Ghisolfi Michele, Pelissero Luca,Leone Gabriele

Documentazione Esame 2022

Contents

Part I

Blockchain

1

La Tecnologia Blockchain

CONTENTS

A component part for an electronic item is manufactured at one of three different factories, and then delivered to the main assembly line.Of the total number supplied, factory A supplies 50%, factory B 30%, and factory C 20%. Of the components manufactured at factory A, 1% are faulty and the corresponding proportions for factories B and C are 4% and 2% respectively. A component is picked at random from the assembly line. What is the probability that it is faulty?

1.1 Introduzione

La blockchain è un registro di contabilità condiviso e immutabile che facilita il processo di registrazione delle transazioni e la tracciabilità dei beni in una rete commerciale. Un asset può essere tangibile (una casa, un'auto, denaro, terra) o intangibile (proprietà intellettuale, brevetti, copyright, branding). Praticamente qualsiasi cosa che abbia un valore può essere rintracciata e scambiata su una rete blockchain, riducendo rischi e costi per tutti gli interessati.

1.1.1 Perchè è importante?

il business si basa sulle informazioni. Più sono rapide e accurate, meglio è. La blockchain è ideale per trasmettere queste dati perché fornisce informazioni immediate, condivise e completamente trasparenti archiviate in un registro immutabile a cui possono accedere solo i membri di rete autorizzati. Una rete blockchain può, tra le altre cose, tracciare ordini, pagamenti, account,

produzione e molto altro ancora. E dato che i membri condividono una visione univoca della verità, è possibile vedere tutti i dettagli di una transazione end-to-end, generando così maggiore fiducia, oltre a nuove opportunità in termini di efficienza.

> "Mentre la maggior parte delle tecnologie tende ad automatizzare i lavoratori alla periferia che svolgono compiti umili, le blockchain automatizzano il centro. Invece di mettere il tassista fuori dal lavoro, la blockchain mette Uber fuori dal lavoro e permette ai tassisti di lavorare direttamente con il cliente."
>
> Vitalik Buterin,
> Co-Fondatore di Ethereum

1.2 Elementi chiave di una blockchain

Tecnologia di registro distribuito: Tutti i partecipanti alla rete hanno accesso al registro distribuito e al record immutabile di transazioni in esso contenuto. Con questo registro condiviso, le transazioni vengono annotate una sola volta, eliminando la duplicazione dei compiti, tipica delle reti di business tradizionali.

Record immutabili: Nessun partecipante potrà modificare o manomettere una transazione, una volta annotata nel registro condiviso. Se un record di transazione contiene un errore, dovrà essere aggiunta una nuova transazione per correggere l'errore, dopodiché entrambe le transazioni saranno visibili.

Contratti intelligentii: Per accelerare le transazioni, un set di regole, chiamate contratto intelligente (smart contract), viene memorizzato sulla blockchain ed eseguito automaticamente. Un contratto intelligente può definire le condizioni per i trasferimenti di obbligazioni aziendali, includere le condizioni per l'assicurazione di viaggio da pagare e molto altro ancora.

1.3 Come funziona la Blockchain

Ogni volta che avviene una transazione, questa viene registrata come un "blocco" di dati: Queste transazioni rappresentano il movimento

di un asset che può essere tangibile (un prodotto) o intangibile (intellettuale). Questo blocco di dati può riportare le informazioni che si desiderano: chi, cosa, quando, dove, quanto e persino delle condizioni - come la temperatura di una spedizione di cibo.

Ogni blocco è collegato a quelli che lo precedono e che lo seguono: Questi blocchi formano una catena di dati man mano che un asset si sposta da un luogo all'altro o cambia il proprietario. I blocchi attestano l'ora e la sequenza esatte delle transazioni e i blocchi si collegano in modo sicuro tra loro per evitare che uno di essi venga alterato o inserito tra due blocchi esistenti.

Le transazioni sono bloccate tra loro in una catena irreversibile: una blockchain: Ogni blocco aggiuntivo rafforza la verifica del blocco precedente e quindi dell'intera blockchain. Questo fa sì che la blockchain sia a prova di manomissione, offrendo l'elemento chiave dell'immutabilità. Questo elimina la possibilità di manomissioni da parte di malintenzionati e crea un registro di transazioni di cui tu e gli altri membri della rete potete fidarvi.

1.4 Vantaggi della Blockchain

Cosa deve cambiare: Le operazioni spesso sprecano risorse in registrazioni duplicate e convalide di terzi. I sistemi di conservazione dei record possono essere vulnerabili a frodi e attacchi informatici. La trasparenza limitata può rallentare la verifica dei dati. E con l'arrivo dell'IoT, i volumi delle transazioni sono esplosi. Tutto questo rallenta l'attività di business e incide negativamente sul risultato finanziario e significa che ci serve un modo migliore. Entra nel mondo della blockchain.

