Università
Ca'Foscari
Venezia

Corso di Laurea
Magistrale in Economia
e Finanza

Tesi di Laurea

BLOCKCHAIN: LA SPINA DORSALE DELLE CRIPTOVALUTE E DEL WEB 3.0

Relatore:
Prof.ssa Marcella Lucchetta

Correlatore:
Prof.re Stefano Colonnello

Laureando:
Leonardo Milan
Matricola 868813

Anno Accademico
2021/2022

RINGRAZIAMENTI

Volevo spendere qualche parola per rendere omaggio a questo periodo della mia vita e alle persone che ne hanno fatto parte.

Il “grazie” più grande va ad Anna, il mio sostegno, che da un po’ di tempo ormai mi supporta, ma soprattutto mi sopporta. Volevo, poi, ringraziare i miei genitori, che mi hanno sempre incoraggiato, permesso di poter portare avanti gli studi, nonché aiutato nei momenti di difficoltà.

Un ringraziamento particolare va alla Professoressa Marcella Lucchetta, dimostratasi un punto di riferimento durante questi anni accademici, rendendosi disponibile, oltre che per la redazione della tesi, anche per l’aiuto e la crescita personale.

Infine, un ringraziamento a tutte le persone che mi sono state vicine.

SOMMARIO

INTRODUZIONE

Oggigiorno la maggior parte della popolazione mondiale utilizza quotidianamente la tecnologia e il web. È inusuale che qualcuno non utilizzi questi strumenti con frequenza, a meno che non ci si rapporti con paesi particolarmente sottosviluppati.

Era il 1991 quando Berners-Lee, capo ricercatore al CERN, pubblicò il primo sito web e da allora il mondo non è più stato lo stesso. Quella prima divulgazione è considerata il primo approccio al Web 1.0, definito anche l'Internet dei contenuti: i siti web erano semplici testi statici, esistevano anche video e immagini, ma non c'era una vera e propria interazione tra utente e contenuto, di conseguenza l'utilizzo era di mero scopo informativo.

Successivamente, dal 2004, dopo la "Web 2.0 Conference" di O'Reilly Media, prese forma il Web 2.0, con il quale si indica un nuovo tipo di esperienza web. In questo modo, si è passati da una semplice navigazione tra siti statici allo sviluppo e alla successiva distribuzione di software, che cercano di creare una vera e propria interconnessione tra utente e contenuto web.

L'idea e l'esigenza di creare un Web 3.0 iniziarono a crearsi e a diffondersi già nel 2006 per alcune dichiarazioni di un critico di nome Jeffrey Zeldman. Il Web 3.0 è l'imminente terza generazione di Internet, in cui i siti web e le app saranno in grado di elaborare le informazioni in modo intelligente, come l'uomo, attraverso tecnologie come l'apprendimento automatico (Machine Learning), i Big Data e la tecnologia di contabilità decentralizzata (Distributed Ledger Tecnology). Il Web 3.0 era originariamente chiamato "Web semantico" dall'inventore del World Wide Web, Tim Berners-Lee, e mirava a essere un Internet più autonomo, intelligente e libero.

Quando il Web 3.0 sarà completamente implementato, i dati saranno interconnessi in modo decentralizzato, il che rappresenta un enorme balzo in avanti rispetto alla nostra attuale generazione di Internet, dove i dati sono per lo più archiviati in database

centralizzati. Affinché il passaggio avvenga, i programmi devono comprendere le informazioni sia concettualmente che contestualmente. Possiamo, dunque, tranquillamente affermare che i due capisaldi del Web 3.0 sono il web semantico e l'intelligenza artificiale.

In questo web, in continua evoluzione, ha fatto la sua comparsa nel 2009 Bitcoin, una criptovaluta e un sistema di pagamento valutario internazionale innovativo. In questo modo, anche il mondo finanziario ha iniziato un processo di evoluzione in un contesto che possiede molteplici possibilità di sviluppo.

Poiché le reti Web 3.0 operano attraverso i protocolli decentralizzati, i blocchi fondanti la tecnologia blockchain e le criptovalute, possiamo notare una forte convergenza e una relazione simbiotica tra queste tre tecnologie. Nonostante il processo sia ancora incompleto, in futuro si auspica che queste tecnologie saranno perfettamente interoperabili, integrate, automatizzate, grazie agli smart contract[1], e utilizzate per alimentare qualsiasi tipo di operazione: dalle micro-transazioni in Africa, all'archiviazione di file di dati P2P[2] resistenti alla censura e molto altro. In questi ultimi due anni, sono stato affascinato dal mondo delle criptovalute e ho cercato di studiarlo in maniera autonoma, testandone anche il funzionamento. Ho provato in prima persona la volatilità di questo strumento così potente, tentando anche qualche speculazione, non sempre conclusasi con esito positivo. In questo elaborato ho effettuato uno studio più approfondito sul concetto di blockchain, sul funzionamento di questo strumento, sull'utilizzo che ne viene fatto, nonché sui possibili sviluppi futuri. Nonostante inizialmente volessi trattare il tema generale delle criptovalute, la loro storia e la loro evoluzione, successivamente mi sono accorto di quanto materiale circolasse all'interno del web in merito a questo argomento. Proprio per questo motivo, ho deciso di approfondire la conoscenza dell'infrastruttura su cui si basano.

Difatti, di criptovalute e di registri distribuiti ne esisto oramai un'infinità, dunque sarebbe stato difficile, se non impossibile, riuscire a parlare di tutte; motivo per cui, per spiegare i concetti principali di questo tema, ho deciso di rifarmi a Bitcoin e alla sua

[1] Smart contract: i "contratti intelligenti", corrispondono a programmi per elaboratori che operano su tecnologie basate su registri distribuiti; la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse.

[2] P2P: Person to person.

blockchain, trattandosi della prima inventata nonché della più sviluppata attualmente. Non sono mancate però le analisi sul funzionamento di altre blockchain particolarmente importanti e influenti.

Non metto in dubbio che la blockchain sia tuttora uno strumento abbastanza giovane, ma non rimarrei stupito se tra qualche anno l'anagrafe, il catasto o il pubblico registro automobilistico si spostassero su blockchain, anzi c'è chi ci sta già pensando.

Infine, ho deciso di portare un esempio di transazione tra wallet cripto per mostrare la trascrizione di queste operazioni on-chain.

CAPITOLO 1

1.0 CRIPTOVALUTE

1.1 DEFINIZIONE

Un documento informatico, per definizione, è replicabile all'infinito e trasferibile senza perderne il possesso. I meccanismi di criptazione e di accesso a chiavi asimmetriche, che sono in dominio solo da parte del soggetto che compie una determinata operazione, riescono a rendere univoco l'accesso a un contenuto digitale. Ciò è il motivo per cui si è potuto creare una moneta virtuale, trasferendo blocchi di informazioni digitali. È noto che una moneta non potrebbe mai esistere se la sua rappresentazione digitale fosse spendibile più di una volta, difatti funziona solo se c'è qualcosa che permette la non-replicazione della disponibilità da parte del cedente. Questa è la creazione degli asset unici, ossia contenuti digitali che possono essere rappresentazione di moneta virtuale.

Una criptovaluta è un'unità di valore digitale, movimentata e nativa online, con delle differenze rispetto alla classica moneta elettronica. Il termine "criptovaluta" ci fa capire una delle principali differenze: l'utilizzo della crittografia[3], la quale gioca un ruolo fondamentale per garantire sicurezza, immutabilità e impossibilità di contraffazione.

È transata e resa sicura in modo decentralizzato nella blockchain, un'infrastruttura che ne garantisce attendibilità e decentramento.

La blockchain, nell'ambito cripto, impedisce la contraffazione, ossia la creazione di moneta falsa, e il "double spending", truffa che consiste nel poter spendere la stessa unità di valore più di una volta. Se c'è possibilità di double spending la moneta digitale non possiede valore.

[3] Crittografia: lo studio di tecniche di comunicazione sicure che consentono di rendere un messaggio non comprensibile a persone non autorizzate a leggerlo.

La criptovaluta è un sistema open source in cui chiunque può provare a creare, modificare o proporre una propria versione di essa, successivamente starà poi all'utenza decidere se utilizzarla o meno.

È essenziale comprendere che cosa si intende quando si parla di decentralizzazione in ambito cripto, in quanto è il principio cardine su cui si basano tutte le blockchain.

La differenza tra un sistema tradizionale di moneta elettronica e quello della criptovaluta è che il primo prevede l'utilizzo di intermediari per poter effettuare le transazioni, mentre il secondo no. Si parla di centralizzazione, nel primo caso, proprio perché ci si basa su un'entità centralizzata che autorizza le operazioni dei vari soggetti operanti nel sistema. Nel momento in cui inviamo un bonifico, ad esempio, inseriamo nell'online banking i dati del beneficiario e la cifra che intendiamo inviare, la banca verifica i dati inseriti, approva il movimento, lo invia alla banca del beneficiario, che a sua volta lo approva e solo successivamente accredita la somma sul conto del destinatario del nostro bonifico.

Dunque, di fatto ci sono due diverse autorizzazioni: quella della banca del mandante e quella della banca del ricevente; questo processo richiede tempo e introduce determinati costi.

Nel caso in cui l'intermediario per qualche motivo riscontrasse problemi di funzionamento, si configurerebbe un disservizio; come, ad esempio, successe il 24 Febbraio 2022 quando le truppe russe entrarono in Ucraina e la Banca Nazionale ucraina attuò una serie di misure restrittive: sospese momentaneamente il mercato valutario, limitò il ritiro dei contanti e proibì l'emissione di valute estere al pubblico. Ciò è avvenuto perché si è fatto affidamento su un ente centralizzato, la banca, e, come si è dimostrato, nel caso in cui vi sia un disservizio oppure una mala gestio, i clienti non hanno più la possibilità di disporre liberamente delle proprie somme. Fermo restando che, nel momento in cui ci si affida a degli istituti bancari, in realtà, non si potrebbe mai parlare di "disporre liberamente delle somme".

Nel caso di operazioni cross-boarder[4], inoltre, vi sono ulteriori tempistiche e costi da sostenere. Si tratta di un sistema inefficiente sia perché introduce spese elevate, causate

[4] Operazioni cross-boarder: con operazioni oltre frontiera si fa riferimento a quelle effettuate all'estero o con l'ausilio di intermediari finanziari esteri.

dalla quantità di intermediari, sia perché, se uno di questi cessa di funzionare, buona parte del sistema potrebbe a sua volta non operare più efficientemente.

Come accennato poco sopra, in banca, di fatto, non si possiede proprietà effettiva di quanto depositato, ma si vanta un credito nei confronti della banca, poiché, proprio per definizione, essa è quell'istituto che raccoglie denaro tra il pubblico ed eroga credito, di conseguenza il capitale che le affidiamo viene prestato ad altri soggetti.

Un sistema decentralizzato, invece, lavora diversamente: è costituito da un insieme di nodi[5] distribuiti nel mondo che comunicano tra di loro. Nel momento in cui inviamo una transazione attraverso questo sistema abbiamo bisogno della convalida dell'operazione, che solo in seguito verrà recapitata al destinatario. In questo caso, vi è proprietà diretta del bene in questione da parte del soggetto, infatti esso non viene affidato ad un intermediario e non serve effettuare nessuna richiesta per poterlo utilizzare. Ciò implica tempi più brevi per effettuare le transazioni, costi minori e una fruibilità costante, non dipendendo da un single point of failure[6].

Si tratta di un sistema borderless[7] poiché la valuta virtuale viene inviata con la medesima metodologia sia all'interno del paese che verso l'estero. In questo caso, avviene una transazione diretta dalla persona A alla persona B, validata e trascritta su un registro distribuito: la blockchain. Non si dipende da un ente, di conseguenza non c'è la possibilità che la transazione venga negata; motivo per cui si definisce anche un sistema "permissionless". Questa è la principale differenza tra un sistema centralizzato (permissioned), in cui si dipende da un'entità o un istituto, e un sistema decentralizzato (permissionless), in cui si è supervisionati da un network che non ha un single point of failure.

Il network in quest'ultimo sistema è completamente indipendente dalla volontà umana, infatti se si dimostra di avere la disponibilità di criptovalute e la possibilità di spenderle attraverso la propria chiave privata, nessuno può decidere di sospendere o negare la transazione.

[5] Nodo: un punto in una rete che distribuisce i dati ad altri nodi o li riceve e basta fungendo da endpoint.
[6] Single point of failure: Un singolo punto di errore (SPOF) è una parte di un sistema che, in caso di guasto, interromperà il funzionamento dell'intero sistema.
[7] Borderless: senza confini tra paesi, divisioni amministrative o di altro genere.

1.2 COME NASCONO

BTC è la prima criptovaluta mai creata, nonché la più sicura e la più decentralizzata, proprio per questo motivo ha uno storico delle transazioni talmente lungo da permettere un alto livello di sicurezza. Tanti più sono gli anni di funzionamento di una criptovaluta, tanto più questa è sicura.

La blockchain Bitcoin è cresciuta a dismisura negli anni: ci sono sempre più nodi e sempre più hash-rate[8]; ciò ha fatto si che questa criptovaluta diventasse ogni giorno più decentrata e più protetta.

Bitcoin è il registro distribuito creato da Satoshi Nakamoto nel 2008, mentre BTC è il nome dei token scambiati all'interno di questa blockchain. Negli anni, il termine "Bitcoin" è stato esteso rispetto al suo significato originale e utilizzato per indicare anche il protocollo su cui si basa e la relativa criptovaluta. All'interno di questo elaborato utilizzeremo "Bitcoin" per indicare la criptovaluta, mentre "blockchain di Bitcoin" per indicare il registro distribuito.

Satoshi Nakamoto corrisponde allo pseudonimo utilizzato dalla persona o dalle persone che hanno sviluppato questo token, creato il white paper su cui si basa e progettato e distribuito l'implementazione di riferimento originale. Nakamoto ha anche ideato il primo database blockchain, che ha preso forma nel 2009 con la creazione del primo blocco. La decisione di non dare un volto al creatore di questa innovazione sembra dipendere dal fatto che si voglia far in modo che il network sia il più possibile indipendente. Di fatto non c'è una persona di riferimento nello sviluppo di Bitcoin con la stessa influenza che potrebbe avere l'ideatore del suddetto sistema. Si tratta di un network interamente in mano alla community, il che lo rende completamente decentralizzato.

Bitocoin è nato in piena crisi economica, nel periodo dei così detti "bail-out", momento in cui le banche rischiavano la bancarotta, assumendosi troppi rischi rispetto a quelli che sarebbero stati in grado di sopportare. È stato creato come libera alternativa al denaro FIAT[9]: infatti, è stata data la possibilità alle persone di poter scegliere se utilizzarlo o meno, senza imporre nulla. Il denaro FIAT, invece, è prescritto e controllato dalle

[8] Hash-rate: è una misura della potenza di calcolo al secondo utilizzata durante il mining.

[9] Denaro FIAT: la moneta cartacea inconvertibile, generalmente accettata come mezzo di pagamento in quanto dichiarata a corso legale dallo Stato che la emette.

politiche monetarie, mentre Bitcoin è sorvegliato da un algoritmo, dalla decentralizzazione e di conseguenza dalla community. Si è cercato di fuggire dal controllo di pochi: queste sono le ceneri dalle quali è nata la fenice Bitcoin, la quale punta ad offrire una via di fuga dalla dipendenza da istituzioni finanziarie.

I Bitcoin vengono creati all'interno della rete e la loro creazione è rigorosamente posta a controllo, ma senza essere governata da un'autorità di emissione centrale. La rete, infatti, è programmata per garantire che il numero totale di Bitcoin esistenti non superi mai i 21 milioni, valore in realtà generato per metà già nel 2013. I Bitcoin vengono "estratti" tramite mining rig[10] dedicati, che creano nuove monete attraverso una serie di attività richiedenti una notevole potenza di calcolo. La rete è progettata per produrre un numero fisso di Bitcoin per unità di tempo: 25 nuovi Bitcoin sono stati generati ogni dieci minuti fino al 2017, tale numero è stato successivamente dimezzato ogni quattro anni e continuerà a dimezzare fino al 2140. Più persone (o rig) si occuperanno del mining di questo tipo di monete, più sarà difficile produrle: ora, solo i rig più potenti, cioè più computer che lavorano insieme, sono in grado di crearne di nuove.

Quindi cosa rende Bitcoin diverso? Mentre solitamente spetta a istituzioni come le banche centrali e il Fondo Monetario Internazionale proteggere il valore del denaro, Bitcoin delega tale compito alle macchine. Questo lo rende sociologicamente interessante, ma allo stesso tempo problematico, perché, di fatto, le macchine non operano mai unicamente in modo autonomo. È qui che si apre un abisso tra l'ideologia dietro Bitcoin e la realtà pratica del suo funzionamento.

Il discorso pubblico su Bitcoin spesso si concentra sull'idea che si tratti di denaro creato dal nulla: è denaro virtuale, non reale. Ma non c'è niente di insolito in questo. Al contrario, alcuni dei fattori più interessanti di Bitcoin sono l'armamentario materiale che lo supporta e il linguaggio materialistico che lo giustifica. Bill Maurer[11] ha categorizzato la filosofia alla base di Bitcoin come una forma di "metallismo[12] digitale", che si basa sulla semiotica[13] del denaro metallico, con il suo linguaggio di mining e rig. Infatti, sono

[10] Mining rig: è una disposizione di elementi hardware, tra cui CPU, GPU, FPGA o ASIC, predisposti per eseguire il mining di criptovaluta.

[11] Bill Maurer: è uno studioso accademico americano di antropologia giuridica ed economica.

[12] Metallismo: teoria monetaria secondo la quale il valore di una moneta è legato a quello del metallo di cui è composta.

[13] Semiotica: la scienza generale dei segni.

i limiti "naturali" dell'offerta, come per quanto riguarda l'oro, che è un elemento limitato in natura e la sua offerta non è aumentabile artificialmente, a dare valore a Bitcoin, dal momento in cui vi è una quantità massima estraibile.

Secondo Nakamoto il problema principale delle forme di denaro più convenzionali è la fiducia necessaria per farle funzionare: ci si deve fidare della banca centrale per non far svalutare la moneta, per esempio. Le proposte di Nakamoto cercano di liberarsi da questa autorità utilizzando una catena di blocchi, condivisa da tutti i computer o nodi all'interno della rete, attraverso la quale la cronologia delle transazioni di ciascuna moneta possa essere pubblicamente nota. La privacy, inoltre, è preservata, nel frattempo, crittografando le chiavi, ossia garantendo che la cronologia di ogni "moneta" sia anonimizzata.

L'idea di Nakamoto è stata straordinariamente potente, catturando l'immaginazione di una vasta gamma di persone. Al centro vi sono quattro idee-chiave: in primo luogo, la rete Bitcoin è decentralizzata e piatta, senza gerarchia e senza un unico punto di autorità; in secondo luogo, Bitcoin offre soluzioni tecnologiche infallibili a problemi secolari di governance monetaria; terzo, Bitcoin rinuncia alla necessità di fidarsi di altre persone, siano essi esperti, politici o gente comune; e quarto, Bitcoin è denaro senza debiti, proprio come l'oro.

Bitcoin potrebbe essere visto come una sorta di valuta di protesta: attira molti sostenitori a causa della doppia disintermediazione, infatti, separa il denaro sia dalle banche che dagli stati. Ciò riecheggia con due assi principali del dibattito politico nel rapporto tra finanza e stato: Bitcoin è in risonanza nei dibattimenti sulla natura del denaro e delle attività bancarie, innescati dalla crisi del 2008. Questa moneta si nutre quindi della stessa vena di malcontento di Positive Money[14] nel Regno Unito, la quale sostiene che le banche dovrebbero essere private del loro diritto di creare denaro attraverso il prestito.

