UNIVERSITÀ DEGLI STUDI DI UDINE

Corso di Laurea in Scienze e Tecnologie Multimediali

Bitcoin e il mercato delle criptovalute

Relatore:
Claudio Piciarelli

Laureando:
Gianluca Ruffino

ANNO ACCADEMICO 2020/2021

Abstract

In this thesis we will talk about cryptocurrencies, with particular attention paid to Bitcoin, the first cryptocurrency to be launched on the market.

All the main points will be touched: history, price, pollution, with particular interest for the technical part of both, Bitcoin and Ethereum (second currency by capitalization).

The thesis first discusses the basic concepts of Bitcoin, and then focuses on advanced aspects that can be found in a more complex project such as Ethereum.

Bitcoin and Ethereum currently are the most relevant examples of cryptocurrencies, their development led to some of the most important innovations in the field of blockchain systems.

The potential of this technology is enormous: in the future it could completely disrupt the use of the internet, making it truly "free".

Indice

CAPITOLO 1

BITCOIN

1.0 Cos’è

Bitcoin è la prima criptovaluta mondiale ad essere stata sviluppata[6]. Viene creata nel 2009 da un anonimo (o gruppo anonimo) noto con lo pseudonimo di Satoshi Nakamoto. Questo nome di derivazione giapponese è composto dalle parole pensiero chiaro, veloce e saggio (satoshi), dentro, relazione (naka), origine o fondamento (moto). Il bitcoin è una moneta virtuale, a differenza delle valute tradizionali, non ha un governo o un ente centrale che si occupa della moneta ma è un complesso sistema autonomo. Attraverso una rete peer-to-peer permette di scambiare denaro online tra due enti senza dover passare tramite un’istituzione finanziaria.

Questo è possibile grazie ai principi della crittografia che permettono di generare monete e farle circolare, senza la presenza di un'autorità che ne convalidi le transazioni.

1.1 Quando e perché nasce

Satoshi Nakamoto pubblicò il protocollo Bitcoin su The Cryptography Mailing nel novembre del 2008. Nel 2009 viene distribuita la prima versione del software client. Bitcoin nasce come innovativo metodo di scambio valore. È la prima moneta completamente digitale, studiata e creata per questo scopo.

1.2 Differenze fiat e DeFi

Le monete fiat (ovvero le monete che vengono utilizzate al giorno d'oggi come dollaro o euro) si differenziano dalle precedenti monete-merci perché non basano più il loro valore sul materiale da cui sono create (come oro e argento) ma su scelta arbitraria da parte del governo o della banca centrale che emette la moneta in questione[7].

Con il termine DeFi (DEcentralized FInance) intendiamo tutto l'ecosistema di servizi finanziari che puntano a ridurre o eliminare gli intermediari nelle operazioni attraverso l'utilizzo di reti informatiche decentralizzate[8].

La finanza classica si affida sulla fiducia di un intermediario (banche e stati) che assicura le transazioni tra due figure. Grazie a Bitcoin finalmente questo sistema di pagamento elettronico viene basato su prova crittografica e non più sulla fiducia. Oltre a questo, le monete fiat circolanti al momento hanno il grosso problema di essere ancorate solamente al valore deciso dallo stato o banca a cui appartengono, che soffre di numerose problematiche.

1.3 1971: USD-Oro

Il 15 agosto del 1971 il presidente americano Richard Nixon fece uno dei cambiamenti più cruciali per la storia dell'economia. Da quel giorno si mise fine alla convertibilità del dollaro in oro, il sistema aureo, in vigore fino a quel momento tramite gli accordi di Bretton Woods del 1944, alla fine del secondo dopoguerra[9].

Il dollaro era l'unica valuta che poteva essere convertita in oro (35 dollari l'oncia) e per questo era utilizzata come riferimento per gli scambi.

Per poter essere prodotta cartamoneta totalmente convertibile in oro doveva essere presente la stessa quantità di oro all'interno della banca centrale.

Per la guerra del Vietnam (1964-75), all'interno del contesto della guerra fredda, gli americani spesero ben oltre 132 miliardi di dollari, spesa che spinse fortemente sulla decisione da parte di Nixon[10].

Oltre a questo, i cittadini iniziavano a pensare che il dollaro fosse sopravvalutato e cominciarono a convertire ingenti somme di dollari in cambio d'oro, cosa che aumentava ulteriormente le speculazioni.

Da questo momento è cominciata l'inflazione costante del dollaro.

Con inflazione, in ambito economico, si indica una crescita generalizzata e continuativa dei prezzi nel tempo[11].

Il poter stampare monete da parte di banche e stati senza nessuna limitazione ha portato una lenta diminuzione del valore del dollaro, con la conseguenza che tutti i prodotti di consumo hanno dovuto aumentare i prezzi per compensare. Gli stipendi medi sono aumentati, ma non proporzionalmente al costo medio della vita, specialmente per determinati prodotti, come in ambito immobiliare.

Nel 1971 una nuova casa costava $25.200 e il reddito medio era di $10.622 all'anno[12] mentre oggi una casa ha raggiunto i $408.800 mentre il reddito medio è di $31.133[13].

Dopo questi 50 anni abbiamo una chiara visione su quanto questa riforma sia poco sostenibile ed abbia seri problemi nel lungo periodo.
Per cercare di sopperire al problema delle fiat currency nasce per l'appunto Bitcoin, che permette di avere una moneta slegata da qualsiasi stato e banca centrale.

1.4 Il valore di bitcoin determinato dal mercato

Al momento viene utilizzato principalmente il dollaro per avere un'idea sul valore di bitcoin (moneta di riferimento per quasi qualsiasi cosa essendo la più importante). Non essendo una moneta classica e non avendo nessuno stato o banca alle proprie spalle, bitcoin non ha un vero e proprio prezzo. Questo, infatti, viene esclusivamente determinato dalla domanda e offerta del mercato. Un utente può decidere autonomamente il prezzo di vendita della propria quantità di bitcoin, se dall'altra parte ci sarà un'acquirente disposto a pagare quel determinato prezzo la transazione andrà in porto. In questa ottica è più corretto vedere il bitcoin più come merce di scambio/baratto rispetto ad una vera e propria moneta[3][4]. Il primo prezzo di bitcoin risale al 22 maggio 2010, quando l'utente Laszlo ha acquistato due pizze da Jeremy Sturdivant in cambio di 10.000btc, con un tasso di cambio di 1btc: 0.003$[14].

Jeremy ha dovuto attendere ben quattro giorni per ricevere le pizze, però come avrebbe detto in seguito lo stesso Jercobs "Dai una pizza a un uomo, mangerà per un giorno; fagli comprare la pizza con bitcoin, rivoluzionerà l'economia."

Dopo aver trovato un utente disposto a spedire le pizze si sono accordati tramite una chat IRC.

Questa fu la prima volta che venne utilizzato per l'acquisto di un bene.

Essendo stato un evento rivoluzionario da quel momento il 22 maggio è diventato ufficialmente il Bitcoin Pizza Day, una ricorrenza annuale nella quale si festeggia questo enorme traguardo raggiunto da Bitcoin[15].

Oggigiorno il valore di un singolo Bitcoin si aggira attorno ai 50/60.000$, questo fa facilmente intuire quanto possano aver guadagnato i primi visionari di questa incredibile tecnologia e del perché sempre più persone ed enti si approcciano a questo mondo.

CAPITOLO 2

COME FUNZIONA

2.0 Utilizzo: seed, private/public keys, wallets

All’atto pratico per utilizzare Bitcoin ci basterà avere un'applicazione client che comunicherà direttamente con il protocollo. Queste applicazioni vengono chiamate “wallets” perché hanno la stessa funzione di un portafoglio fisico, ovvero di poterci inserire e rimuovere certi quantitativi di moneta. Esistono moltissimi tipi di wallet, principalmente suddivisi nelle varie piattaforme utilizzate[2].

Desktop wallet: la prima tipologia creata. Esistono per tutti i principali sistemi operativi, quindi Windows, Linux e Mac OS. Hanno molte funzionalità ma spesso risultano poco sicuri e poco configurabili.

Mobile wallet: il tipo di wallets più utilizzato. Sia per Apple iOS e Android, molto semplici e facili da usare, specialmente per i nuovi utenti.

Web wallet: categoria sempre per dispositivi desktop ma con uso molto più semplice e intuitivo. Attraverso il nostro web browser possiamo facilmente accedere al nostro wallet che permette un utilizzo pratico e veloce per le transazioni. Per fare ciò i nostri dati devono essere trasmessi ad un server di terze parti che li custodirà, abbassando drasticamente la sicurezza.

Hardware wallet: dispositivi hardware che si interfacciano solitamente attraverso porte usb o nfc. Con questa soluzione possiamo mantenere il seed del nostro wallet offline, una delle soluzioni più sicure per detenere i nostri bitcoin.

Il nostro portafoglio di bitcoin è formato principalmente da due chiavi: chiave privata e chiave pubblica.

La chiave privata è una stringa lunga 256-bit, che solitamente viene convertita in 64 cifre esadecimali per essere più semplice da utilizzare[16].

