noto per il suo modello di governance comunitario, dove i detentori di token CRV hanno diritto di voto sulle decisioni relative al protocollo.
Balancer	Balancer è una piattaforma di scambio decentralizzata basata su Ethereum che consente agli utenti di creare e personalizzare pool di liquidità. I pool di Balancer sono costituiti da una combinazione di token con un peso percentuale assegnato a ciascuno. Gli utenti possono depositare i loro token in un pool esistente o creare uno nuovo. Balancer consente di avere fino a 8 token in un pool, consentendo agli utenti di diversificare i loro investimenti in modo più flessibile. Gli utenti possono anche fornire liquidità ai pool e guadagnare una parte delle commissioni di trading generate in quel pool.
Sushiswap	Sushiswap è una piattaforma di scambio decentralizzata basata su Ethereum, lanciata nel settembre 2020. La piattaforma è stata creata con l'obiettivo di fornire una maggiore incentivazione per gli utenti che forniscono liquidità ai pool di scambio. Sushiswap ha introdotto un sistema di incentivazione con token, in cui gli utenti che forniscono liquidità ai pool di scambio possono guadagnare SUSHI, il token nativo della piattaforma. SUSHI può essere utilizzato per votare sulle decisioni della comunità sulla piattaforma, nonché per accedere a servizi aggiuntivi come il lending.

Gli operatori di liquidità (LP) sono uno dei pilastri della finanza decentralizzata (DeFi), in particolare delle piattaforme di scambio decentralizzate che utilizzano i meccanismi degli Automated Market Maker (AMM).

Gli AMM sono utilizzati per determinare il prezzo delle attività all'interno di questi pool di liquidità.

Invece di utilizzare il modello di prezzo tradizionale dell'offerta e della domanda, gli AMM utilizzano un algoritmo che tiene conto della quantità di attività presenti nel pool di liquidità. Questo algoritmo viene utilizzato per calcolare il prezzo in modo automatico e continuo.

In DeFi, gli LP sono coloro che forniscono liquidità ai protocolli DeFi, depositando le loro attività in cambio di una parte delle commissioni di transazione. Gli **LP creano “pools” di liquidità per ogni coppia di trading che desiderano supportare**. Ad esempio, se desiderano fornire liquidità alla coppia di trading ETH/USDT, depositano una quantità di ETH e USDT in un pool specifico. Questo pool di liquidità è quindi utilizzato dai trader per scambiare ETH con USDT e viceversa.

In confronto alla finanza centralizzata, gli LP svolgono un ruolo più attivo e diretto nella determinazione dei prezzi e nella liquidità sul mercato. Invece di essere intermediati da intermediari finanziari come le banche o le società di intermediazione, gli LP interagiscono direttamente con la piattaforma di scambio decentralizzata, fornendo liquidità in cambio di una quota delle commissioni di transazione. In questo modo, gli **LP possono guadagnare denaro dalla fornitura di liquidità senza dover pagare commissioni alle società di intermediazione finanziaria**.

La relazione tra AMM, liquidity provider e liquidity pool è fondamentale per il corretto funzionamento degli scambi decentralizzati. Gli AMM utilizzano i pool di liquidità creati dai liquidity provider per determinare il prezzo degli asset scambiati sulla piattaforma. Inoltre, i liquidity provider sono incentivati a fornire liquidità in quanto ricevono una quota delle commissioni di transazione generate dagli scambi effettuati all'interno del pool.

Tuttavia, è possibile che ci possono essere dei problemi legati al design di una liquidity pool, che può scaturire in quello che viene definito come slippage e/o Impairment Loss

Termino	Definizione	Ruolo	Esempio di mercato
Liquidity Pool	Un insieme di fondi di diversi token che possono essere scambiati tra loro.	Fornisce la liquidità per gli scambi sulla piattaforma e determina il prezzo degli asset scambiati.	Uniswap, SushiSwap, Curve, Bancor.
Liquidity Provider	Un individuo o un'entità che deposita fondi in una liquidity pool.	Fornisce liquidità per gli scambi sulla piattaforma e riceve una quota delle commissioni di transazione generate dal pool.	Un utente che deposita 50% di ETH e 50% di DAI in una liquidity pool su Uniswap.
AMM (Automated Market Maker)	Un algoritmo che utilizza una formula matematica per stabilire il prezzo degli asset all'interno di una liquidity pool.	Fornisce la struttura per l'esecuzione degli scambi sulla piattaforma senza la necessità di intermediari.	Balancer, Kyber Network, Bancor.

In ambito finanziario e dei digital asset, lo **slippage** è un **fenomeno che si verifica quando il prezzo di un asset subisce una variazione improvvisa durante l'esecuzione di una transazione**. Questo può avvenire, ad esempio, quando si acquista o si vende un digital asset su una piattaforma di trading con un volume elevato di scambi.

L'impairment loss, invece, è un termine utilizzato per descrivere la perdita temporanea di valore che un liquidity provider (LP) può subire quando fornisce liquidità a un pool di trading su una piattaforma di DeFi (Decentralized Finance). Questa perdita si verifica quando il prezzo di un asset all'interno del pool cambia rispetto al prezzo sul mercato. In particolare, quando il prezzo di un asset scende rispetto all'altro, l'LP subisce una perdita in quanto il valore del suo investimento in quel particolare asset diminuisce. La relazione tra lo slippage e l'impairment loss è che entrambi sono **fenomeni legati alla volatilità del mercato**. Lo slippage può influenzare il prezzo di un asset in modo significativo, causando una variazione del prezzo dell'asset all'interno del pool rispetto al prezzo di mercato. Questa variazione può portare all'impairment loss per l'LP che ha fornito la liquidità al pool.

Per proteggere se stessi dall'impairment loss, gli LP possono utilizzare diverse strategie. Ad esempio, possono bilanciare i loro investimenti in modo da minimizzare la perdita, oppure possono scegliere di fornire liquidità solo a pool con asset che si muovono insieme. Inoltre, possono utilizzare strumenti di analisi del rischio per monitorare le fluttuazioni del mercato e adattare le proprie strategie di conseguenza.

	Slippage	Impairment loss
Definizione	Lo slippage è la differenza tra il prezzo a cui un trader desidera eseguire un'operazione e il prezzo effettivo al quale viene eseguita l'operazione. Questa differenza può essere causata da vari fattori, come la mancanza di liquidità, il ritardo nell'esecuzione dell'ordine o la volatilità del mercato.	L'impairment loss è un termine contabile che indica la perdita di valore di un'attività di una società. Si verifica quando il valore contabile di un'attività supera il suo valore di mercato attuale o il suo valore recuperabile. In altre parole, l'impairment loss rappresenta la differenza tra il valore di un'attività registrato nei libri contabili della società e il suo valore di mercato effettivo.
Problemi	Lo slippage può causare problemi ai trader, poiché possono vedere il prezzo di esecuzione dell'operazione differire dal prezzo desiderato, e questo può influenzare i loro profitti o perdite. Inoltre, lo slippage può essere particolarmente problematico per i trader che operano con posizioni di grandi dimensioni.	L'impairment loss può rappresentare un problema per le società, poiché può ridurre il valore del patrimonio netto e la redditività dell'azienda. Inoltre, l'impairment loss può indicare che l'attività non sta svolgendo un ruolo redditizio nel mercato o che la società sta subendo difficoltà finanziarie.
Soluzioni	Per mitigare lo slippage, i trader possono utilizzare ordini stop-loss o ordini di mercato, che vengono eseguiti immediatamente al miglior prezzo disponibile. Inoltre, l'utilizzo di piattaforme di trading con una maggiore liquidità può anche aiutare a ridurre lo slippage.	Per mitigare l'impairment loss, le società possono effettuare una valutazione regolare delle proprie attività per determinare il loro valore attuale e il loro valore recuperabile. Inoltre, le società possono cercare di diversificare il loro portafoglio di attività per mitigare i rischi e ridurre l'impatto di eventuali perdite di valore.

4.5

Che cos'è una Rugpull?

Informatica

● Hard

Il termine "rug pull" è diventato popolare nel settore della finanza decentralizzata (DeFi) e si riferisce a una serie di scenari in cui gli sviluppatori, gli amministratori o gli alti dirigenti di un progetto DeFi ritirano il loro supporto in modo inaspettato, causando un crollo del valore del token o del progetto. Questo può avvenire in vari modi, tra cui la rimozione di liquidità, la modifica del codice sorgente o l'abbandono del progetto.

In un contesto positivo, un rug pull può essere visto come **un meccanismo di protezione per gli sviluppatori e gli investitori**. Per esempio, gli sviluppatori di un progetto potrebbero decidere di ritirare il loro supporto se ritengono che il progetto non sia più sostenibile o se ci sono preoccupazioni legali o di conformità. In questo caso, il rug pull può essere visto come un modo per proteggere gli investitori da ulteriori perdite. Inoltre, in alcuni casi, il rug pull può essere utilizzato come un meccanismo per trasferire la proprietà o il controllo di un progetto a una nuova squadra o comunità.

Tuttavia, il termine "rug pull" è più **comunemente associato a scenari in cui gli sviluppatori o gli amministratori di un progetto DeFi agiscono in modo fraudolento**.

Gli sviluppatori possono mettere delle back-door nel codice del loro smart contract, che consente loro di accedere ai fondi degli investitori o di modificare le regole del gioco in loro favore. Questo può essere fatto in diversi modi, come l'inclusione di una funzione di prelievo automatico che trasferisce i fondi degli investitori direttamente agli sviluppatori, l'inclusione di un codice che permette loro di modificare il prezzo del token in modo arbitrario, o l'inclusione di altre vulnerabilità di sicurezza che consentono loro di accedere ai fondi degli investitori. Questo è spesso accompagnato da un'exit scam, in cui gli sviluppatori scompaiono con i fondi degli investitori.