Maggiore fiducia: Con la blockchain, in qualità di membro di una rete di soli partecipanti, puoi confidare nel fatto che stai ricevendo dati accurati e tempestivi e che i tuoi record della blockchain confidenziali saranno condivisi solo con i membri della rete a cui hai specificamente concesso l'accesso.

Maggiore sicurezza: Il consenso sull'accuratezza dei dati è richiesto per tutti i membri della rete e tutte le transazioni convalidate sono immutabili perché vengono registrate in modo permanente. Nessuno, nemmeno un amministratore di sistema, può eliminare una transazione.

Più efficienze: Avendo un registro distribuito condiviso tra i membri di una rete, le riconciliazioni di record diventano inutili e possono essere eliminate. E per accelerare le transazioni, un set di regole, il cosiddetto contratto intelligente (o smart contract), può essere memorizzato sulla blockchain ed eseguito automaticamente.

Part II

Tecnologie Utilizzate

2

Tecnologie Utilizzate

CONTENTS

“nobreak

2.1 Ethereum

Ethereum è una tecnologia che ti permette di inviare criptovalute a chiunque, versando solo una piccola commissione. Inoltre sta alla base di applicazioni che chiunque può utilizzare e che nessuno può mandare in tilt.

È la blockchain mondiale programmabile.

Ethereum si basa sull'innovazione di Bitcoin, ma con grandi differenze.

Entrambe ti permettono di utilizzare moneta digitale senza ricorrere a intermediari o banche. Ma Ethereum è programmabile, quindi la puoi usare per molti tipi diversi di risorse digitali, anche per Bitcoin!

Questo significa anche che Ethereum non è solo pagamenti. È una piazza di servizi finanziari, giochi e app che non possono rubarti i dati e o censurarti.

2.1.1 Casi di Utilizzo

Ethereum ha portato alla creazione di nuovi prodotti e servizi in grado di migliorare diversi aspetti delle nostre vite. Siamo ancora nelle prime fasi, ma c'è molto di cui esser entusiasti.

Finanza decentralizzata (DeFi): Un sistema finanziario più aperto che offre maggiore controllo sul proprio denaro e apre nuove possibilità.

Token non fungibili (NFT): Un modo per rappresentare oggetti unici come gli asset Ethereum, che possono essere scambiati, utilizzati come prova di proprietà, e generare nuove opportunità per i creatori.

Organizzazioni autonome decentralizzate (DAO): Un nuovo modo per collaborare e creare comunità online con obiettivi comuni e risorse condivise.

2.2 Polygon

Tecnicamente Polygon (MATIC) non è altro che una criptovaluta P2P decentralizzata, basata su un sistema open source che pone in primo piano la sicurezza, la privacy e la velocità.

Grazie al sistema avanzato di crittografia, è possibile consentire le conversioni delle transazioni tra due parti escludendo un intermediario supplementare. Polygon si propone come una nuova e innovativa tecnologia di blockchain e criptovaluta capace di migliorare le falle presenti nelle criptovalute tradizionali, come la sicurezza, la velocità e la privacy delle transazioni appunto.

2.2.1 Storia e Origini

Le menti che hanno dato vita a questo progetto sono Sandeep Nailwal, Jaynti Kanani e Anurag Arjun, ingegneri informatici indiani che inizialmente chiamarono la loro creatura Matic Network. Polygon nasce con lo scopo di risolvere il problema della scalabilità di Ethereum, attraverso un incremento della velocità di transazione. Tale processo è possibile grazie all'utilizzo dell'algoritmo SHA-256 che viene a implementarsi nel processo di mining.

Il progetto MATIC venne lanciato sul mercato nel 2017, mentre quello Polygon ha visto la sua comparsa nella seconda metà del 2019.

2.2.2 Come Funziona

Affinché si possa comprendere il funzionamento della criptovaluta Polygon, è necessario iniziare da Ethereum Plasma. Con questo termine si identifica quella funzionalità capace di supportare soluzioni specifiche off-chain che garantiscono di aumentare le prestazioni complessive del network Ethereum. Tale condizione è dovuta alla creazione di una struttura ad albero composta a sua volta da differenti catene più piccole.

Preso atto di questo concetto, è possibile traslare il ragionamento verso il funzionamento di Polygon. Attraverso quest'ultimo strumento è quindi possibile integrare le diverse blockchain, dando modo a quella principale di verificare la correttezza delle transazioni in atto. Utilizzando questo sistema è

possibile gestire un numero elevatissimo di transazioni per blocco di criptovalute, teoricamente più di 65 mila; al momento un numero che pochissime blockchain riescono a supportare.

Il percorso delle transazioni avviene grazie all'algoritmo proof of stake, che mette a disposizione degli utenti una sezione dove condividere la propria rete e soprattutto i token, essenziali per rendere possibile il mantenimento del network e ottenerne una ricompensa.