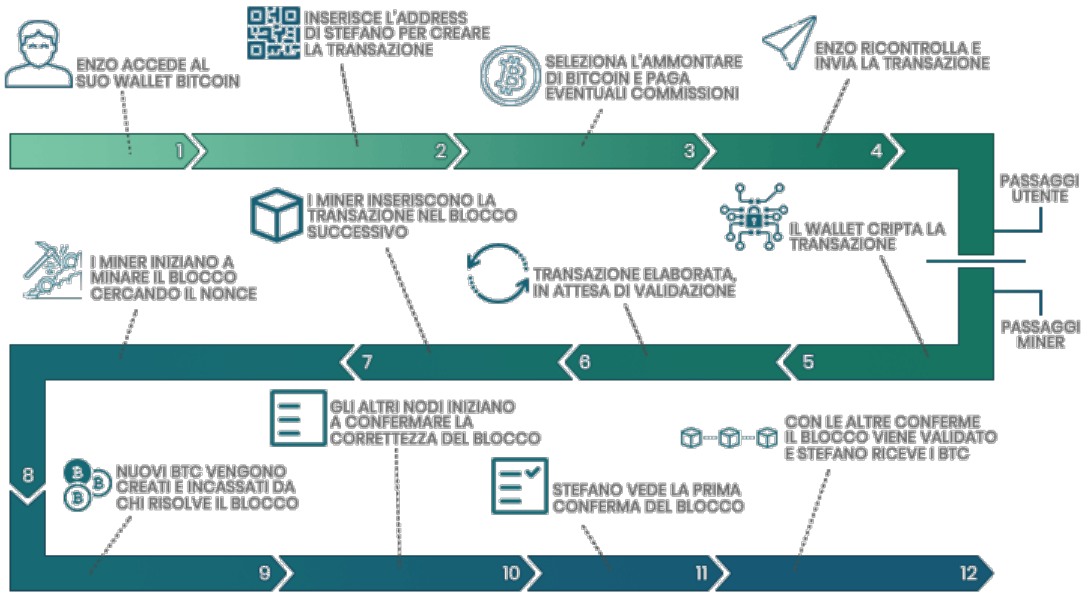
Un esempio di chiave privata in forma esadecimale: 6Ld9slfmvE34Snt3mNto7mNNfitR3Dfe81SdmFeGR39KFLeMfkEw.

Questa chiave privata per essere ancor meglio appresa a livello umano viene ulteriormente convertita nella frase mnemonica, il seed[17].

Il seed, infatti, è una frase composta da 12-24 parole in inglese. Queste parole hanno un loro numero associato da 1 a 2048. Prendendo ogni numero relativo alle parole contenute nel nostro seed e convertendo questi numeri in binario otterremo esattamente la nostra chiave privata (private key).

Questo è il codice più importante del portafoglio, permette di avere il completo accesso al backup del wallet: perso questo codice non ci sarà alcuna possibilità di poter accedere nuovamente al portafoglio, essendo gli unici proprietari, senza terze parti che potranno aiutarci.

Il momento più rischioso di una operazione su rete Bitcoin avviene prima del raggiungimento del primo nodo da cui partirà la transazione.



[18]

Prima che la transazione sia criptata ed inserita nel sistema al punto 5, i dati passano sia nel pc sia attraverso internet.

Questo rende la fase iniziale la meno sicura, visto che non dipende dalla rete Bitcoin vera e propria ma fa affidamento ai sistemi classici.

Il collegamento ad Internet, l'ip ed il seed facilmente accessibile sono le cose a cui prestare più attenzione. È buona norma, per chi possiede grossi quantitativi di criptomonete, utilizzare un hardware wallet, avere un proprio full-node (per ridurre ulteriormente "il tragitto" della nostra transazione) e salvare la propria frase mnemonica su due fogli cartacei da tenere in due sedi separate (in modo che un possibile attacco hacker non abbia accesso a queste informazioni essendo non digitalizzate).

La maggior parte delle perdite di wallets, infatti, è causata da errori umani da parte dei proprietari.

La chiave pubblica viene anche lei generata direttamente dalla chiave privata mediante crittografia basata su curve ellittiche secondo l'algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm)[19].

Questo processo crittografico è unidirezionale, di conseguenza dalla chiave pubblica non si potrà ottenere la chiave privata. Questo sistema viene chiamato crittografia asimmetrica.

L'algoritmo ECDSA è uno dei più complessi algoritmi di crittografia per le chiavi pubbliche. Fa le stesse cose di un qualsiasi altro sistema di firma digitale ma in maniera più efficiente.

Da questa seconda chiave potrà essere ottenuto l'indirizzo Bitcoin vero e proprio che potrà essere utilizzato per ricevere bitcoin[20].

Questo processo è completamente automatizzato ma è comunque utile a livello informativo sapere il suo meccanismo:

- la chiave pubblica viene sottoposta ad una doppia funzione di hash, prima SHA256 e poi RIPEMD160 (con quest'ultimo oltre a crittografare ulteriormente verrà prodotta una stringa di 160bit, quindi più leggera);
- viene aggiunto il prefisso 0x00;
- viene calcolato il checksum (questo servirà a garantire che l'indirizzo sarà digitato completo e preciso);
- viene codificato in Base58.

Finite queste operazioni l'indirizzo bitcoin sarà composto solitamente da 26-34 caratteri.

Esistono diverse tipologie di indirizzi, facilmente riconoscibili osservando l'indirizzo generato:

- Indirizzi che iniziano con 1: Legacy (P2PKH), la prima versione e la più compatibile. Le transazioni sono le più pesanti e perciò richiedono più fee per essere confermate.
- Indirizzi che iniziano con 3: SegWit[21] (P2SH), utilizza un diverso script al posto del doppio hash che permette di ridurre i costi fee del 26% rispetto al Legacy.
- Indirizzi che iniziano con bc1p: Native SegWit (P2WPKH), con questo nuovo indirizzo si riesce ulteriormente a ridurre la quantità di informazioni da spedire, riducendo le fee del 38% rispetto al Legacy.

- Indirizzi che iniziano con bc1p: Taproot (P2TR), nuova tipologia ancora non disponibile. Il nuovo soft-fork è stato approvato nel novembre 2021. Il peso delle transazioni aumenta leggermente rispetto a Native SegWit ma ottimizza le transazioni complesse, per cui le fee saranno ulteriormente più economiche[22].

Questo indirizzo potrà essere condiviso in maniera pubblica per ricevere bitcoin, mentre la chiave privata ci permetterà di gestire l'intero wallet.

Oltre all'indirizzo in maniera testuale sarà presente anche un qr code associato, che agevolerà di molto le transazioni tramite dispositivi mobili.

Per ottenere bitcoin ci sono diversi sistemi:

- scambiare valuta (EUR/USD) tramite un exchange dedicato;
- comprarli attraverso amici o privati tramite denaro fisico;
- attraverso un ATM Bitcoin;
- offrendo le proprie prestazioni o i propri prodotti ad accettando pagamenti in bitcoin;
- chiedere al proprio datore di lavoro o clienti di essere pagati in bitcoin[2].

2.1 Blockchain

La blockchain è il motore sulla quale si basa l'intero progetto Bitcoin. Tramite questa catena di blocchi è possibile scambiare ed ottenere bitcoin. Questa tecnologia, non solo applicabile a bitcoin, sta rivoluzionando Internet permettendo di avere sicurezza su un sistema distribuito senza necessitare di una figura esterna che abbia l'intero controllo su quell'azione o transazione, rendendo il tutto più democratico.

Le tecnologie Blockchain sono incluse nel settore di Distribuited Ledger (DTL), ovvero sistemi basati su un registro distribuito, in cui tutti i nodi di una rete possiedono la medesima copia dello stesso database, che può essere letto e modificato in modo indipendente dai singoli nodi.

Le principali caratteristiche che permettono di ottenere questa tecnologia sono 7:

1.Digitalizzazione e trasformazione dei dati in formato digitale;

2.Decentralizzazione, essendo le informazioni distribuite a più nodi aumenterà la sicurezza;

3. Tracciabilità dei trasferimenti, ogni elemento sul registro è tracciabile e si può risalire all'esatta provenienza in qualsiasi momento;

4.Disintermediazione, assenza di intermediari, ovvero enti centrali fidati che gestiscono le transazioni;

5.Trasparenza e Verificabilità, i registri e il loro contenuto sono facilmente verificabili e consultabili da chiunque;

6.Immutabilità del Registro, i dati una volta scritti all'interno del registro non possono essere modificati senza il consenso della rete;

7. Programmabilità dei trasferimenti, possibilità di programmare azioni da effettuare al verificarsi di determinate condizioni[23].

Come funziona la blockchain e perché è così sicura?

All’interno di un singolo blocco ci saranno queste informazioni più i dettagli delle varie transazioni.

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block’s transactions
4 bytes	Timestamp	The approximate creation time of this block (in seconds elapsed since Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

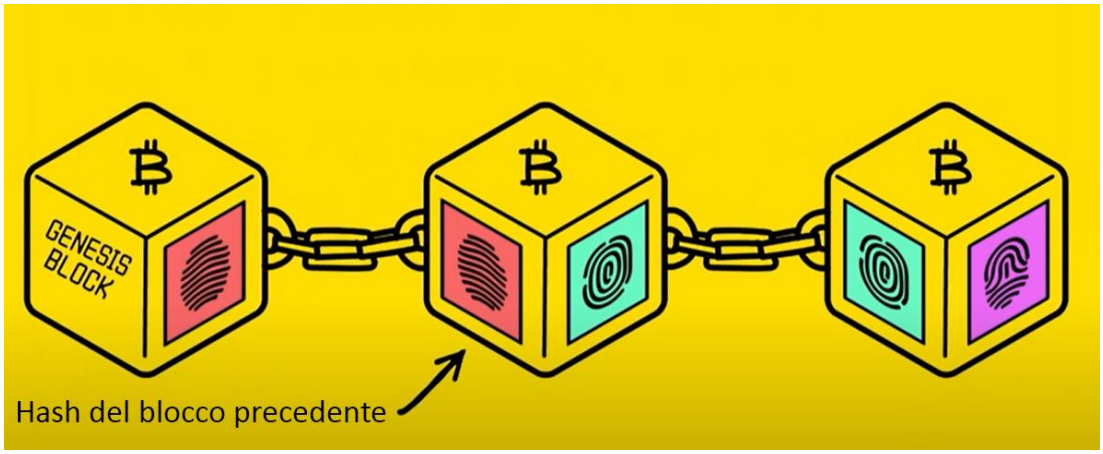
[24][2]

Ogni blocco, in base alle informazioni contenute all’interno, tramite l’algoritmo SHA-256, genera un hash lungo 256 bit (in esadecimale 64 caratteri), che svolge il ruolo di impronta digitale di tale blocco.