In generale, una **backdoor in una DApp** può essere una porzione di codice che consente a un'entità non autorizzata di accedere e controllare il sistema, senza che gli utenti della stessa ne siano a conoscenza. In questo caso, gli sviluppatori potrebbero inserire deliberatamente la backdoor nel codice della DApp per scopi fraudolenti, come un rugpull.

È importante notare che **non tutti i progetti DeFi sono truffe e che la maggior parte degli sviluppatori di progetti DeFi sono onesti e trasparenti**. Per proteggersi da questo tipo di rug pull, gli investitori dovrebbero fare la dovuta diligenza prima di investire in un progetto DeFi, compresa la ricerca sugli sviluppatori, la comprensione del codice sorgente e la valutazione della trasparenza e della governance del progetto.

4.6

Informatica

● Hard

Flash Loans e le vulnerabilità dei protocolli DEFI

I flash loan rappresentano un meccanismo innovativo nel settore delle finanze decentralizzate (DeFi), consentendo agli utenti di prendere in prestito asset digitali senza fornire alcuna garanzia. Questo è possibile grazie allo standard ERC-3156, che fornisce un framework per l'implementazione dei flash loan sulle blockchain EVM.

Il funzionamento dei flash loan si basa su un principio semplice: il prestito deve essere rimborsato entro la stessa transazione in cui è stato concesso. Questo meccanismo apre la porta a una serie di operazioni, in particolare quelle di arbitraggio tra diverse piattaforme DeFi.

Ecco un esempio di come potrebbe funzionare un flash loan:

1. Un utente prende in prestito ETH su Aave, una piattaforma DeFi.
2. Utilizza gli ETH per acquistare un asset B su Uniswap, dove il prezzo è 1.
3. Vende l'asset B su Curve, dove il prezzo è 1,1.
4. Utilizza il ricavato per rimborsare il prestito su Aave, pagando anche gli interessi.

Tutte queste operazioni avvengono all'interno di una singola transazione. Perché questa operazione generi profitto, è fondamentale che esista un margine di arbitraggio. Se tale margine non esiste, la transazione non includerà operazioni di arbitraggio e salderà immediatamente il prestito, pagando gli interessi. Questo comporterebbe una perdita per l'utente, dato che avrebbe pagato gli interessi senza realizzare alcun profitto dall'arbitraggio.

Tuttavia, è importante notare che al giorno d'oggi è diventato sempre più difficile realizzare profitti con i flash loan. Questo è dovuto al fatto che i prezzi degli asset su quasi tutti i DEX sono allineati, grazie alla presenza di molti utenti che effettuano operazioni di arbitraggio con i flash loan. Questo ha portato a una competizione elevata, riducendo i margini di arbitraggio disponibili.

Tuttavia, questo strumento può essere anche sfruttato in maniera fraudolenta. Infatti, tra i più famosi exploit nel DeFi, possiamo citare il “flash loan exploit” di dicembre 2020 sul protocollo **Aave**. **Questo exploit ha permesso a un attaccante di prelevare fondi da un contratto smart senza fornire alcun tipo di garanzia**. L'attacco è stato condotto da un indirizzo che ha sottratto più di 10 milioni di dollari in stablecoin, tra cui DAI, USDC, BUSD, TUSD e USDT.

In sintesi, i flash loan offrono la possibilità di prendere in prestito denaro senza collaterale o garanzie, a condizione che il prestito venga restituito, più gli interessi, all'interno della stessa transazione. Questo meccanismo unico ha aperto nuove opportunità nel settore DeFi, nonostante le sfide associate alla competizione elevata e alla necessità di identificare opportunità di arbitraggio redditizie.

4.7

Informatica

● Hard

Exploit e vulnerabilità: il caso THE DAO

Un exploit è una vulnerabilità che sfrutta un bug o una mancanza di sicurezza nel codice per ottenere un vantaggio ingiusto. In un contesto di DeFi, un exploit potrebbe comportare la manipolazione di contratti smart o la sottrazione di fondi da un portafoglio.

La sicurezza del codice è fondamentale per garantire la sicurezza degli utenti e delle loro risorse in un sistema DeFi. Gli exploit e gli hack possono causare perdite significative per gli utenti e minare la fiducia nel sistema. Ecco perché è **importante che i contratti smart siano rigorosamente controllati e testati per eventuali vulnerabilità prima di essere pubblicati sulla blockchain**. La collaborazione della comunità per identificare e correggere eventuali problemi di sicurezza è altrettanto importante per garantire la sicurezza di tutti.

Ad esempio, uno degli exploit più comuni è la vulnerabilità del contratto denominata “reentrancy”. Un attaccante potrebbe invocare il contratto, depositare fondi e quindi richiamare di nuovo il contratto per prelevare più fondi di quanto dovrebbe.

In questo esempio, l'attaccante potrebbe invocare il contratto Attacker e quindi eseguire la **funzione attack()**. Questa funzione prima deposita tutto il proprio saldo nel contratto Reentrant e quindi preleva il proprio saldo dal contratto. Durante il processo di prelievo, il contratto Reentrant è ancora in esecuzione, ma è stato già sfruttato, poiché l'attaccante ha già prelevato i fondi prima che l'esecuzione del contratto fosse terminata.

Nel 2016, un'organizzazione autonoma decentralizzata (DAO) chiamata “The DAO” è stata istituita. Si trattava di un fondo di investimento controllato dalla comunità che ha raccolto 150 milioni di dollari in ether vendendo il proprio token comunitario. Tuttavia, meno di tre mesi dopo il lancio di The DAO, è stato attaccato da un hacker che ha drenato la maggior parte dei 150 milioni di dollari in ETH dal contratto intelligente di The DAO. L'hacker ha utilizzato un tipo di attacco noto come attacco di reentrancy.

Un attacco di reentrancy sfrutta il modo in cui funzionano le funzioni di fallback in Solidity. Queste funzioni vengono attivate in situazioni specifiche e possono includere logica arbitraria. L'attacco di reentrancy si basa anche su un certo ordine delle operazioni nel contratto vittima. In un attacco di reentrancy, il contratto dell'hacker chiama una funzione nel contratto vittima che invia ETH al contratto dell'hacker. Tuttavia, il contratto dell'hacker ha una funzione di fallback che richiama la funzione di prelievo nel contratto vittima, creando un ciclo di chiamate che prosciuga i fondi del contratto vittima.

La vulnerabilità è stata sfruttata nel seguente modo: l'attaccante ha inviato una transazione che ha richiamato la funzione **splitDAO** con un **_proposalID** che puntava a una proposta che aveva già passato e che non era ancora stata eseguita. L'attaccante ha quindi potuto prendere il controllo della nuova DAO e prelevare fondi senza il consenso degli altri partecipanti.

La vulnerabilità è stata causata dalla mancata verifica del fatto che la transazione che richiamava la funzione veniva da un indirizzo autorizzato, permettendo all'attaccante di inviare la transazione da un indirizzo non autorizzato. Questo ha causato una falla di sicurezza nello smart contract, che ha permesso all'attaccante di prelevare fondi senza autorizzazione.

L'attacco a The DAO ha portato a un profondo dibattito ideologico sulla risposta appropriata. Alla fine, la decisione è stata quella di eseguire un hard fork della blockchain di Ethereum, creando due versioni separate di Ethereum: Ethereum Classic e l'Ethereum che conosciamo oggi. Questa decisione è stata presa nonostante il fatto che alcuni minatori si siano opposti, poiché non c'era un difetto effettivo nel protocollo Ethereum. La decisione di eseguire l'hard fork è stata sostenuta dal 85% dei voti.

La biforcazione ha portato alla creazione di due blockchain Ethereum parallele. Ethereum Classic è la versione originale di Ethereum che continua a eseguire la vecchia versione del protocollo Ethereum. L'Ethereum che conosciamo oggi è la versione che ha implementato l'hard fork e opera come se l'attacco non fosse mai avvenuto.

In conclusione, l'attacco a The DAO è stato un evento significativo nella storia di Ethereum e ha portato a importanti cambiamenti nel modo in cui la blockchain di Ethereum opera. Ha anche evidenziato l'importanza della sicurezza e della corretta strutturazione del codice negli smart contract per prevenire attacchi come l'attacco di reentrancy.

5

Analisi rischio legale e compliance per area investimenti e pagamenti

- 5.1 Data Act
- 5.2 Basilea
- 5.3 GDPR
- 5.4 PSD2
- 5.5 SLA e OLA nei protocolli permissionless
- 5.6 Digital Finance Package e MiCA
- 5.7 Gestione Fiscale dei Digital Assets
- 5.8 MIFID II
- 5.9 Definizione normativa degli NFT
- 5.10 DORA
- 5.11 EMD2
- 5.12 AML Act

5.1

Data Act

Legale

● Medium

Il 14 marzo 2023, l'Unione Europea ha votato per l'**approvazione del testo del cosiddetto Data Act**, il quale ha come obiettivo quello di **regolamentare l'accesso e l'utilizzo dei dati, sia personali sia non**.

Tale legge europea include al suo interno anche un riferimento agli smart contract, in particolare all'articolo 30, il quale include dei "meccanismi rigorosi di controllo degli accessi" e la protezione dei segreti commerciali integrati nella progettazione degli smart contract. Inizialmente la proposta di legge doveva contenere anche una serie di rigorosi parametri da rispettare per l'approvazione di un contratto intelligente, ma nel testo approvato tale disposizione è stata eliminata.

Natalie Linhart, consulente legale per la società di software blockchain ConsenSys, ha affermato: "Vediamo l'articolo 30 come una disposizione marginale applicabile agli Smart Contract che facilitano il trasferimento di dati riguardanti prodotti IoT, non quelli utilizzati nelle applicazioni DeFi". Di fatto sembrerebbe che la nuova legge non dovrebbe portare ad un'oppressione dello sviluppo degli smart contract, ma rappresenta un primo passo verso una legislazione su di essi.

Tuttavia, la stessa Linhart ha dichiarato a The Block che "Imporre requisiti sostanziali per lo sviluppo della blockchain limiterebbe l'innovazione e farebbe dell'UE un luogo non accogliente per gli sviluppatori di software".