Come è facile dedurre dalle tecnologie utilizzate, lo scopo principale di Polygon è quello di permettere a Ethereum di completare le transazioni in modo rapido, condizione in molti casi deficitaria sulle applicazioni decentralizzate. Sebbene al momento l'Ethereum sia una componente essenziale per Polygon, il progetto sta virando verso un'implementazione di soluzioni che possano inglobare più blockchain Bitcoin. Condizione che renderebbe oggettivamente interessante la posizione di Polygon agli occhi degli investitori.

I MATIC Coin, criptomoneta di Polygon, possono essere generati attraverso il mining oppure mettendo a disposizione i propri coin per ampliare la rete, ricavandone un guadagno dai processi di consenso proof of stake.

2.2.3 Il Progetto di Polygon

Non vi è alcun dubbio sul fatto che il legame con Ethereum sia una condizione di grande vantaggio per Polygon. ETH è ormai da anni una criptovaluta di interesse mondiale e le sue oscillazioni finanziarie danno sempre ottime prospettive. Benché tale condizione sia sotto gli occhi di tutti, il progetto può assumere una forma completamente nuova nel momento in cui vi è un'interazione supplementare con i Bitcoin o altre forme di criptovalute.

Fino a maggio del 2021, Polygon copriva un market cap di oltre 4.3 miliardi di dollari, fornendo circa 10 miliardi di token sottoforma di MATIC coin.

Tecnicamente, al momento, il valore di un singolo token è di 0.7 dollari, ma è interessante analizzare come nel 2020 il valore fosse solo di 0.003 dollari. Come è intuibile, l'incremento notevole è dovuto all'interesse, all'inizio del 2021, di Bitcoin che ha messo in chiaro il progetto portandolo a un aumento del 4200

Oltre a tali dinamiche di marketing, è interessante valutare quelle che sono le modalità con cui è possibile acquistare MATIC coin. Escludendo il sistema del mining, la criptovaluta Polygon può essere facilmente acquistata tramite piattaforme di exchange e broker online. Piattaforme rinomate come eToro consentono l'acquisto e la vendita di questa criptovaluta in modo facile e veloce.

Sicuramente il progetto sembra poggiarsi su solide basi e l'interesse di Bitcoin potrebbe dar vita a un ulteriore slancio.

Part III

Linguaggio di Programmazione - Solidity

3

Solidity Programming Language

CONTENTS

La programmazione Solidity è il linguaggio del codice per i contratti intelligenti basati su Ethereum e le applicazioni blockchain e viene eseguita sulla macchina virtuale di Ethereum.

Solidity è un linguaggio di programmazione del contratto intelligente nativo di Ethereum. È stata una parola d'ordine per un bel po 'di tempo grazie alla sua capacità di implementare contratti intelligenti su blockchain. La programmazione solidità affronta le soluzioni del mondo reale con un approccio semplicistico usando un linguaggio simile a C ++ e JavaScript.

Attualmente, la programmazione Solidità (Solidity) può generare contratti intelligenti per vari usi, tra cui aste non vedenti, votazioni, crowdfunding e portafogli multi-firma. Vediamo come funziona.

3.1 Cosa sono i contratti intelligenti?

Il termine contratto intelligente è stato introdotto per la prima volta nel 1994 e si riferisce alla registrazione di contratti sotto forma di codice informatico. Quando vengono soddisfatte le condizioni preimpostate, il contratto viene automaticamente attivato.

I contratti intelligenti consentono transazioni auto-eseguite, senza la necessità di intermediari come banche o altre istituzioni. 25 anni fa, l'idea era troppo lungimirante per essere messa in pratica in quanto non esisteva la tecnologia disponibile per supportare questo tipo di codice.

Grazie allo sviluppo della tecnologia blockchain, sono possibili contratti intelligenti su Ethereum e altri blockchain. Oltre alla sua criptovaluta ETH,

Ethereum è una piattaforma di sviluppo basata su blockchain che consente di creare su altre applicazioni basate su blockchain utilizzando contratti intelligenti.

3.2 Cosa implicano i contratti intelligenti?

Due parti (individui o organizzazioni) raggiungono un accordo utilizzando il codice del computer.

Con la programmazione Solidity, l'accordo viene eseguito sulla blockchain di Ethereum, il che significa che tutti i dettagli del contratto sono memorizzati su un libro mastro pubblico.

- Nessuna parte può modificare da sola i termini del contratto.
- Tutte le azioni risultanti dal contratto intelligente sono automatiche e avvengono senza intermediari.
- Tutte le transazioni sono registrate sulla blockchain e sono irreversibili.
- Quando le condizioni preimpostate non sono soddisfatte, le transazioni non si verificano.