Paradossalmente, l'ideologia di Satoshi Nakamoto si basa sul trattare questa criptovaluta come uno strumento controllato dalla tecnologia. Egli pone l'obbiettivo di eliminare qualsiasi intermediario centrale, che si frapponga tra gli utenti e le transazioni

[14] Positive Money UK: è un gruppo di difesa senza scopo di lucro con sede a Londra e Bruxelles, la cui missione è promuovere un'economia equa, democratica e sostenibile attraverso le riforme delle banche centrali e una politica monetaria alternativa.

che questi intendono effettuare. Esaminando tale pensiero, però, si può notare come, nonostante sia fondamentale il supporto tecnologico, lo sia ancor di più quello sociale. Bitcoin, infatti, è caratterizzato da un forte senso di comunità e ciò si riflette nei gruppi di discussione, nei forum su Internet e nelle organizzazioni ad esso associate.

Esso è attualmente sostenuto da caratteristiche sociologiche che sono direttamente in contrasto con l'ideologia politica e la teoria del denaro da cui è nato, queste includono: la leadership, l'organizzazione e la struttura sociale, l'utopismo e la fiducia.

È necessario riflettere sul fatto che gli artefatti tecnologici non siano in grado di creare e far prosperare forme organizzative senza una forte comunità che li sostiene. L'utenza che utilizza questo tipo di tecnologia modella ed è modellata dal suo uso pratico, creando una simbiosi impossibile da spezzare, pena lo sfaldamento del sistema.

Saremo in grado di capire appieno l'uso e il funzionamento delle criptovalute solo nel momento in cui ci renderemo conto che questo tipo di tecnologia non potrebbe esistere senza una forte comunità che la supporta.

1.3 IL FUNZIONAMENTO

Per poter utilizzare le criptovalute occorre quello che si chiama "wallet": un software, un programma, un'applicazione che permette di riceverle, conservale e inviarle.

Esistono anche i "portafogli hardware": tipo speciale di portafoglio cripto che memorizza le chiavi private dell'utente in un dispositivo hardware sicuro.

Questo argomento verrà analizzato in maniera più approfondita tramite un caso pratico nel Capitolo 4.

1.3.1 Wallet crypto e chiavi

Un "wallet crypto" è un portafoglio di criptovalute che consente agli utenti di gestire diversi tipi di token, come ad esempio Bitcoin o Ether, e di scambiare facilmente i propri fondi. Le transazioni sono sicure, poiché sono firmate crittograficamente. Il portafoglio è accessibile da dispositivi web, compresi quelli mobili, e la privacy e l'identità dell'utente sono preservate. Quindi, un portafoglio di criptovalute fornisce tutte le funzionalità necessarie per trasferimenti e scambi di fondi sicuri e protetti tra diverse parti.

È molto simile al processo di invio o ricezione di denaro tramite PayPal o qualsiasi altro gateway utilizzato oggi, ma al posto di transazioni in denaro FIAT, vengono adoperate le

criptovalute. Esempi di questi portafogli includono Electrum, Jaxx, Mycelium, Blockchain.info, Samurai ed Etoro Money.

Il funzionamento di questi wallet è garantito grazie a due chiavi: una pubblica e una privata. Proprio per questo motivo, immaginarlo come un portafoglio fisico, contenente le nostre criptovalute, è sbagliato: esso, grazie alle chiavi contenute, permette di utilizzarle al fine di ricevere, conservare e inviare Bitcoin o altri token.

La chiave pubblica è ricavabile da quella privata tramite un algoritmo crittografico chiamato "Elliptic Curve Digital Signature Algoritm"[15]. Infatti, se quella privata viene inserita come input in questo algoritmo, dà come output quella pubblica; di conseguenza, chi è in possesso della prima può derivare la seconda. Questo procedimento è però unidirezionale: è questa la funzionalità della crittografia a curva ellittica.

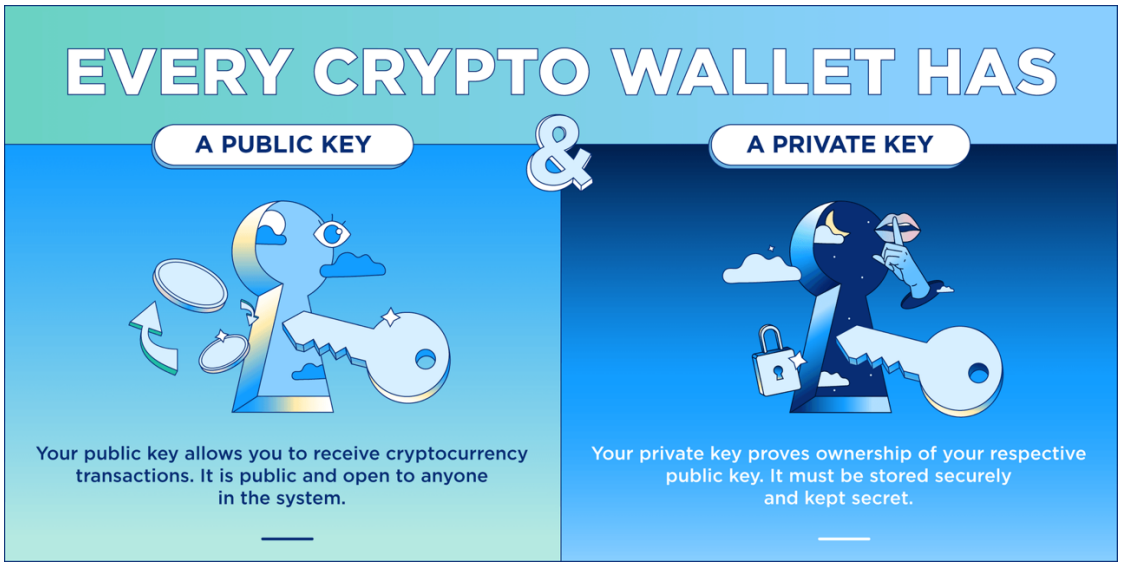
In sostanza, noi possediamo una chiave pubblica, attraverso la quale possiamo ricavarci l'address del nostro portafoglio, che poi possiamo diffondere per poter ricevere le criptovalute. Se un soggetto A comunica la propria chiave pubblica ad un soggetto B, quest'ultimo può solamente inviare e non può spendere i token del soggetto A. Se il soggetto A, invece, diffonde la propria chiave privata al soggetto B, egli è in grado anche di poter spendere le criptovalute del primo. La chiave privata deve essere custodita in maniera maniacale: se persa o distrutta sarà impossibile recuperarla e non si potranno più firmare le transazioni di uscita dai propri wallet.

Facendo un parallelismo con il sistema bancario, possiamo pensare alla chiave pubblica come al codice IBAN associato al nostro conto corrente. Si tratta di un codice che, idealmente, potremmo divulgare senza problemi e attraverso il quale altri soggetti potrebbero solamente inviarci denaro senza spendere quello che abbiamo a disposizione. Possiamo, d'altro canto, attribuire alla chiave privata l'importanza del codice pin associato al nostro bancomat: un'informazione che assolutamente non dobbiamo divulgare a terzi se non vogliamo che queste persone possano disporre delle nostre somme presenti nel conto corrente.

Il funzionamento è tale per cui si ricevono Bitcoin o altre criptovalute grazie alla propria chiave pubblica e si spendono firmandole grazie a quella privata.

[15]Elliptic Curve Digital Signature Algoritm: algoritmo di firma digitale a curva ellittica.

Figura 1: Public and Private Key.



Fonte: crypto.com

Le criptovalute sono al sicuro solo se il metodo che utilizziamo per archiviarle è quello corretto: sebbene ci sia la possibilità di archiviare le criptovalute direttamente sull' exchange[16], non è consigliabile farlo se non in piccole quantità o se non si prevede di scambiarle frequentemente. Per importi di un certo valore, si consiglia di prelevarne la maggior parte su un portafoglio crittografico, sia esso un portafoglio caldo o uno freddo. In questo modo, si ha maggiore controllo sulle proprie chiavi private e di conseguenza anche sulle proprie finanze crittografiche.

Gli hot wallets sono portafogli online attraverso i quali è possibile trasferire rapidamente le criptovalute, esempi sono Coinbase e Blockchain.info.; inoltre, sono accessibili online 24 ore su 24, 7 giorni su 7 tramite un dispositivo desktop o mobile. Attraverso questi, le chiavi private vengono archiviate nel cloud per un trasferimento più rapido. Presentano, però, il rischio di furti irrecuperabili se hackerati.

I cold wallets, invece, sono portafogli digitali offline, in cui le transazioni vengono firmate offline e solo successivamente divulgate online: non vengono mantenuti nel cloud Internet, ciò per garantire un'elevata sicurezza. Esempi di cold wallet sono Trezor e Ledger. Attraverso questi, le chiavi private vengono archiviate in un hardware separato, non connesso a Internet o al cloud, oppure su un documento cartaceo. In questo caso,

[16] Exchange: piattaforma tecnologica, che permette lo scambio di criptovalute.

il metodo della transazione aiuta a proteggere il wallet da accessi non autorizzati derivanti ad esempio dall'hacking.

Possiamo ulteriormente suddividere i portafogli in tre tipi:

- Software wallets;
- Hardware wallets, che colleghiamo all'unità USB;
- Tipici portafogli cartacei, per i quali stampiamo la chiave pubblica e privata su un pezzo di carta e la conserviamo in un luogo sicuro.

Un portafoglio software comprende sia un'applicazione che viene scaricata su un dispositivo, inteso sia come un desktop oppure come un dispositivo mobile, sia un portafoglio basato sul Web a cui è possibile accedere online. Possiamo ulteriormente classificare i portafogli software come portafogli desktop, portafogli online (portafogli web) e portafogli mobili.

- Desktop wallets: sono portafogli freddi in cui le chiavi private sono archiviate in server freddi (nel desktop). Possiamo scollegare il portafoglio da Internet, eseguire alcune transazioni offline e successivamente riportarlo online. Questi portafogli possono essere scaricati su qualsiasi computer, ma sono accessibili solo dal sistema su cui sono installati; quindi, è necessario assicurarsi che il desktop o la macchina su cui si sta scaricando il portafoglio sia sicuro (abbia un backup e si trovi in una posizione protetta) e che si effettui la manutenzione dell'hardware.

  Questi portafogli sono decisamente convenienti.

  Electrum è uno dei portafogli desktop più popolari.
- Online wallets: sono altri tipi di portafogli caldi che funzionano su Internet. Gli utenti hanno il vantaggio di accedere a questi portafogli su qualsiasi dispositivo, sia un tablet o un desktop, oppure direttamente dal browser mobile. Le chiavi private sono archiviate online e sono gestite da terzi. Ad esempio, GreenAddress è un portafoglio Bitcoin disponibile sul Web, su un desktop, ha un'app per Android e anche per iOS.
- Portafogli mobile: sono simili ai portafogli online tranne per il fatto che sono creati solo per l'uso e l'accessibilità da telefono cellulare. Questi portafogli hanno un'interfaccia intuitiva che aiuta gli utenti a svolgere transazioni in modo molto semplice. Etoro Money è un esempio di questo tipo di wallet.

Un portafoglio hardware è un tipo di dispositivo di archiviazione freddo, in genere come una chiavetta USB, che memorizza la chiave privata dell'utente in un dispositivo hardware protetto. Questi portafogli sono simili ai dispositivi portatili che possono essere collegati al computer. Come notato in precedenza, sono meno inclini ad attacchi dannosi e sono a prova di hacker.

Per effettuare una transazione dal proprio portafoglio hardware, bisogna assicurarsi che esso sia collegato ad un computer.

Infine, un portafoglio di carta è un pezzo di carta in cui sono stampate o scritte le nostre chiavi private e pubbliche. Alcuni potrebbero anche avere un codice a barre scansionabile creato da un'app: un modo per archiviare e accedere alle proprie criptovalute offline. Quando stampiamo le nostre chiavi, vengono rimosse dalla rete, a differenza dei token che rimangono; i quali, tuttavia, sono inaccessibili senza le chiavi stesse.

I portafogli di carta venivano generalmente molto utilizzati prima che le criptovalute diventassero così popolari.

Questo sistema di gestione tramite portafogli si basa sul fatto che è necessario ricevere le criptovalute per poterle spendere. Infatti, la prima domanda che il network si pone nel momento in cui deve validare una transazione è: "Il soggetto in questione si può permettere di spendere queste criptovalute? Le ha mai ricevute prima?". Nel momento in cui proviamo a inviare una transazione al network, in cui ad esempio spendiamo un'unità di Bitcoin, il network cerca di risalire alla provenienza di questa somma. Se risulta, dallo storico delle transazioni, che il soggetto non abbia mai ricevuto quelle quantità di criptovalute, la transazione viene bloccata automaticamente. Non è possibile creare dei token dal nulla, l'UTXO[17] è alla base di queste verifiche.

Le transazioni, una volta inviate, finiscono in coda sulla blockchain e man mano vengono validate e inserite all'interno dei blocchi. Una volta raggiunto il numero massimo di transazioni che possono essere contenute dal singolo blocco, questo viene chiuso e propagato all'intero network.

Nel momento in cui si decide di aprire un wallet di criptovalute e di detenerle, è fondamentale sapere che le monete virtuali dovranno successivamente essere

[17] UTXO: Unspent Transaction Output consiste in una transazione ricevuta, ma non ancora spesa.

dichiarate allo Stato, in quanto attività di natura estera. In Italia, l'articolo 4 del decreto legislativo 167/90 obbliga i possessori di tali token ad indicarli nel quadro RW della dichiarazione dei redditi. Le imposte risultano dovute sulle eventuali plusvalenze maturate solo e soltanto se la giacenza media dei portafogli elettronici (wallet), detenuti dal medesimo contribuente, supera, per almeno 7 giorni consecutivi, la detenzione di controvalore pari ad euro 51645,69.

1.4 CARATTERISTICHE DI UNA TRANSAZIONE

Nel momento in cui si vuole creare una transazione, bisogna inserire degli input in appositi software che in seguito genereranno degli output. Vi sono dei wallet che facilitano l'operazione: infatti, per inviare ad esempio dei Bitcoin, inseriti un address e la quantità, genereranno per noi la transazione. Una volta ottenuto lo script[18], si firma con la propria chiave privata e successivamente vi sarà l'invio alla blockchain delle informazioni per la validazione dell'operazione. Se la transazione non è firmata con la propria chiave privata, non si può dimostrare di poter spendere le criptovalute. La firma generata dalla crittografia a curva ellittica[19] permette al validatore di controllare che il firmatario della transazione sia veramente il titolare di quei token. Una volta fatto ciò, la transazione validata verrà inclusa nei blocchi e verrà propagata nella blockchain.
I dati contenuti dalle transazioni sono: input, fee, output e altri dati.

- Input: l'address di colui che invia e valore delle transazioni fino ad ora ricevute e non spese (UTXO). Si tratta, dunque, di dichiarare quanto si è in grado di spendere in base a quanto si è ricevuto e non si è ancora speso. Inoltre, vengono forniti dei dati sull'autenticità dell'input e sulla firma della transazione.
- Fee: quanta priorità dare alla transazione nella coda, in base alla percentuale di commissioni.
- Output: l'address del destinatario, la quantità di cripto inviate e il "change": l'eccedenza dell'input che viene rimandata al portafoglio di colui che invia. Ad esempio, se io ho ricevuto una transazione del valore di 1 Bitcoin e voglio mandarne 0.3, io spenderò quell'unspent transaction output da 1 Bitcoin e

[18] Script: stringa alfanumerica contenente le informazioni sulla transazione.
[19] Crittografia a curva ellittica: utilizza le proprietà matematiche delle curve ellittiche per produrre sistemi crittografici a chiave pubblica.

genererò 2 output: 0.3 Bitcoin da mandare al destinatario e 0.7 Bitcoin che torneranno nel mio wallet. Sorge spontaneo il dubbio: perché questa complicazione? Si tratta di una questione di sicurezza e di gestione ottimale delle transazioni: una volta speso, un output non può essere parzialmente erogato. In questo modo si riesce a garantire coerenza e verificabilità delle transazioni.

1.5 COSA DA' VALORE A BITCOIN

Nonostante la loro volatilità, le criptovalute continuano ad attirare l'interesse degli investitori per il loro record a lungo termine di costruzione e mantenimento del valore. A differenza di un'azione, la quale possiede valore perché rappresenta la proprietà parziale di un'azienda, o un'obbligazione, che rispecchia il valore di un debito che verrà rimborsato ad una data scadenza, può essere più difficile individuare il controvalore creato da una valuta digitale decentralizzata con una storia, tutto sommato, così breve. Le criptovalute non sono state supportate da alcuna autorità centrale, a differenza delle valute legali o di altri mezzi di scambio autorizzati dal governo. Il sostegno da parte di quest'ultimo può certamente aumentare la fiducia nel valore di una valuta tra i consumatori, ma, dato che le criptovalute sono generalmente decentralizzate, derivano il loro valore da altre fonti, tra cui: la domanda e l'offerta, i costi di produzione, la concorrenza, la disponibilità sugli exhange, la governance e le regolamentazioni.

- La domanda e l'offerta: il valore della criptovaluta è determinato dalla domanda e dall'offerta, proprio come per qualsiasi altro bene. Se, in un dato momento, la domanda è maggiore rispetto all'offerta, il prezzo aumenterà.

  Il meccanismo di fornitura delle varie criptovalute è noto: infatti, ognuna pubblica i propri piani di conio dei token. Alcuni, come Bitcoin, hanno una fornitura massima fissa: sappiamo che arriveremo ad avere al massimo 21 milioni di Bitcoin. Altri, come Ether, non hanno limiti al conio. Alcune criptovalute hanno addirittura meccanismi che "bruciano" i token esistenti per evitare che l'offerta circolante cresca troppo.

  La politica monetaria di ogni criptovaluta è diversa. L'offerta di Bitcoin aumenta di un importo fisso con ogni nuovo blocco minato sulla blockchain. Ethereum offre una ricompensa fissa per blocco estratto, ma paga anche per la creazione

di "uncle block[20]", il che aiuta a facilitare l'efficienza della blockchain. Di conseguenza, l'aumento dell'offerta non è fisso. Alcune forniture di criptovaluta sono dettate interamente dal team responsabile di un progetto, che può scegliere di rilasciare oppure "bruciare" token per gestire l'offerta di denaro.

La domanda può aumentare man mano che un progetto acquisisce consapevolezza e accresce la propria utilità. Inoltre, l'adozione più ampia di una criptovaluta come investimento aumenta anche la domanda, limitando efficacemente l'offerta circolante. Ad esempio, quando gli investitori istituzionali hanno iniziato ad acquistare e detenere Bitcoin all'inizio del 2021, il prezzo è aumentato in modo significativo, poiché la domanda ha superato il ritmo con cui sono state create nuove monete, diminuendo di fatto l'offerta totale disponibile. Accade ugualmente quando vengono promossi più progetti di finanza decentralizzata (DeFi) sulla blockchain di Ethereum: la domanda di Ether aumenta.

- I costi di produzione: i token vengono creati attraverso vari processi, come possono essere il mining, lo staking e molti altri. Questi procedimenti implicano l'utilizzo di un hardware per verificare l'adeguatezza del blocco che si andrà ad aggiungere alla blockchain. La rete decentralizzata è ciò che consente alla criptovaluta di funzionare come deve. In cambio, il protocollo produce una ricompensa sotto forma di nuovi token.

  La verifica della validità della blockchain richiede potenza di calcolo: difatti, i partecipanti investono in apparecchiature costose ed elettricità per creare criptovalute. In un sistema proof of work[21], come quello utilizzato da Bitcoin, maggiore è la concorrenza per il mining di una determinata criptovaluta, più è difficile e dispendioso "estrarre" i blocchi[22]. Questo perché i "minatori" essenzialmente gareggiano tra loro per risolvere un complesso problema di matematica, al fine di verificare le transazioni. Di conseguenza, il costo per

[20] Uncle Block: nella blockchain di Ethereum, quando due blocchi vengono estratti e inviati alla blockchain nello stesso momento, uno solo di questi è convalidato, l'altro è un "uncle block".
[21] Proof of work: algoritmo di consenso distribuito, utilizzato in ambito blockchain, basato sulla competizione nella validazione delle transazioni.
[22] Blocco: anello della blockchain, contenente gruppi di transazioni.

l'estrazione aumenta poiché è necessario un equipaggiamento più potente per validare i blocchi con successo.