Per ora quali saranno i **prossimi passi da parte della legislazione a riguardo degli smart contract non sono chiari**, ma sicuramente essi saranno determinanti nel definire l'evoluzione degli smart contract stessi.

Fonti

- ▶ <https://www.agendadigitale.eu/cittadinanza-digitale/data-management/eu-data-act-proposte-per-un-mercato-unico-dei-dati-opportunita-e-ostacoli/>
- ▶ <https://www.theblock.co/post/219590/eu-parliament-passes-smart-contract-regulation-under-data-act>

5.2

Basilea

Compliance

● Medium

La normativa di Basilea fornisce un **quadro regolamentare per la gestione dei rischi nelle banche**. Tuttavia, i concetti della normativa di Basilea potrebbero essere **applicati anche al mercato delle stablecoin e della loro riserva**. Ecco alcuni esempi di come potrebbero essere applicati questi concetti:

- **Riserve di capitale adeguato:** le banche sono tenute ad avere un'**adeguata riserva di capitale per proteggersi dai rischi**. Allo stesso modo, le aziende emittenti di stable coin **dovrebbero essere soggette a regole simili** per garantire che vi sia una riserva di capitale adeguata a coprire eventuali perdite. Questo potrebbe garantire la stabilità della stablecoin e ridurre il rischio di insolvenza dell'emittente. Inoltre, la società non può utilizzare quanto depositato dal cliente senza la sua autorizzazione.
- **Valutazione del rischio di credito:** le banche devono **valutare il rischio di credito associato ai loro prestiti e alle loro attività di investimento**. Nel caso delle **stablecoin**, potrebbe essere necessario **valutare il rischio di credito associato alla valuta sottostante o alla riserva di asset**. Ciò potrebbe

aiutare gli investitori a comprendere meglio il rischio associato alle stablecoin e a prendere decisioni di investimento informate.

- **Requisiti di liquidità:** le banche sono tenute a **soddisfare requisiti di liquidità** per garantire che siano in grado di far fronte a eventuali richieste di prelievo da parte dei clienti. Anche le **stablecoin potrebbero essere soggette a requisiti di liquidità per garantire che gli investitori possano facilmente acquistare e vendere stablecoin in modo sicuro e rapido.**
- **Controllo interno e adeguati sistemi di gestione del rischio:** le banche sono tenute ad avere **adeguati sistemi di controllo interno e di gestione del rischio** per garantire che siano in grado di identificare e gestire i rischi in modo efficace. Anche le **stablecoin potrebbero essere soggette a controlli e sistemi di gestione del rischio simili per garantire che siano gestite in modo sicuro e responsabile.**

I principi alla base della normativa di Basilea potrebbero essere applicati al mercato delle stablecoin per garantire la stabilità e la sicurezza delle stesse e proteggere gli investitori.

Nel giugno 2022, il Comitato di Basilea per la Vigilanza Bancaria ha emesso la sua seconda consultazione sul trattamento prudenziale delle esposizioni delle banche ai digital assets.

Il documento **“Prudential treatment of cryptoasset exposures”** **delinea il trattamento prudenziale delle esposizioni delle banche ai criptoasset.** Il documento è stato finalizzato e approvato dal Gruppo dei Governatori e dei Capi della Supervisione, e sarà implementato entro il 1° gennaio 2025.

Il documento classifica i criptoasset in due gruppi:

- **Gruppo 1:** criptoasset che soddisfano pienamente un insieme di condizioni di classificazione. Questi includono asset tradizionali tokenizzati (Gruppo 1a) e criptoasset con meccanismi di stabilizzazione efficaci (Gruppo 1b). I criptoasset del Gruppo 1 sono soggetti a requisiti di capitale basati sui pesi di rischio delle esposizioni sottostanti come stabilito nell'attuale Quadro di Basilea, ai quali si applica un meccanismo di add on.
- **Gruppo 2:** criptoasset che non soddisfano alcuna delle condizioni di classificazione. Questi presentano rischi aggiuntivi e superiori rispetto ai criptoasset del Gruppo 1 e sono quindi soggetti ad un trattamento del capitale conservativo e particolarmente oneroso.

Per quanto riguarda le **stablecoin**, il documento stabilisce che devono superare un test di rischio di riscatto (peg one to one) e un requisito di supervisione/regolamentazione per essere idonee all'inclusione nel **Gruppo 1**. Questi criteri cercano di garantire che solo le stablecoin emesse da entità supervisionate e regolamentate che hanno diritti di riscatto robusti e una governance solida siano idonee per l'inclusione.

Il documento prevede anche un **limite di esposizione al Gruppo 2**: l'esposizione totale di una banca ai criptoasset del Gruppo 2 non deve superare il 2% del capitale di Tier 1 della banca e dovrebbe generalmente essere inferiore all'1%. Le banche che superano il limite dell'1% applicheranno un particolare trattamento.

In sintesi, il Comitato di Basilea ha stabilito una serie di linee guida prudenziali per le esposizioni delle banche ai criptoasset, comprese le stablecoin, e prevede di monitorare e rivedere queste linee guida nel tempo.

5.3

GDPR

Compliance

● Medium

Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** dell'Unione Europea stabilisce le regole per la **protezione dei dati personali**. Gli articoli del GDPR che possono riguardare l'utilizzo della blockchain e dei digital asset includono:

- **Articolo 5: Principi relativi al trattamento dei dati personali**, che stabilisce la necessità di trattare i dati personali in modo lecito, equo e trasparente.
- **Articolo 6: Base giuridica per il trattamento dei dati personali**, che stabilisce le condizioni per il trattamento legittimo dei dati personali.
- **Articolo 7: Diritto dell'interessato di opporsi al trattamento dei dati personali**, che stabilisce il diritto dell'interessato di opporsi al trattamento dei suoi dati personali.
- **Articolo 8: Trattamento dei dati personali di un minore**, che stabilisce regole speciali per il trattamento dei dati personali di minori.
- **Articolo 9: Trattamento di categorie particolari di dati personali**, che stabilisce regole per il trattamento di determinate categorie di dati personali, come le informazioni biometriche o genetiche.
- **Articolo 17: Diritto alla cancellazione (diritto all'oblio)**, che stabilisce il diritto dell'interessato di ottenere la cancellazione dei suoi dati personali.
- **Articolo 32: Obblighi in materia di sicurezza dei dati**, che stabilisce gli obblighi per i titolari del trattamento di garantire la sicurezza dei dati personali trattati.

Questi articoli sono applicabili anche all'utilizzo della blockchain e dei digital asset se questi comportano il trattamento di dati personali.

Il **diritto alla cancellazione stabilito dall'Articolo 17** del Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea stabilisce il diritto dell'interessato di ottenere la cancellazione dei suoi dati personali. Tuttavia, **l'utilizzo della blockchain come repository immutabile può l'applicazione di tale obbligo** in quanto le informazioni registrate sulla blockchain sono permanenti e non possono essere modificate o eliminate.

Questo significa che **se i dati personali dell'interessato sono registrati sulla blockchain, non possono essere cancellati**, il che potrebbe portare ad una violazione del diritto alla cancellazione stabilito dal GDPR. Inoltre, la natura decentralizzata e condivisa della blockchain può rendere difficile identificare il responsabile del trattamento dei dati personali e, di conseguenza, esercitare il diritto alla cancellazione. Queste possibili contraddizioni dimostrano la necessità di trovare un equilibrio tra la necessità di proteggere la privacy dei dati personali e la necessità di utilizzare la blockchain come un repository affidabile e immutabile. Potrebbero essere necessarie soluzioni tecnologiche avanzate, come le tecniche di anonimizzazione dei dati o l'utilizzo di schemi di autorizzazione, per gestire queste sfide.

5.4 PSD2

Legale

● Medium

La PSD2 è una direttiva dell'Unione Europea (UE) che regolamenta la prestazione di servizi di pagamento in Europa. La direttiva ha lo **scopo di creare un mercato unico dei servizi di pagamento nell'UE**, migliorando la concorrenza e la sicurezza dei servizi di pagamento e proteggendo i diritti dei consumatori. La PSD2 ha introdotto nuove regole per i fornitori di servizi di pagamento, compresi i fornitori di servizi di pagamento online.

In base alla PSD2, un servizio di pagamento è definito come “un servizio che consiste in operazioni di incasso, pagamento e trasferimento di fondi”. I fornitori di servizi di pagamento che offrono questi servizi sono tenuti ad aderire agli obblighi – ivi compresi quelli di sicurezza e protezione, nonché autorizzativi - previsti dalla direttiva.

Per quanto riguarda i pagamenti con stablecoin e payment token, come precedentemente indicato, la loro inclusione nella definizione di servizi di pagamento ai sensi della PSD2 dipende dalle loro caratteristiche specifiche e, in particolare, se tali caratteristiche ne comportino la riconducibilità alla classe regolamentare della “moneta elettronica” e quindi dei “fondi”. Inoltre, la Banca Centrale Europea (BCE) ha indicato che le stablecoin potrebbero rientrare nella definizione di servizi di pagamento se rispettano determinati requisiti, tra cui la stabilità del valore e l’accessibilità e ferma restando la necessità di valutarne la riconducibilità alle classi normative sopramenzionate.

Inoltre, la PSD2 ha introdotto nuove regole per i fornitori di servizi di pagamento, noti come PSP (Payment Service Provider), tra cui anche quelli che operano nel settore dei pagamenti con digital assets classificabili come “moneta elettronica” e comunque come “fondi”. In particolare, i PSP sono tenuti a implementare misure di sicurezza per la prevenzione delle frodi e la protezione dei dati dei clienti, e ad adottare procedure di autenticazione a due fattori per i pagamenti online. Inoltre, i PSP devono anche fornire ai clienti accesso ai loro conti di pagamento attraverso le cosiddette API (Application Programming Interface).