I contratti intelligenti sono possibili grazie alla capacità della tecnologia blockchain di ricordare tutto e le parti non hanno problemi di fiducia. Le persone coinvolte non hanno nemmeno bisogno di fidarsi l'una dell'altra poiché i contratti vengono eseguiti solo quando i termini concordati sono rispettati.

3.3 Cos'è la programmazione Solidity?

Solidity è un linguaggio di codifica relativamente nuovo rilasciato con Ethereum nel 2015 ed è progettato per gli sviluppatori blockchain. La programmazione solidale consente agli sviluppatori di scrivere e implementare contratti intelligenti sulla blockchain di Ethereum, che è ancora la piattaforma più popolare per i contratti intelligenti.

È stato sviluppato da Gavin Wood, un co-fondatore ed ex CTO di Ethereum. Anche i programmatori di Ethereum, Alex Beregszaszi, Christian Reitwiessner, Liana Husikyan e Yoichi Hirai facevano parte della squadra.

Solidity viene eseguito su Ethereum Virtual Machine (EVM), che consente lo sviluppo di sistemi di contratto intelligenti.

Il linguaggio di codifica di Ethereum consente a un contratto di interagire

con altri contratti e di aggiornare i termini quando necessario. Poiché i contratti intelligenti sono auto-eseguibili, i programmatori dovrebbero prestare particolare attenzione ai dati che inseriscono nel codice. Qualsiasi errore o errore in un contratto intelligente può causare danni impensabili, come nel caso dell'hack DAO nel 2016.

La programmazione Solidity consente ai contratti di essere eseguiti letteralmente, quindi qualsiasi ambiguità può bloccare le transazioni. Con i contratti tradizionali, le parti possono lavorare insieme e raggiungere un accordo. Ma questo non accade su una blockchain dove le transazioni sono irreversibili.

La programmazione della solidità (Solidity) non è per principianti. Dovresti già avere familiarità con C ++, JavaScript o Python per scrivere contratti intelligenti e creare applicazioni blockchain su Ethereum.

3.4 I contratti intelligenti sono legalmente vincolanti?

Finché il contratto intelligente ha tutti gli elementi di rilegatura di un documento firmato contratto , allora sì, sono giuridicamente vincolante. Mentre non sostituiscono gli accordi contrattuali, i contratti intelligenti possono automatizzare parti di accordi tradizionali, soprattutto quando si tratta di pagamenti.

Ecco gli elementi vincolanti da considerare:

Un'offerta dovrebbe sostenere il contratto – una delle parti deve offrire beni o servizi all'altro. Entrambe le parti dovrebbero essere a conoscenza dei dettagli di questa offerta. Il contratto dovrebbe menzionare uno scambio di valore tra le parti, non necessariamente denaro. Entrambe le parti dovrebbero avere la competenza per stipulare un accordo legale. Inoltre, dovrebbero anche mostrare una chiara intenzione di creare una relazione legale.

3.5 A cosa servono i contratti intelligenti?

La programmazione della solidità (Solidity) non è stata creata per trasformare il futuro. I contratti intelligenti fanno parte del presente, con molte industrie che li implementano per una maggiore efficienza.

Le compagnie di assicurazione e persino i governi utilizzano contratti intelligenti per automatizzare i pagamenti e ridurre i costi. Sono anche utilizzati nella gestione aziendale, nell'industria sanitaria e nelle Ico .

Altri settori inizieranno sicuramente ad adottare contratti intelligenti in quanto riducono al minimo i rischi di frodi e truffe. Allo stesso tempo, l'utilizzo

di software per automatizzare i contratti può eliminare gli intermediari, ridurre i costi e accelerare le transazioni.

La programmazione Solidity è il linguaggio di codice principale attualmente utilizzato per l'implementazione di contratti intelligenti. Sviluppato sulla piattaforma Ethereum, Solidity consente ai programmatori di scrivere contratti intelligenti e dApp blockchain.

Questo linguaggio di programmazione non è semplice e gli sviluppatori devono prestare particolare attenzione a ciò che inseriscono nel contratto poiché i contratti intelligenti sono auto-eseguibili e qualsiasi errore potrebbe portare a transazioni errate.

3.6 Immutabilità del contratto intelligente

Un fatto interessante sugli smart contract è la loro natura immutabile. Ciò significa che una volta che il contratto è stato eseguito, non può essere annullato . Questa è una caratteristica fondamentale di un buon contratto intelligente per ottenere il risultato desiderato. Ad esempio, una volta pagato un appartamento, il proprietario non può restituirlo . Pensala in questo modo: i contratti intelligenti sono "un accordo tra le parti per fare qualcosa in futuro". È un modo automatizzato e trasparente per far rispettare un accordo. Si basa su una serie di regole e su un consenso concordato. Le regole e le condizioni sono codificate e archiviate in una blockchain. I contratti intelligenti sono parte integrante della rete Ethereum, dove sono diventati una pietra angolare dell'infrastruttura di fiducia su quella blockchain. Ethereum può essere considerata una piattaforma di valuta digitale, che presenta anche contratti intelligenti.