Questa funzione di hash ha due caratteristiche principali:

- ottenere da una stringa di lunghezza casuale una stringa di lunghezza definita;
- essere una funzione irreversibile, dal risultato ottenuto non si potrà risalire alla stringa di partenza.

All’interno di un blocco si trova anche l’hash relativo al blocco precedente, dando vita ad una vera e propria catena di blocchi. Il primo blocco non potendo avere un hash precedente viene definito “genesis block”.



[25]

Questa catena viene distribuita a tutti i full nodes della blockchain, che assicureranno il corretto funzionamento di tale sistema. Un blocco per essere accettato deve essere approvato dal 50%+1 dei nodi, che in un sistema distribuito in ampia scala come nel caso di Bitcoin, rende pressoché impossibile modificarne il contenuto in maniera fraudolenta.

Per aumentare ulteriormente la sicurezza un blocco contiene anche un campo chiamato “Nonce”, il quale è un numero utilizzato per ottenere un hash che inizi con una serie di zeri.

Al momento per essere valido un hash necessita di ben 19 zeri iniziali.

Guardando la tabella sottostante possiamo farci un'idea della mole di tentativi necessari per trovare un valore nonce che sia valido per il nostro hash.

digits	nonce	time estimate
4	500,000	15 minutes
5	8,000,000	4 hours
6	128,000,000	3 days
7	2,048,000,000	a month
8	32,768,000,000	2 years
9	524,288,000,000	30 years
10	8,388,608,000,000	481 years
11	134,217,728,000,000	7,690 years
12	2,147,483,648,000,000	123,036 years
13	34,359,738,368,000,000	1,968,581 years
14	549,755,813,888,000,000	31,497,291 years
15	8,796,093,022,208,000,000	503,956,662 years

[2]

Questo calcolo molto pesante è alla base dell'algoritmo della Proof-of-Work, che approfondiremo successivamente. Il primo che riesce a trovare il valore nonce valido per quel blocco ha diritto di ricevere una ricompensa aggiuntiva e tutte le fee delle transazioni associate a quel blocco. Chi si occupa di questi calcoli viene definito miner.

Un nuovo blocco viene confermato ogni dieci minuti. Se un hacker provasse ad attaccare un blocco precedente dovrebbe ricalcolare il nonce di tutti i blocchi successivi, rendendola una pratica inefficace.

Sempre all'interno del blocco troveremo i due indirizzi pubblici (ricevente e destinatario) e la quantità di bitcoin da spostare. Ci sono più transazioni per ogni singolo blocco.

All'inizio esisteva un singolo software che fungeva sia da nodo sia da wallet, che serviva anche per minare Bitcoin. Nel corso del tempo queste tre strade si sono separate per adattarsi al meglio ai bisogni di ogni utente. Un full-node ad oggi pesa oltre i 400gb e sarebbe poco pratico per l'utente che vuole solamente detenere bitcoin all'interno di un wallet o per chi vuole minare. I full-node (oltre 10.000 pubblici ad oggi) rimangono comunque fondamentali per mantenere la decentralizzazione e la sicurezza della rete.

2.2 Transazioni

Con il termine transazione (per abbreviare si può usare TX) indichiamo una spedizione o un trasferimento di un valore tra due parti[26].

Gli elementi di cui si compone sono:

1. Entrate (input), che servono a confermare l'origine degli asset che verranno utilizzati in una transazione, contengono l'indirizzo dove sono stati originariamente ricevuti i bitcoin.
2. Uscite (output), indirizzo a cui viene effettuato il bonifico e l'importo inviato. Una transazione può contenere più output.
3. Identificatore (TXid) l'hash indicativo del blocco all'interno della blockchain utilizzato per la transazione.
4. Tasso di commissione (fee), piccolo pagamento che i miners ricevono per l'elaborazione della transazione. Più si paga e più priorità si avrà, quindi la transazione sarà più veloce.

All'atto pratico basterà essere in possesso dell'indirizzo a cui vogliamo spedire una certa somma di bitcoin per poter avviare la transazione. In alternativa si può generare un link con una cifra prestabilita da inviare a chi dovrà inviare i fondi verso il nostro indirizzo Bitcoin.

Anche se le fee sono sempre state molto più economiche rispetto ad una qualsiasi altra transazione attraverso il sistema finanziario tradizionale, con il grosso afflusso di gente degli ultimi anni sono salite drasticamente.

Un nuovo blocco della blockchain richiede sempre circa 10 minuti per essere generato e confermato, la grandezza del blocco è rimasta quasi invariata 1-4 mb ma le transazioni sono aumentate esponenzialmente. Se uniamo questo al sistema prioritario relativo a chi paga più fees basterà poco a capire del perché i costi stanno aumentando a dismisura[4].

Ancora non si è trovata una soluzione a questo problema di scalabilità.

2.3 Peer-to-peer

Nelle telecomunicazioni il termine peer-to-peer (P2P) indica un modello di architettura logica di rete informatica in cui i nodi di tale rete non sono gerarchizzati sotto forma di client o server fissi ma ogni nodo è capace di fungere al contempo sia da client sia da server verso gli altri nodi[27].

Nel caso di Bitcoin abbiamo un P2P puro, ovvero non c'è un server centrale e tutti i nodi della rete hanno lo stesso ruolo. Distribuendo la blockchain ad ogni nodo si otterrà un sistema decentralizzato e molto sicuro visto che non basterà attaccare un singolo server.

Questa tecnologia non viene solamente utilizzata in ambito criptomonete, ma ha molti applicativi all'interno del panorama digitale.

Oltre ai vantaggi sopra citati c'è anche uno svantaggio, un enorme consumo energetico.

Considerando i 10.000 full-node pubblici, con oltre 400gb di dati scaricati, che devono rimanere costantemente alimentati e connessi ad internet possiamo farci un'idea di quanto dispendioso sia questo sistema.

2.4 Proof of Work e Mining

Come già citato, con il termine Proof of Work (PoW), si intende l'algoritmo di consenso alla base della rete Blockchain.

Una volta trovata la nonce del nuovo blocco ed essere stata approvata dai nodi della rete, questo nuovo blocco verrà aggiunto alla catena della Blockchain.

Per incentivare questo calcolo da parte degli utenti, chi per primo trova la soluzione del blocco, riceve delle ricompense[28]. Nel caso di Bitcoin è presente un halving, evento programmato che riduce la ricompensa destinata ai miners per l'estrazione di nuovi blocchi, che dimezza la quantità di ricompense ogni circa quattro anni[29]. Questi eventi importanti riducono il numero di moneta "prodotta" ed è uno dei motivi che ne sta facendo aumentare il prezzo. Con questo sistema sosteniamo il prezzo della cripto che altrimenti rischierebbe di diminuire nel tempo. Il prossimo halving avverrà attorno a maggio 2024. Una volta raggiunto il limite di 21 milioni di bitcoin non sarà più possibile produrne ulteriormente[30].

Questa produzione durerà ancora molto vista la presenza di halving, si stima che l'ultimo bitcoin non sarà disponibile prima del 2140.

Inizialmente il minare era fatto da chiunque utilizzasse il software di Bitcoin sul proprio pc tramite processore CPU (la prima reward del primo blocco di Bitcoin è stata di ben 50.00000000btc[31]), blocco dopo blocco il calcolo è diventato sempre più complesso, rendendo necessario il passaggio ad hardware dedicato. Con più potenza di calcolo si ha più possibilità di trovare la soluzione prima rispetto alla concorrenza, ottenendo così le ricompense. Per aumentare tale potenza di calcolo ben presto si passò ad utilizzare le schede grafiche (GPU), molto più performanti, con una velocità maggiore di 50/100 volte rispetto alle classiche CPU.

Nel 2011 arrivarono le schede FPGA (Field-Programmable Gate Array), dedicate esclusivamente sull'estrazione di Bitcoin. Ridussero il consumo di energia e

aumentarono le velocità di calcolo, rendendo economicamente possibile la nascita di aziende specializzate in mining.

Le più recenti sono le schede ASIC (Application Specific Integrated Circuit) che hanno ulteriormente aumentato la velocità e ridotto il consumo energetico. A livello industriale viene utilizzata esclusivamente questa tipologia di schede.

Per minare, questi sistemi dovranno calcolare ininterrottamente al massimo delle loro prestazioni per essere efficienti, rendendo i consumi elettrici veramente elevati. Per questo le mining farm più grandi e importanti (aziende con il solo scopo di produrre criptomonete) vengono collocate in paesi e zone rurali che hanno dei costi di elettricità contenuti.

Anche se le schede ASIC sono più performanti rispetto alle GPU sono più ricercate queste ultime[32].

Ci sono diversi motivi per cui ciò avviene:

- Le GPU sono utili anche in altri ambiti, come per i videogiochi;
- Le GPU hanno una rivendibilità nel mercato superiore alle ASIC;
- Le GPU hanno una garanzia tipicamente di 3 anni, rispetto ai 3 mesi di una scheda ASIC;
- Le GPU possono essere utilizzate anche per altre monete digitali e non solo per Bitcoin (infatti vengono usate quasi esclusivamente per altre cripto);
-Sono più economiche, silenziose e permettono aggiornamenti di memoria e chip.