In sintesi, la PSD2 ha introdotto regole specifiche per i fornitori di servizi di pagamento online, inclusi quelli che operano nel settore di alcuni specifici digital assets classificabili come “moneta elettronica” e comunque come “fondi”. Per quanto riguarda i pagamenti con stablecoin e payment token, la loro inclusione nella definizione di servizi di pagamento ai sensi della PSD2 dipende dalle loro caratteristiche e funzioni specifiche.

5.5 SLA e OLA nei protocolli permissionless

Compliance

● Medium

SLA e OLA nei protocolli permissionless

SLA (Service Level Agreement) e OLA (Operational Level Agreement) sono due **tipi di accordi utilizzati nell'ambito dei servizi informatici per garantire che il servizio offerto soddisfi le aspettative degli utenti**.

Lo **SLA è un accordo formale tra il provider di servizi e l'utente finale** che definisce i livelli di servizio attesi e le relative metriche di performance. Lo **scopo principale dello SLA è quello di definire e garantire il livello di servizio che l'utente finale si aspetta di ricevere dal provider**.

L'OLA, d'altra parte, è un accordo interno tra il provider di servizi che definisce le responsabilità **e le**

attività necessarie per garantire il corretto funzionamento del servizio. Lo scopo principale dell'OLA è quello di garantire che il provider di servizi possa rispettare gli SLA concordati con l'utente finale. Per quanto riguarda l'applicazione di SLA e OLA ai protocolli informatici peer-to-peer, questi accordi possono essere utilizzati per garantire la qualità del servizio offerto dalla rete peer-to-peer. Ad esempio, gli SLA possono definire le metriche di performance per il throughput di dati, il tempo di risposta delle richieste e la disponibilità della rete. L'OLA può definire le attività necessarie per garantire il corretto funzionamento dei nodi della rete, l'aggiornamento dei software, la sicurezza dei dati e altro ancora. In generale, la soluzione migliore per lanciare una soluzione peer-to-peer potrebbe essere quella di utilizzare più protocolli in modo da garantire una maggiore ridondanza e la possibilità di scalare il sistema. Utilizzare diversi protocolli può inoltre ridurre il rischio di un singolo punto di fallimento e migliorare la sicurezza della rete. In questo caso, gli SLA e OLA dovrebbero essere definiti per ogni protocollo utilizzato e coordinati in modo da garantire la qualità del servizio offerto dalla rete nel suo complesso.

5.6

Compliance

● Medium

Digital Finance Package e MiCA

La Commissione Europea ha adottato un pacchetto di finanza digitale il 24 settembre 2020, che include una strategia di finanza digitale e proposte legislative su cripto-attività e resilienza digitale. Questo pacchetto mira a creare un settore finanziario competitivo nell'UE che offre ai consumatori l'accesso a prodotti finanziari innovativi, garantendo al contempo la protezione dei consumatori e la stabilità finanziaria.

- **Priorità della strategia di finanza digitale:** La strategia stabilisce quattro priorità principali: rimuovere la frammentazione nel Mercato Unico Digitale, adattare il quadro normativo dell'UE per facilitare l'innovazione digitale, promuovere una finanza basata sui dati e affrontare le sfide e i rischi con la trasformazione digitale, compreso il miglioramento della resilienza operativa digitale del sistema finanziario.
- **Proposte legislative su cripto-attività:** La Commissione propone un quadro sulle cripto-attività per consentire l'innovazione in un modo che preserva la stabilità finanziaria e protegge gli investitori. Le cripto-attività sono rappresentazioni digitali di valori o diritti, che vengono trasferiti e conservati elettronicamente.
- **Regolamento sui mercati delle cripto-attività:** La Commissione propone un regime pilota per le infrastrutture di mercato che desiderano provare a negoziare e regolare le transazioni in strumenti finanziari sotto forma di cripto-attività. Per le cripto-attività precedentemente non regolamentate, comprese le 'stablecoins', la Commissione propone un regime su misura.
- **Resilienza operativa digitale:** La Commissione propone che tutte le imprese si assicurino di poter resistere a tutti i tipi di interruzioni e minacce relative alle tecnologie dell'informazione e della comunicazione (ICT). Le banche, le borse, le camere di compensazione, così come le fintech, dovranno rispettare standard rigorosi per prevenire e limitare l'impatto degli incidenti legati alle ICT.
- **Strategia per i pagamenti al dettaglio:** La strategia per i pagamenti al dettaglio dell'UE mira a sviluppare ulteriormente il mercato dei pagamenti europeo in modo che l'Europa possa beneficiare appieno dell'innovazione e delle opportunità che derivano dalla digitalizzazione. La strategia si concentra sulla creazione delle condizioni per rendere possibile lo sviluppo di pagamenti istantanei e soluzioni di pagamento a livello di UE, sulla protezione dei consumatori e sulla garanzia che le soluzioni di pagamento siano sicure.

Il Regolamento **MiCA** (Mercati degli Strumenti Finanziari Regolamentati), recentemente **approvato dal Parlamento e dal Consiglio dell'Unione Europea**, ha l'obiettivo di fornire un **quadro normativo per la regolamentazione dei mercati dei digital assets**. Ecco i punti focali di questo regolamento:

- **Regolamentazione dei mercati di digital assets:** MiCA mira a regolamentare i mercati di digital assets fornendo un quadro normativo, tra le altre, per le attività di negoziazione di questi assets.
- **Requisiti di licenza:** le imprese che desiderano prestare servizi su digital assets devono richiedere una licenza da parte delle autorità competenti.
- **Protezione degli investitori:** MiCA ha tra i propri obiettivi la protezione dei consumatori, fornendo, tra le altre, regole di trasparenza. Questo aiuta a prevenire la manipolazione dei prezzi e a garantire che gli investitori abbiano accesso a informazioni complete e trasparenti sui prodotti offerti.
- **Requisiti di trasparenza:** le imprese che offrono digital assets al pubblico o prestano servizi aventi ad oggetto questi ultimi devono fornire informazioni complete e trasparenti sui prodotti offerti agli investitori. Questo comprende informazioni sul prezzo, sul volume degli scambi, sul rischio associato ai prodotti e sui requisiti di margine.
- **Reporting e supervisione:** le imprese devono fornire rapporti regolari sulle loro attività ai regulatori e sottoporsi ad una supervisione costante per garantire che siano in conformità con le leggi e i regolamenti applicabili.
- **Gestione dei conflitti di interessi:** le imprese devono implementare misure efficaci per gestire i conflitti di interessi tra loro e i loro clienti.
- **Responsabilità per la sicurezza dei dati:** le imprese sono responsabili per la sicurezza dei dati degli investitori, compresi i dati sulle transazioni e le informazioni personali. Devono implementare misure di sicurezza appropriate per proteggere i dati e prevenire la perdita o il furto di informazioni sensibili.

Questi sono solo alcuni dei punti focali del regolamento MiCA, che mira a fornire un quadro normativo sicuro e trasparente per la regolamentazione dei mercati dei digital assets. Questo aiuterà a garantire che la protezione dei consumatori e che i mercati funzionino in modo equo e trasparente.

In Italia, in attesa dell'applicazione del Regolamento MiCA, la prestazione di servizi aventi ad oggetto **digital asset è regolamentata principalmente dal Decreto Legislativo 90/2017**, che ha introdotto la definizione di “**valute virtuali**” e ha stabilito **obblighi di registrazione e di conformità alle normative antiriciclaggio per i soggetti che svolgono attività con i digital asset**. Un'azienda che presta tali servizi, e che pertanto sia qualificabile come VASP (virtual asset service provider), deve richiedere e ottenere l'iscrizione all'interno di un apposito registro dell'OAM ((Organismo degli Agenti e dei Mediatori) per poter operare. L'OAM è l'**organismo che si occupa della gestione degli elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi**, come previsto dal Decreto Legislativo 141/2010.

5.7

Legale

● Hard

Gestione fiscale dei digital assets

In Italia, il trattamento fiscale dei digital assets è stato oggetto di una serie di provvedimenti legislativi e interpretazioni giuridiche negli ultimi anni. Andremo a vedere, qui di seguito, come vengono trattati i digital assets a livello fiscale nella nostra nazione.

LA CIRCOLARE DELL'AGENZIA DELLE ENTRATE SULLE CRIPTOATTIVITÀ

La Circolare in commento illustra il quadro normativo di riferimento in ambito europeo sulla disciplina di tassazione delle cripto-attività, le interpretazioni adottate prima dell'introduzione della L. 197/2022 (legge di bilancio 2023) e le norme in vigore a partire dal **1° gennaio 2023**.

Nel documento vengono **confermate le interpretazioni** fornite con riferimento ai periodi d'imposta **anteriori** al 2023, adottando il principio secondo cui alle operazioni aventi ad oggetto valute virtuali risul-

tano applicabili, in generale, le disposizioni fiscali vigenti in materia di valute estere aventi corso legale. A decorrere dal 2023, invece, il quadro di riferimento muta radicalmente a seguito dell'introduzione di un articolato impianto normativo.

Attualmente, il regime impositivo delle cripto-attività per i soggetti non imprenditori si rinvie nell'art. 67 comma 1 lett. c-sexies del TUIR (introdotto dalla L. 197/2022) che fa rientrare tra i **redditi diversi di natura finanziaria** “le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, comunque denominate”.

La norma prevede, inoltre che:

- tali redditi non sono assoggettati a tassazione se **inferiori**, complessivamente, a **2.000 euro** nel periodo d'imposta;
- in ogni caso non costituisce fattispecie fiscalmente rilevante la permuta tra cripto-attività aventi le medesime caratteristiche e funzioni.

In merito, la circolare precisa che la **cessione degli NFT** da parte dell'**autore** non determina un reddito diverso. Si afferma che il medesimo, qualora non costituisca un reddito conseguito nell'esercizio di impresa commerciale, si considera un reddito di lavoro autonomo ai sensi dell'art. 53, comma 2, lett. b), del TUIR, nel caso in cui l'attività sia oggetto dell'esercizio di arti o professioni, ovvero ai sensi dell'art. 67, comma 1, lett. I), del TUIR nel caso in cui l'attività non sia esercitata abitualmente.