Con l'aumento dei costi di produzione è essenziale un ampliamento del valore della criptovaluta: nessuno metterebbe a disposizione tutta questa energia se il valore della valuta che si sta creando non fosse abbastanza alto da compensare i costi.

- La concorrenza: esistono migliaia di diverse criptovalute, con nuovi progetti e token promossi ogni giorno. La barriera all'ingresso è relativamente bassa per i nuovi concorrenti, ma la creazione di una criptovaluta si basa anche sulla realizzazione di un network di utenti che la sostengano.

  Un'applicazione utile sulla blockchain può creare rapidamente una rete di utenti interessati a sostenerla, soprattutto se ne migliora in qualche modo una già esistente.
- La disponibilità sugli exhange: le criptovalute tradizionali come Bitcoin ed Ether vengono scambiate su tantissimi exchange. Quasi tutti gli exchange di criptovalute listano i token più popolari, ma alcuni più piccoli potrebbero essere disponibili solo su mercati selezionati, limitando così l'accesso per alcuni investitori. Più sono piccole le dimensioni dei mercati in cui viene negoziata una certa criptovaluta, più è possibile per l'exchange applicare uno spread alto se decide di listarla.

  Se una criptovaluta viene quotata su più mercati, può aumentare il numero di investitori disposti e in grado di acquistarla, incrementando così la domanda. A parità di condizioni, poi, all'ampliamento della domanda corrisponderà un aumento di prezzo.
- Le regolamentazioni: l'argomento riguardante la regolamentazione dello scambio di criptovalute è sempre stato molto discusso: non è ben chiaro a chi appartenga questo compito. La Securities and Exchange Commission[23] (SEC) afferma che le criptovalute sono titoli come azioni e obbligazioni, mentre la

[23] Securities and Exchange Commission: è un'agenzia governativa statunitense creata dal Congresso per regolamentare i mercati mobiliari e proteggere gli investitori.

Commodity Futures Trading Commission[24] (CFTC) dichiara che sono materie prime come il caffè o l'oro.

Entrambe le agenzie non possono rivendicare l'autorità di regolamentazione sugli scambi di criptovalute. Una sentenza determinante da parte di un organo superiore potrebbe fornire maggiore chiarezza e, di conseguenza, migliorare i valori delle criptovalute, aprendo la porta a prodotti finanziari legati a queste più ampiamente scambiati.

È fondamentale tener conto della natura della tecnologia sottostante queste valute decentralizzate, la quale consente transazioni transfrontaliere senza la necessità di intermediari finanziari.

Inoltre, nuove applicazioni e modelli come tokenizzazione[25], finanza decentralizzata, NFT (token non fungibili) e organizzazioni autonome decentralizzate sfidano i modelli tradizionali, che delineano le "persone", cos'è il "valore" e come quest'ultimo possa essere negoziato. Ciò rischia di entrare in conflitto diretto con le normative esistenti relative ai flussi di dati transfrontalieri, ai diritti di proprietà intellettuale e ai controlli sui capitali. Potrebbe anche comportare ambiguità nell'ambiente fiscale, oltre a porre una serie di ulteriori preoccupazioni politiche.

Le potenziali implicazioni delle criptovalute, per la stabilità finanziaria globale e la natura distintiva della tecnologia sottostante, evidenziano l'importanza di dare priorità alle decisioni normative, sia a livello nazionale che globale.

Secondo il World Economic Forum's Global Future Council on Cryptocurrencies[26], non esiste una regolamentazione coordinata a livello internazionale delle criptovalute, sebbene gli organismi internazionali abbiano lavorato alla valutazione dei rischi e alle risposte politiche appropriate all'ascesa delle stesse.

A livello globale, le banche centrali e le autorità di regolamentazione hanno già gli occhi puntati su questo strumento. Sebbene condividano un obiettivo

[24] Commodity Futures Trading Commission: è un'agenzia indipendente del governo degli Stati Uniti che regola i mercati dei derivati statunitensi, che include future, swap e alcuni tipi di opzioni.

[25] Tokenizzazione: comporta la rappresentazione digitale di asset fisici su registri distribuiti o l'emissione di asset class tradizionali sotto forma di token.

[26] World Economic Forum's Global Future Council on Cryptocurrencies: si tratta di un consiglio progettato per creare una comunità di 30 esperti, al fine di condividere le proprie conoscenze con la rete più ampia del WEF, allo scopo di far progredire la comprensione globale delle criptovalute.

comune, ossia stabilizzare i loro sistemi monetari e stimolare l'innovazione e la crescita economica, paesi come la Cina e El Salvador hanno già iniziato a valutare e attuare diverse opzioni normative. I loro obiettivi sembrano sostanzialmente allineati: proteggere il consumatore e l'integrità del mercato, prevenire i finanziamenti illeciti e promuovere l'innovazione. I loro approcci però sono differenti. Mentre alcune giurisdizioni, come l'India, hanno modificato le leggi esistenti, altre, come il Liechtenstein, hanno proposto modelli su misura. Un altro approccio, apparentemente favorito dall'Unione Europea e dagli Emirati Arabi Uniti, propone di istituire regolatori completamente nuovi per potersi concentrare sul settore a 360 gradi.

Le differenze territoriali, pur offrendo opportunità di arbitraggio giurisdizionale, creano incertezze e un maggiore onere di conformità per le imprese operanti nel settore. Ciò è aggravato dall'assenza di standard e terminologie comuni.

Al fine di attuare un approccio coordinato globale, i paesi e le organizzazioni internazionali dovrebbero lavorare insieme, facendo leva sulle regolamentazioni più efficaci e imparando gli uni dagli altri. Un sistema coordinato a livello globale, che comprende la cooperazione internazionale sulla regolamentazione delle criptovalute, sarà economicamente ottimale, proteggerà i consumatori e preverrà l'abuso di criptovalute per attività illecite.

Oltre alla valutazione del rischio e alla definizione di standard comuni, è anche urgente sfruttare la tecnologia stessa per sviluppare soluzioni adatte allo scopo, attraverso la collaborazione pubblico-privato.

I regolamenti potrebbero anche avere un impatto negativo sulla domanda di criptovaluta: se un organo di governo modificasse le regole per sfavorire l'investimento o l'uso di questi token, potrebbe farne abbassare notevolmente il livello in circolazione.

- La governance: i network di criptovalute raramente rispettano un insieme statico di regole. Infatti, gli sviluppatori adattano i progetti in base alla comunità che li utilizza. Alcuni token, chiamati token di governance, danno voce ai loro titolari in merito a decisioni riguardanti il futuro del progetto, incluso il modo in cui un token viene "estratto" o utilizzato. Per apportare modifiche riguardanti la governance, è necessario che ci sia consenso tra le parti interessate.

Ad esempio, il 15 Settembre 2022, Ethereum ha effettuato il passaggio da un sistema proof-of-work a un sistema proof of stake[27], rendendo di fatto inutili gran parte delle costose apparecchiature minerarie situate nei data center o nelle case dei validatori. Le ragioni che hanno spinto ad effettuate il cosiddetto "Merge" comprendono il risparmio energetico, derivante dal minore consumo rispetto al precedente sistema, e il fatto che il token diventa potenzialmente deflazionistico, attraverso un processo di combustione dell'offerta. Al momento, a dieci giorni da tale data, il valore di Ethereum è sceso, seguendo il trend ribassista del mondo cripto in generale. Molto probabilmente, questo fattore è stato accentuato dal fatto che molti miner, prima occupati nella validazione dei blocchi nel sistema proof of work di Ethereum, hanno convertito la tecnologia in loro possesso, spostandosi su altre blockchain che tuttora supportano questo algoritmo di consenso. Gli impatti di questa svolta epocale, in ambito criptovalute, sono da valutare nel lungo periodo e, non di certo, nel breve periodo con un mercato ribassista da ormai più di nove mesi.

In generale, gli investitori prediligono una governance stabile: infatti, anche se sono presenti difetti nel modo in cui opera una criptovaluta, preferiscono ciò che conoscono all'ignoto. In quanto tale, una governance stabile, in cui non ci sono grossi cambiamenti che scombinano l'equilibrio del progetto, può essere utile per fornire prezzi più solidi.

D'altra parte, il lento processo di aggiornamento del software per migliorare i protocolli può limitare il rialzo dei valori delle criptovalute.

1.6 CRIPTOVALUTE E ANONIMATO

Numerosi sono i falsi miti che incombono su Bitcoin e sulle critpovalute in generale, come ad esempio quello che si tratti di uno strumento ideale per i criminali in quanto anonimo. Ciò corrisponde a un luogo comune che molti media, soprattutto quelli mainstream, hanno diffuso per parecchi anni; ad ogni modo, può crollare facilmente se analizzato.

[27] Proof of stake: algoritmo di consenso distribuito, utilizzato in ambito blockchain, basato sul principio della corrispondenza tra potere decisionale e token messi in gioco.

Bitcoin non è anonimo e anzi, se non viene utilizzato con le dovute precauzioni dal lato della privacy, rispecchia lo strumento esistente più agli antipodi dall'anonimato stesso. Una delle caratteristiche fondamentali della blockchain è, infatti, la trasparenza e l'immutabilità: se un determinato utente compie una transazione di Bitcoin o criptovalute tramite il proprio wallet, questa sarà visualizzabile da chiunque abbia accesso al registro distribuito. Tale operazione rimarrà scritta su di esso per sempre, anche nel caso in cui venissero effettuati scambi successivi di token derivanti da quella specifica transazione.

È vero che all'interno dei dati della transazione non vengono riportati nome e cognome di colui che la effettua, ma è comunque possibile risalirci. La blockchain Bitcoin si definisce "pseudonima", proprio perché non contiene i nominativi degli utenti, ma solamente gli address. Non è presente, inoltre, un limite agli address che un singolo utente può creare e detenere. Difatti, se un soggetto decidesse di essere proprietario di più wallet e, in questi, di movimentarci i Bitcoin o le criptovalute, nel momento in cui dovesse decidere di fare "cash out[28]", dovrebbe utilizzare un exchange. Per fare "cash out" esistono pochi modi, soprattutto nel caso di somme importanti: o si effettuano operazioni peer-to-peer[29], tramite le quali, senza l'ausilio di un intermediario, il soggetto trasferisce i token a qualcuno che lo remunera per queste coin, oppure è necessario l'utilizzo delle piattaforme centralizzate. Quest'ultima soluzione è solitamente la più utilizzata.

Tutte le piattaforme centralizzate devono per legge adottare il processo di KYC[30] obbligatorio, tramite il quale verificano l'identità dei clienti: consente, infatti, alle istituzioni finanziarie di valutare il profilo di rischio dell'utente, in base alla sua propensione alla criminalità finanziaria. Qualsiasi trasferimento di denaro da un wallet cripto ad un exchange, anche se di piccolo importo, collega immediatamente l'identità del soggetto in questione al portafoglio; in questi casi, viene a mancare l'anonimato, che sarebbe garantito dalla blockchain. È sufficiente che ci sia un solo link con una

[28] Cash out: trasformare le criptovalute in denaro FIAT.

[29] Operazioni peer-to-peer: operazioni che permettono il trasferimento di denaro istantaneamente tra persone, tramite una piattaforma digitale.

[30] KYC: "Know your customer" è un processo tramite in quale si raccolgono informazioni sul cliente.

piattaforma centralizzata per permettere di risalire all'identità del possessore delle criptovalute.

Per rimanere completamente anonimi all'interno della blockchain, l'unico modo è "minare" i blocchi e riuscire a validarli, ottenendo le criptovalute come ricompensa, facendole accreditare in wallet che non hanno mai fatto uso del KYC. Al giorno d'oggi, esistono dei software di intelligence che hanno lo scopo di tracciare le transazioni tra i vari portafogli e di fare un'analisi delle identità. Quando ci si iscrive ad un exchange che rispetta la compliance normativa[31], bisogna essere a conoscenza che esso deve, per legge, avere uno di questi servizi di analisi. Viene analizzato tutto il flusso di movimenti effettuati e, nel caso in cui venisse rilevata una transazione sospetta, si verrebbe flaggati[32]. Ciò non corrisponde ad una denuncia alla guardia di finanza o alla polizia postale, ma, a seguito di questa azione, si viene inseriti in una lista di nominativi tenuta sotto controllo da parte delle autorità.

Di norma gli exchanges e le autorità non monitorano le normali transazioni degli utenti; solamente in determinati casi, come ad esempio l'utilizzo improprio della rete, vengono effettuate indagini più approfondite.

È quindi sbagliato affermare che legato al concetto di criptovalute c'è quello di anonimato: devono sussistere delle condizioni molto particolari per cui ricorra questa fattispecie.

Il contante rimane sempre il miglior modo per mantenere l'anonimato.

[31] Compliance normativa: si fa riferimento alla conformità delle procedure interne, con l'obbiettivo di prevenire la violazione di norme di etero regolamentazione e autoregolamentazione, al fine di evitare rischi di incorrere in sanzioni, perdite finanziarie o danni di reputazione.

[32] Flaggare: in gergo informatico significa "segnalare".

CAPITOLO 2

2.0 BLOCKCHAIN

2.1 CARATTERISTICHE

La blockchain, in italiano “registro distribuito”, è un database sincronizzato, replicato e condiviso in rete tra più nodi. È fondamentale il termine “distribuito” in quanto si basa sul concetto della decentralizzazione e quindi non fa riferimento ad un’amministrazione centrale.

Trattandosi di un’infrastruttura decentralizzata non può per definizione dipendere da pochi nodi, motivo per cui deve essere sempre online e raggiungibile. Inoltre, deve essere sicura: si vuole scongiurare la possibilità che qualcuno possa manometterla al fine di modificare informazioni passate. È importante, a tal fine, la trasparenza per permettere a chiunque e in ogni momento la fruibilità del database e la possibilità di visualizzare tutte le informazioni di cui si ha bisogno.

L’unità funzionale della blockchain, l’atomo della stessa, prende il nome di blocco. Se parliamo di blockchain definendola come la spina dorsale delle criptovalute, possiamo pensare ai blocchi come alle vertebre che la compongono. Infatti, concatenati l’uno con l’altro e contenenti le transazioni, danno vita al registro distribuito.

Questi ultimi vengono finalizzati a ritmo costante, in base a quanto definito dal protocollo di riferimento: vengono chiusi, salvati e in seguito aggiunti al database, motivo per cui si può parlare di “battito cardiaco" della blockchain.

Quali sono le caratteristiche del registro distribuito? Procediamo per punti:

2.1.1 Decentramento

Il decentramento è il processo mediante il quale le attività di un'organizzazione, in particolare quelle relative alla pianificazione e al processo decisionale, sono distribuite o delegate lontano da un luogo o da un gruppo centrale autorevole.

Questi concetti sono stati applicati alle dinamiche di gruppo e alle scienze gestionali nelle imprese, nelle organizzazioni private, nelle scienze politiche, nel diritto, nella pubblica amministrazione, nell'economia, nel denaro e nella tecnologia.

Il decentramento fa sì che la blockchain sia distribuita su una moltitudine di nodi, ognuno dei quali contenente tutta la storia del database in versione aggiornata. Non dobbiamo confondere i blocchi con i nodi: i primi raggruppano le voci del registro distribuito, sono concatenati in ordine cronologico e la loro integrità è garantita dall'uso della crittografia. Il blocco contiene un dato numero di transazioni tra quelle in coda, più i dati contenuti in quello precedente. Questo è molto importante per la sicurezza della blockchain: infatti, dal momento che ogni blocco contiene anche i dati di quello antecedente, si crea una serie concatenata di informazioni. Nel caso in cui un attore malevolo volesse modificare, ad esempio, il blocco T-5, dovrebbe alterare anche tutti quelli successivi; altrimenti cambierebbero i dati del T-5, ma il T-4 porterebbe all'interno le informazioni del tempo -4 più quelle veritiere del tempo -5. Un blocco, quindi, più viene incluso negli altri, più ne riceve in coda; di conseguenza è più veritiero, in quanto servirebbe falsificare non solo quello, ma anche tutti quelli successivi per non essere, momentaneamente, colti in fallo. Ogniqualvolta verrà validato un nuovo blocco, esso sarà propagato a tutti gli altri nodi e, solo in seguito, si penserà a produrre e convalidare un blocco successivo.

I nodi, anch'essi fondamentali per la blockchain, consistono in dispositivi di rete, tramite i quali possono essere creati, trasmessi o ricevuti messaggi; possono agire anche come communication endpoint[33]. Sono dotati di un codice identificativo univoco, collegato al proprio dispositivo, il che consente agli utenti di identificare i nodi all'interno della rete. In quanto detentori degli storici delle transazioni, permettono agli utenti del network di

[33] Communication endpoint: è un'interfaccia esposta da una parte comunicante o da un canale di comunicazione.

poter visualizzare i dati relativi alle singole transazioni senza alcuna restrizione. È possibile, in maniera molto semplice, tracciare un'operazione nella blockchain utilizzando il proprio codice identificativo.

La decentralizzazione fa sì che i blocchi siano distribuiti ovunque, il che è importante anche da un punto di vista del consenso: tutti i nodi devono concordare sulla stessa versione del registro. Si tratta di un tema molto importante, soprattutto per quanto riguarda la sicurezza.

Come si mantiene nel tempo la decentralizzazione? Come si fa a non avere un nodo più forte rispetto agli altri? Una maggiore decentralizzazione impone che lo stesso nodo debba avere poche probabilità di validare i blocchi frequentemente. Il tutto dipende dall'algoritmo di consenso che viene utilizzato. Un più elevato numero di nodi porta ad una maggiore decentralizzazione, ma è necessario un incentivo affinché ci siano sempre nuovi utenti che competano per validare sempre più blocchi, evitando il rischio dell'accentramento di potere. Si tratta di una delle difficoltà più grandi degli algoritmi di consenso distribuito.

2.1.2 Sicurezza

Esistono algoritmi di consenso distribuito, come ad esempio il "proof of work" e il "proof of stake", per mettere d'accordo il network su un'unica versione della blockchain. Infatti, non possono coesistere due versioni della stessa, altrimenti vi sarebbe un contenzioso.

La sicurezza è proporzionale alla decentralizzazione e, quindi, al numero di partecipanti al network. Un nodo o un gruppo organizzato di nodi non devono essere in grado di manomettere il registro; in caso contrario, questi utenti potrebbero prenderne il controllo. Ogni diverso algoritmo possiede le proprie caratteristiche per evitare che ciò avvenga.

2.1.3 Trasparenza

Nella blockchain è possibile ripercorrere a ritroso tutte le transazioni, fino ad arrivare all'origine della criptovaluta scambiata. L'Unspent Transaction Output deve necessariamente derivare da un'operazione precedente, a meno che questa non sia l'origine stessa della criptovaluta. La coinbase transaction[34] è quella transazione che

[34] Coinbase transaction: sono le transazioni generate dalla creazione del blocco, non si tratta di scambi di moneta virtuale, ma di ricompense per il lavoro svolto.