Per aumentare maggiormente la potenza di calcolo e permettere anche a chi ha hardware meno performante di partecipare al mining, nel novembre del 2010, l'utente Slush ha creato il primo mining pool[33]. Una pool è l'unione di più sistemi di mining di diversi utenti a distanza per avere maggiori chance di ottenere le ricompense, che verranno suddivise tra tutti i partecipanti. Oggi giorno quasi la totalità dei minatori fa parte di una pool.

Questa funzionalità era già presente nel client base di Bitcoin, chiamata getwork. Con il tempo è stata perfezionata rendendola molto più funzionale.

Per poter unire la potenza di calcolo in una pool è necessario un server che elabori tutti i calcoli dei singoli utenti, ottenendo di fatto un sistema centralizzato in una tecnologia decentralizzata. Questo è motivo di critiche da parte di molti ma permette di essere profittevoli anche a chi non ha la potenza di calcolo necessaria ad elaborare il nonce in maniera autonoma. Se una singola pool dovesse superare il controllo di oltre il 51% del network complessivo attraverso quel server si potrebbero creare blocchi falsi da immettere nella blockchain diventando un serio problema a livello di sicurezza[1][34].

2.5 Sicurezza e Trasparenza

La rete decentralizzata (anche se formata quasi esclusivamente da poche grandi pool) è molto più difficile da essere attaccata rispetto ad un singolo server. Come trattato in precedenza, abbiamo già avuto modo di capire a livello tecnico quanto sia sicura una struttura simile.

Per quanto riguarda la trasparenza di Bitcoin anch'essa è molto elevata. La possibilità di consultare da tutti il registro della blockchain che al proprio interno contiene tutte le transazioni avvenute dal suo lancio nel 2009 è un suo vero punto di forza.

Se però a livello tecnico sono così "solidi" non si può dire lo stesso della sua volatilità di prezzo[4].

Oltre a questo, si aggiunge il non essere ben vista da molte nazioni e sistemi basati su moneta fiat, che possono limitarne o addirittura vietarne l'utilizzo all'interno del proprio paese. Alcuni stati già hanno attuato politiche restrittive come in Bolivia, Egitto, Marocco e Cina[35].

2.6 Anonimato

Molte persone credono erroneamente che Bitcoin sia una piattaforma completamente anonima. Questo è solamente in parte vero: Bitcoin permette di avere uno pseudo-anonimato[36]. Come abbiamo visto il registro di tutte le transazioni è sempre consultabile; perciò, in ogni momento sarà possibile risalire all'esatta cifra presente in ogni wallet. L'unico vero lato anonimo è l'associare un determinato wallet al proprio proprietario. Se qualcuno è in possesso di questa informazione è in grado di sapere sia il nostro quantitativo di bitcoin sia tutte le nostre operazioni con quel determinato wallet[37]. Con un po' di attenzione però non è difficile mantenere i propri wallet (una persona può detenere più di un singolo wallet) in completo anonimato.

La criminalità e le attività illecite hanno visto fin da subito un certo potenziale in questa tecnologia. Riciclaggio di denaro tramite ATM, vendita di qualsiasi materiale ritenuto illegale e riscatti digitali (principalmente ransomware[38]) sono i più presenti in questo mercato.

Questo però rimane una piccola fetta rispetto al quadro generale. Anche lo stesso internet ha al proprio interno un settore di attività criminali, definito Dark Web. Nessuna piattaforma è completamente libera da attività simili, bisogna attribuire ad ogni informazione il giusto peso. Sia internet sia Bitcoin hanno portato e continuano a portare decisamente più vantaggi positivi rispetto a quelli negativi.

2.7 Soft Fork e Hard Fork

Come un qualsiasi altro software Bitcoin viene continuamente aggiornato, correggendo bug, ottimizzando gli algoritmi, semplificando il codice e aggiungendo funzionalità. Essendo un progetto decentralizzato ed opensource ogni persona ha la possibilità di suggerire modifiche al software anche se per mantenere Bitcoin sicuro è un processo molto lento.

Per fare ciò una volta organizzate le idee ed aver creato un aggiornamento valido si dovrà fare una pull request sulla pagina di gitHub dedicata[39]. Una volta che sarà stata approvata riceverà un numero indicativo e sarà inserita nella lista di bips (Bitcoin Improvment Proposals[40]). Qui verrà ulteriormente delineata e definita la struttura di tale upgrade e nel caso fosse valida passerà all'ultimo stadio di approvazione da parte dei miners. Infatti, dopo esser stato completamente approvato dalla community e dagli sviluppatori dovrà essere implementato in un numero sufficiente di blocchi minati per modificare il codice a tutti gli effetti.

Esistono principalmente due categorie di bip: soft fork e hard fork[41].

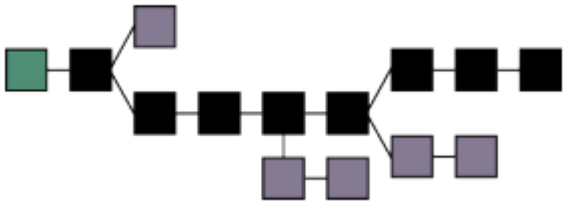
I soft fork si differenziano per essere retroattivi e perciò potranno funzionare tranquillamente sulla stessa rete anche se non tutti i nodi non presentano questa versione del software. Ad esempio, un possibile soft-fork potrebbe essere la riduzione di un blocco da 1mb ad 800kb: in questo caso non ci sarà alcun problema ad inviare 800kb verso un nodo ancora non aggiornato.

I più importanti soft fork sono SegWit che permette di aumentare la dimensione di un singolo blocco separando script e transazioni e il recentissimo Taproot[42].

Mentre gli hard fork non sono retrocompatibili e perciò necessitano di una completa nuova blockchain dedicata[43]. In questa maniera verranno create due monete separate che avranno entrambe un loro proseguimento nelle corrispettive blockchain. Con la stessa chiave privata avremo la possibilità di accedere ad

entrambe le blockchain, ottenendo lo stesso quantitativo di cripto moneta. Ovviamente sarà necessario utilizzare due diversi wallet.

Gli hard fork di Bitcoin avvenuti nel corso del tempo sono diversi: Bitcoin Cash, Bitcoin SV, eCash e Bitcoin Gold.



In questo esempio vediamo differenti hard fork (quelli grigi) che vengono creati in maniera parallela rispetto alla linea blockchain ritenuta principale (ovvero quella nera)[5].

CAPITOLO 3

ETHEREUM E ALTCOIN

3.0 Panoramica altcoin

Successivamente a Bitcoin sono state sviluppate centinaia di altre criptovalute. Queste vengono chiamate Altcoin[44]. La differenza principale tra Altcoin e Bitcoin è che solitamente tutte le criptovalute subiscono le stesse oscillazioni di prezzo, definite dall'andamento di Bitcoin.

Bitcoin è la più storica e quella che ancora oggi rimane la più utilizzata, avendo una dominance del 40% (da sola vale ⅔ dell'intero mercato cripto)[45].

Essendo Bitcoin un primo esperimento in questo panorama soffre di molti problemi, che non sempre possono essere corretti tramite un semplice soft fork, molte altcoin nascono con l'intento di migliorare le lacune della cripto più famosa. Ad oggi però nessuna moneta è ancora riuscita ad essere più efficace di bitcoin. Ci sono però monete dall'importante rilevanza, che nel corso del tempo si sono ritagliate la propria parte di mercato.

Spesso a livello speculativo trader e semplici interessati preferiscono optare per operazioni su cripto molto meno conosciute, che permettono guadagni decisamente più interessanti.

Però non tutti sono interessati al lato speculativo e preferirebbero un valore più stabile delle monete, come per le monete fiat che utilizziamo normalmente.
Vista l'alta volatilità generale delle cripto è nato un filone chiamato “stablecoin” che cerca di ridurre al minimo la volatilità[46].
Esistono tre tipologie principali di stablecoin:
- stablecoin con collaterale in valuta fiat: in proporzione 1 a 1 sarà depositata la stessa quantità di moneta a corso legale (o di bene, come l’oro). Sebbene questo metodo sia solido, necessita di una centralizzazione ed è un sistema molto costoso.
- stablecoin con collaterale in altre criptovalute: in questo caso potrà rimanere un sistema decentralizzato, però per mantenere il prezzo stabile si dovrà sovra-garantire con il collaterale. Ad esempio, potrà essere in proporzione 1 a 2, in modo che se anche il prezzo del collaterale scende del 50% il prezzo potrà rimanere invariato. Nel caso di un cigno nero (evento finanziario imprevedibile) della cripto usata come collaterale anche la stablecoin collasserebbe, rischiando addirittura di amplificare le perdite. Per questa ragione è un approccio fortemente sconsigliato da parte degli esperti.
- stablecoin non collaterizzate: queste monete non hanno garanzie ma si basano esclusivamente sulla fiducia. Il prezzo rimarrà stabile solo se sufficienti persone manterranno alta la convinzione di quel prezzo, creando pressione al rialzo e al ribasso sul prezzo.
Non c’è una tipologia migliore di stablecoin, tutte hanno pregi e difetti facilmente intuibili.

3.1 Ethereum

La seconda cripto per ordine d'importanza è Ether, con il suo 20% di dominance[47]. Ether è la cripto che viene utilizzata all'interno della piattaforma digitale Ethereum (spesso si utilizza questo termine erroneamente per riferirsi solo alla moneta).