Per quanto riguarda la **permuta**, la norma stabilisce che non costituisce evento fiscalmente rilevante quella tra cripto-attività aventi eguali caratteristiche e funzioni.

L'interpretazione suggerita dall'Agenzia delle Entrate è, correttamente, quella secondo cui non rappresenta una fattispecie realizzativa lo scambio di un digital asset con un altro (ad esempio, l'acquisto di ethereum con bitcoin) né lo scambio di un NFT con un altro NFT. Si considera, invece, una fattispecie fiscalmente rilevante come permuta, ad esempio, l'acquisto di un NFT con un digital asset.

Con riferimento alla disciplina sul **monitoraggio fiscale**, l'attuale formulazione dell'art. 4 del DL 167/90 prevede la compilazione del quadro RW per le persone fisiche, le società semplici e gli enti non commerciali che detengono cripto-attività.

L'Agenzia delle Entrate conferma la sua impostazione per la quale devono essere oggetto di monitoraggio tutte le fattispecie di cripto-attività detenute attraverso “portafogli”, “conti digitali” (comunemente detti “wallet”) o **altri sistemi di archiviazione** o conservazione.

Si precisa anche che le cripto-attività possano rientrare nelle previsioni di **esonero** dalla compilazione del quadro RW del comma 3, dell'art. 4 del DL 167/90, il quale stabilisce che gli obblighi di indicazione nella dichiarazione dei redditi non sussistono per le attività finanziarie e patrimoniali affidate in gestione o in amministrazione agli intermediari residenti e per i contratti comunque conclusi attraverso il loro intervento, qualora i flussi finanziari e i redditi derivanti da tali attività e contratti siano stati assoggettati a ritenuta o imposta sostitutiva dagli intermediari stessi. Resta fermo, infine, che l'IVAFE (Imposta sul Valore delle Attività Finanziarie detenute all'Estero) sulle cripto-attività si applica a partire dal 1° gennaio 2023.

Relativamente all'IVA la bozza di circolare sottolinea che le operazioni vanno considerate **caso per caso, indagando sulla reale natura e funzione dei singoli digital asset**:

1. **Se sono digital asset utilizzati solo come mezzo di pagamento contrattuale (es bitcoin)**, ossia non ha altre finalità oltre a quella di un mezzo di pagamento, **le operazioni ad esse relative sono in genere esenti IVA ART 10** ed in particolare sono esenti il cambio di valuta tradizionale contro valuta virtuale, mining su valute virtuali, servizi di digital wallet, staking (validazione transazioni).
2. Se non è possibile individuare una controprestazione o un rapporto sinallagmatico fra prestatore del servizio e un beneficiario indentificato e identificabile, l'operazione è fuori campo IVA.
3. Se invece i servizi sono disciplinati contrattualmente e sono note le controparti interessate, il mining di digital assets sarà imponibile, non imponibile o esente a seconda della specifica cripto-attività.
4. I **security token** sono esenti IVA in quanto strumenti di investimento (attenzione non tratta il caso del deposito di tali strumenti).
5. **Utility token**
 - a. Se simili a **buoni acquisto**, seguono le regole di tali buoni (imponibilità IVA immediata se è individuabile immediatamente la natura dei servizi resi o dei beni ceduti, altrimenti escluse IVA fino a

- definizione dei servizi e beni individuati). Per essere buoni corrispettivo occorre che siano accettati dal potenziale fornitore come parziale corrispettivo e che vi sia indicazione di beni e servizi che il token consente di acquistare, o, in alternativa, l'identità dei potenziali fornitori.
- b. **Hybrid token** devono essere valutati caso per caso, infatti se identificati come titoli di legittimazione senza individuazione servizi, la cessione è senza IVA. **Non è invece un voucher quando:**
 - i. opera come digital asset, per cui è assimilato a servizi di pagamento esenti IVA;
 - ii. non sono sufficientemente dettagliati i beni e servizi cui darebbe diritto, per cui la cessione è fuori campo fino a definizione di tali beni;
 - iii. lo scopo è suscettibile di modifica, cui la cessione è fuori campo fino a definizione di tali beni
 - c. Va visto caso per caso per stabilire se token voucher o strumento di pagamento.
6. Pe gli **NFT** vanno verificate le pattuizioni contrattuali intese, quali ad esempio i diritti e asset che incorpora, le modalità di circolazione, se sono accessori ai beni che rappresenta e incorpora, per cui:
 - a. se sottostanti a beni fisici, valgono le regole IVA del bene sottostante;
 - b. se sottostanti a beni digitali, vale la disciplina dei servizi elettronici (con tutte le regole previste di OSS per il B2C e IVA nel Paese del committente) - aliquota delle prestazioni generiche
 - c. casi particolari sono le opere d'arte digitali o i beni immateriali come prestazione di servizi.

“Voluntary disclosure sulle criptoattività”: il MEF ha precisato che, con una disposizione normativa di prossima emanazione, saranno prorogati di tre mesi, e precisamente dal 30 giugno 2023 al **30 settembre 2023**, “i termini per il versamento dell’imposta sostitutiva delle cripto-attività, il cui regime fiscale è stato ridefinito in legge di bilancio”.

La proroga dovrebbe riguardare il termine per il versamento dell’**imposta sostitutiva del 14%** necessaria per la rideterminazione opzionale del valore delle cripto-attività, risulta quindi opportuno richiamare brevemente gli ambiti in cui si è mossa la L. 197/2022 (legge di bilancio 2023) al fine di regolare la fiscalità di tali attività, i quali sono essenzialmente cinque:

1. con il nuovo art. 67 comma 1 lettera c-sexies) del TUIR è stato introdotto ex novo dal 2023 un **regime fiscale ad hoc per i redditi dei soggetti non imprenditori legati alle cripto-attività**, in precedenza tratteggiato solo dalla prassi, e con regole in sostanza mutuate da quelle applicabili alle valute estere (sostanzialmente eliminate dalla Circolare in bozza);
2. si è stabilito per legge, con delle modifiche all'art. 4 del DL 167/90, che il **possesso di cripto-attività determina l’obbligo di compilazione del quadro RW**, pur rimanendo punti di incertezza notevoli per le cripto-attività detenute per il tramite di intermediari italiani (le quali dovrebbero essere escluse dal monitoraggio, a dispetto di indicazioni non chiarissime della Relazione al Ddl. di bilancio 2023);
3. è stato previsto un **meccanismo opzionale di rideterminazione del valore delle cripto-attività possedute al 1° gennaio 2023**, che presenta similitudini con quello, ben oliato, delle partecipazioni, e che consente di assumere quale nuovo costo fiscale riconosciuto ai fini del *capital gain* il valore normale di tali asset al 1° gennaio 2023, dietro il pagamento di una imposta sostitutiva del 14%. Non è allo scopo prevista alcuna perizia di stima;
4. una **voluntary disclosure delle cripto-attività, riservata ai soggetti che non hanno adempiuto agli obblighi fiscali e che consente di rimuovere le violazioni con il pagamento di un onere** dello 0,5% del valore delle attività non dichiarate nel quadro RW per ciascuna annualità (a cui si aggiunge un 3,5% se non sono stati dichiarati i redditi, se realizzati, connessi alle attività in questione). Per questo adempimento, quindi, occorrerà attendere un provvedimento dell’Agenzia delle Entrate sperando nella sua emanazione in tempi brevi.
5. sono stati **razionalizzati gli obblighi in materia di imposta di bollo e di IVAFE** (o, più precisamente, di “imposta sul valore delle cripto-attività detenute da soggetti residenti nel territorio dello Stato”, pur se di fatto le regole sono quelle dell’IVAFE).

In particolare, l'art. 1 commi 134 e 135 della L. 197/2022 precisa che l’imposta sostitutiva è versata in un’unica soluzione entro il 30 giugno 2023 o in un massimo di tre rate annuali di pari importo, con interessi del 3% annuo sulle rate successive alla prima, la quale scadrebbe comunque al **30 giugno 2023**. La proroga è opportuna, visto che ad oggi mancano istruzioni in merito a come determinare l’onere per imposta sostitutiva. Il meccanismo dovrebbe essere quello previsto per le partecipazioni, per cui la base imponibile non è pari alla differenza tra il valore normale al 1° gennaio 2023 e il costo di acquisto, ma al

valore normale “lordo”; rimangono però alcuni aspetti dubbi: ad esempio, il fatto che si possa assumere quale valore quello indicato da un singolo exchange o si debba, al contrario, assumere una media tra le quotazioni disponibili delle varie piattaforme.

Quello che invece dovrebbe essere assodato è che, non essendo le cripto-attività assimilabili alle azioni e alle obbligazioni quotate, non si dovrebbe fare riferimento al principio contenuto nell'[art. 9 comma 4 lettera a\) del TUIR](#), per cui si assume la media dei prezzi dell’ultimo mese: il valore è, invece, quello **puntuale al 1° gennaio 2023**.

Progetto servizio custodia criptoattività nel Gruppo Sella

Nel Gruppo per quanto riguarda il progetto di cui all’attività di un servizio di custodia delle cripto-attività per i clienti di BSE, con la funzionalità di deposito/prelievo da/verso wallet esterni, senza funzioni di acquisto/vendita su piattaforme di exchange o di scambio tra clienti comporterà la necessità di approfondire ed integrare nel processo tutte le implicazioni di natura fiscale inerenti anagrafe dei rapporti, monitoraggio fiscale, regime fiscale dei redditi diversi di natura finanziaria e imposta di bollo, oltre, naturalmente, alle tematiche IVA, CRS, Fatca e Dac 8, anche alla luce delle nuove disposizioni entrate in vigore il 1 gennaio 2023 per effetto della Legge di Bilancio.