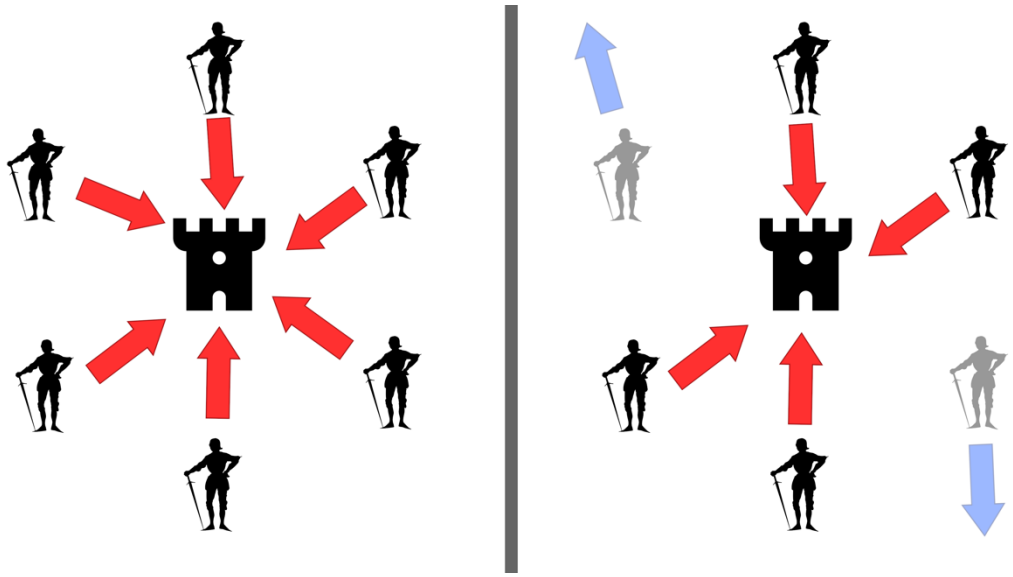
viene generata dalla creazione di un blocco: infatti, la validazione crea una certa quantità di criptovalute. Tutti i movimenti che andiamo a tracciare all'indietro derivano da una coinbase transaction.

Una volta che una transazione viene spesa, solo l'ultimo ricevente può vantarne una unspent, finché non decide di inviarla a qualcun altro. Di conseguenza, ci saranno una serie di transazioni spent, fino ad arrivare ad una unspent, la quale è fondamentale per capire dove si trovano al momento le criptovalute. Il termine "unspent" vuol dire spendibile, mentre "spent" vuol dire speso.

2.2 CONSENSO DISTRIBUITO E GENERALI BIZANTINI

"Il problema dei generali bizantini" è una sorta di indovinello che ci pone di fronte a due possibili scenari riguardanti la distribuzione del consenso, così come avviene nel caso delle blockchain. Sono presenti dei generali bizantini, che si devono coordinare per sferrare un attacco ad una roccaforte.

Figura 2: Bizantine Fault Tolerance.



Fonte: wikipedia.com

Sono possibili due scenari, come possiamo vedere dalla figura 2: il primo è quello in cui tutti i generali sono d'accordo sull'attacco; il secondo, invece, è caratterizzato dal fatto che ci sono alcuni traditori decisi a non assalire.

Un attacco coordinato condurrebbe alla vittoria; invece, nel caso in cui i traditori decidessero di boicottare l'incursione, ci sarebbe il rischio di essere sconfitti dalla roccaforte. In questo caso vi sono due diverse tipologie di attori: i generali non traditori, che vogliono attaccare e sono consapevoli che questo sia l'unico modo per vincere, e quelli traditori, che invece vogliono scappare e salvarsi.

Entrambe le tipologie si trovano assieme nell'attacco, ma, non potendo comunicare con tutti nello stesso momento, potrebbero incappare nella problematica in cui un traditore divulghi false informazioni, convincendo altri generali alla ritirata.

La domanda allora è: quale potrebbe essere un metodo, poste queste condizioni, per coordinare tutti questi generali al raggiungimento di un obbiettivo comune, ossia quello dell'attacco coordinato, al fine di vincere e conquistare la roccaforte?

Questo è passato alla storia come "il problema dei generali bizantini", una problematica più attuale che mai nei sistemi distribuiti[35]. Nella blockchain, ad esempio, è presente una moltitudine di nodi che deve essere d'accordo su un'unica versione della stessa, ossia quella corretta. Anche in questo caso, come nell'indovinello precedente, potrebbero esserci dei "traditori" che vogliono proporre una versione fallace della blockchain per modificare alcune transazioni e permettere, ad esempio, il double spending.

Un sistema centralizzato è caratterizzato da un server centrale: di conseguenza, è come se tutti i generali fossero assieme con il loro comandante, il quale riesce a comunicare con tutti e a ordinare loro come muoversi. Il server centrale, infatti, coordina tutti i suoi nodi e impone la sua versione dei fatti; ma possiede tutta la serie di debolezze precedentemente indicate.

Il sistema decentralizzato, d'altro canto, è una via di mezzo dove sono presenti alcuni nodi con dei nodi "figli": allora, l'importante è coordinare quelli intermedi, in quanto saranno loro poi a organizzare tutti gli altri.

Il nostro caso è quello del sistema distribuito, ossia un sistema "peer to peer[36]", in cui tutti i nodi comunicano tra loro, o meglio dove tutti dovrebbero in qualche modo farlo.

[35] Sistema distribuito: è un sistema con più componenti situati su hardware diversi che comunicano e coordinano le azioni in modo da apparire all'utente finale come un unico sistema coerente.

[36] Sistema peer to peer: è un modello di comunicazione decentralizzato in cui ciascuna parte ha le stesse capacità e ciascuna parte può avviare una sessione di comunicazione.

In realtà non è, ora come ora, possibile che ogni singolo nodo della blockchain Bitcoin istantaneamente parli a tutti gli altri, ma è quello a cui si ambisce. Se fosse già stato implementato, non sarebbe possibile mantenere il livello di comunicazione, velocità e scalabilità[37] di cui disponiamo ora. A noi interessa estremamente questo argomento ed è proprio il problema che si pone come obbiettivo la blockchain, ossia quello di riuscire a coordinare tutti i nodi verso un'unica soluzione e ciò che permette di farlo è la creazione e l'applicazione nel network degli algoritmi di consenso distribuito.

Il consenso distribuito ha come scopo, infatti, quello di mettere d'accordo tutti i nodi partecipanti su un'unica versione del registro. Chiaramente non si tratta di un'impresa banale, dal momento in cui vi sono alcuni problemi su cui riporre l'attenzione: primo tra tutti è capire a chi attribuire la ragione in caso di contenziosi. Nel momento in cui, ad esempio, avessimo tre versioni della blockchain, come sarebbe possibile individuare quella corretta? Un'altra domanda potrebbe essere quella che ci si pone quando si deve capire come trovare una versione obiettivamente giusta di questo registro distribuito. È figlia della prima questione, ma è fondamentale comprendere come decidere arbitrariamente quale sia la versione veritiera e quali siano i criteri attraverso i quali possiamo effettuare questa scrematura. È essenziale, inoltre, comprendere come concedere a tutti la possibilità di partecipare equamente a questo consenso, al fine di evitare di incappare nel modello centralizzato. Infine, come evitare che degli attori malevoli, che vogliono proporre una versione differente da quella veritiera della blockchain, influenzino il processo di consenso? Si tratta di domande a cui devono rispondere i vari algoritmi di consenso; molti hanno tentato a farlo, ma solo alcuni ci sono riusciti.

Esistono una miriade di algoritmi di consenso distribuito, i più famosi sono sicuramente:

- Proof of Work: Bitcoin, Ethereum fino al 15 Settembre
- Proof of Stake: Polygon, Elrond, Ethereum dal 15 Settembre.
- Proof of Authority: Vechain.
- Proof of History: Solana.
- Proof of Capacity: Chia.

[37] Scalabilità: la caratteristica di un sistema software o hardware facilmente modificabile nel caso di variazioni della mole o della tipologia dei dati trattati.

È importante comprendere i meccanismi di funzionamento dei primi due per poter capire come opera la stragrande maggioranza delle criptovalute.

2.2.1 Resistenza al 51% attack

Il metodo pensato dal protocollo Bitcoin per superare il problema dei generali bizantini è quello di mettere d'accordo tutti i nodi su un'unica versione della blockchain. Il tutto si basa sulla competizione e sullo sforzo computazionale: difatti, si tratta di un sistema in cui la meritocrazia regna sovrana. Bisogna dimostrare di essere giunti al traguardo attraverso uno sforzo maggiore rispetto agli altri.

La versione della blockchain più lunga, quella fornita dal miner che convalida il nuovo blocco, è quella corretta e che deve essere accettata da tutti.

Questo meccanismo impone che, nel caso in cui ci fosse un nodo malevolo, con la maggioranza dell'hash rate[38], riuscirebbe a validare la maggior parte delle volte i blocchi; infatti, statisticamente, sarebbe sempre questo nodo a trovare per primo la soluzione. Affinché il problema dei generali bizantini venga risolto a favore dei nodi non malevoli, la percentuale di non traditori deve essere maggiore del 51%. Maggiore è la decentralizzazione, minore è il rischio che vi sia un aggregato di utenti o macchine che detenga un potere prevaricante sul network. Si tratta di una situazione che non dovrebbe mai verificarsi, pena la stabilità della blockchain.

Ci sono stati degli attacchi 51% su blockchain, ma Bitcoin ha un hash power[39] talmente alto da renderne quasi impossibile il crollo. Per compiere un 51% attack su Bitcoin, infatti, servirebbe avere la maggioranza tra i 200 milioni di tera hash al secondo che la blockchain sviluppa e questo tipo di aggressione avrebbe un costo non sostenibile da una persona o un'istituzione.

Più cresce l'hash power complessivo e più Bitcoin diventa sicuro, dal momento che, per attuare un takeover[40], serve sempre più energia e, di conseguenza, economicamente non ne varrebbe la pena. Infine, dopo essere stato individuato, il miner maligno verrebbe inoltre cacciato dal network.

[38] Hash rate: capacità nella rete di una criptovaluta di risolvere enigmi crittografici.
[39] Hash power: potenza di hash.
[40] Takeover: atto volto ad assumere il controllo di qualcosa.

Esistono registri distribuiti come Ethereum Classic[41] che hanno subito il 51% attack e non sono mai crollate, rimanendo tuttora in vita.

2.3 PROOF OF WORK

Il "proof of work" è un algoritmo che basa i propri presupposti sul lavoro e sulla fatica, come vedremo prossimamente si tratta di uno dei più grandi esempi di meritocrazia.
In questo algoritmo di consenso distribuito ogni nodo propone la propria versione della blockchain, utilizzando, al fine della dimostrazione della veridicità, il lavoro che ha svolto. Difatti, ciascuno palesa di aver dedicato una certa potenza di calcolo alla creazione della propria versione del registro e il risultato che ne consegue funge da validazione.
I nodi competono, ognuno con la propria proof of work, per poter risolvere il problema relativo alla validazione dell'ultimo blocco della catena, quello che, al momento, è da finalizzare. Chi per primo riuscirà a trovare la soluzione e, di conseguenza, a convalidare il nuovo blocco, ne avrà uno in più rispetto agli altri. Avendo una catena più lunga a confronto di quella degli altri nodi, nel momento in cui verrà accertata l'effettiva risoluzione del problema, egli verrà accettato univocamente dal network come "vincitore".
I partecipanti al network devono poter provare di aver svolto il lavoro per chiudere questo blocco e dimostrare di non aver aggirato il consenso distribuito e, di conseguenza, di avere la "skin in the game[42]".
Il processo consistente nella validazione dei blocchi da parte dei nodi del network è chiamato "mining". Per capirne i meccanismi di funzionamento, bisogna innanzitutto comprendere come opera l'hashing.
L'hashing è quel procedimento che, partendo da un input di dimensioni variabili, utilizza funzioni matematiche, come quelle di hash, per generare un output di dimensione fissa. Queste funzioni non necessariamente implicano l'uso della crittografia, ma quelle crittografiche sono alla base delle criptovalute. Esse permettono di raggiungere ottimi

[41] Ethereum Classic: è la blockchain parallela ad Ethereum, il 20 luglio 2016 ha dichiarato la sua indipendenza dal progetto originale.
[42] Skin in the game: avere un investimento personale in un'organizzazione o impresa e, quindi, un interesse acquisito nel suo successo.

livelli di sicurezza dei dati e integrità per quanto riguarda la blockchain e i sistemi distribuiti in generale.

Una delle caratteristiche principali di tutte le funzioni di hash è che sono deterministiche: ogniqualvolta noi inseriamo uno stesso input, la funzione ci restituirà sempre il medesimo output. Un'ulteriore peculiarità è che gli algoritmi di hashing delle criptovalute sono funzioni unidirezionali[43]: è relativamente semplice creare l'output dall'input, ma risulta molto difficile generare l'input partendo solo dall'output. Più è complicato concludere questo secondo passaggio, più è considerato sicuro tale algoritmo.

Esistono varie funzioni di hash, le quali produrranno output di dimensioni differenti, ma per ciascun algoritmo le grandezze di quest'ultimi saranno sempre le medesime.

Ad esempio, l'SHA256[44], ossia l'algoritmo utilizzato da Bitcoin, produrrà sempre output a 256 bit, mentre l'SHA1 produrrà sempre output a 160 bit.

Per dimostrare in maniera pratica quanto appena detto, possiamo affidarci a dei simulatori di hash online.

Il più utilizzato è il seguente sito: https://emn178.github.io/online-tools/sha256.html, nel quale possiamo inserire un input e, attraverso la funzione SHA256, verrà generato un output.

Si possono prendere come esempio due parole che differiscono solamente per una lettera maiuscola, ossia "Bitcoin" e "bitcoin".

Tabella 1: L'output dell'SHA256.

SHA256	
Input	Output (256 bit)
Bitcoin	b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4
bitcoin	6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b

Fonte: SHA256 online.

[43] Funzione unidirezionale: funzione per la quale il calcolo in una direzione è semplice, mentre il calcolo nella direzione inversa è molto più difficile.

[44] SHA: Safe Hash Algorithms.

Possiamo notare come una variazione dal carattere maiuscolo a quello minuscolo di una sola lettera ci restituisca un valore di hash completamente differente. Utilizzando lo SHA256, gli output presenteranno sempre una dimensione di 256 bit, indipendentemente dalla lunghezza dell'input. Questa operazione possiamo ripeterla infinite volte, ma il prodotto riportato sarà sempre il medesimo.

Non bisogna pensare che le funzioni di hash vengano utilizzate solo nell'ambito delle criptovalute; al contrario, possiedono una vasta gamma di casi d'uso tra cui: la gestione dei dati, la ricerca in database e l'analisi di grandi file. Per quanto concerne Bitcoin, però, tali funzioni sono una caratteristica essenziale riguardo il processo di mining e hanno un ruolo fondamentale nella creazione di nuovi indirizzi e chiavi.

Il gran potere di cui l'hashing dispone può essere osservato quando ci si rapporta con enormi quantità di informazioni da gestire. Grazie alla natura deterministica, possiamo, ad esempio, elaborare un grande database e usare il suo output per verificare l'integrità e l'accuratezza dei dati. Questa tecnica permette di rimuovere la necessità di archiviare grandi quantità di nozioni.

La blockchain di Bitcoin è caratterizzata da diverse operazioni che dipendono dall'hashing, gran parte delle quali si trovano all'interno del processo di mining. Quasi tutti i protocolli di criptovaluta basano il collegamento e l'archiviazione delle transazioni nei blocchi su questo algoritmo.

Per riuscire a "invertire" una funzione crittografica di hash è necessario indovinare l'input, con innumerevoli tentativi, fino a quando non viene prodotto l'output corrispondente. È necessario, però, sapere che sussiste la possibilità che lo stesso output sia restituito da diversi input: in questo caso avviene la cosiddetta "collisione[45]".

Una funzione crittografica di hash deve possedere tre proprietà per essere effettivamente sicura: la resistenza alle collisioni, alla pre-immagine e alla seconda pre-immagine.

- Resistenza alle collisioni: deve essere computazionalmente intrattabile la ricerca di una coppia di stringhe di input che diano lo stesso hash come output. Di conseguenza, dati due input "m1" e "m2" deve risultare difficile che abbiano lo stesso output di hash, ossia che si crei una collisione. Un algoritmo di hash si

[45] Collisione: una collisione di hash è una corrispondenza casuale nei valori di hash che si verifica quando un algoritmo produce lo stesso valore di hash per due distinti input di dati.

definisce resistente se la possibilità di trovarne una è talmente bassa che sarebbero necessari svariati anni di computazioni per riscontrarla.

Nonostante non esistano nella realtà funzioni di hash che possano contrastare completamente le collisioni, alcune di queste sono abbastanza solide e, per tale ragione, vengono considerate comunque alquanto resistenti.

- Resistenza alla pre-immagine: deve essere computazionalmente intrattabile la ricerca di una stringa di input che dia un output di hash uguale ad un dato hash. Pertanto, dato un valore di hash "h" deve risultare difficile risalire ai vari messaggi "m" con "hash(m) = h". Tale proprietà deriva dal concetto di funzione unidirezionale.

  È una proprietà assai importante, in quanto un semplice prodotto di hash può dimostrare l'autenticità di un soggetto, senza dover rivelarne informazioni personali.
- Resistenza alla seconda pre-immagine: deve essere computazionalmente intrattabile la ricerca di una stringa di input che dia un hash uguale a quello di un'altra data stringa. Perciò, dato un input "m1" deve risultare estremamente complesso trovare un secondo input "m2" tale che "hash(m1) = hash(m2)".

Facendo nuovamente riferimento al mining, il blocco da validare contiene tutte le transazioni compiute in un periodo; se, però, dovessero superare un determinato numero, entrerebbero nel blocco successivo.

Il sistema delle fees[46] prioritizza chi è disposto a pagare più commissioni ai miner, ma questo argomento lo tratteremo in modo più approfondito in seguito. Il blocco al tempo T contiene tutte le transazioni "attuali" e la storia completa di quelle passate, rappresentata dal blocco T-1. Il riferimento del blocco precedente altro non è che l'hash del blocco T-1.

In definitiva, il miner elabora il blocco antecedente attraverso la funzione di hash, la quale poi genererà una sequenza alfanumerica, che corrisponde all'output del blocco T-1 e che sarà inserita all'interno del blocco T.

Ponendo il caso che qualche malintenzionato voglia manomettere il contenuto del blocco T-1, cambiando completamente l'hash del blocco stesso, modificherebbe anche

[46] Fee: commissione.

quello del blocco T, in quanto contenente quello precedente. Di conseguenza, dovrebbe riuscire nello stesso tempo a modificare tutti i blocchi successivi, senza essere scoperto. Più si vuole andare a ritroso con la modifica dei blocchi, maggiore sarà il numero di quelli successivi con valori di SHA256 da modificare.

Nel momento in cui qualcuno si accorgesse di tale modifica, la catena si romperebbe e sarebbe necessario creare dei nuovi blocchi a partire dal primo invalidato. Questa è la peculiarità derivante dal concatenamento dei blocchi.

Oltre alla parte fissa, contenente le transazioni al tempo T e l'hash del blocco T-1, è presente anche una variabile da fare elaborare alla funzione di hash durante il processo di mining. Esso, infatti, consiste nell'elaborazione di tante operazioni di hash per trovare un output compreso all'interno di una soglia determinata all'interno del protocollo del registro distribuito. Se ci fosse solo una parte fissa, l'hash sarebbe sempre lo stesso e tutti avrebbero sempre la medesima risposta dalla funzione. Necessario è quindi aggiungere una variabile al fine di permettere una competizione tra tutti i nodi in maniera casuale, senza decidere un vincitore ancora prima che questa venga attuata. Ognuno deve dimostrare di partecipare attivamente al network, spendendo energia. Con un algoritmo di questo tipo, solamente attraverso il dispendio di energia e la creazione di lavoro, c'è la possibilità di dimostrare di aver raggiunto l'obiettivo.

Lo scopo è, quindi, quello di trovare un hash che sia minore di un determinato valore, deciso in base alla difficoltà, ossia ad un parametro variabile che, più è maggiore, più sarà difficile risolvere il problema.

Nel momento in cui qualcuno reclama di aver trovato la soluzione, la verifica

è semplice e veloce: quando viene comunicato l'input, che dovrebbe aver fornito un determinato output, è sufficiente inserirlo all'interno della funzione di hash per verificare se il blocco sia stato correttamente validato.

Il lavoro del miner è faticoso, non dal punto di vista della forza fisica impiegata, ma da quello della quantità di energia spesa per cercare la soluzione alla funzione di hash. Lo sforzo apportato da questi soggetti è misurato in tera hash al secondo; tenendo presente che 1 tera corrisponde a 10 elevato alla dodicesima e, inoltre, sapendo che il network utilizza 200 tera hash al secondo, è possibile avere un'idea della quantità di operazioni svolte da questi elaboratori.