L'immutabilità è una caratteristica interessante per blockchain e contratti intelligenti perché impedisce la modifica della blockchain. Ad esempio, se vendi i biglietti per un concerto, potresti utilizzare un contratto intelligente che li vende a un prezzo particolare. Questo contratto è quindi collegato alla blockchain. Ciò significa che una volta che qualcuno acquista un biglietto, non può rivenderlo . Puoi anche utilizzare la blockchain per rilasciare e inviare automaticamente fondi al venditore una volta venduto un biglietto. Questo è uno degli effetti collaterali più noti della tecnologia blockchain.

Part IV

NFTs - Non-Fungible Tokens

4

Token Non-Fungibili

CONTENTS

Non-fungible token (NFT), certificati "di proprietà" su opere digitali: questi strumenti stanno avendo un ampio successo, è quindi interessante approfondire nel dettaglio le loro caratteristiche per capire cosa davvero "compra" chi acquista un NFT e cosa potrà poi fare con quel "token".

E questo approfondimento è doveroso sia dal punto di vista giuridico che tecnico e ci permette di comprendere le fragilità del sistema. Se andiamo ad esaminare nel dettaglio che cosa è un NFT e cosa viene effettivamente registrato su blockchain ci rendiamo conto che ben poco del "contratto" di acquisto è contenuto su questo registro distribuito e che tutti gli altri dati (l'opera stessa, le condizioni del suo acquisto e i diritti del "proprietario") sono in realtà al di fuori del registro, con severi problemi di conservazione e di accessibilità nel tempo del dato.

Ci accorgiamo inoltre del fatto che questi NFT non dipendono solo dalla tecnologia blockchain, ma anche da altre soluzioni (come il processo di hashing) che potrebbero essere superate nel tempo (il continuo aumento della potenza di calcolo potrebbe infatti permettere di "rompere" alcuni di questi algoritmi, rendendo così ben poco affidabile il riferimento univoco all'NFT).

Dal punto di vista giuridico ci accorgiamo che il valore (l'unicità) dell'NFT non poggia davvero sulla tecnologia blockchain, ma sulla fiducia intercorrente fra il venditore e l'acquirente, con il primo che confida sul fatto che il secondo non venderà o non abbia già venduto la stessa identica opera più e più volte, riducendo quell'NFT (pagato magari milioni di dollari) a un valore irrisorio (perché se non può esistere un NFT uguale all'altro, ne possono esistere un'infinità di estremamente simili e tutti rivolti a trasferire la "proprietà" della medesima opera).

4.1 Che cos'è davvero un NFT (non fungible token)

NFT è l'acronimo di non fungible token che in italiano significa gettone non copiabile ossia qualcosa di unico che non può essere sostituito da altro. Ad esempio una criptovaluta può essere scambiata con un'altra criptovaluta mentre un'opera d'arte è unica e quindi non fungible. Un NFT è un contenuto digitale che rappresenta oggetti del mondo reale come opere d'arte, musica, giochi e collezioni di qualsiasi tipo.

Chi acquista un'opera legata a un non-fungible token non acquista l'opera in sé, ma semplicemente la possibilità di dimostrare un diritto sull'opera, garantito tramite uno smart contract. Tutto comincia con una versione digitale dell'opera d'arte. Tipicamente, si usa una foto digitale o una sua documentazione filmata e salvata in formato digitale. Questa versione digitale non è altro che una lunga sequenza di numeri, 0 e 1 nel linguaggio informatico.

Tale sequenza viene quindi "compressa" in una sequenza, chiamata hash, derivata da essa ma molto più corta, con un processo non invertibile conosciuto come hashing. È importante sottolineare che chi possiede il documento digitale può facilmente calcolarne l'hash, mentre è praticamente impossibile per chiunque altro ricostruire un documento digitale a partire da un hash.

Il passo successivo è la memorizzazione di questo hash su una blockchain, con una marca temporale associata. L'uso di questi token ha aperto la strada a un mercato automatizzato di hash, in cui il creatore dell'hash può usare il token per aggiungere al suo interno il proprio hash e successivamente venderlo in cambio di un pagamento in criptovaluta, come per esempio la moneta ETH usata in Ethereum.

L'NFT tiene al suo interno traccia delle vendite dell'hash, in modo che risulta possibile tracciare i passaggi di mano dell'hash, fino al suo creatore, quindi dimostrandone il possesso. Questo meccanismo fornisce quindi una prova di autenticità e, al contempo, di proprietà dell'opera.