I predetti adempimenti saranno da coniugare con il Regolamento UE MICA –la cui entrata in vigore è in parte prevista al 30/6 ed in parte al 30/12/2024, la DAC 7, entrata in vigore dal 26/03/2023 e la DAC 8, con entrata in vigore stimata dal 2026.

Di seguito, per comodità di consultazione,
una sintesi della normativa di cui al Regolamento MICA, DAC7 e DAC 8.

IL REGOLAMENTO SUI MERCATI DELLE CRIPTO-ATTIVITÀ (MICA) con entrata in vigore in parte al 30/6 ed in parte al 30/12/2024

Venerdì 9 giugno 2023 è stato pubblicato in Gazzetta ufficiale europea il **nuovo Regolamento del Parlamento europeo e del Consiglio n. 1114 del 2023, che introduce la nuova disciplina sui mercati delle cripto-attività** ed è parte della “Strategia sulla finanza digitale per il settore finanziario dell’UE” applicabile alle cripto-attività, agli emittenti di cripto-attività e ai fornitori di servizi per le cripto-attività (quali le piattaforme di negoziazione e i portafogli in cui sono detenute le cripto-attività).

L’obiettivo dell’Unione europea è di definire le regole per le **tipologie di cripto-attività che non risultano al momento inquadrabili in nessuna altra disciplina vigente**:

- i. **token di moneta elettronica**, ossia cripto-attività che mirano a stabilizzare il loro valore facendo riferimento a una sola valuta ufficiale;
- ii. **token collegati ad attività**, che mirano a stabilizzare il loro valore facendo riferimento ad un altro valore o diritto, o a una combinazione degli stessi, comprese una o più valute ufficiali;
- iii. **cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica**, categoria nella quale rientrano, tra l’altro, anche i c.d. utility token;

Parallelamente si attendono le disposizioni di chiarimento che definiranno quali cripto attività siano invece confermate come strumenti finanziari e quindi regolati dalla già esistente normativa “MIFID”.

Il Regolamento introduce un vero e proprio nuovo framework generale di riferimento, in relazione al quale EBA, ESMA, Commissione europea e Banca centrale europea sono chiamate a esercitare l’attuazione di **oltre 50 deleghe** al fine di:

- definire le **regole di emissione e ammissione sul mercato** delle tipologie di cripto-attività in esame;
- stabilire la regolamentazione applicabile ai **prestatori di servizi per le cripto-attività (c.d. CASP)**, ossia i soggetti che su base professionale forniscono i seguenti servizi: i) prestazione di custodia e amministrazione di cripto-attività per conto di clienti; ii) gestione di una piattaforma di negoziazione di cripto-attività; iii) scambio di cripto-attività con fondi; iv) scambio di cripto-attività con altre cripto-attività; v) esecuzione di ordini di cripto-attività per conto di clienti; vi) collocamento di cripto-attività; vii) ricezione e trasmissione di ordini di cripto-attività per conto di clienti; viii) prestazione di consulenza sulle cripto-attività; ix) prestazione di gestione di portafoglio sulle cripto-attività; x) prestazione di servizi di trasferimento di cripto-attività per conto dei clienti;

- completare il quadro di riferimento con **misure specifiche su tutte le tematiche rilevanti** per le cripto attività, considerando temi come **la Market abuse, l'antiriciclaggio, i conflitti di interesse, la prestazione dei servizi verso la clientela finale, la tutela dell'investitore, la continuità operativa e le esternalizzazioni, la disciplina di vigilanza prudenziale e la governance.**

La nuova disciplina definisce le modalità di esercizio e i procedimenti di richiesta di autorizzazione ad intraprendere le attività. La vigilanza sulla disciplina sarà affidata ad EBA ed ESMA, chiamate anche sul tema a completare il quadro di riferimento con l'introduzione di alcune norme tecniche specifiche.

Sono esplicitamente previsti **requisiti e procedure di avvio delle attività in tale mercato semplificate e ridotte nel caso in cui ad operare siano talune tipologie di società appartenenti al settore finanziario;** ad esempio in ambito di prestazione dei servizi per le cripto-attività, i soggetti già autorizzati alla prestazione dei servizi di investimento secondo la disciplina Mifid potranno avviare i nuovi servizi come CASP previa comunicazione all'Autorità di riferimento, senza dover attivare il processo autorizzativo previsto, molto più complesso e strutturato.

Il nuovo quadro, una volta completato il processo di attuazione delle deleghe che meglio definiranno nella forma di norme tecniche, orientamenti comunitari e infine, attuative nazionali, l'intero insieme di regole di riferimento, sarà applicabile progressivamente:

- dal **30 giugno 2024** per quel che concerne le norme in merito ad emissione e ammissione alla negoziazione di token collegati ad attività e token di moneta elettronica;
- dal **30 dicembre 2024** per tutti gli altri aspetti della disciplina.

DAC 7 in vigore dal 26/03/2023

La Direttiva UE 2021/514 (DAC 7) (recepita con il Decreto Legislativo n. 32 del 1° marzo 2023 pubblicato in Gazzetta Ufficiale n. 72 del 25 marzo 2023) relativa alla **cooperazione amministrativa nel settore fiscale** ha introdotto **nuovi obblighi di comunicazione e si propone di rafforzare il regime di scambio informativo e la cooperazione amministrativa tra gli Stati sull'estensione dello scambio automatico di informazioni alle attività dei Gestori di piattaforme digitali**, che dal 26/03/2023 sono soggetti ad obblighi di **raccolta e verifica di informazioni sui venditori presenti sulla piattaforma stessa**. Questo comporta con decorrenza 26/03/2023 nuovi obblighi di comunicazione a carico dei Gestori e degli I.P. (information provider), che devono fornire **informazioni sulle transazioni** effettuate attraverso la loro piattaforma.

Tra le principali novità previste dalla **Direttiva DAC 7** per il rafforzamento del regime di scambio informativo, ci sono il **concepto di prevedibile pertinenza** delle informazioni, le **richieste collettive** concernenti un gruppo di contribuenti, l'estensione alle **royalties** dello **scambio automatico obbligatorio di informazioni**, l'ampliamento delle informazioni da trasmettere e l'**esecuzione dei controlli congiunti**. Il Decreto di attuazione della DAC 7 è composto da cinque Capi: i **primi quattro Capi disciplinano gli obblighi di comunicazione e di adeguata verifica** a carico dei Gestori di piattaforme digitali, mentre il **quinto Capo riguarda altre disposizioni relative alla protezione e violazione dei dati, alle verifiche congiunte ed ai termini di decorrenza del provvedimento**.

Le nuove norme previste dalla DAC 7 riguardano le **piattaforme digitali situate sia all'interno che all'esterno dell'UE** e saranno applicabili a partire dal 1° gennaio 2023 per quanto riguarda i soggetti interessati. Tuttavia, l'**accelerazione e il potenziamento dei meccanismi di scambio automatico di informazioni** che interessano principalmente gli Stati, avranno un orizzonte applicativo più ampio che si estenderà entro il 2024.

Il decreto di recepimento della DAC 7 è entrato in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana ovvero il **26 marzo 2023**.

DAC 8 con ipotetica entrata in vigore dal 2026

Il **Consiglio UE** ha raggiunto un **accordo sulla proposta di direttiva (DAC 8)** recante modifiche alla direttiva 2011/16/UE relativa alla cooperazione amministrativa nel settore fiscale al fine di rafforzare la trasparenza fiscale delle cripto-attività.

Le modifiche della DAC 8 **riguardano** in particolare **comunicazione e scambio automatico di informazioni**:

- sui **proventi delle operazioni in cripto-attività**
- sui rulling fiscali preventivi per i soggetti privati con alti patrimoni.

Previste quindi **nuove categorie di attività e di reddito**, quali le cripto-attività, su cui le autorità fiscali si scambieranno le informazioni fornite dai relativi prestatori di servizi.

In questo modo con la DAC 8 verrà **garantito il rispetto degli obblighi fiscali**, reso fisiologicamente difficile dalla natura transfrontaliera delle **cripto-attività**.

Oggetto degli obblighi di comunicazione un **ampio novero di cripto-attività**, che seguono le fattispecie individuate dal regolamento sui mercati delle stesse (MiCA), adottato dal Consiglio.

Rilevano quindi le cripto-attività emesse in modo **decentralizzato**, le **stablecoin**, compresi i **token di moneta elettronica**, e alcuni **token non fungibili** (NFT).

Sintesi servizio custodia (digital wallet) ai fini IVA in ragione del tipo di asset in custodia:

- In caso di asset assimilabili a moneta estera il corrispettivo è esente IVA ex art 10.
- In caso di asset assimilabili a prodotti finanziari il corrispettivo è soggetto ad IVA.
- In caso di un MIX tra i due con unico corrispettivo è soggetto ad IVA.

5.8 MIFID 2

Compliance

● Medium

La **direttiva MiFID 2** (Markets in Financial Instruments Directive) è una **normativa europea che regola i mercati degli strumenti finanziari e i servizi di investimento nell'Unione Europea**. La direttiva è stata introdotta per **proteggere gli investitori e garantire la trasparenza e l'integrità dei mercati finanziari**.

La MIFID 2 è applicabile a tutti gli strumenti finanziari, ivi compresi quelli emessi e/o circolanti su DLT. La direttiva impone regole e obblighi specifici per gli operatori che prestano servizi di investimento, allo scopo di tutelare gli investitori e garantire la stabilità e l'efficienza dei mercati.

In particolare, la MIFID 2 prevede che gli **operatori che offrono servizi di investimento debbano essere registrati e autorizzati dalle autorità di vigilanza competenti**, come la CONSOB in Italia. Gli operatori devono anche **fornire ai clienti informazioni chiare e precise sui rischi e sui costi dei servizi offerti**, nonché sui criteri di valutazione dei digital assets.

La direttiva impone anche l'**obbligo di monitoraggio e di valutazione dei rischi legati alle attività di investimento – ivi comprese quelle su digital assets classificabili come strumenti finanziari**. Tutto ciò impone la necessità di verifiche case by case sulla natura e sulle caratteristiche specifiche di ogni digital assets per valutarne la corretta qualificazione giuridico-regolamentare.