Tutta questa potenza computazionale necessita di altrettanta energia per permettere ai miner di poter operare nella rete. È fondamentale tener presente che questi soggetti non lavorano al solo scopo di favorire l'ascesa di questo strumento rivoluzionario, ma prima di tutto, per interesse personale. Proprio per questo motivo, un sistema efficiente deve incentivare la partecipazione, principio per cui la blockchain di Bitcoin promuove il lavoro con la creazione e la conseguente assegnazione di nuovi Bitcoin ai validatori dei blocchi.

Negli anni, l'hash rate totale ha avuto una crescita generale; inoltre, più questo aumenta, più di conseguenza cresce la difficoltà di validazione dei blocchi.

Maggiori sono i miner presenti nel network, minore è la tempistica per riuscire a trovare il nonce[47] giusto; efficace per comprendere questo concetto è il paragone con l'urna. Immaginiamo di avere un'urna di diametro infinito e un determinato numero di persone che pescano risultati da questa; il tempo per trovare un numero inferiore ad una soglia prefissata è completamente diverso in base alla quantità di persone presenti. Nel caso della blockchain, lo sforzo non dipende dal numero di miner, ma dalla sommatoria della potenza di tutti gli elaboratori.

Il parametro della difficoltà, ossia il nonce, è molto importante: se fosse rimasto sempre la stesso, con gli hardware di cui disponiamo attualmente, in qualche secondo si riuscirebbe a trovare l'hash adeguato e in poco tempo si creerebbe una quantità di blocchi infinita.

Bitcoin possiede una regola, ossia quella secondo cui tra un blocco e il successivo deve esserci un distacco temporale di dieci minuti. Conoscendo il valore dell'hash rate, la difficoltà si deriva con un semplice calcolo. Nel caso in cui l'hash rate e, di conseguenza, la potenza computazionale, che lavora sulla blockchain di Bitcoin, aumenti, sarà necessario incrementare anche la difficoltà di risoluzione dell'SHA256. Quest'ultima, infatti, è un parametro che periodicamente viene reimpostato in base alla formula che è all'interno del codice sorgente di Bitcoin.

In questo modo si rende la criptovaluta stabile rispetto alle oscillazioni di hash rate, come ad esempio nell'episodio dell'esodo della Cina, risalente al 2021. Lo scorso anno, difatti, il mining è stato bandito dalla Cina e i blocchi inizialmente venivano validati con

[47] Nonce: " number that can only be used once" è un numero arbitrario utilizzato all'interno dei cosiddetti protocolli di autenticazione.

tempistiche più elevate, non essendo ancora diminuita la difficoltà, contrariamente all'hash rate. Di conseguenza, meno persone lavoravano sulla blockchain e quelle rimaste dovevano adoperarsi maggiormente. Una volta "aggiustata" la difficoltà, però, tutto è tornato perfettamente a regime.

Riprendendo i concetti importanti sopraindicati, abbiamo compreso che, in linea generale, l'hash rate continua ad aumentare di valore e che c'è sempre più competitività per trovare l'output che permetta di avere la catena più lunga rispetto agli altri nodi del network.

Minare i Bitcoin da soli è pressoché impossibile; inizialmente, l'erogazione corrispondeva a 50 Bitcoin per blocco minato, dopodiché si è passati a 25, 12,5 e via via questo valore è stato dimezzato. Non è pensabile che un soggetto detenente anche dieci calcolatori continui a svolgere questa attività individualmente con la speranza di trovare l'output di hash che gli permetta di validare un blocco, così da poter ottenere la propria ricompensa. Svolgendo semplici calcoli, si nota che la probabilità di minare un blocco, data la potenza di calcolo totale, anche per il più potente miner, è davvero bassa. Esistono per questa ragione i mining pool: gruppi di miner che si aggregano all'interno di uno stesso pool. Unendosi, sono in grado di essere più competitivi e di avere maggiore probabilità di ottenere una ricompensa, che successivamente si divideranno in base allo sforzo computazionale apportato. Inoltre, il creatore di un mining pool solitamente trattiene una percentuale sul totale a fronte del coordinamento dei vari nodi.

La domanda che potrebbe sorgere spontanea è la seguente: questa non risulta essere una forma di centralizzazione? Se il pool dovesse comportarsi in maniera malevola, i piccoli miner potrebbero facilmente abbandonare il gruppo e trasferire il loro hash power altrove. Quindi, il mining pool non ha incentivo a comportarsi in modo scorretto, altrimenti, se lo facesse, perderebbe la fiducia deposta dai piccoli miner.

Tutte le transazioni in criptovaluta sono registrate in modo permanente sulla blockchain. La validazione e la protezione di queste transazioni su ciascuna rete richiedono hardware altamente specializzati, responsabili dell'aggiunta dei blocchi sui rispettivi registri. Poiché tali reti sono protette e gestite da "volontari", le commissioni sono ciò che rendono utili gli sforzi dei "minatori" e dei validatori.

Ogni blockchain è diversa, ma tutte hanno un numero limite di transazioni che possono rientrare in un blocco. Ad esempio, ciascun blocco su quella di Bitcoin può contenere

circa 2.800 operazioni. Le commissioni dei “minatori” possono variare a seconda di quante transazioni sono in attesa di essere aggiunte. Durante i periodi di traffico di rete elevato, i miner danno la priorità alla convalida di nuove transazioni in base all’importo di queste commissioni. Gli utenti che desiderano completare l’operazione più rapidamente possono persino incrementare il valore delle commissioni per aumentare le possibilità di essere inclusi nel prossimo blocco disponibile.

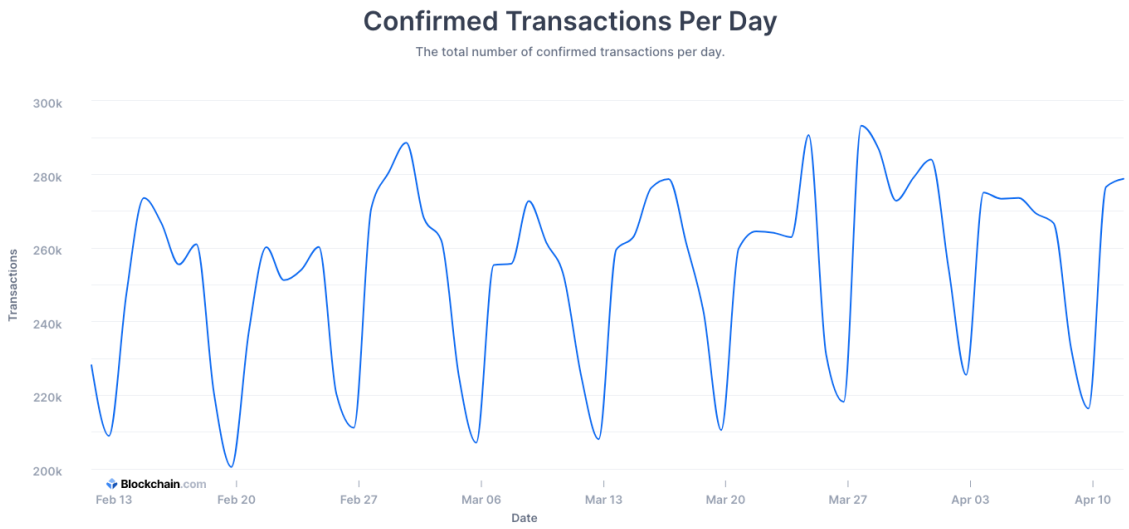
Gestire un'attività che valida le transazioni crittografiche costa denaro e le commissioni di servizio, sostenute dagli utenti, sono la principale fonte di reddito per coloro che si occupano di fornire questo servizio. Corrispondono al costo di “fare affari" e sono una percentuale di qualsiasi operazione avviata; variano notevolmente in base a una serie di fattori, come il tipo di transazione, il metodo di pagamento e la blockchain su cui viene effettuata la transazione.

È probabile che l'ora del giorno in cui venga effettuata la transazione in criptovaluta abbia un impatto significativo su ciò che si pagherà poi di commissioni: si possono evitare i picchi di utilizzo delle reti blockchain quando le commissioni di transazione sono al massimo. Allora qual è il momento migliore per evitare tasse elevate dei miner? Generalmente tali reti tendono ad essere più occupate durante le ore in cui la popolazione degli Stati Uniti è attiva, poiché è lì che si trova la più grande concentrazione mondiale di utenti di criptovaluta. Inoltre, i fine settimana mostrano meno attività, in particolare il sabato. Sono numerose le risorse online che forniscono dati sul traffico di rete per le varie blockchain, in modo da poter visualizzare in tempo reale quante transazioni sono in coda e farsi un’idea sulla cifra da pagare in commissioni.

Non dimentichiamo, come detto in precedenza, che la velocità con cui si desidera che la propria transazione venga verificata influirà sulle commissioni che si pagheranno. Infatti, nel caso in cui possedessimo una transazione ad alta priorità e desiderassimo che venisse confermata più rapidamente possibile, ci dovremmo aspettare una commissione di servizio maggiore. Se, invece, la validazione non è urgente, un tempo di verifica più lento corrisponderà ad una commissione di transazione inferiore. Ogni volta che si inviano pagamenti dal portafoglio Binance, ad esempio, si ha la possibilità di scegliere la velocità di transazione desiderata e controllare l'importo delle FEES che pagheremo.

Come accennato, proprio come per il sistema dei trasporti, le reti di criptovalute sono soggette a periodi di traffico elevato, durante i quali le transazioni rallentano e le commissioni aumentano. I conducenti, cercando di evitare di rimanere bloccati nel traffico, possono scegliere di programmare il viaggio per evitare l'ora di punta o utilizzare mezzi di trasporto più efficienti. Allo stesso modo, gli utenti che utilizzano le criptovalute possono monitorare il numero di transazioni in coda, utilizzare monete o protocolli alternativi e confrontare le tariffe tra i fornitori, per pagare una percentuale inferiore sulle commissioni dei miner.

Figura 3: Numero di transazioni validate per giorno.



Fonte: Blockchain.com

La questione energetica relativa al mining è stata molto dibattuta negli ultimi tempi. Non si può di certo negare l'evidenza, ossia il fatto che il business con il quale si creano criptovalute consumi un'elevata quantità di energia; ma è fondamentale valutare l'importanza della finalità di questo impiego. È sicuramente sbagliato parlare dell'energia utilizzata da questi calcolatori come risorsa sprecata; certamente si potrebbe anche evitare di consumarla, ma al fine dell'utilizzo delle criptovalute è necessario giungere a compromessi. Il fine è quello di proteggere un registro decentrato, un network che permette di transare in tutto il mondo queste monete virtuali tramite blockchain. Ricordiamoci che senza questo tipo di energia non potrebbe esistere nessun

genere di registro distribuito e, di conseguenza, alcuna sorta di moneta elettronica decentralizzata.

Una ricerca di Glaxy Digital[48] ha confrontato il costo di estrazione di Bitcoin con quello dell'oro e il sistema bancario. Questa comparazione deriva dal fatto che si è voluto mettere a confronto il consumo energetico proveniente dal mining con l'estrazione dell'asset.

È innegabile il fatto che il network legato al mining utilizzi un'elevata quantità d'energia, analizzando però i consumi del sistema bancario si è stimato un impiego di 250 tera wattora. L'utilizzo energetico complessivo stimato dell'industria dell'estrazione dell'oro è di 200 tera wattora, mentre quello di Bitcoin è di circa 100 tera wattora.

Paragonando il valore delle transazioni che vengono gestite dal sistema bancario e quelle che vengono condotte dalla blockchain di Bitcoin, certamente le prime hanno un valore molto più elevato rispetto alle seconde. Il consumo energetico di Bitcoin, però, non muta al variare del valore delle operazioni sul network; infatti, esso dipende dalla potenza complessiva dei miner che partecipano alla rete. Nel caso in cui venisse transato un volume pari a 10 dollari, a livello di consumi energetici non ci sarebbe alcuna differenza rispetto ad una operazione comprendente 10 trilioni di dollari.

Bitcoin potrebbe diventare uno dei veicoli che incentiva ad investire nell'energia rinnovabile, ma, al momento, essendo il suo mining un business, tende ad approvvigionarsi nel modo meno costoso possibile. Nel caso in cui, ad esempio, ci fosse l'opportunità di rifornirsi tramite combustibili fossili a costo bassissimo, purtroppo la preferenza sarebbe per questa opzione, in quanto oggigiorno non è ancora possibile disporre di fonti di energia rinnovabile su larga scala.

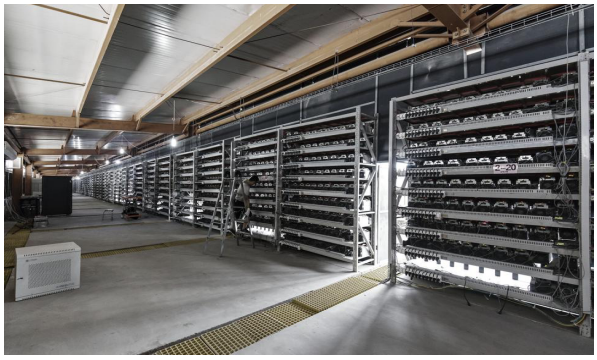
Sono numerose le aziende americane che fanno mining con grossi investitori alle spalle, per poi definirsi "aziende green", sia per il trend di transazione che si allontana dai combustibili fossili e sicuramente anche per determinati benefici legati all'ambito ESG[49].

Invece di ostacolare Bitcoin sarebbe più opportuno trovare delle valide alternative affinché questa evoluzione non danneggi l'ambiente in cui viviamo, anche perché, come dimostrato, ci sono attività che inquinano molto di più.

[48] Galaxy digital: uno dei fondi d'investimento più importanti nel settore di asset digitali.
[49] ESG: Environmental, Social and Governance.

Non si può negare che Bitcoin consumi parecchia energia, ma, appurato questo fatto, bisogna far in modo che le risorse che vengono utilizzate siano per quanto possibile ricavate attraverso fonti rinnovabili.

Figura 4: Una centrale di mining in Cina.



Fonte: forbes.com

Figura 5: Una centrale di mining a Milano.

Fonte: forbes.it

Esistono, inoltre, ulteriori soluzioni tecnologiche a bassissimo impatto energetico come il lightning network[50], che ha lo scopo di superare il limite fisico della dimensione dei blocchi. Si tratta di un livello secondario sulla blockchain che consente agli utenti di creare canali di pagamento, in cui le transazioni, note come “fuori catena”, possono avvenire lontano dal registro distribuito principale, beneficiando comunque della sicurezza e della decentralizzazione. Questa soluzione offre velocità, risparmio sui costi e scalabilità all'intera rete.

Il lightning network si basa su smart contract che originano canali di pagamento esterni alla chain principale; questa possibilità è data a tutti e, una volta aperto il canale, si può effettuare un numero illimitato di operazioni. Le transazioni, in questo livello secondario, avvengono istantaneamente e ad un prezzo assai inferiore rispetto al costo che avrebbero sulla blockchain, tenendo conto delle fees. Il canale di pagamento secondario ha un proprio registro in cui le transazioni vengono annotate, lontano dalla blockchain principale.

Nel momento in cui le parti decidono di chiudere il lightning network, tutte le operazioni avvenute all'interno di questo registro vengono consolidate e quindi trasmesse a quello della blockchain principale. Senza canali di pagamento come questo, le innumerevoli

[50] Lightning network: è un protocollo di pagamento di "livello 2" sovrapposto a Bitcoin.

transazioni di piccoli importi rischierebbero di ostacolare quelle più grandi, rallentando l'operatività della blockchain.

Indubbiamente non è vietato effettuare operazioni di importo piccolo all'interno della rete principale, ma probabilmente si pagherebbero commissioni troppo elevate. Invece, con il lightning network le uniche fees che si corrispondono riguardano l'apertura e la chiusura del canale di pagamento.

La combinazione di pagamenti effettuati tramite la blockchain principale e il canale secondario si traduce in un'esperienza di versamento complessivamente migliore, poiché veloce, a basso costo e scalabile. La rete lightning è in grado di gestire un milione di transazioni al secondo, mentre la blockchain principale di Bitcoin solamente circa sette operazioni al secondo.

Il canale di pagamento secondario fornisce un metodo per effettuare versamenti di qualsiasi entità, anche a intervalli regolari. Ciò incentiva ad effettuare micro-corresponsioni quotidiane in criptovaluta, come per l'acquisto di un caffè, una pizza o qualsiasi altro bene o servizio che è possibile acquistare tramite token.

Il lightning network, inoltre, consente agli utenti di muoversi liberamente attraverso i vari canali di pagamento: se l'utente A è collegato al soggetto B e quest'ultimo è connesso all'individuo C, A può effettuare dirette transazioni con C senza creare un nuovo registro di transazioni.

2.4 PROOF OF STAKE

Il modello proof of stake offre ai possessori di criptovalute un modo per utilizzare le proprie risorse digitali e guadagnare entrate passive[51], senza doverle vendere. Si tratta di uno dei concetti più mal interpretati in ambito blockchain e addirittura c'è chi, ogniqualvolta si generi una rendita passiva, parla impropriamente di staking.

Lo staking può essere paragonato all'equivalente crittografico del versamento di denaro in un conto di risparmio ad alto rendimento. Nel momento in cui si depositano fondi in un conto di risparmio, la banca utilizza quei soldi e, in genere, li concede ad altri soggetti sotto forma di prestito. In cambio di questo versamento, vengono corrisposti una parte degli interessi maturati dal prestito, anche se in percentuale molto bassa.

[51] Entrate passive: attività che consentono di guadagnare senza lavorare attivamente.

Allo stesso modo, quando si mettono in staking le proprie risorse digitali, si mettono in gioco i propri token per partecipare alla gestione della blockchain e al mantenimento della sua sicurezza. In cambio si guadagnano premi, calcolati in percentuale al rendimento; questi profitti sono in genere molto più elevati di qualsiasi altro tasso di interesse offerto dalle banche.

Questo processo è diventato un metodo comune per realizzare un guadagno in criptovalute senza necessariamente scambiare monete. Ad aprile 2022, il valore totale delle coin in gioco ha superato la soglia di $ 280 miliardi, secondo Staking Reward[52].

Spesso impropriamente si ritiene che, nel momento in cui si detengono i propri token sugli exchanges, li si sta mettendo in staking, ma ciò non ha niente a che vedere con il vero significato della parola.

Esso consiste nel prendere parte attivamente alla messa in sicurezza di una blockchain con un algoritmo di consenso di tipo proof of stake. Anche in questo caso, è fondamentale tenere a mente il "problema dei generali bizantini" e del consenso distribuito, dal momento che tutti gli algoritmi di consenso, in generale, si occupano di scovare metodologie per mettere d'accordo i vari network su una stessa versione dei registri.

Ogni nodo della rete deve dimostrare di avere la "skin in the game" nel mantenimento della sicurezza, validando e proponendo nuovi blocchi. Nel caso del proof of work ciò si traduce nel consumo di energia, mentre in quello del proof of stake la dimostrazione non è il work, ma lo stake. Questo termine deriva dal mondo del gioco d'azzardo, infatti, mettendo in palio qualcosa, lo si mette in "stake", ossia in gioco. Infatti, gli utenti partecipano attivamente al processo decisionale di validazione dei blocchi di un registro distribuito di questo tipo, mettendo in gioco alcune delle proprie coin; da ciò deriva il termine "mettere in staking".

La blockchain opera in questo modo: se un nodo mette in gioco una quantità elevata di token, avrà quasi sicuramente interesse a far in modo che il network funzioni correttamente, per non subire una perdita ingente. Supponiamo che un utente abbia messo in staking il 20% di criptovalute totali circolanti nel network, nel caso in cui si trovasse un errore nella validazione o il protocollo non funzionasse correttamente, la

[52] Staking Rewards: il principale fornitore di dati sullo staking e strumenti per la cripto-crescita.

coin perderebbe valore e, di conseguenza, il nodo verrebbe danneggiato in modo importante. Questo corrisponde al primo principio su cui si basa il concetto di proof of stake: più un soggetto ha token "at stake", più è direttamente coinvolto in caso di successo o insuccesso del sistema. Sono presenti anche ulteriori incentivi e deterrenti per i partecipanti ad un network con questo algoritmo di consenso, come a breve illustreremo.