Questa piattaforma fu creata da Vitalik Buterin nel 2015, che al tempo aveva solamente 19 anni. Vedendo le potenzialità della blockchain con le transazioni decise di estendere l'utilizzo di un sistema decentralizzato anche a delle intere applicazioni[48]. Da qui nascono le dApp, decentralized application, ovvero tutte le applicazioni che non hanno un server principale ma sono decentralizzate come la rete Bitcoin[49].

Ad oggi ci sono più di 3000 dApp presenti sulla blockchain di Ethereum.

Tra queste applicazioni sono presenti le DeFi dApp, che puntano ad avere le stesse funzionalità di un servizio bancario classico. Si potranno guadagnare interessi, convertire le proprie criptomonete, ottenere dei prestiti in maniera automatizzata e decentralizzata. L'ecosistema di Ethereum però non si ferma solo a questo.

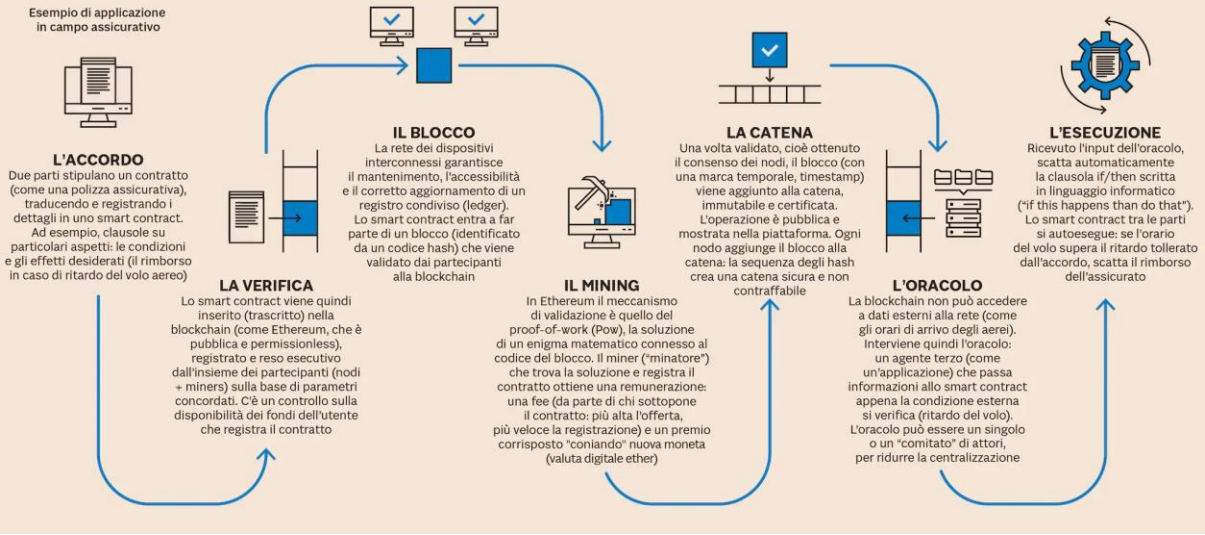
3.2 Smart Contracts

Ethereum è la blockchain di riferimento per la creazione di smart contract[50]. Tramite questi contratti scambiabili nella blockchain, oltre al trasferimento di valore come su Bitcoin, avremo molte più operazioni possibili: finanziarie, registrazione domini, sistemi elettorali, crowdfunding e molto altro. Questi software basati sulle funzioni if/then automatizzano il pagamento al verificarsi di una determinata condizione, senza necessitare di un terzo che faccia da garante[51].

Le due parti interessate stipulano un contratto, poi trascrivono le clausole all'interno di uno smart contract. Lo smart contract verrà inserito nella blockchain dopo essere stato approvato tramite Proof of Work. La responsabilità di monitorare che le condizioni del contratto si verifichino viene affidata ad un agente terzo, solitamente un'applicazione (uno smart contract non può ottenere da solo informazioni sugli eventi reali, per aggirare questa condizione verranno utilizzati gli oracoli). Quando l'app invierà il segnale dell'avvenuta condizione o più verrà avviata automaticamente l'esecuzione dello smart contract.

Questo sistema, alla stessa maniera di quello Bitcoin, permette di eliminare le figure intermediarie, riducendo i costi e aumentando la sicurezza. Un contratto simile ha notevole accuratezza in più, diminuiscono gli errori e i difetti che possono avvenire da parte di persone umane.

L'utilizzo di uno smart contract però nutre anche di certe criticità: un sistema così automatizzato e chiuso diventa freddo e rigido in qualsiasi occasione, se pensiamo ad un mutuo e al mancato pagamento di una rata, l'utente rischierà di perdere tutta la caparra senza potersi giustificare o trovando compromessi. Per questo motivo difficilmente gli smart contracts sostituiranno completamente figure di notai, avvocati ed altri intermediari.



[52]

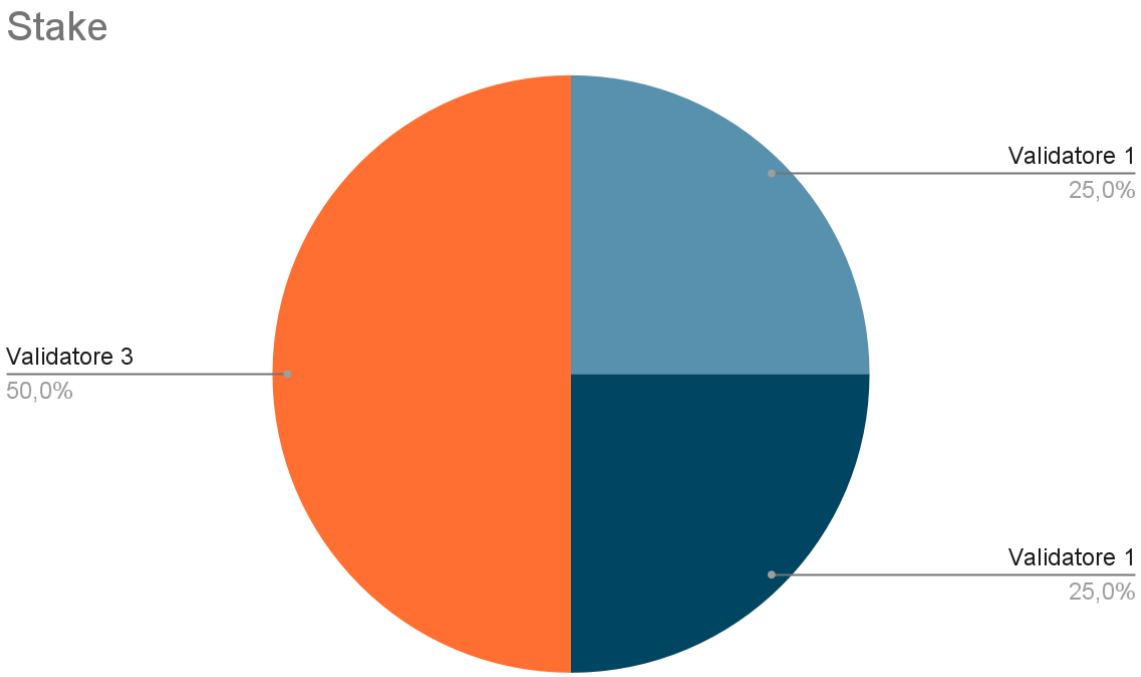
I linguaggi di programmazione degli smart contract su rete Ethereum sono Solidity e Vyper (alternativamente si può usare anche Yul/Yul +)[53].

Javascript e Python aiuteranno a capire le differenze dei linguaggi utilizzati; perciò, sono un buon punto di partenza per approcciarsi al mondo degli smart contract.

3.3 Proof of Stake

Al momento la rete Ethereum sta ancora utilizzando la Proof of Work. Questo sistema a livello elettrico e hardware è un vero problema, non permette una decentralizzazione capillare e al tempo stesso consuma enormi quantità di energia solo per dei calcoli non fondamentali. Per questo motivo Ethereum sta lavorando per spostare la produzione di nuovi blocchi da calcolo hardware a staking di Ether. Con questo metodo basterà essere un validatore per poter creare il successivo blocco della blockchain. Questo verrà selezionato in maniera casuale in base alla quantità di criptomoneta depositata per questo scopo.

Ogni volta che sarà generato un nuovo blocco verrà selezionato casualmente uno dei vari validatori con Ether in staking. Questo sarà designato come creatore del nuovo blocco, ottenendo così la ricompensa della creazione del nuovo blocco e le fee delle transazioni all'interno di questo blocco.



Prendiamo questo grafico d'esempio. Se ci fossero solamente questi 3 validatori ogni blocco verrebbe assegnato ad uno dei 3 partecipanti. Il validatore 3, avendo depositato il doppio quantitativo di Ether ha il doppio di possibilità essere selezionato come creatore del blocco rispetto agli altri due validatori.

Nella proof of stake chi mette in staking più Ether ha maggiori probabilità di essere selezionato. Nel caso ci fosse qualche operazione fraudolenta da parte del creatore del nuovo blocco questo perderebbe l'intera cifra in staking, decisamente maggiore rispetto ai possibili guadagni. Questo aumenta notevolmente sicurezza e serietà da parte dei validatori in staking. Anche in questo caso probabilmente si opterà per la creazione di grandi pool dove anche i più piccoli potranno trarne profitto.

Questo nuovo metodo fa parte di una serie di cambiamenti che avverranno su rete Ethereum che porteranno alla nuova versione di questa piattaforma chiamata Ethereum 2.

Il primo aggiornamento chiamato Beacon Chain (definito anche fase 0 all'interno della road map) è avvenuto il 1° dicembre 2020.