Tra gli obblighi del regolamento MiFID 2 vi è quello di valutare i prodotti finanziari che l'impresa di investimento offre ai propri clienti, in modo da assicurare che siano adatti alle esigenze degli investitori. Questo potrebbe essere applicabile anche alle società che offrono digital assets classificabili come strumenti finanziari.

In conclusione, sebbene il regolamento MiFID 2 non fornisca una regolamentazione specifica per i digital assets e i mercati decentralizzati, le sue disposizioni relative alla protezione degli investitori e alla trasparenza potrebbero essere applicabili anche ad alcuni di questi ed in particolare ai security-token, in quanto riconducibili alla nozione di strumento finanziario.

5.9

Compliance

● Basic

Definizione normativa degli NFT

Attualmente non esiste una definizione normativa specifica per gli NFT (Non-Fungible Token) a livello europeo. Tuttavia, gli NFT possono essere considerati come beni digitali unici e indivisibili, che rappresentano una proprietà o un diritto su un determinato oggetto digitale come, ad esempio, un'opera d'arte o un videogioco.

In ottica di compliance e legalità, gli NFT devono rispettare, tra le altre, **le normative in materia di diritto d'autore, proprietà intellettuale e protezione dei dati personali**. In particolare, la vendita di NFT che rappresentano opere d'arte o altri beni protetti da diritto d'autore deve essere in linea con le leggi sulla proprietà intellettuale e sui diritti d'autore, come la Direttiva europea sul copyright.

La Direttiva europea sul copyright, entrata in vigore nel 2019, ha introdotto importanti novità per la tutela dei diritti dell'autore nell'era digitale. In particolare, la direttiva prevede **l'introduzione di nuove regole sulle piattaforme online che ospitano contenuti protetti da copyright, al fine di garantire una maggiore equità nella remunerazione degli autori e degli artisti**.

Nel contesto degli NFT, la direttiva europea sul copyright è rilevante soprattutto per quanto riguarda la vendita di NFT che rappresentano opere d'arte o altri beni protetti da diritto d'autore. In base alla direttiva, **gli autori hanno il diritto di controllare l'utilizzo delle loro opere e di ricevere una giusta remunerazione per l'utilizzo delle stesse**. Ciò significa che la vendita di NFT che rappresentano opere d'arte o altri beni protetti da copyright deve essere in linea con le leggi sulla proprietà intellettuale e sui diritti d'autore. Inoltre, gli NFT possono essere utilizzati come puntatori di beni fisici o immobili, ad esempio per rappresentare la proprietà di un'auto o di un immobile. In questo caso, gli NFT possono essere qualificati come titoli di proprietà digitali, che **conferiscono al proprietario il diritto di possesso del bene fisico o immobile rappresentato dal token**.

Anche in questo caso, è importante rispettare le normative in materia di proprietà intellettuale e protezione dei dati personali. Inoltre, è importante considerare le implicazioni fiscali della compravendita di NFT **come titoli di proprietà digitali, che possono essere soggetti a tasse sulle plusvalenze o sulle transazioni finanziarie**. Ciò significa che le piattaforme che ospitano la compravendita di NFT devono rispettare il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea.

5.10 DORA

Legale

● Medium

La Digital Operational Resilience Act (DORA) rappresenta un nuovo paradigma europeo per una gestione efficace e completa dei temi di Cybersecurity e ICT nei servizi finanziari. Questo approccio si basa su una visione olistica end-to-end che integra la gestione dei rischi e include il controllo delle terze parti. L'evoluzione di DORA dal 2019 al 2025 può essere riassunta nei seguenti punti:

- Inizio consultazione e pubblicazione bozza (24 dicembre 2020):** La Commissione EU ha avviato un'attività di consultazione e ha pubblicato la bozza del Regolamento nell'ambito del Digital Finance Package.
- Attività di Advocacy e Approvazione (27 dicembre 2022):** Sono state svolte attività di advocacy e un processo approvativo da parte del Parlamento e della Commissione EU. Il Regolamento è stato emanato in Gazzetta Ufficiale EU.
- Entrata in vigore (16 Gennaio 2023):** Il Regolamento DORA è entrato in vigore.
- Pubblicazione RTS:** Le Autorità di Vigilanza EU (EBA, ESMA, EIOPA) hanno emanato i Regulatory Technical Standards, specificando indicazioni operative per specifici requisiti DORA.
- Applicazione e compliance DORA (17 Gennaio 2025):** L'applicazione del Regolamento DORA avverrà 24 mesi dopo l'entrata in vigore. Le entità finanziarie dovranno completare le attività di adeguamento a DORA entro questa data.

DORA mira a stabilire una chiara baseline per i Regolatori e le Autorità di Vigilanza per la gestione end-to-end ICT e Cybersecurity, inclusa la gestione degli incidenti. Il Regolamento si applicherà a circa 22.000 società dei servizi finanziari, comprese le entità del settore finanziario tradizionale e i fornitori di servizi di criptovaluta, emittenti di cripto-asset ed emettitori di token.

Per affrontare le sfide poste da DORA, è importante sviluppare un approccio unico ed integrato per la comprensione, analisi, prioritizzazione ed implementazione delle attività di adeguamento al Regolamento. Questo approccio dovrebbe coinvolgere competenze specialistiche in ambito Technology Consulting, Risk Consulting, Management Consulting e Legal.

5.11 EMD2

Legale

● Medium

La Seconda Direttiva sulla Moneta Elettronica (EMD2) è stata adottata per allineare i requisiti dell'UE e supervisionare gli istituti di moneta elettronica. Questa direttiva stabilisce le regole per l'emissione di moneta elettronica e definisce le categorie di emittenti di denaro elettronico che gli Stati membri dell'UE devono riconoscere. Queste categorie includono, tra le altre:

- Istituti di credito
- Istituti di moneta elettronica

La direttiva EMD2 stabilisce anche una serie di regole prudenziali generali. Queste regole delineano i requisiti relativi alla gestione e alla supervisione degli istituti di moneta elettronica, i quali devono informare le autorità competenti su come salvaguardano i fondi che sono stati ricevuti in cambio di moneta elettronica emessa.

Inoltre, la direttiva stabilisce che gli Stati membri richiedono agli IMEL di detenere, al fine di ottenere l'autorizzazione, un capitale iniziale non inferiore a 350.000 euro.

Oltre all'emissione di denaro elettronico, le istituzioni di denaro elettronico sono autorizzate a svolgere una serie di altre attività. Queste attività includono la fornitura di servizi di pagamento elencati nella direttiva PSD2, l'operazione di sistemi di pagamento e l'esecuzione di attività commerciali diverse dall'emissione di denaro elettronico in conformità con la legge comunitaria e nazionale applicabile.

Infine, è importante notare che gli IMEL non possono accettare depositi o altri fondi rimborsabili dal pubblico in generale se non sono istituti di credito. Devono scambiare qualsiasi fondo ricevuto da titolari di denaro elettronico senza ritardi. Tali fondi non devono essere un deposito o altri fondi rimborsabili ricevuti dal pubblico in generale se non sono istituti di credito.

La normativa EMD2 si applica solo ai crypto-asset classificabili come "moneta elettronica".

5.12 AML Act

Compliance

● Medium

Nel luglio 2021, la Commissione Europea ha adottato un pacchetto legislativo per contrastare il riciclaggio di denaro e il finanziamento del terrorismo, che includeva una proposta per la revisione del Regolamento 2015/847/EU. Questa revisione mirava a estendere l'obbligo dei fornitori di servizi di pagamento di accompagnare i trasferimenti di fondi con informazioni sul pagatore e sul beneficiario ai cripto-asset. Avanzando velocemente a dicembre dello stesso anno, il Consiglio ha concordato il suo mandato negoziale per negoziare con il Parlamento sulla proposta. Le modifiche introdotte dal Consiglio hanno chiarito la proposta della Commissione, introducendo requisiti per i trasferimenti di cripto-asset tra fornitori di servizi di cripto-asset e portafogli non ospitati.

Nel giugno 2022, i negoziatori della presidenza del Consiglio e del Parlamento hanno raggiunto un accordo provvisorio sulla proposta. L'accordo richiedeva che l'intero insieme di informazioni sull'originatore viaggiasse con il trasferimento del cripto-asset, indipendentemente dall'importo dei cripto-asset in transazione.

Infine, nel maggio 2023, il Consiglio ha approvato la posizione del Parlamento e il Regolamento è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (Regolamento (UE) n. 1113/2023). Questo regolamento mira a garantire la tracciabilità dei trasferimenti di cripto-asset, rendendo più difficile per le persone e le entità soggette a misure restrittive cercare di eluderle.

6

Overview normativa sull'identità digitale

- 6.1 Regolamento eIDAS per l'identità digitale
- 6.2 EU Digital Identity Wallet con l'aggiornamento eIDAS
- 6.3 Che cosa sono gli SSI eIDAS Bridge?

6.1

Legale
Basic

Regolamento eIDAS per l'identità digitale

Con il Regolamento eIDAS (*electronic IDentification Authentication and Signature*), l'obiettivo è stato quello di creare una cornice internazionale per migliorare la validità e l'interoperabilità dei servizi cross-border tramite *l'identità digitale*. EIDAS è stato concepito nel 2014, diventando però effettivo solo nel 2016. L'impatto nella vita reale è evidente: la carta d'identità elettronica o/e lo spid.

Riprendendo la sua descrizione formale:

“Regolamento UE n° 910/2014 sull'identità digitale – ha l'**obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i servizi di identificazione elettronica degli stati membri**. Il regolamento eIDAS ha l'obiettivo di rafforzare la fiducia nelle transazioni nell'Unione Europea, fornendo una base normativa comune per interazione elettroniche sicure fra i cittadini, imprese e pubbliche amministrazioni.”

Il regolamento è nato con lo scopo di garantire il buon funzionamento del mercato interno perseguiendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari.