È essenziale, dunque, comprendere che, in questo algoritmo di consenso distribuito, un nodo vincola i propri token, li mette in gioco e, successivamente, ottiene un potere di voto proporzionale alla quantità di coin messi in staking. A chi possiede più monete virtuali, è attribuito un potere decisionale maggiore e, di conseguenza, più probabilità di essere scelto come validatore di un blocco. Vi è, quindi, proporzionalità tra rischio e potere.

L'algoritmo più utilizzato è sicuramente il Tendermint BFT, la cui sigla sta a indicare "Bizantine Fault Tolerant", in quanto questo sistema proof of stake è stato ideato per tollerare e resistere anche ad eventuali "generali bizantini traditori". Tendermint, utilizzato ad esempio dalla blockchain Terra, è caratterizzato dalla scelta del block producer, ossia di quell'utente che avrà l'onere di creare e propagare il blocco. Tale selezione è "randomica" e dipende dal voting power che i vari validatori possiedono. Corrisponde, quindi, ad un'estrazione aleatoria del block producer, con probabilità pesata per il potere di voto di ogni singolo nodo o gruppo di nodi. Nel caso in cui vi fosse un validatore con un voting power dello 0.01% e un altro con il 10%, ovviamente verrà estratto molto più frequentemente il soggetto che possiede potere di voto maggiore.

Il block producer, avendo l'onere di creare e propagare il blocco, deve raggruppare le transazioni in coda in uno nuovo, includendo, come nel caso della blockchain basata sul proof or work, quello precedente. Una volta eseguito ciò, propagherà il nuovo blocco agli altri nodi, i quali voteranno per l'eventuale accordo o disaccordo con la versione divulgata dal block producer. Quando viene raggiunto un quorum deliberativo di due terzi dei nodi con voto favorevole sulla versione aggiornata, allora il blocco viene validato e la nuova blockchain viene propagata.

Il proof of stake si definisce algoritmo di consenso asincrono proprio perché, a differenza del proof of work, non viene richiesto il consenso unanime, quindi non è necessario che

tutti i nodi analizzino il blocco ed esprimano il loro voto, ma è sufficiente che due terzi l'abbiano analizzato e abbiano espresso la loro valutazione.

È chiaro, dunque, come il sistema proof of stake sia in grado di tollerare anche "generali bizantini disertori". Il nuovo blocco, difatti, viene propagato solamente nel caso di raggiungimento del quorum.

Dopo aver enunciato in linea generale il funzionamento di questo algoritmo, possiamo approfondire il tema dei provvedimenti nei confronti di chi cerca di ostacolare il network.

Le sanzioni inflitte ai validatori che si comportano in modo malevolo sono varie: alcune dirette, altre indirette. La prima tra tutte è del secondo tipo e consiste nella devalorizzazione delle coin messe in staking. Ponendo il caso in cui un nodo riesca a falsificare un blocco, nel momento in cui viene trovato in fallo, la blockchain sarebbe compromessa e il valore dei token su di essa scenderebbero di valore. Ciò risulterebbe dannoso per tutti gli utenti che detengono quelle coin e anche per il soggetto stesso che ha tentato l'attacco.

Lo slashing, invece, è la pena diretta inflitta dal network al validatore che non si comporta in maniera adeguata. Se un block producer cerca, infatti, di proporre un blocco falso, esegue un double signing[53] oppure semplicemente rimane offline per un determinato periodo, viene punito. Questa tipologia di provvedimento mira a garantire che tutto il potere derivante dalle monete in staking non sia utilizzato in modo da danneggiare il network. Quando un nodo validatore agisce in maniera da compromettere il buon funzionamento della rete, può perdere tra il 5% e il 20% delle criptovalute in staking. I token decurtati dal patrimonio vengono, di conseguenza, redistribuiti ad altre parti interessate o banditi dalla blockchain.

Alcuni dei fattori che possono causare lo slashing sono i seguenti:

- Tempo di inattività: caso in cui un nodo non è attivo o non autentica le transazioni. A seconda dei protocolli, riguardo alla durata del tempo di inattività tollerata, una volta che un nodo soddisfa questo parametro, di conseguenza perde automaticamente il suo status di validatore e parte dei token in staking.

[53] Double signing: la doppia firma si verifica quando un'entità di convalida invia due sottoscrizioni per la convalida dello stesso blocco.

Questo fattore potrebbe anche semplicemente verificarsi a seguito di un'interruzione temporanea di corrente elettrica.

- Doppia firma: la sottoscrizione di un blocco due volte. Nella maggior parte dei casi, solitamente si tratta di un atto di un hacker, il quale tenta di “attaccare” la rete. Al fine di proteggerla, i nodi che attuano il double signing perdono i loro privilegi e parte dei token in staking.

Quindi, in definitiva, lo slashing è una funzionalità del sistema proof of stake che comporta la perdita di criptovalute per i soggetti che non partecipano e cooperano nel garantire il regolare funzionamento della rete.

Le blockchain che ricorrono a questo provvedimento, in casi di inadempienza degli utenti, sono più propense a funzionare per la maggior parte del tempo senza problematiche. Questo poiché i validatori, avendo dei token in gioco, sono sottoposti al rischio e, di conseguenza, sono motivati a garantire il buon funzionamento del network.

Ora che è stato esplicato come funziona, in linea generale, questo algoritmo, è necessario introdurre i delegators[54].

È raro e difficile che un singolo utente possa essere uno dei validatori di una chain, a meno che il registro distribuito non sia di dimensioni davvero ristrette. È necessario, dunque, avere grandi quantità di token in staking per poter competere con gli altri validatori. Gli slot disponibili per ricoprire questa carica sono limitati: solitamente si tratta di un centinaio di soggetti, ma il numero dipende da protocollo a protocollo. Generalmente, ci sono, quindi, un numero determinato di slot, i quali sono dedicati ai migliori stakers. Una persona fisica, dunque, anche se possedesse molte coin, avrebbe pochissime probabilità di essere compresa tra questi.

Solitamente gli utenti inclusi sono di due tipi: soggetti influenti che partecipano alle attività della commuity di una chain, in grado di raccogliere abbastanza consensi da poter entrate nelle posizioni più elevate, o società con ingenti disponibilità di criptovalute. Solitamente si tratta di exchanges come Binance, Cripto.com, Kraken, Coinbase, ecc.

I requisiti hardware per i validatori sono caratterizzati dal fatto che il sistema di convalida deve essere sempre online e disponibile, garantendo una certa sicurezza ed

[54] Delegator: utente che delega ad un validatore una quantità di coin da mettere in staking.

affidabilità per quanto riguarda la banda larga[55]. Anche questa tipologia di requisito varia però da chain a chain.

In ogni caso, sono presenti diverse spese che i validatori devono sostenere: quelle relative all'acquisto degli hardware, quelle per il mantenimento dell'infrastruttura e, infine, quelle riguardanti il vero e proprio svolgimento delle operazioni. Nell'ipotesi in cui, invece, non si vogliano sostenere questi esborsi, sussiste la possibilità di delegare le proprie coin a dei pool di validazione.

Questi utenti posso affidare lo staking dei propri token ad un validatore, il quale nel momento in cui convalida un blocco e riceve una ricompensa, la distribuirà tra la propria community, in proporzione alla quota partecipativa, misurata in base alle coin investite. Ad esempio, se un soggetto possiede 10.000 unità di criptovaluta da poter mettere in stake e gliene vengono delegate ulteriori 10.000 da altri utenti, egli, nel momento in cui valida un blocco, tiene il 50% della ricompensa per sé. Il restante lo distribuisce tra i vari delegators, dopo aver trattenuto una commissione per aver gestito ed amministrato l'operato della community. Facendo una stima macroscopica, da ogni delegatore, il validatore trattiene circa il 5% delle ricompense a titolo di commissione.

L'ideologia comune di colui che delega le proprie coin è quella di rinunciare a quel 5% di ricompense, dal momento che non ha la possibilità di possedere una quantità ingente di token in staking e, quindi, di esser incluso tra i migliori stakers. Inoltre, è esonerato dal dover acquistare l'hardware di validazione, sostenere i costi per il mantenimento dell'infrastruttura e essere sempre disponibile online.

Il delegatore non deve scegliere il validatore solamente sulla base della percentuale di commissioni da quest'ultimo richieste; nonostante si tratti di un dato di rilievo, non può essere l'unico contemplato nel momento della scrematura. Il validatore deve, infatti, risultare affidabile ed è, quindi, fondamentale assicurarsi che la probabilità di subire slashing da parte di questo sia molto bassa, in quanto le ripercussioni della malagestio ricadono anche su coloro che hanno delegato i token.

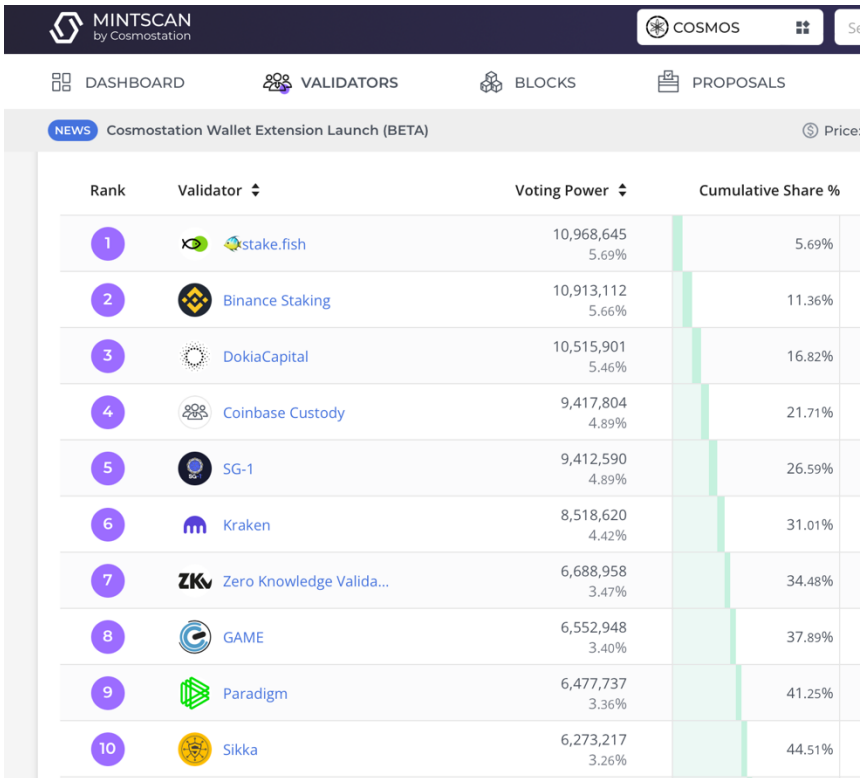
Il voting power non viene attribuito solamente in base a quante coin vengono messe in staking, ma anche alla quantità di deleghe ricevute dal validatore. Tale opportunità serve

[55] Banda larga: identificazione di un vasto insieme di tecnologie, che hanno in comune il collegamento ad Internet.

sia per la proposta di nuovi blocchi, sia per assumere potere decisionale all'interno della governance della blockchain.

Visualizzando un chain explorer[56], ad esempio Mintscan[57], nella sezione "blockchain Cosmos", è possibile notare la voce "voting power", contenente una classifica ordinata dei validatori con più potere.

Figura 6: Cosmos Top 10 Validators.



Fonte: mintscan.io

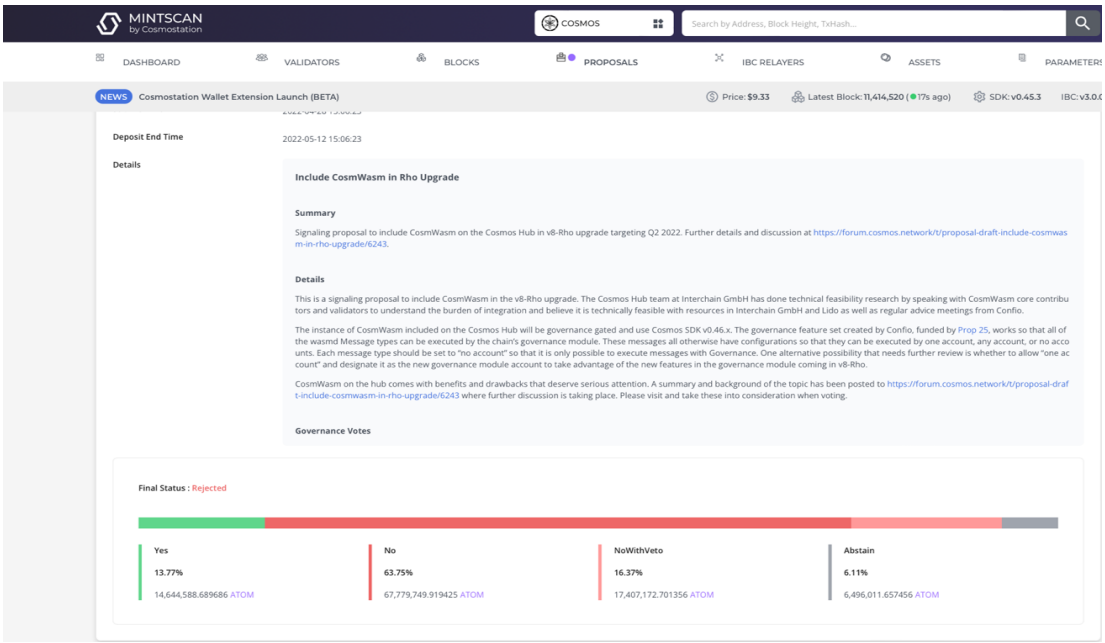
In questo registro distribuito, come è illustrato nella figura 5, appaiono nomi di exchanges come "Binance", "Coinbase", "Kraken", "Stake.fish". Ciò deriva dal fatto che è possibile delegare lo staking delle coin al validatore nelle principali piattaforme cripto. Di conseguenza, è compito del validatore stesso mettere in staking i token, dopo aver raccolto le relative deleghe.

[56] Chain explorer: un software per visualizzare blocchi, transazioni e metriche di rete blockchain (ad es. commissioni di transazione medie, hashrate, dimensione del blocco, difficoltà del blocco).
[57] Mintscan: è il blockchain explorer di Cosmos.

Numerosi utenti retail utilizzano questo metodo negli exchanges, accrescendo, quindi, il voting power di queste piattaforme. Se si prende come esempio Binance Staking, si può notare come questo exchange possegga il 5.66% del potere di voto totale sulla chain Cosmos, corrispondente alla probabilità di essere scelto come block producer. Inoltre, avrà tale percentuale di voto anche per quanto riguarda le decisioni di governance. Nel caso in cui i validatori, che si vogliono mettere in gioco, fossero in numero maggiore rispetto agli slot disponibili, solamente quelli con il voting power più elevato riuscirebbero a rientrare nella classifica dei più potenti.
Per quanto riguarda la governance, solitamente, nei registri distribuiti caratterizzati dall'algoritmo di consenso proof of stake, è data la possibilità a coloro che hanno una percentuale minima di potere di voto di avanzare proposte in merito al funzionamento del protocollo. Successivamente, sarà compito solamente degli stakers votare queste proposals; le varie tipologie di voto sono le seguenti:

- YES: sì.
- NO: no.
- NOWITHVETO: non solo si vota a sfavore della proposta, ma si promuove l'idea di voler punire colui che l'ha avanzata.
- ABSTAIN: astenuto.

Figura 7: Esempio di proposta di governance.



Fonte: mintscan.io

Solamente nel caso in cui il quorum costitutivo minimo venga superato e la maggioranza dei voti corrisponda al "Sì", si prosegue con l'implementazione della proposta nel protocollo. Ciò si traduce in una differenza sostanziale con l'algoritmo proof of work in termini di efficienza della blockchain, dal momento che in quest'ultimo è necessario l'utilizzo di un fork[58] per attuare modifiche. Ne esistono due tipologie: gli hard e i soft. Un hard fork è essenzialmente una divergenza permanente dall'ultima versione di una blockchain, che porta a una separazione della stessa: dal momento in cui i nodi non sono più concordi sull'operato, due diverse versioni della rete vengono eseguite separatamente. Ciò comporta la creazione di un fork all'interno della blockchain, in cui un percorso continua a seguire la sua precedente regolamentazione, mentre un altro ne rispetta una nuova. Questa tipologia di fork è spesso considerata "pericolosa" a causa della rottura del network che ne comporta. Difatti, nell'ipotesi in cui si dovesse verificare una divisione tra i vari nodi, che convalidano le transazioni, la rete stessa diventerebbe meno sicura e più vulnerabile agli attacchi. Ad ogni modo, esistono anche hard fork che, nonostante la divisione della blockchain, hanno permesso ad entrambe le versioni di continuare a funzionare correttamente, come è successo su Bitcoin e su Bitcoin cash[59].
Nel momento in cui si genera un hard fork e, di conseguenza, una nuova versione del registro distribuito, i validatori hanno la possibilità di decidere autonomamente su quale operare. Se lo spostamento avvenisse su una chain che dimostra di possedere solidità nel progetto, la transazione potrebbe anche essere definitiva; nel caso in cui, al contrario, il fork dovesse dimostrarsi fallace, le transazioni scomparirebbero e gli utenti tornerebbero ad adoperare la versione originaria.
I soft fork, invece, sono un'alternativa più sicura, compatibile con la blockchain di riferimento; i nodi che non eseguono l'aggiornamento a versioni più recenti, possono comunque visualizzare tutte le informazioni presenti su di essa, continuando ad operare. Tale tipologia di fork può essere utilizzata per aggiungere nuove funzionalità a livello di programmazione, senza mutare le regole che una blockchain normalmente deve seguire.

[58] Fork: nell'ambito dell'ingegneria del software dell'informatica, indica lo sviluppo di un nuovo progetto software che parte dal codice sorgente di un altro già esistente, a opera di un programmatore.
[59] Bitcoin Cash: una criptovaluta creata nell'agosto 2017, da un hard fork di Bitcoin. Rispetto a quest'ultima ha aumentato la dimensione dei blocchi, consentendo l'elaborazione di più transazioni e migliorando la scalabilità.

Per comprendere meglio la differenza tra hard fork e soft fork, si può considerare quest'ultimo come un aggiornamento del sistema operativo di base su un dispositivo mobile o un computer. Dopo tale processo, tutte le applicazioni sul dispositivo continuano a funzionare con la nuova versione del sistema operativo. Un hard fork, in questo scenario, rappresenterebbe una modifica completa, ossia il passaggio ad un nuovo sistema operativo. Generato un fork, nel caso del proof of work la democrazia si esplica nella possibilità di scegliere in quale versione della blockchain operare, mentre nel proof of stake la libertà dei nodi consiste nella messa ai voti della proposta.

In quest'ultimo algoritmo di consenso, la decentralizzazione ha un'importanza elevata: difatti, nel caso in cui un numero ristretto di validatori fosse in possesso della maggioranza del voting power, allora firmerebbero la maggior parte dei blocchi e controllerebbero gli aggiornamenti del protocollo. Potrebbe, di conseguenza, generarsi una blockchain dipendente da pochi validatori; in tal caso si sfocerebbe in un sistema centralizzato, casistica contrastata dagli algoritmi di consenso distribuito. Per evitare ciò, è necessario impedire l'accentramento del voting power tra pochi validatori, che causerebbe il controllo oligarchico dell'intera chain; a tal fine, è fondamentale implementare sistemi di incentivazione che supportino i bottom validator [60] . Un'esemplificazione di quanto appena affermato la si può scorgere su registri distribuiti come Terra e Cosmos, in cui sono presenti piattaforme che permettono di delegare lo staking delle proprie coin a soggetti affidabili, i quali non ricoprono una posizione di vantaggio che potrebbe in qualche modo ledere il sistema democratico della community.