Questo Beacon Chain, fino al successivo aggiornamento, che avverrà circa nella prima metà del 2022, non apporta modifiche alla rete principale, ma getta le basi di stake e shard (altro punto importante per la scalabilità di Eth 2). Al momento è possibile depositare stake di Eth per ottenere una percentuale d' interessi. Con la successiva fase 1 avverrà il vero e proprio passaggio alla stake of proof.

Il completo passaggio ad Ethereum 2 ci sarà con la fase 3, che dovrebbe arrivare nel corso del 2023.

3.4 NFT e Gaming

Ethereum oltre alle dApp incentrate su strumenti finanziari ha ampliato gli orizzonti anche in altri settori. Tra questi spicca sicuramente il fenomeno degli NFT.

Questa sigla significa Not Fungible Token, token non fungibile, ovvero token che non può essere scambiato con un altro bene o un altro asset di pari valore[54].

Un lotto di terra è molto simile come concetto, visto che ha proprietà uniche e perciò definibile non fungibile.

Un'opera d'arte è un altro bene dal valore altamente soggettivo. A quest'ultimo esempio gli NFT sono molto legati.

Un NFT indica la proprietà esclusiva di un particolare asset digitale, che può spaziare tra immagini, video e musica.

Comprando un NFT non si diventa il proprietario dell'opera, ma si ha la possibilità di rivendicare un diritto sull'opera, entrando nella lista degli acquirenti nella blockchain.

Nascono nel 2014 ma solo ultimamente hanno avuto ricevuto tutte queste attenzioni.

Molti progetti principali, come per esempio i CryptoPunks[55], hanno raggiunto cifre da capogiro (al momento il totale del valore scambiato in questa collezione è di $1.89B). Molti artisti e aziende del settore moda hanno cavalcato questa moda per vendere opere create da loro.

Ad aumentare verticalmente il prezzo di tutto il mercato NFT hanno aiutato anche le fee di Ethereum molto alte: se un utente A acquista un opera spenderà una fee, che successivamente verrà inglobata nel prezzo dell'NFT nel caso venisse rivenduta ad un utente B in modo da non chiudere in perdita. Questo è il motivo per il quale anche i progetti di poco rilievo raggiungono velocemente cifre che superano i due zeri. Oltre a questo, siamo in un periodo di speculazione estrema in questo mercato, per cui la maggior parte degli acquirenti acquistano NFT solamente per poterli

rivendere a prezzo superiore senza essere realmente interessati al detenere tali asset.

Visto il grande successo degli NFT anche il mondo gaming si sta interessando alla cosa. Ad oggi già esistono molteplici giochi play-to-earn che utilizzano questi elementi. Tra i progetti più di rilievo ci sono: The Sandbox, Axie Infinity e Star Atlas.

3.5 Gas fee

Il Gas è l'unità di misura utilizzata per calcolare qualsiasi transazione o smart contract all'interno di Ethereum. A differenza di Bitcoin nel quale sono presenti solamente transazioni semplici, sulla blockchain di Ethereum abbiamo anche veri e propri programmi, che possono essere molto complessi. Avendo quindi più possibili soluzioni, di diversa grandezza, da inserire nella blockchain, si utilizzerà questa unità di misura per avere un'idea delle commissioni da pagare.

Solitamente viene espresso in Gwei (o nanoether), che è equiparabile ad un miliardesimo di Ether.

Per una singola transazione il Gas Limit è di 21000 Gas, per uno smart contract solitamente siamo intorno ai 130.000/140.000 Gas[56].

Un singolo blocco della blockchain non può superare gli 8 milioni di Gas.

Solitamente troviamo tre diversi valori di Gas:

- FAST: transazione rapida, più costosa ma con più priorità, in modo da essere eseguita in minor tempo;
- STANDARD: transazione normale, eseguita in un tempo medio;
- SAFE LOW: transazione al minor prezzo possibile, che però assicura che la transazione abbia successo (almeno il 5% dell'hash power della rete deve accettare tale prezzo).

Per calcolare le fee basterà utilizzare la semplice formula Numero di Gas Unit * Gas Price.

Per cui, prendendo in considerazione le attuali Gas Fee[57], per una semplice transazione avremo:

- Fast: 21000*125Gwei = 21000 * 0.000000125 = 0.002625 Eth (6.92$)
- STANDARD: 21000*92Gwei = 21000*0.000000092 = 0.001932 Eth (5.09$)
- SAFE LOW: 21000*86Gwei = 21000*0.000000086 = 0.001806 Eth (4.76$)

Viene utilizzato il termine “Gas” perché il funzionamento è simile a quello della benzina: una volta scelto il benzinaio con il suo prezzo, pagheremo in base alla quantità di carburante inserito nella nostra vettura.

In maniera ancora più accentuata rispetto a Bitcoin, le commissioni di Ethereum sono tra le più costose del mercato cripto. Più informazioni complesse da dover inserire all’interno della blockchain hanno portato ulteriori problemi di scalabilità del sistema.

Fortunatamente è già in programma una soluzione per tale problema, tramite shard chain, che suddividono il carico su molteplici blockchain differenti.

Queste però verranno implementate solamente nell’ultimo aggiornamento prima di raggiungere effettivamente Ethereum 2, che verrà rilasciato nel corso del 2023.

CAPITOLO 4

IMPATTO MEDIATICO E SUL MONDO

4.0 Elon Musk

Elon Musk è una delle figure più influenti degli ultimi anni. La seconda persona più ricca al mondo ha sempre dimostrato grandi capacità imprenditoriali e sempre con una visione ambiziosa del futuro[58].

Il suo metodo, spesso giudicato troppo eccessivo, lo ha sempre ripagato.

Cofondatore di X.com nel 1999, che successivamente diventerà la famosissima PayPal, fondatore di Tesla Motors nel 2003 rivoluzionando il concetto di auto elettrica e fondatore di SpaceX nel 2002, con l'obiettivo di portare gli esseri umani su Marte. Oltre a questi enormi progetti è sempre alla ricerca di altri settori da poter innovare, come lo sviluppo di un treno supersonico e nella realizzazione della batteria agli ioni più potente al mondo.

Da molti viene considerato un visionario, visti gli enormi risultati ottenuti nel corso della sua carriera.

Elon è anche una persona molto attiva nel mondo social, specialmente su Twitter, dove ha ben 70 milioni di followers.

Con questi enormi successi alle spalle nutre di molta attenzione da parte del pubblico, anche se spesso si diverte a scherzare o semplicemente a mandare meme, un suo Twitter è in grado di fare movimenti del mercato anche piuttosto drastici.

Un esempio sono i tweet di febbraio/marzo 2021, nei quali annuncia di aver investito 1.5 miliardi di dollari in Bitcoin e la possibilità di acquistare le automobili Tesla in Bitcoin.

Questi due semplici tweet sono riusciti a far alzare il prezzo di Bitcoin del 10%.

Nel mese di maggio Elon sempre, tramite Twitter, sospende l'acquisto di Tesla in Bitcoin, visto che la maggior parte dell'energia utilizzata dal mining proviene da combustibili fossili.

Questo fa precipitare nuovamente il prezzo di Bitcoin.

Dal grafico possiamo vedere esattamente il movimento di prezzo di BTC in seguito alle affermazioni di Elon.

I tweet non riguardano esclusivamente le criptovalute, come il consiglio di utilizzare l'app di messaggistica Signal al posto del suo competitor più famoso WhatsApp.

4.1 Dogecoin

Il modus operandi di Elon da sempre molto ironico e scherzoso unito al suo grande interesse per il panorama cripto lo hanno portato ben presto a diventare un grande sostenitore della moneta Dogecoin.

Questa criptovaluta, infatti, nasce per scherzo durante il 2013, da Jackson Palmer e Billy Markus[59]. Il suo nome deriva dal famoso meme "Doge", che rappresenta molteplici versioni del cane giapponese Shiba Inu.

È un hard fork di Luckycoin, fork di Litecoin, che a sua volta è un fork di Bitcoin.

Le differenze rispetto a Bitcoin sono:

- non ha un limite di produzione, per cui è una cripto inflazionistica;
- necessita di una minore potenza di calcolo per essere minata, utilizzando l'algoritmo mining script in alternativa al SHA-256;
- ogni nuovo blocco viene generato in 1 minuto, rispetto ai circa 10minuti di Bitcoin;
- le ricompense per i miners, nei primi 600.000 blocchi, erano un numero generato casualmente, successivamente diventarono 10.000 dogecoin a blocco[60];
- nessuno sviluppatore che continua a lavorare al progetto.

Nel 2014 il prezzo di Dogecoin iniziava a non essere più sufficientemente allettante per i miners, che diventarono sempre meno. Preoccupati di un possibile attacco al 51%, venne abilitato il merge mining, ovvero un sistema che permette di ricevere ulteriore "lavoro" da parte di altri miner di altre blockchain con lo stesso algoritmo (in questo caso su script, in particolare da litecoin).

Tutte queste caratteristiche a livello tecnico rendono la moneta destinata a perdere completamente il proprio valore nel corso del tempo.

Questo però solamente a livello teorico. Con l'appoggio di Elon Musk e di un'enorme community (come per i meme anche questa moneta nutre di grandi attenzioni da parte del web) il valore ad oggi di questo mercato è superiore ai 20 miliardi di dollari.

La FOMO (fear of missing out, paura di essere tagliati fuori) generata da tutta la visibilità a questa criptomoneta sta facendo aumentare la richiesta a dismisura e di conseguenza il valore.

Negli ultimi tempi non è difficile trovare persone che sono a conoscenza di Dogecoin ma non di Bitcoin, l'impatto mediatico gioca un ruolo fondamentale, come in qualsiasi altro settore, motivo per il quale il marketing ha così tanto rilievo.