Il possessore dell'hash, secondo quanto riportato nell'NFT, può dimostrare i suoi diritti senza necessità di rivolgersi a intermediari e senza limiti di tempo (finché la blockchain su cui è ospitato il suo token continuerà ad essere attiva).

4.2 Cosa "contiene" un NFT?

Se andiamo quindi ad esaminare più da vicino che cosa "contiene" l'NFT ci accorgiamo però che i dati inseriti sono davvero pochi. Anche per una questione di energia impiegata e di spazio disponibile, non è infatti possibile inserire nella blockchain file di grandi dimensioni (che finirebbero per appesantire tutta la catena), ma solo pochi elementi (l'hash del file insieme ad alcune proprietà).

Quindi il proprietario dell'opera di Beeple battuta all'asta da Christie's

(pagata ben 69 milioni di dollari) ora possiede un certificato ospitato sulla blockchain di Ethereum che include un identificativo unico del "contratto" stipulato. Il certificato (non direttamente "scritto" nella blockchain ma ad essa collegato) conterrà (verosimilmente) alcune proprietà del token e l'hash che rimanda ad un file che contiene l'immagine realizzata da Beeple.

Alcuni di questi NFT contengono anche le condizioni contrattuali della compravendita, ma più spesso queste si trovano solo sul sito che la intermedia (con il rischio però che la compiuta disciplina dell'acquisto finisca persa al venir meno del sito web della piattaforma). Qui iniziano i primi problemi.

4.2.1 I fronti critici

Cosa succederà quando le funzioni di hash verranno superate? Come è capitato alla funzione SHA1, ingannata dalla stessa Google, potrebbe capitare alla funzione SHA256, che oggi costituisce lo standard? Cosa succederà se la blockchain di Ethereum dovesse essere abbandonata (e quindi non più mantenuta da una collettività di soggetti che possono efficacemente "mettere in minoranza" chiunque dovesse provare a far passare per buona una blockchain in realtà non genuina)? Cosa succederà quando i contenuti esterni a cui rimandano i link/hash contenuti nello smart contract verranno meno? Per affrontare alcuni dei problemi appena esposti sono state proposte interessanti soluzioni tecniche.

4.2.2 Le soluzioni tecniche

Ad esempio, per evitare di lasciare ad un hash/indirizzo url la rappresentazione dell'opera venduta, spesso gli NFT fanno uso degli indirizzi IPFS (InterPlanetary File System). Un semplice url potrebbe infatti venir meno semplicemente perché il gestore del sito smette di pagare l'hosting o perché magari elimina il file per far spazio a nuovi contenuti. E un hash potrebbe non servire più a nulla nel momento in cui il file cui fa riferimento viene smarrito.

Gli indirizzi IPFS invece sono "link" rivolti a un contenuto sulla rete IPFS (un file system distribuito, che potremmo associare, nel suo funzionamento, ai sistemi di scambio file peer to peer). Finché qualcuno sulla rete IPFS ospita quel contenuto è possibile trovarlo. Si crea quindi una potenziale moltitudine di host che garantisce il mantenimento del file online e questo aumenta le probabilità che il contenuto sopravviva nel tempo. Quanto alle diverse blockchain su cui è ospitato l'NFT, è evidente che le stesse dovranno iniziare a fornire qualche "garanzia" di sopravvivenza se vorranno conquistare fette di mercato.

Se la blockchain di Ethereum ha verosimilmente un futuro assicurato anche per gli anni a venire visto che la stessa muove una criptovaluta popolare e un sistema di smart contract utilizzato per numerosi fini diversi, è evidente che le altre blockchain concorrenti dovranno invece offrire rassicurazioni di diverso tipo per "garantire" la loro sopravvivenza.

Con il fiorire del fenomeno degli NFT, inoltre, gli investitori dovranno

prestare massima attenzione alla blockchain su cui sono ospitati gli smart-contract, per evitare di acquistare certificati fondati su blockchain improvvisate, scarsamente decentralizzate e conseguentemente inaffidabili e che potrebbero essere in seguito abbandonate.

4.3 Quali sono i diritti del titolare di un NFT?

Quando un soggetto acquista un NFT l'unica cosa che può affermare con (relativa) certezza, è di possedere un NFT, un non-fungible token che rimanda a "qualcosa" (un'opera d'arte, un tweet, un bel canestro di Le Bron James). Definire i diritti su quel "qualcosa" a cui rimanda l'NFT diventa complicato. Dal punto di vista giuridico, infatti, non tutti gli NFT sono uguali. La già menzionata piattaforma CryptoKitties ad esempio è specializzata nella vendita di "tweet" su blockchain Ethereum (ed ha negoziato la vendita del primo tweet di Jack Dorsey per quasi tre milioni di dollari).