Per comprendere il grado di decentralizzazione di una blockchain, si potrebbe, per esempio, osservare il potere di voto cumulato dai primi dieci validatori. È fondamentale che questi utenti non detengano più del 50% del voting power totale per mantenere un adeguato livello di democrazia. Nella figura 5, possiamo notare come, per quanto riguarda la blockchain Cosmos, il 44.5% del potere di voto complessivo appartenga ai migliori dieci validatori.

Nonostante sussista la possibilità per i delegators di rimuovere in qualsiasi momento la carica affidata ad un validatore e assegnarla ad un altro nodo, consegnandogli la

[60] Bottom Validator: validator con minore voting rate.

gestione delle proprie coin, a seguito di mala gestio, quando si verifica una votazione, i validatori possono sfruttare appieno tutte le deleghe di cui disponevano fino a quell'istante.

In tema di proposte riguardanti la governance, alcuni validatori, in qualità di "rappresentanti", mettono a disposizione un sistema tale per cui votano sulla base dell'opinione maggiormente affermata tra i propri delegators, dopo essersi confrontati con questi.

Alcuni protocolli, come quelli utilizzati da Cardano o Elrond, penalizzano addirittura i validatori troppo potenti, riducendo, in proporzione, le ricompense a chi detiene più di una certa soglia prestabilita di voting power. Questo sistema incentiva i delegators a affidare la gestione dei token a soggetti che posseggono una percentuale di voting power ridotta, evitando in questo modo il rischio di incorrere in ricompense minime. Inoltre, incoraggia i possessori di ingenti quantità di coin a creare diversi pool di validazione, in modo tale da poter ricevere maggiori premi.

2.5 BLOCKCHAIN PRIVATE

Finora abbiamo definito la blockchain come un registro distribuito, costituito da un network, capace di propagarsi in ogni parte del mondo. L'evoluzione di questa infrastruttura, però, ha persino portato alla creazione di alcune blockchain private, le quali possiedono differenze abissali con quelle pubbliche finora descritte. In realtà, accostare l'aggettivo "privata" al termine "blockchain" è un ossimoro: infatti, fino a questo momento, l'abbiamo descritta come quel registro distribuito su più nodi, non dipendente da un'entità centrale.

Una blockchain privata corrisponde ad un tipo speciale di tecnologia, in cui solamente una singola organizzazione è rivestita di autorità sulla rete. Non si tratta, infatti, di un database aperto al pubblico, nel quale gli utenti possono liberamente parteciparvi e muoversi. Ragion per cui, tutte le blockchain private sono dotate di una qualche forma di autorizzazione d'identità per poter accedere alla piattaforma.

Sorge spontaneo chiedersi come mai tale tecnologia, famosa perché gestita direttamente dal network che la sostiene, sia stata adattata per essere resa anche privata. La risposta si può scorgere nel fatto che un numero elevato di soggetti ha compreso l'utilità di archiviare dati come transazioni, documenti, codici e quant'altro,

su un registro distribuito crittografato. Ciò corrisponde ad una funzionalità interessante poiché possiede molteplici possibilità di evoluzione.

Le blockchain private vengono principalmente sviluppate e utilizzate all'interno dei sistemi aziendali, come database per l'archiviazione di dati. In questi casi, solamente i dipendenti dell'azienda stessa sono abilitati alla visione dei codici scritti su tale registro. Come avviene, allora, la decentralizzazione? Una blockchain privata non è completamente decentrata come quelle pubbliche: lo è, ma solamente in parte. Nonostante questa caratteristica giochi a sfavore di tali registri, essi possono ugualmente vantare ulteriori benefici quali regolamentazioni ad hoc, non possedute dalla blockchain tradizionale.

La fattispecie della blockchain privata soddisfa appieno le esigenze delle attività aziendali, dal momento che queste ultime necessitano di privacy nella conservazione di dati. Senza un adeguato sistema di tutela, la concorrenza sarebbe in grado di accedere alle piattaforme di archiviazione e, successivamente, divulgare informazioni preziose oppure utilizzarle per scopi personali. Di conseguenza, se anche un solo dato aziendale trapelasse all'esterno, questo potrebbe causare una perdita enorme per l'attività.

Nonostante la nascita dei registri distribuiti pubblici sia stata antecedente a quella delle blochckain private, i primi scarseggiano di efficienza, poiché permettono l'accesso a tutti coloro che ne fanno richiesta in rete, la successiva visualizzazione del libro mastro e la partecipazione attiva al processo di consenso. Di conseguenza, essendo caratterizzate da una moltitudine di nodi e traffico di dati, risulta difficile e impegnativo compiere operazioni di archiviazione, come il backup.

Al contrario, la blockchain privata consente l'accesso solamente ad una élite di utenti, superando le problematiche sopra citate.

Le varie aziende necessitano di una tecnologia potente, capace di eseguire il backup dei loro processi in modo celere. L'utilizzo di questo metodo di archiviazione è funzionale se viene sfruttato come database di informazioni solo all'interno del complesso aziendale. Risulta, però, complesso provare la veridicità dei dati contenuti in una blockchain privata, validati da un'autorità interna, nell'ipotesi in cui debbano essere riportati a stakeholders esterni. Infatti, un soggetto estraneo all'azienda, nella maggior parte dei casi, diffiderebbe dei dati riportati, dal momento che non sarebbe da escludere

un'eventuale modifica, avvenuta da parte dell'autorità vigilante, al fine di correggere i codici e i blocchi.

Le blockchain private risultano, comunque, fondamentalmente stabili per quanto concerne la gestione delle varie operazioni. In ogni rete pubblica, infatti, per effettuare una transazione, è necessario corrispondere una determinata commissione, al fine della validazione della stessa; talvolta, tale tariffa può risultare molto elevata, a causa della scarsità di nodi validatori, e soggetta a continui cambiamenti temporanei di valore.

Raramente si riscontrano difficoltà nella gestione delle operazioni dovute ad accumuli di ritardi, dal momento che, in questi tipi di database, non è necessario un consenso distribuito al fine della validazione.

All'interno delle piattaforme private, il valore delle fees dovute per ogni operazione è estremamente basso, se non, in alcuni casi, addirittura nullo. Contrariamente a quanto accade nelle blockchain pubbliche, in quelle private le commissioni non dipendono dal numero di richieste di validazione. Di conseguenza, è irrilevante quanti utenti richiedano la trascrizione di un'operazione, poiché il valore delle fees rimarrà sempre costante, non comportando quindi la presenza di alcun tipo di costo variabile.

Le spese relative al mantenimento di un registro distribuito privato sono relativamente inferiori a quelle necessarie per la conservazione di blockchain pubbliche, a causa del limitato utilizzo di risorse. Queste ultime, infatti, richiedono un'infrastruttura più complessa e dispendiosa, al fine di supportare l'ingente quantità di utenti che la utilizzano.

I registri distribuiti privati, come accennato in precedenza, sono dotati di processi di autenticazione, che entrano in gioco nel momento in cui un utente tenta l'accesso alla rete. In questo modo è possibile filtrare il flusso di utenti, individuando e impedendo l'accesso ad eventuali intrusi. Ciò, invece, non avviene all'interno delle blockchain pubbliche, le quali, anzi, dal momento in cui sono state create, sono sempre state soggette alla criminalità. Infatti, l'anonimato che può essere garantito da una blockchain come Bitcoin è spesso stato sfruttato a proprio vantaggio da soggetti malintenzionati, al fine di svolgere transazioni di compravendita relative a beni o servizi illegali. Ovviamente, questo fenomeno lo si cerca di evitare il più possibile in un contesto aziendale, motivo per cui l'autorizzazione di accesso al sistema è concessa solamente a persone verificate.

Nel caso in cui si fosse alla ricerca di un database sicuro per la propria azienda, allora la blockchain privata corrisponderebbe alla soluzione migliore da intraprendere. Risulta assai semplice, in un registro distribuito di questo genere, applicare un determinato tipo di regolamentazione, a cui i dipendenti dovranno sottostare.

La blockchain privata può, inoltre, essere utilizzata come strumento di marketing: l'uso di tale database, al giorno d'oggi, denota quanto l'azienda sia all'avanguardia in ambito tecnologico.

Come già dimostrato, la struttura che opta per questo tipo di tecnologia non avrebbe alcun incentivo a modificare e falsificare i dati archiviati, dal momento che questi ultimi sarebbero utilizzati solamente per scopi interni all'azienda stessa. Nel caso in cui, invece, fosse necessario condividere tali dati con soggetti esterni, come una banca, la situazione muterebbe completamente. Infatti, se l'istituto di credito dovesse basare la scelta di erogazione di un finanziamento sulla base di dati archiviati nella blockchain privata, sarebbe necessario che contemplasse la possibilità di un'eventuale modifica dei blocchi.

2.5.1 Differenze tra blockchain pubbliche e private

Il completo decentramento può essere ottenuto solamente all'interno di una blockchain pubblica; infatti, si tratta di una caratteristica per lo più assente in quelle private. Le prime sono tratteggiate da una natura distribuita, rappresentata dal fatto che tutti i nodi partecipanti al network possiedono una copia aggiornata del registro stesso. Le blockchain private ripongono la propria forza, invece, su un'unica autorità, che controlla l'intero sistema.

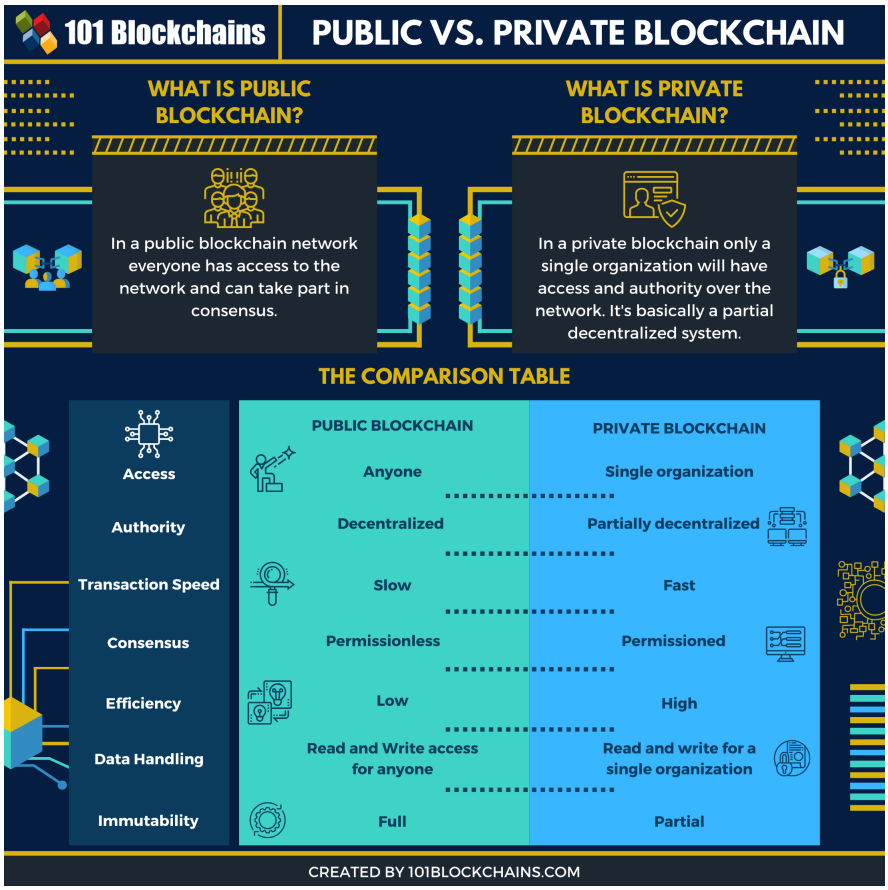
Per quanto concerne l'ambito del consenso, in un registro distribuito pubblico, tutti i nodi possono prendervi parte e ottenere i vantaggi della piattaforma, dal momento che non possiedono restrizioni a riguardo. D'altro canto, la blockchain privata, come denotato precedentemente, applica un rigido processo di scrematura, decidendo in anticipo a quali soggetti conferire l'opzione di visualizzazione dei dati contenuti all'interno del registro.

Infine, la rete pubblica è completamente immutabile: nel momento in cui un blocco viene implementato nella catena, non sussiste la possibilità di poterlo modificare o eliminare. Questa fattispecie, quindi, fa in modo che a nessun utente sia concessa la facoltà di falsificare i dati delle transazioni, al fine di ottenere vantaggi a scapito di altri

soggetti. Solamente al verificarsi di alcune circostanze, la community può decidere se apporre modifiche ad un determinato blocco: si tratta di casi eccezionali.

Le blockchain private troveranno sempre di più spazio all'interno di enti e di organizzazioni, contrariamente a ciò che pensano e si auspicano gli utenti più "puristi". Eppure questi ultimi difficilmente potranno promuovere un uso di massa di questo database distribuito, per il semplice motivo che quello che al giorno d'oggi viene definito "blockchain" si discosta sempre più dal protocollo pensato e progettato da Satoshi Nakamoto. L'utilizzo di questa tecnologia da parte dell'intero sistema economico è, infatti, un passaggio fondamentale per permettere alla società di poterne beneficiare in un futuro. Ai posteri l'ardua sentenza.

Figura 8: Differenze tra public e private blockchain.



Fonte: 101blockchains.com

CAPITOLO 3

3.0 SMART CONTRACT

3.1 DEFINIZIONE

Uno smart contract è un codice destinato a contribuire, verificare o implementare la negoziazione o l'esecuzione di un accordo. Consente, infatti, di concludere transazioni senza l'ausilio di terze parti, limitatamente all'ambito operativo, in quanto si tratta di contratti scritti, tracciabili e irreversibili. Gli smart contract, definiti anche "contratti intelligenti", contengono tutte le informazioni e le clausole di un normale contratto, ma eseguono tutte le azioni programmate in maniera automatizzata. In termini più pratici, si tratta di protocolli informatici, che verificano e fanno rispettare la negoziazione o l'esecuzione di un accordo.

Essi corrispondono alla traduzione o alla trasposizione in codice software di un vero e proprio contratto. Tale programma è definito in modo che possa verificarsi in modo automatico all'avverarsi di particolari condizioni: ossia effettua il controllo dei dati pattuiti ed esegue in automatico azioni e disposizioni, affinché si possano produrre gli effetti conseguenti a quanto stabilito tra le parti. Negli smart contract non dovrebbe, idealmente, essere presente l'intervento umano, poiché, in tal caso, verrebbe meno l'oggettività richiesta dalla valutazione.

In altre parole, tale tipologia di contratto è basata su un codice che analizza sia le clausole, che sono state concordate, sia le condizioni operative, alle quali devono verificarsi tali accordi. Esso si auto-innesca nel momento in cui i dati riferiti alle situazioni reali corrispondono a quelli indicati nelle condizioni dell'accordo. È perciò essenziale che

le fonti delle informazioni reali siano affidabili e, inoltre, leggibili automaticamente dallo smart contract stesso.

Figura 9: Gli smart contract.

Fonte: academy.shrimpy.io

Si definisce con il termine "oracolo[61]" l'applicazione che si frappone tra il mondo reale e lo smart contract, con lo scopo di raccogliere e trasmettere informazioni nel momento esatto in cui una certa condizione o fatto si verifica. L'oracolo deve essere in grado di riportare dati credibili in merito a quanto pattuito all'interno dell'accordo e, di conseguenza, li deve reperire da fonti che hanno una certa credibilità, leggendoli e trasferendoli in maniera trasparente, sicura ed affidabile.

Tali software recuperano dall'esterno le informazioni indicate nel contratto, per poi trasmetterle alla blockchain. Alla base di ciò, è presente il presupposto secondo cui i vari utenti sono, in qualche modo, "obbligati" a confidare che i dati forniti da essi siano accurati e precisi. Questa problematica potrebbe essere risolta utilizzando informazioni provenienti da diverse basi di dati, ma ciò aumenterebbe i costi di transazione, corrispondenti alle commissioni degli oracoli utilizzati. Inoltre, non è consigliabile fare affidamento su informazioni provenienti da diverse fonti, in quanto si potrebbe incorrere in nuove problematiche di consenso.

[61] Oracolo: responso fornito da un'entità superiore in merito ad una relativa domanda su cose ignote del presente, del passato o del futuro o anche alla giusta maniera di agire in determinate circostanze.

Lo scopo della creazione degli smart contract è quella di limitare i casi in cui l'esecuzione è influenzata e ostacolata da decisioni umane. Oggigiorno è molto frequente, soprattutto nell'ambito commerciale, che, nonostante avvenga la stipula di un contratto tra due parti, ad una prestazione non corrisponda l'obbligazione pattuita tra le clausole. Di esempi si potrebbero citarne centinaia: dal contratto di vendita, nel quale, a seguito della consegna della merce, non corrisponde un effettivo pagamento; all'accordo per la prestazione di servizi, in cui la corresponsione del servizio non viene effettuata entro le tempistiche pattuite.

Lo smart contract si pone come obbiettivo principale quello di superare tutte queste problematiche, essendo esente dalla volontà umana. Se, come detto precedentemente, la blockchain corrisponde ad un registro digitale generalmente immutabile, tracciabile e non alterabile e il contratto intelligente si configura come uno strumento che fornisce istruzioni per gli elaboratori, è facilmente intuibile come le due tecnologie possano unirsi in un matrimonio perfetto.

L'obbiettivo degli smart contract consiste nella riduzione della necessità di avvalersi di intermediari di fiducia, dei costi degli arbitrati, delle perdite per frodi, nonché delle eccezioni dolose e accidentali. Esemplificazione di questa tecnologia sono i distributori automatici, i quali vengono definiti come il più antico strumento ad averla utilizzata.

3.1.1 Nascita e sviluppo degli smart contract

I contratti intelligenti sono stati proposti per la prima volta all'inizio degli anni '90 da Nick Szabo[62], che ne ha coniato il termine per riferirsi a "una serie di promesse, specificate in forma digitale, inclusi i protocolli all'interno dei quali le parti mantengono queste promesse". Egli ha proposto l'implementazione dell'infrastruttura di tali contratti, replicando alcuni registri, e l'esecuzione di accordi, utilizzando catene di hash crittografiche e bizantine fault tolerance.

Oggigiorno, sono comunemente associati alle criptovalute, in quanto la loro diffusione è stata resa possibile principalmente tramite la blockchain Ethereum. Proprio per questo motivo, sono generalmente considerati un elemento fondamentale per le applicazioni

[62] Nick Szabo: uno scienziato informatico, studioso di diritto e crittografo, noto per le sue ricerche sui contratti digitali e la valuta digitale.

di finanza decentralizzata (DeFi). Il white paper originale di Ethereum di Vitalik Buterin[63], pubblicato nel 2014, descrive il protocollo Bitcoin come una versione debole del concetto di contratto intelligente originariamente definito da Nick Szabo e ne propone una più forte, basata sul linguaggio Solidity[64], Turing complete[65]. In questa piattaforma, infatti, gli smart contract sono generalmente scritti in un linguaggio di programmazione completo di Turing, chiamato Solidity, e compilati in bytecode[66] di basso livello, al fine di poter essere eseguiti dalla macchina virtuale di Ethereum.

Dal lancio della blockchain di Ethereum, il termine "smart contract" è stato associato, in modo più specifico, alla nozione di calcolo, per scopi generici, su una blockchain o un libro mastro distribuito.

Il National Institute of Standards and Technology[67] degli Stati Uniti descrive un contratto intelligente come una "raccolta di codici e dati che viene distribuita, utilizzando transazioni firmate crittograficamente, sulla rete blockchain". Secondo questa interpretazione, sostenuta ad esempio da Ethereum Foundation o IBM[68], un accordo di questo tipo non è necessariamente correlato al concetto classico di contratto, ma può configurarsi come qualsiasi tipo di software basato su blockchain. Infatti, esso è anche considerato una procedura memorizzata protetta, poiché la sua esecuzione e i suoi effetti, come il trasferimento di un valore tra le parti, sono rigorosamente applicati e non possono essere manipolati, a seguito della sua archiviazione all'interno di un registro distribuito. Questo perché l'effettiva esecuzione dei contratti è controllata e verificata dalla piattaforma, non da programmi arbitrari che si connettono ad essa.