- L'idea è garantire **una sorta di cittadinanza europea nel mondo del web**. Gli obiettivi sono quindi quelli di **eliminare gli ostacoli all'esercizio dei diritti dei cittadini europei, consentire ai cittadini di utilizzare la loro identificazione elettronica per autenticarsi in un altro Stato membro e realizzare una base comune per le interazioni economiche sicure tra imprese, migliorando l'efficacia dei servizi elettronici per pubblici e privati**.

I punti cardine del regolamento eIDAS sono:

1. **Fissare le condizioni a cui gli stati membri riconoscono i mezzi di identificazione elettronica** delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro stato membro.
2. **Stabilire le norme relative ai servizi fiduciari**, in particolare per le transazioni elettroniche.
3. **Istituire un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web**.

L'obiettivo è quindi quello di realizzare **un mercato comune dell'identità digitale** che possa facilitare le imprese, i cittadini e la pubblica amministrazione nei processi di digitalizzazione dei processi e nella dematerializzazione dei documenti e delle pratiche.

Entrando più nel tecnico, il regolamento eIDAS crea delle linee guida per i seguenti scopi

- **Delineare i diritti e i doveri di tutti i prestatori di servizi fiduciari**, in funzione delle loro caratteristiche.
- **Fornire un pieno riconoscimento della firma digitale** all'interno del regime normativo
- **Individuare gli standard tecnici delle firme digitali europei**.
- **Facilitare l'identificazione, l'autenticazione e l'autorizzazione** quando un utente, azienda o pubblica amministrazione vuole operare all'interno del infosfera.

Il ruolo del trust service provider (TSP) è proprio quello di essere l'anello di congiunzione tra il regolamento, l'identità digitale e il cittadino o l'impresa. Tra le tipologie di trust service provider, esiste un sottogruppo definito come **Qualified Trust Service Provider (QTSP)**, i quali attori vengono certificati per emettere uno standard di identità col valore massimo rispetto ai gradi di attendibilità.

Il regolamento eIDAS, così per come è stato pensato, è basato su una struttura centralizzata e quindi ha la necessità di avere delle terze parti fiduciarie che possono emettere servizi fiduciari all'interno del mercato digitale. La distinzione tra i ruoli all'interno del mercato può essere spiegata dal momento in cui vi si ha la necessità di avere **diversi livelli di affidabilità verso una identità digitale**.

eIDAS quindi si pone come un vero e proprio regolamento che permette ai cittadini europei di utilizzare un'identità "verificata" all'interno degli stessi servizi pubblici e privati europei.

6.2

Legale

● Medium

Eu Digital Identity Wallet con l'aggiornamento di eIDAS

La nuova bozza del rinnovato Regolamento eIDAS (Electronic Identification, Authentication and Trust Services) **include un riferimento esplicito all'EU Digital Identity Wallet**, una soluzione digitale di identità che ha un ruolo rilevante nella proposta di regolamento. Il testo si articola in diverse sezioni, ognuna delle quali contiene riferimenti specifici all'EU Digital Identity Wallet.

La prima sezione del testo riguarda la definizione e gli obiettivi del regolamento eIDAS. In questa sezione, viene specificato che **l'obiettivo del regolamento è quello di stabilire un quadro normativo per le identità elettroniche affidabili e interoperabili, che consentano di accedere in modo sicuro ai servizi online transfrontalieri**. Inoltre, viene indicato che il regolamento **promuove l'adozione di soluzioni di identità digitale come l'EU Digital Identity Wallet**.

La seconda sezione del testo riguarda le disposizioni generali del regolamento. In questa sezione, viene specificato che **le identità elettroniche riconosciute ai sensi del regolamento possono essere utilizzate per accedere a servizi online transfrontalieri**. Inoltre, viene indicato che **l'EU Digital Identity Wallet deve rispettare gli standard tecnici e le specifiche stabiliti dal regolamento eIDAS**.

La terza sezione del testo riguarda le identità elettroniche qualificate. In questa sezione, viene specificato che **le identità elettroniche qualificate riconosciute ai sensi del regolamento eIDAS possono essere utilizzate per accedere a servizi online transfrontalieri**. Inoltre, viene indicato che **l'EU Digital Identity Wallet può essere utilizzato come soluzione di identità elettronica qualificata**.

La quarta sezione del testo riguarda le disposizioni relative alla fiducia elettronica. In questa sezione, viene specificato che **il regolamento eIDAS promuove la fiducia nella comunicazione elettronica attraverso l'utilizzo di soluzioni di identità digitale affidabili e interoperabili**.

Infine, **l'ultima sezione** del testo riguarda le **disposizioni finali e le disposizioni transitorie**. In questa sezione, viene specificato che il regolamento eIDAS entrerà in vigore il giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea. Inoltre, viene indicato che le disposizioni del regolamento si applicano alle identità elettroniche emesse prima e dopo la sua entrata in vigore, compresa l'EU Digital Identity Wallet.

6.3

Che cosa sono gli SSI eIDAS Bridge?

Informatica / Legale

● Medium

A livello Europeo, si sta già sviluppando l'idea che la Self Sovereign Identity abbia il potenziale per migliorare il modo in cui i cittadini gestiscono la loro identità digitali, nonché la capacità di offrire alle pubbliche amministrazioni nuove modalità di verificare le identità dei cittadini e offrire servizi pubblici più efficienti. Pertanto, una delle iniziative nate per fare in modo di autenticare con questo innovativo metodo i cittadini ai servizi pubblici, in maniera allineata alle normative, è il SSI **bridge eIDAS**.

Il Bridge funge quindi da “allineamento” tra la normativa “tradizionale” relativa all’identità digitale e a questo nuovo paradigma di identità digitale che sta sempre più crescendo ma che deve essere supportato da appropriate garanzie dal punto di vista normativo.

Il progetto eIDAS Bridge è una fase iniziale di implementazione, e sta venendo implementato all'interno del contesto dell'European Self-Sovereign Identity Framework (ESSIE), uno dei casi d'uso selezionati dalla European Blockchain Partnership (EBP) e dalla Commissione Europea che è sviluppato nell'ambito della European Blockchain Services Infrastructure.

Nell'ambito dell'azione Innovative Public Services del programma ISA2, la Commissione Europea ha sperimentato il nuovo modello di verifica delle identità, riscontrando dei grandi benefici in ottica di protezione e miglioramento nella gestione dei dati personali dei cittadini.

Grazie alla SSI, il cittadino dovrebbe richiedere una sola volta una credenziale ad una pubblica amministrazione, conservarla e condividerla senza perderne il controllo quando inizia a utilizzare servizi diversi tra le diverse pubbliche amministrazioni. Una standardizzazione efficace potrà garantire che diversi sistemi di identità decentralizzata funzionino insieme in modo coordinato, senza incompatibilità o conflitti tra di loro.

Conclusioni

La **complessità della tecnologia Distributed Ledger Technology (DLT) e dei digital assets può rappresentare una barriera all'adozione** da parte degli attori del sistema finanziario. Per questa ragione, **l'educazione è un fattore fondamentale per garantire che tutti gli attori coinvolti abbiano una comprensione chiara delle implicazioni delle tecnologie emergenti e dei loro benefici e rischi potenziali.** L'educazione può contribuire a ridurre l'incertezza e la resistenza al cambiamento, fornendo una base comune di conoscenza a tutti gli attori del sistema finanziario.

La **cooperazione tra gli attori del sistema finanziario è essenziale**, poiché può contribuire a **creare standard comuni, adottare processi di condivisione delle informazioni e ridurre le inefficienze del sistema finanziario.** La cooperazione può anche consentire di identificare nuove opportunità e di sviluppare nuovi modelli di business basati su queste tecnologie.

L'implementazione di tecnologie come i DLT e i digital assets possono migliorare l'efficienza e la trasparenza del sistema finanziario, ma è importante affrontare le sfide legate all'educazione, all'asimmetria informativa e rafforzare la cooperazione tra gli attori per garantire una maggiore partecipazione e adozione della tecnologia da parte di tutti gli attori del sistema finanziario.

Ringraziamenti

Questo manuale didattico è stato realizzato grazie alla collaborazione dei diversi colleghi del **Gruppo Sella**, che hanno scritto e revisionato la documentazione, e creato i percorsi formativi per i propri colleghi. L'obiettivo è stato quello di creare un manuale interdisciplinare attraverso la somma delle molte hard e soft skills condivise tra i contributori, col fine di far comprendere al meglio l'evoluzione della finanza e della moneta.

Contributori:

- **Jacopo Sesana**, *Blockchain Business Analyst* presso Banca Sella
- **Filippo Chiricozzi**, *Stream Manager, web3 & Digital Asset* presso Banca Sella
- **Samuele Rota**, *Innovation Intern* presso Banca Sella
- **Andrea Daly**, *Responsabile Compliance Servizi di Investimento, Research and Consulting & Digital Assets* presso Sella Holding
- **Gianluca Santavicca**, *Legal Specialist Open Finance & DLT* presso Banca Sella
- **Roberto Pozzuolo**, *Responsabile rischi non finanziari - Responsabile anti frode e cybercrime* presso Sella Holding
- **Marco Coda**, *Crypto Digital Asset Analyst and Alternative Investment Specialist* presso Sella Holding
- **Satwinder Singh**, *Product Owner Blockchain* presso Banca Sella
- **Alessandro Giordano**, *Product Specialist* presso Banca Sella
- **Andrea Tessera**, *Chief Innovation Office* presso Banca Sella
- **Valerio Cicco**, *Co-Head DLT & Digital Assets Team* presso Sella Holding
- **Mico Curatolo**, *Co-Head - DLT & Digital Assets Team* presso Sella Holding
- **Stefano Priola**, *CTO at Centrico Spa - Gruppo Sella*
- **Andrea Pozzi**, *Head of Banking and Payments* presso Banca Sella
- **Alessandro Bocca**, *CEO* presso Axerve