4.2 Tesla, diversificazione finanziaria e asset sulle cripto

Dopo l'investimento di 1.5 miliardi di dollari da parte di Tesla in Bitcoin molte aziende e investitori istituzionali hanno cominciato, a loro volta, a considerare BTC come una valida opzione in cui poter investire.

Bitcoin insieme alle altre altcoin, rimangono un mercato molto volatile con drastici cambiamenti di prezzo, che però in ottica di diversificazione finanziaria si può rivelare una alternativa molto interessante agli asset classici.

Con il termine diversificazione finanziaria si fa riferimento alla pratica di ripartire il proprio capitale in più azioni, obbligazioni, liquidità o immobili.

Ad esempio, investendo il 10% del totale in Bitcoin, nel caso ci fosse un completo crollo si perderà solamente quel 10% presente in quel determinato asset. Questo riduce i guadagni possibili, ma riduce anche notevolmente il margine di rischio. Detenere esclusivamente denaro fiat, come visto, porta ad una lenta diminuzione del capitale, senza escludere la completa dipendenza da tale valuta: se la fiat in questione dovesse perdere tutto il valore, si perderà l'intero capitale.

Aziende e istituzionali, con i loro massicci investimenti nelle criptovalute, stanno facendo aumentare la domanda/offerta, innalzando il valore di questo mercato. Una maggiore adozione di Bitcoin rende questo mercato sempre più stabile.

4.3 Inquinamento

La produzione di Bitcoin di per sé non è inquinante, il vero problema è il Proof of Work. Ci sono numerose mining farm che operano calcoli in modo costante. A livello energetico, nel 2021, BTC ha consumato circa 95TWh, equivalente al consumo delle Filippine[61]. Il consumo elettrico non è un problema per l'ambiente, però il consumo mondiale è così elevato da non poter rinunciare alla produzione di elettricità tramite carbone e altri combustibili fossili. La produzione di energia utilizzando il carbone è ancora superiore all'80% a livello mondiale. Anche se si spinge molto sull'abbandono completo del carbone entro il 2050 nei prossimi anni, quest'anno e probabilmente nei prossimi ci sarà un incremento della produzione[62]. Oltre ai molteplici problemi di salute derivanti dall'inalazione delle sostanze prodotte da queste centrali[63], bisogna considerare anche che sono la maggiore causa di produzione di CO2. Queste emissioni di anidride carbonica sono la causa principale del surriscaldamento globale.

Secondo le Nazioni Unite entro il 2030 la temperatura globale salirà di 2,7 gradi, con conseguenze disastrose[64]. Per evitare questa catastrofe hanno calcolato che il mondo dovrà dimezzare le emissioni per riuscire a mantenere le temperature al di sotto dei fatidici 1,5 gradi. Anche se tutti sono consci dei pericoli che stiamo correndo, a livello politico ed economico, difficilmente ci sono prese di posizioni in difesa dell'ambiente, specialmente dalle nazioni più importanti e che producono più inquinamento.

Oltre all'enorme consumo energetico da parte della potenza di calcolo per minare Bitcoin c'è anche un altro problema: i rifiuti elettronici. Si stima che una singola transazione produca 272 grammi di rifiuti elettronici, per lo più costituiti da vecchio hardware.

4.4 Ethereum: una soluzione più sostenibile

Come altre altcoin, Ethereum sta lavorando per sviluppare una soluzione a minor impatto ambientale rispetto a Bitcoin. Grazie al passaggio alla Proof of Stake e la rimozione della figura di miner i consumi elettrici e i rifiuti saranno notevolmente ridotti (rimanendo esclusivamente i nodi a dover funzionare).

Togliendo però questi consumi Ethereum non si baserà più sulla conversione di altri beni (energia elettrica ed hardware) ma sarà a tutti gli effetti un bene senza nessun legame con il mondo reale, con minore sicurezza, ciò potrebbe ridurre il proprio valore all'interno del mercato[65].

Valutando altre possibili criticità del sistema, il rischio di perdere l'intera caparra in stake, potrebbe non essere appetibile per molti validatori. Questo sistema premia maggiormente chi ha più valuta da poter inserire in stake e perciò tenderà ad aumentare il divario tra i più ricchi e i meno ricchi.

Nel caso ci fossero hard fork di un sistema proof of stake c'è il rischio teorico di una falla di sicurezza, ovvero un attacco double-spending[66]. Non essendoci motivi per i quali un validatore dovrebbe scegliere un determinato fork continuerà a mettere in stake entrambi.

La Proof of Stake resta comunque un interessante cambiamento con molteplici lati positivi, che dovrà essere testata anche a livello pratico prima di diventare il nuovo standard delle criptovalute.

4.5 Cripto nel mondo

La regolamentazione e la presa di posizione da parte delle nazioni ancora non hanno delineato delle vere e proprie linee guida internazionali. In Italia l'unica vera e propria regolamentazione riguarda solamente il riciclaggio di denaro tramite criptovalute[67].

In molti paesi dalla mentalità più chiusa, le cripto sono addirittura considerate illegali, come Russia, Vietnam, Bolivia, Colombia, Ecuador e la recente Cina[68].

La Cina ne fa una questione di sicurezza nazionale e stabilità sociale, a detta loro "le criptovalute possono alimentare un sottobosco di attività illegali"[69]. Prima di questo ban la produzione di Bitcoin all'interno del paese era superiore al 70% globale, anche se è stato un duro colpo la migrazione di molti miners in altre nazioni ha permesso una maggiore decentralizzazione del sistema. Anche se ad oggi è una pratica illegale, si stima che ci sia ancora il 10% del totale di hashrate all'interno del suolo cinese.

Nel primo mondo ancora non sì è deciso come schierarsi: le politiche proibizioniste non hanno dato grandi risultati nelle epoche precedenti e molti stanno ancora cercando la quadra che permetta alle criptovalute di integrarsi con i sistemi finanziari classici.

Altro punto di vista su questo tema arriva dai paesi del terzo mondo: non avendo la propria moneta fiat e dovendo basare la propria economia su una valuta di un'altra nazione più potente sono più propensi ad adottare delle criptovalute che non appartengono ad altri.

4.6 El Salvador: Bitcoin a corso legale

Il 7 settembre 2021, nel paese del Centro America, Bitcoin diventa ufficialmente la moneta a corso legale[70].

All'interno di El Salvador ora si può acquistare qualsiasi merce o servizio sia in dollari sia in Bitcoin.

Il presidente Nayib Bukele è un grande estimatore delle criptovalute ed è riuscito, non esente da critiche, ad approvare Bitcoin come moneta a corso legale per la prima volta al mondo.

Ad El Salvador circa il 70% dei cittadini non ha accesso ai servizi finanziari tradizionali e il denaro che arriva dai migranti rappresenta un enorme fetta dell'economia del paese. Senza servizi finanziari l'entrata di denaro fisico avviene tramite terzi che spesso richiedono cifre assurde per questi spostamenti. Grazie a Bitcoin si può arginare notevolmente questo problema, visto che basta un semplice smartphone con all'interno un wallet per poter inviare e ricevere denaro.

Molte altre nazioni del terzo mondo stanno spingendo sulla possibilità di abbracciare questa filosofia.

Per poter utilizzare Bitcoin come moneta a corso legale si fa uso del Lightning Network, soluzione che permette di ridurre i problemi di scalabilità presenti ad oggi nella blockchain principale di BTC[71]. Tramite questo layer 2 possono avvenire molteplici transazioni da parte di due o più utenti, che verranno gestite al di fuori della blockchain. Una volta terminate tutte le transazioni all'interno di questo sistema, verranno riportate esclusivamente le transazioni finali all'interno dei classici blocchi. In questo modo si potranno avere molteplici transazioni veloci e gratuite tra i vari wallet che successivamente entreranno nella catena di blocchi rappresentate da una singola transazione.

Con questo sistema si rendono possibili le microtransazioni che altrimenti sarebbero troppo dispendiose in termini di fee[72].

CAPITOLO 5

CONCLUSIONI

Esistono molteplici scuole di pensiero per quanto riguarda il futuro del mercato delle criptovalute e Bitcoin, spesso ci si trova a schierarsi per le due supposizioni più estremiste, ovvero la completa rimozione delle monete fiat, sostituite dalle cripto oppure il completo abbandono di tutte le cripto monete per tornare all'esclusivo utilizzo di monete fiat.

Come in qualsiasi altro ambito, credo che la verità stia nel mezzo.

Bitcoin ha portato alla luce la tecnologia blockchain, che come dimostrato da Ethereum è in grado di applicarsi ad infinite soluzioni in ambito tecnologico: Internet di oggi, basato quasi esclusivamente su server privati, diventerà sempre più libero senza dover continuare a dipendere da intermediari di terze parti.

Per quanto riguarda la finanza è chiaro che Bitcoin, come tutte le altre altcoin, abbia seri problemi (scalabilità, inquinamento, valore volatile) e al momento attuale non sia ancora pronto per sostituire le monete fiat.

Anche le monete fiat non sono esenti da problemi, quindi il successo o l'abbandono delle criptovalute a livello finanziario dipenderà da chi riuscirà per primo a realizzare una moneta funzionale che non abbia alcun tipo di problema.

Fino a quel momento monete fiat e criptovalute vivranno in maniera parallela.