Sul proprio sito Valuables precisa che l'acquisto non garantisce al proprietario alcun diritto sul "tweet" venduto: si tratta solo della cessione di tweet "autografati" dall'autore (identificato attraverso il suo profilo twitter e il suo portafogli Ethereum). L'autore, nel vendere il tweet, si impegna a non venderlo più di una volta su Valuables così da non creare una proliferazione di copie autografate.

È evidente quindi che il tweet in sé e per sé è vendibile più e più volte (esattamente come è possibile "autografare" diverse copie stampate del tweet stesso) ed è solo un impegno giuridico a "limitarne" la proliferazione. Se l'autore del tweet dovesse decidere di vendere due volte lo stesso tweet su Valuables evidentemente si potrebbe agire contro Valuables e l'autore del tweet, mentre risulterebbe ben difficile agire contro Jack Dorsey se questo dovesse decidere di (ri)vendere il suo primo tweet su un'altra piattaforma concorrente rispetto a Valuables (salvo sussistano accordi interni fra lui e Valuables, nel caso però sarebbe unicamente quest'ultima a poter agire) o in altre forme.

Ma anche gli NFT che trasferiscono la "proprietà" di un'opera, in realtà il più delle volte trasferiscono la proprietà su quella copia dell'opera, senza impedire la libera proliferazione della stessa sul web.

Se con un NFT si acquistassero ulteriori diritti sull'opera (es. con una cessione di diritti d'autore come quello di pubblicazione, riproduzione o di elaborazione dell'opera), questi sarebbero regolati da un contratto esterno alla blockchain (o al più datacertato su blockchain) che magari al suo interno potrebbe far riferimento alla cessione dell'NFT, ma torneremmo comunque a parlare di un contratto "ordinario" nelle forme e nelle tutele.

Ciò significa che gli impegni dell'autore "accertati" nella blockchain sono unicamente quelli di cedere l'opera Se Beeple un domani dovesse rivendere la sua opera "EVERYDAYS: THE FIRST 5000 DAYS", variando un semplice

pixel e così cambiandone l'hash, sarebbe legittimato a farlo e i rimedi per impedirglielo sarebbero solo contrattuali (è quindi imprescindibile un contratto in cui sia precisato che quello che è stato venduto non è "l'NFT contenente quella copia informatica" di "EVERYDAYS: THE FIRST 5000 DAYS", bensì l'opera stessa) e non tecnologici.

La tecnologia blockchain ci consente di dire solamente che l'acquisto battuto in asta da Christie's per 69 milioni di dollari costituisce la prima cessione dell'opera, non altro (e nemmeno con assoluta certezza, Beeple potrebbe aver già ceduto l'opera mille volte mesi prima, generando ogni volta hash diversi al variare di qualche minimo pixel).

Ancora, se Beeple un domani dovesse invece decidere di creare una serie di 5000 variazioni sul tema della sua opera "Everydays: the first 5.000 days", sarebbe senz'altro legittimato a farlo, salvo il suo contratto con la casa d'aste Christie's o quello con l'acquirente escludano questo diritto esplicitamente. Quel che è indiscutibile, quindi, è che il mercato dell'arte sui NFT non è mosso da un sistema tecnologico inaggirabile, ma è mosso, ancora una volta e come è stato per migliaia di anni, dalla fiducia corrente fra autore e compratore.

4.4 Lo scenario Futuro

Gli NFT sono una deriva artistica che ha scosso il mondo dell'arte, che ha dato per un lato finalmente dignità ad una forma creativa svilita dalla sua riproducibilità infinita, ma dall'altro lato ha creato occasione per bolle speculative e incursioni di prodotti artistici non esattamente degni di questo nome.

È verosimile che questa forma d'arte sia qui per rimanere e che le prime reazioni denigratorie (che da secoli accompagnano le evoluzioni del mondo dell'arte che precorrono i tempi) siano destinate ad essere sconfessate. È importante però che gli appassionati affrontino questo mercato con le dovute conoscenze, anche tecniche e giuridiche, per essere in grado di separare il grano dalla crusca.

Part V

Smart Contracts - Contatti Digitali Intelligenti

5

Cosa sono i contratti intelligenti

CONTENTS

Dai rimborsi assicurativi alle transazioni finanziarie, dalle operazioni societarie alla tracciabilità delle merci e alla tutela della proprietà intellettuale. Il campo d'azione degli smart contract è potenzialmente esteso, ma ha confini ben visibili. E sottolinearlo serve a tener lontana qualsiasi tentazione di eleggere questi strumenti a sostituti tout court delle forme contrattuali tradizionali. Anche se - è indubbio - aprono nuovi spazi professionali.

È l'espressione "smart contract", però, che può esser fuorviante. Perché, anche rispetto alle differenze dei vari sistemi normativi, in alcuni casi non è possibile parlare di "contratti" in senso strettamente giuridico, ma di funzioni "if/then" incorporate in software o protocolli informatici. Del tipo: se c'è una scadenza, allora parte il pagamento, spiega Andrea Reghelin, associate partner di P4I, società di advisory del gruppo Digital360. In altre parole, tramite gli smart contract – continua Reghelin – può anche avvenire una trasposizione "informatica" di accordi che si concludono al di fuori dalla piattaforma tecnologica.

5.1 Come Funziona uno Smart Contract?

"nobreak

5.2 La spinta della blockchain

La piattaforma tecnologica, oggi, è la blockchain . Perché il concetto di smart contract esiste già da tempo (teorizzato dall'informatico Nick Szabo negli anni 90), ma proprio nella "catena dei blocchi" ha trovato un approdo ideale, che ne esalta le qualità: tra automatismi, trasparenza e sicurezza. Un esempio attuale? Ingegneri e avvocati citano subito le polizze assicurative di tipo parametrico, basate cioè sul verificarsi (o meno) di determinate condizioni. Pensiamo ad Etherisc - risponde il direttore dell'Osservatorio blockchain del Politecnico di Milano, Francesco Bruschi -. È un'assicurazione sui viaggi aerei decentralizzata, che opera sulla piattaforma Ethereum. Lo smart contract interroga delle Api (interfacce per la programmazione di applicazioni, ndr) per avere informazioni sugli orari di partenza e, in caso di ritardo del volo garantito dalla polizza, fa scattare automaticamente il rimborso. Per far questo, in teoria, basterebbe anche un "semplice" programma informatico. Sì, ma con uno script che gira su blockchain è il sistema stesso a garantire il funzionamento trasparente e verificabile e i soldi investiti, dice Bruschi, secondo cui oggi tutti intendono lo smart contract come programma su Ethereum, che è una forma di blockchain pubblica e aperta, permissionless, e dopo Bitcoin è quella a maggior capitalizzazione. Il motivo è semplice: la sicurezza delle transazioni aumenta al grado di diffusione della piattaforma. L'accento torna dunque sulle caratteristiche della "catena dei blocchi": distribuita, disintermediata (meglio, diversamente intermediata), certificata e immodificabile. Ma anche sugli incentivi economici: infatti i contratti di Ethereum, gestibili peer-to-pee r, da persona a persona, "pagano" l'uso della sua potenza computazionale tramite un'unità di conto, la criptovaluta ether.

5.2.1 I campi di applicazione

In ambito assicurativo - racconta l'avvocato Salvatore Iannitti, partner di Norton Rose Fulbright - si è mossa anche Axa, prima grande compagnia a consentire rimborsi automatici su carta di credito per i ritardi dei voli aerei, grazie alla polizza Fizzy già attiva in Italia, acquistabile via web e basata su blockchain (anche qui Ethereum, ndr). E un altro esempio è nella logistica, dove il colosso Maersk, con società assicurative come Ms Amlin e Axa Xl, ha avviato una piattaforma che sfrutta la blockchain per certificare le movimentazioni delle merci tra i vari porti.

Lo studio Norton Rose Fulbright, che ha collaborato a questi progetti, sta ora sviluppando dei prototipi di smart contract per la liquidazione degli indennizzi nelle operazioni MA. Accorciare i tempi per ottenere le somme depositate in garanzia, attraverso un "escrow agreement" automatizzato, può favorire - osserva Iannitti - soprattutto le transazioni delle medie imprese.

5.3 I confini applicativi

Resta il fatto che gli smart contract incontrano inevitabili limiti tecnico-giuridici. Eche la loro applicazione è profittevole solo quando è semplice tradurre le clausole contrattuali in linguaggio informatico:se c'è un ritardo del volo, scatta il rimborso; se c'è una scadenza, parte il pagamento. La complessità, insomma, non è gestibile (si veda l'articolo in basso).

Anzi, la tendenziale immodificabilità della blockchain può ritorcersi contro: che cosa accade se c'è una traduzione errata, se il codice è sbagliato? Gli adempimenti seguono l'errore - sentenzia Giulio Novellini, counsel di Portolano Cavallo -. Ecco perchéconcepisco piuttosto un'evoluzione dei computer contract.Partire da un documento cartaceo che è solo parzialmente demandato a smart contract su Ethereum e già prevede una funzione "kill" che annulla l'azione in caso di errore.

Lo studio legale Lca, invece, ha lanciato un servizio di archiviazione documentale per la tutela della proprietà intellettuale, che utilizza la blockchain. E intende allargare il raggio d'azione del servizio agli ambiti dell'MA, della crisi d'impresa e del food.

Se i documenti complessi non possono essere certo demandati completamente a uno smart contract – rimarca Gianluca De Cristofaro, capo del dipartimento Ip di Lca –, lo smart contract può ben essere usato per una specifica clausola di un deal più composito. Innovando ancora il ruolo dell'avvocato e le professionalità richieste.