Bibliografia

[1] Nakamoto Satoshi. “Bitcoin: A peer-to-peer electronic cash system.”, Decentralized Business Review, 2008

[2] Antonopoulos Andreas M. “Mastering Bitcoin”, O’Reilly Media, 2015

[3] Schilling Linda, Harald Uhlig. “Some simple bitcoin economics”, Journal of Monetary Economics, 2019

[4] Lemme Giuliano, Peluso Sara. “Criptomoneta e distacco dalla moneta legale: il caso bitcoin”, Rivista di Diritto Bancario, 2016

[5] Di Nicola Marco. “Bitcoin: una descrizione architetturale”, Blockchain technology and applications from a financial perspective, 2015

Sitografia

[6] https://www.bergamonews.it/2021/03/14/storia-del-bitcoin-come-e-nato-e-cosa-e-diventato-oggi/424301/ ultima consultazione in data 14/02/2022

[7] https://www.ig.com/it/glossario-trading/definizione-di-moneta-fiat ultima consultazione in data 14/02/2022

[8] https://www.blockchain4innovation.it/mercati/defi-cose-la-finanza-decentralizzata-e-come-sta-cambiando-il-mercato-delle-criptovalute/ ultima consultazione in data 14/02/2022

[9]https://www.studiocorvi.net/bretton-woods-50-anni-dalla-fine-della-convertibilita-del-dollaro-in-oro/ ultima consultazione in data 14/02/2022

[10] https://www.studenti.it/guerra-del-vietnam-cronologia-battaglie-protagonisti.html ultima consultazione in data 14/02/2022

[11] https://www.borsaitaliana.it/notizie/sotto-la-lente/inflazione.htm ultima consultazione in data 14/02/2022

[12] https://wtfhappenedin1971.com/ ultima consultazione in data 14/02/2022

[13] https://www.statista.com/statistics/240991/average-sales-prices-of-new-homes-sold-in-the-us/ ultima consultazione in data 14/02/2022

[14] https://academy.bit2me.com/it/prezzo-bitcoin/#:~:text=Il%20primo%20prezzo%20dato%20a,cambio%20di%201BTC%20%3D%20%24%200.003 ultima consultazione in data 14/02/2022

[15] https://academy.bit2me.com/it/cos%27%C3%A8-il-giorno-della-pizza-bitcoin/ ultima consultazione in data 14/02/2022

[16] https://cryptonomist.ch/2019/07/13/bitcoin-chiavi-indirizzi/ ultima consultazione in data 14/02/2022

[17] https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-what-is-public-key-cryptography ultima consultazione in data 14/02/2022

[18] https://www.criptoinvestire.com/mining-come-funziona-la-verifica-delle-transazioni.html ultima consultazione in data 14/02/2022

[19] https://academy.bit2me.com/it/qual-%C3%A8-la-chiave-pubblica/ ultima consultazione in data 14/02/2022

[20] https://ascuoladibitcoin.com/2021/03/26/lezione-04-transazioni-in-bitcoin-chiave-privata-chiave-pubblica-e-indirizzo/ ultima consultazione in data 14/02/2022

[21] https://academy.bit2me.com/it/cos%27%C3%A8-segwit/ ultima consultazione in data 14/02/2022

[22] https://shiftcrypto.ch/blog/what-are-bitcoin-address-types/ ultima consultazione in data 14/02/2022

[23] https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni ultima consultazione in data 14/02/2022

[24] https://ascuoladibitcoin.com/2021/10/30/lezione-05-la-blockchain-spiegazione-e-dimostrazione-pratica-parte-1/ ultima consultazione in data 14/02/2022

[25] https://www.youtube.com/watch?v=sX25z_-zMgI ultima consultazione in data 14/02/2022

[26] https://academy.bit2me.com/it/transazioni-bitcoin/ ultima consultazione in data 14/02/2022

[27] https://www.tradingmania.it/peer-to-peer-cosa-vuol-dire-e-come-funziona/ ultima consultazione in data 14/02/2022

[28] https://www.pandasecurity.com/it/mediacenter/mobile-news/bitcoin-mining/ ultima consultazione in data 14/02/2022

[29] https://www.wired.it/economia/finanza/2019/11/23/bitcoin-halving-2020/ ultima consultazione in data 14/02/2022

[30] https://www.criptovaluta.it/7391/halving-bitcoin ultima consultazione in data 14/02/2022

[31] https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f ultima consultazione in data 14/02/2022

[32] https://italiancrypto.it/asic-gpu-quali-sone-le-differenze-minare-bitcoin-ed-monete-digitali/ ultima consultazione in data 14/02/2022

[33] https://academy.bit2me.com/it/cos%27%C3%A8-il-pool-di-mining-di-criptovaluta/ ultima consultazione in data 14/02/2022

[34] https://cryptonomist.ch/2019/09/14/attacco-51-hashrate-blockchain/ ultima consultazione in data 14/02/2022

[35] https://www.idealista.it/news/finanza/investimenti/2021/06/15/154436-i-paesi-che-vietano-i-bitcoin ultima consultazione in data 14/02/2022

[36] https://dracmaservice.it/il-sistema-bitcoin-e-usato-dai-criminali/ ultima consultazione in data 14/02/2022

[37] https://www.ilpost.it/2021/06/19/bitcoin-anonimato-riscatto-colonial-pipeline/ ultima consultazione in data 14/02/2022

[38] https://it.wikipedia.org/wiki/Ransomware ultima consultazione in data 14/02/2022

[39] https://github.com/bitcoin/bips ultima consultazione in data 14/02/2022

[40] https://river.com/learn/what-is-a-bitcoin-improvement-proposal-bip/ ultima consultazione in data 14/02/2022

[41] https://www.bbvaopenmind.com/en/technology/digital-world/soft-fork-hard-fork-in-blockchain/ ultima consultazione in data 14/02/2022

[42] https://en.wikipedia.org/wiki/List_of_bitcoin_forks ultima consultazione in data 14/02/2022

[43] https://freemanlaw.com/hard-and-soft-forks-a-detailed-and-simplified-explanation-of-how-blockchains-evolve/ ultima consultazione in data 14/02/2022

[44] https://www.giocareinborsa.com/blog/altcoin-cosa-sono ultima consultazione in data 14/02/2022

[45] https://www.redditoinclusione.it/altcoin/ ultima consultazione in data 14/02/2022

[46] https://www.wired.it/economia/finanza/2018/07/18/stablecoin-criptovalute-bitcoin-prezzo-stabile-volatilita/ ultima consultazione in data 14/02/2022

[47] https://coinmarketcap.com/currencies/ethereum/ ultima consultazione in data 14/02/2022

[48] https://www.ig.com/it-ch/ethereum-trading/cosa-e-ethereum-e-come-funziona ultima consultazione in data 14/02/2022

[49] https://www.criptovaluta.it/12906/defi ultima consultazione in data 14/02/2022

[50] https://cryptonomist.ch/2019/09/07/ethereum-cosa-sono-come-funzionano-smart-contract/ ultima consultazione in data 14/02/2022

[51] https://www.money.it/Smart-Contract-cosa-sono-come-funzionano ultima consultazione in data 14/02/2022

[52] https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P ultima consultazione in data 14/02/2022

[53] https://ethereum.org/it/developers/docs/smart-contracts/ ultima consultazione in data 14/02/2022

[54] https://n26.com/it-it/blog/nft-cosa-sono ultima consultazione in data 14/02/2022

[55] https://www.larvalabs.com/cryptopunks# ultima consultazione in data 14/02/2022

[56] https://ethereum-news.it/ethereum-gas-cost-fees/ ultima consultazione in data 14/02/2022

[57] https://ethgasstation.info/ ultima consultazione in data 14/02/2022

[58] https://www.lifegate.it/elon-musk-biografia-tesla-spacex-storia ultima consultazione in data 14/02/2022

[59] https://cepabismoney.com/la-storia-del-dogecoin-da-meme-a-criptovaluta/ ultima consultazione in data 14/02/2022

[60] https://bitcoin.stackexchange.com/questions/19867/reward-schedule-and-maximum-number-of-dogecoins ultima consultazione in data 14/02/2022

[61] https://it.cointelegraph.com/news/2021-s-btc-energy-use-passes-2020-s-new-study-suggests-each-tx-produces-272g-of-e-waste ultima consultazione in data 14/02/2022

[62] https://www.huffingtonpost.it/entry/2021-il-picco-del-carbone-in-barba-al-patto-sul-clima_it_61bc57e4e4b01828d1eced83 ultima consultazione in data 14/02/2022

[63] https://www.focus.it/scienza/energia/inquinamento-gli-effetti-sulla-salute-di-8000-centrali-a-carbone-nel-mondo ultima consultazione in data 14/02/2022

[64] https://www.wired.it/article/clima-cop26-ambiente-emissioni-temperature-aumento/ ultima consultazione in data 14/02/2022

[65] https://medium.blockchainedu.net/introduzione-ai-sistemi-di-consenso-proof-of-work-e-proof-of-stake-e6564ddad6aa ultima consultazione in data 14/02/2022

[66] https://golden.com/wiki/Nothing-at-stake_problem ultima consultazione in data 14/02/2022

[67] https://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-crittovalute-nei-diversi-paesi-quadro/ ultima consultazione in data 14/02/2022

[68] https://www.torinoggi.it/2021/09/16/leggi-notizia/argomenti/economia-4/articolo/paesi-in-cui-bitcoin-e-legale-e-illegale.html ultima consultazione in data 14/02/2022

[69] https://tech.everyeye.it/notizie/perche-cina-bannato-bitcoin-crypto-motivazioni-ufficiali-543064.html ultima consultazione in data 14/02/2022

[70] https://www.corrierecomunicazioni.it/finance/e-payment/bitcoin-moneta-legale-a-el-salvador-come-il-dollaro-primo-paese-al-mondo/ ultima consultazione in data 14/02/2022

[71] https://cryptonomist.ch/2021/06/28/bitcoin-ora-lightning-network/ ultima consultazione in data 14/02/2022

[72] https://www.webeconomia.it/lightning-network/ ultima consultazione in data 14/02/2022