A partire dal 2015, il gruppo UBS[69] ha sperimentato l'utilizzo degli "smart bond[70]". Tali obbligazioni, servendosi della blockchain Bitcoin, in cui i flussi di pagamento potevano

[63] Vitalik Buterin: un programmatore e scrittore canadese, noto soprattutto come uno dei co-fondatori di Ethereum.
[64] Solidity: un linguaggio di alto livello, orientato al contratto e tipizzato staticamente per l'implementazione di contratti intelligenti sulla piattaforma Ethereum.
[65] Turing complete: un linguaggio che può svolgere qualsiasi calcolo.
[66] Bytecode: un linguaggio intermedio più astratto tra quello di macchina e quello di programmazione; usato generalmente per descrivere le operazioni che costituiscono un programma.
[67] National Institute of Standards and Technology: promuove l'innovazione e la competitività industriale degli Stati Uniti.
[68] IBM: International Business Machines Corporation, la più anziana azienda statunitense e tra le maggiori al mondo nel settore informatico.
[69] UBS: banca svizzera, con sede a Zurigo e Basilea, che principalmente offre servizi di investimento.
[70] Smart bond: tipo di obbligazione basata sul concetto di smart contract.

essere ipoteticamente automatizzati del tutto, cercavano di creare uno strumento di pagamento automatico. Questo tipo di tecnologia non è mai stato implementato dal gruppo UBS, ma ci sono molti altri istituti bancari che, prendendone spunto, oggigiorno offrono tale servizio.

Nel 2017, a seguito dell'attuazione del Decreto sullo sviluppo dell'economia digitale, la Bielorussia si è configurata come il primo Paese in assoluto a legalizzare gli smart contract. L'avvocato bielorusso Denis Aleinikov è considerato l'autore principale del concetto legale di "contratto intelligente" introdotto dal decreto in questione.

Nel 2018, un rapporto del Senato degli Stati Uniti affermava: "Sebbene i contratti intelligenti possano apparire come una novità, il concetto su cui si fondano è radicato nel diritto contrattuale di base. Solitamente, il sistema giudiziario giudica le controversie contrattuali e ne fa rispettare i termini, ma è comune anche avere un altro metodo di arbitrato, in particolare per le transazioni internazionali. Con gli smart contract, un software fa rispettare il contratto integrato in un codice." Numerosi Stati degli Stati Uniti hanno approvato leggi sull'uso di questa tipologia di accordo, come Arizona, Nevada, Tennessee e Wyoming. Inoltre, nell'aprile 2020, la Camera dei Rappresentanti dell'Iowa ha varato un disegno di legge che riconosce legalmente i contratti intelligenti all'interno dello Stato.

Nell'aprile 2021, la UK Jurisdiction Taskforce [71] ha pubblicato le "Digital Dispute Resolution Rules[72]", al fine di consentire la rapida risoluzione delle controversie legali relative a blockchain e criptovalute in Gran Bretagna.

3.1.2 Caratteristiche

Operando similmente ad un trasferimento di valore crittografico, l'implementazione di uno smart contract su un registro distribuito avviene mediante l'invio di una transazione da un wallet. Tale operazione include il codice identificativo del contratto intelligente e l'indirizzo del destinatario. Al fine di stabilirne lo stato iniziale, la transazione deve, quindi, essere compresa in un blocco, che verrà aggiunto alla blockchain per eseguirne il relativo codice. Gli algoritmi bizantini, in tale piattaforma, proteggono lo smart

[71] UK Jurisdiction Taskforce: una sussidiaria del LawTech Delivery Panel del Regno Unito.

[72] Digital Dispute Resolution Rules: un nuovo insieme di regole arbitrali per la risoluzione delle controversie nelle relazioni digitali on-chain e negli smart contract.

contract in modo decentralizzato dai tentativi di manomissione. Una volta distribuito, infine, uno contratto intelligente non può essere aggiornato o modificato.

Un equivoco comune consiste nel confondere questa tipologia di accordo con i contratti legali intelligenti: si tratta, però, di due strumenti che non necessariamente coincidono. Questi ultimi, infatti, fanno riferimento ai tradizionali accordi legalmente vincolanti in linguaggio naturale, che sono stati implementati in codice leggibile da un calcolatore. Uno smart contract, invece, non costituisce obbligatoriamente un valido accordo vincolante per legge. Alcuni giuristi affermano, a tal proposito, che non si tratti di un accordo legale, ma di un mezzo per l'esecuzione di obblighi derivanti da pattuizioni, come l'automazione dei vincoli di pagamento o quelli relativi al trasferimento di criptovalute. Altri studiosi, invece, sostengono che la natura imperativa o dichiarativa dei linguaggi di programmazione possa influire sulla validità legale dei contratti intelligenti.

Questa tipologia di contratti possiede numerosi punti a favore, che permettono di ipotizzare un utilizzo sempre più vasto di questo strumento nei prossimi anni.

Il principale beneficio derivante dalla trascrizione di questa tipologia di contratti all'interno di un registro distribuito si configura nella garanzia dell'archiviazione, consistente nell'impossibilità di cancellare o modificare il codice del documento in questione, senza lasciarne traccia. La sicurezza è garantita dalla struttura stessa della blockchain. I blocchi contenenti le transazioni sono crittografati, il che li rende quasi impossibili da hackerare. Inoltre, poiché, come spiegato nel capitolo 2, ogni blocco è concatenato con quelli precedenti e successivi, all'interno di un registro distribuito, gli hacker dovrebbero modificare una porzione di catena per falsificare i dati contenuti da un singolo blocco. Sono presenti, infatti, svariate misure di sicurezza, garantita con l'utilizzo degli smart contract: backup e duplicati sono integrati nel sistema.

Beneficio collegato alle peculiari sicurezza e affidabilità, proprie di questa tecnologia, consiste nel lungo elenco di applicazioni e, quindi, casi d'uso di successo.

Ad esempio, l'avvento recente della pandemia legata al virus COVID-19 ha illustrato quanto facilmente il settore della sanità possa riscontrare difficoltà, anche nei Paesi più sviluppati. Grazie ad una chiave privata, la blockchain potrebbe facilmente sollevare tale settore in alcune mansioni, archiviando, per esempio, le cartelle cliniche codificate dei pazienti. La sicurezza, inoltre, rende questi record decodificati accessibili solo a

determinati individui, facilitando così anche il lavoro di particolari professionisti che fondano le proprie decisioni sulla base di questi dati. Esempio possono essere gli assicuratori, per quanto riguarda la sottoscrizione di polizze vita o morte, e coloro che gestiscono l'offerta di farmaci. L'organizzazione internazionale "Medici senza frontiere [73] " ha utilizzato questa tecnologia per caricare i documenti delle immunizzazioni all'interno della blockchain.

Un altro ambito di applicazione degli smart contract è quello finanziario: non solo sono stati utilizzati in questo campo, ma hanno, addirittura, trasformato i principi su cui si basavano i servizi inerenti convenzionali. Un esempio consiste nella richiesta di risarcimento assicurativo: in tale processo, il contratto digitale verifica gli errori, li elabora e, infine, invia i fondi risarcitori all'utente al momento della convalida. I grandi fornitori di servizi finanziari che utilizzano smart contract includono, tra gli altri, JP Morgan, Wells Fargo e HSBC.

Ulteriore aspetto di importante rilevanza corrisponde alla possibile comunicazione in tempo reale, conseguente alla ricerca e sviluppo all'interno di un registro distribuito. Si tratta di un fattore essenziale tra le istituzioni per evitare l'effetto "silo"[74]. I brevetti, altri diritti di proprietà intellettuale e i rilasci automatici dei fondi relativi a sovvenzioni stanno adottando sempre più la tecnologia del contratto intelligente. Aziende come ARTiFACTS, Pluto, Orvium e ScienceMatters-EUREKA stanno studiando soluzioni basate su questo sistema al fine di semplificare la ricerca della provenienza dei dati e la mole lavorativa.

Ulteriori punti di forza di questa tecnologia corrispondono sicuramente alla velocità, all'efficienza e alla precisione del contratto stesso. Difatti, una volta che le condizioni del contratto vengono soddisfatte, questo viene eseguito immediatamente, in maniera autonoma, indipendentemente dalla volontà delle parti. Inoltre, essendo i contratti intelligenti digitali e automatizzati, non richiedono al fine dell'attuazione pratiche cartacee da elaborare e tempo speso per correggere eventuali errori, che solitamente derivano dalla compilazione manuale dei documenti. Di conseguenza, la maggior parte

[73] Medici senza frontiere: organizzazione internazionale, fondata nel 1971 a Parigi, la cui missione è offrire assistenza medica nei Paesi in cui ce n'è maggiormente bisogno.

[74] Effetto silo: mancanza di scambio di informazioni tra i sistemi di database all'interno di un'entità o con entità esterne.

degli intermediari, che solitamente si interpone tra le parti contrattuali, con questo procedimento, viene completamente elisa e, di conseguenza, eliminati anche i ritardi e le commissioni associati.

Gli smart contract sono anche caratterizzati da fiducia e trasparenza: nonostante non siano coinvolte terze parti, grazie allo sharing dei record crittografici delle transazioni tra i partecipanti, non è possibile che le informazioni siano alterate a vantaggio personale. L'oracolo è l'unico agente esterno che influenza l'andamento del contratto, motivo per cui è necessario affidarsi ad una base dati il più possibile sicura.

Uno smart contract basato su blockchain è visibile a tutti gli utenti di tale piattaforma; tuttavia, questa peculiarità comporta una situazione in cui anche i bug, comprese le falle di sicurezza, sono visibili a tutti gli utenti e, di conseguenza, se non risolti rapidamente, possono comportare gravi problematiche e ingenti danni.

Difatti, i contratti intelligenti comportano anche alcuni svantaggi di cui è necessario essere consapevoli, come il fatto che il loro codice sorgente è scritto dagli utenti, i quali possono talvolta commettere errori.

3.1.3 The DAO Attack

Un attacco è stato eseguito con successo alla blockchain Ethereum nel 2016, anno in cui una delle prime organizzazioni di venture capital decentralizzate subì un "furto" del valore di quasi 70 milioni di dollari di Ether. A seguito di un errore di trascrizione del codice di uno smart contract, interno al proprio sistema, questa organizzazione, di nome "DAO[75]", introdotta all'inizio di quell'anno e nota anche come "Genesis DAO", venne privata di 3.6 milioni di Ether.

Il relativo framework[76] di codifica era stato sviluppato in maniera open source dal team di Slock.It, ma in seguito fu distribuito con il nome "The DAO" dai membri della comunità di Ethereum.

Questa organizzazione inizialmente raccolse grande quantità di capitale: durante tale periodo, chiunque, aveva la possibilità di inviare loro Ether in cambio di token DAO. Si configurò come un successo inaspettato, poiché riuscì a raccogliere 12,7 milioni di Ether,

[75] DAO: Decentralized Autonomous Organizations.

[76] Framework: architettura logica di supporto, sulla quale un software può essere progettato e realizzato.

per un valore di circa $150 milioni all'epoca, rendendo The DAO il più grande crowdfund di sempre.

Nel momento in cui Ether veniva scambiato a $20, il valore totale posseduto da The DAO era oltre $250 milioni.

La piattaforma, inoltre, consentiva a chiunque avesse un progetto di presentare la propria idea alla comunità e potenzialmente ricevere finanziamenti a tal fine a spese della stessa. I soggetti detentori di token DAO possedevano la facoltà di votare le varie proposte, per poi ricevere ricompense nel momento in cui le iniziative sostenute avessero realizzato un profitto.

Nonostante il successo iniziale, il 17 giugno 2016, un hacker trovò una falla nella codifica degli smart contract di questo venture capital fund, che gli permise di drenare fondi da The DAO. Durante le prime ore dell'attacco si stima che siano stati rubati 3.6 milioni di ETH, l'equivalente di 70 milioni di dollari all'epoca.

Come accennato precedentemente, la causa di tale evento si configura in un errore di scrittura in uno dei contratti intelligenti di The DAO, in cui sono state invertite dagli utenti, involontariamente, due righe del codice identificativo. La conseguenza fu che, nella porzione che gestiva il lato “prelievo”, il prelievo stesso non era più direttamente collegato con l’aggiornamento del saldo; di conseguenza, l’hacker ha avuto la possibilità di effettuare ipotetici infiniti prelievi senza che il suo saldo venisse decurtato.

È fondamentale comprendere che questo bug non proveniva da un errore di trascrittura del protocollo di Ethereum stesso, ma da questa organizzazione sviluppata su Ethereum. Il codice scritto per The DAO, infatti, includeva diversi difetti e l'exploit delle richieste di rimborso era uno di questi. Esemplificazione per apprendere appieno questa situazione si configura nell’associare Ethereum a Internet e qualsiasi applicazione basata su questa blockchain ad un sito web: il malfunzionamento di un sito web, infatti, non comporta l’inefficienza di Internet. Restano tuttora ignote le ragioni per cui l'hacker smise di prosciugare The DAO, nonostante il ripristino dell’errore da parte della community dovesse ancora essere effettuato.

In seguito a tale avvenimento, la comunità e il team di Ethereum recuperarono rapidamente il controllo della situazione e presentarono molteplici proposte per affrontare l'exploit. Per rimborsare il denaro perso, Ethereum effettuò un hard fork per

inviare i fondi compromessi ai proprietari originali, ai quali era stato assegnato un tasso di cambio da 1 ETH per 100 token DAO, lo stesso tasso dell'offerta iniziale.

Non sorprende che l'hacking sia stato l'inizio della fine dell'esistenza di questa organizzazione. Il fork stesso fu contestato da molti utenti di Ethereum, i quali sostenevano che violasse i principi di base della tecnologia blockchain. Da quel momento, la community si divise in due schieramenti: una parte riteneva che fosse giusto e corretto riconsegnare i token ai legittimi proprietari, un'altra supportava la non-restituzione delle criptovalute, non avendo l'hacker rubato nulla, ma solamente sfruttato, a suo favore, un contratto intelligente scritto in modo errato. A seguito di tale partizione, i sostenitori dell'ideologia della "blockchain immutabile" continuarono ad operare sulla blockchain "classica", chiamata anche Ethereum Classic; gli altri utenti, invece, decisero di effettuare un hard fork e creare Ethereum, una versione del registro distribuito in cui i token "rubati" sono stati rimborsati, ripristinando la blockchain al periodo precedente all'attacco. Oggigiorno Ethereum ed Ethereum Classic sono entrambe operative, ma la prima è quella che ha sicuramente riscosso più successo tra la community.

Ulteriore problematica intrinseca a questa tecnologia, particolarmente importante, corrisponde al relativo stato normativo. Attualmente, tali contratti non sono chiaramente regolati da alcun governo: realtà che si auspica possa mutare prossimamente.

I contratti intelligenti richiedono anche un'elevata manutenzione in termini di competenze ingegneristiche necessarie al fine di renderli operativi. Per generare smart contract a prova di errore, concordi con la tecnologia e i processi esistenti all'interno dell'azienda, è necessario, infatti, il lavoro di un programmatore esperto.

Varie sono le problematiche intrinseche agli smart contract di Ethereum, in particolare, includono: ambiguità, facili costrutti, bug del compilatore, bug di Ethereum Virtual Machine, attacchi alla rete blockchain. Causa dell'esistenza di tali difficoltà è l'assenza di una documentazione di origine centrale.

I contratti intelligenti, infatti, potrebbero completamente rivoluzionare il modo in cui viviamo, ma, ora come ora, necessitano ancora numerose modifiche e ottimizzazioni.

3.2 ALTCOIN

Le altcoin rappresentano tutte le criptovalute “alternative”, rispetto a Bitcoin.

Particolarmente degni di nota sono i cosiddetti "token di utilità", che forniscono diritti di accesso e utilizzo a una determinata risorsa digitale, la quale potrebbe essere alla base del valore del token. Un sottogruppo principale di tale categoria sono le coin native delle blockchain abilitate all’utilizzo degli smart contract, come Ethereum, Solana, Cardano, Tezos, Avalanche, Terra, Binance Smart Chain ed EOS. Sebbene alcune di esse possano essere considerate una "riserva di valore" dagli investitori, primo fra tutte Ether, il relativo valore principale è determinato dalla loro utilità come "gas digitale [77] ". Quest’ultimo deve essere speso al fine di gestire smart contract. Pertanto, il prezzo dei token nativi delle blockchain abilitate all’utilizzo dei contratti intelligenti, dipende dal volume delle transazioni eseguite sulle piattaforme con questo strumento.

Quanto sopra indicato rappresenta il lato della domanda di token, mentre, l’offerta, ossia l'emissione di nuove coin e il riscatto di quelle esistenti, è definita all’interno dei protocolli delle rispettive blockchain. In molte di esse, la diffusione può essere modificata dai partecipanti alla rete in base al framework di governance deciso dalla blockchain stessa. Un esempio di ciò, come trattato nel capitolo 1.3, è una delle conseguenze al cosiddetto Merge di Ethereum, attraverso cui è "bruciata" e, quindi, rimossa dalla circolazione una quantità di monete corrispondente alla FEE base pagata per ogni transazione. In periodi di elevata concentrazione di attività di rete, questo processo può compensare la nuova offerta di monete coniate e rendere deflazionistica la criptovaluta, ossia vengono "bruciati" più token di quelli emessi.

Esistono anche ulteriori token di utilità, come ad esempio LINK, il quale consente agli utenti di recuperare i dati dalla rete decentralizzata di "oracoli" di Chainlink, e FIL, che viene utilizzato, invece, per pagare i servizi di archiviazione sulla rete Filecoin.

Analogamente a quanto avviene per le materie prime, anche in questo caso non esistono metodi consolidati per valutare tali token, di conseguenza, l'attenzione degli investitori è spesso incentrata sull'analisi del rapporto tra domanda e offerta. Detto ciò, si può notare che l'algoritmo di consenso di un dato numero di blockchain sopra menzionate è il proof of stake. Questo modello, infatti, risulta il più utilizzato in quanto

[77] Gas digitale: unità di misura che indica la quantità di potenza di calcolo necessaria per eseguire specifiche operazioni all’interno della rete.

uno tra i più facili da applicare tra quelli di consenso distribuito; inoltre, permette di ottenere una certa efficienza nella gestione della governance. A differenza degli algoritmi proof of work, come illustrato nel capitolo 2, i POS permettono di utilizzare una quantità di energia inferiore, ottenendo simili risultati, se non, addirittura, più performanti.

Il range di valutazione potrebbe risultare piuttosto ampio dal momento che questi token e le loro relative blockchain sono un'implementazione dell'infrastruttura Web 3.0, la quale è tuttora in fase di sviluppo. Ciò rende difficile, quindi, prevedere una potenziale diffusione di queste coin all'interno della società.

È interessante notare che i detentori di alcuni dei token di governance dei protocolli DeFi ricevono o potrebbero, in qualche fase, iniziare a ricevere parte delle entrate generate dalla blockchain di riferimento. Ad esempio, i titolari di SUSHI, token di governance dell'exchange decentralizzato (DEX) SushiSwap, hanno la possibilità di mettere in staking le proprie coin al fine di ricevere parte delle commissioni pagate dagli utenti. In questo modo, parte del valore del protocollo viene trasferito ai possessori di token di governance, facilitando gli investitori nel valutare l'attrattività relativa delle coin ad un determinato prezzo di mercato.

Inoltre, è necessario tener conto che questa tipologia di token è soggetta ad un elevato rischio normativo, dal momento che la relativa emissione potrebbe essere considerata come un'offerta di titoli non registrata.

CAPITOLO 4

4.0 CASO PRATICO

4.1 TRANSAZIONE SU BLOCKCHAIN

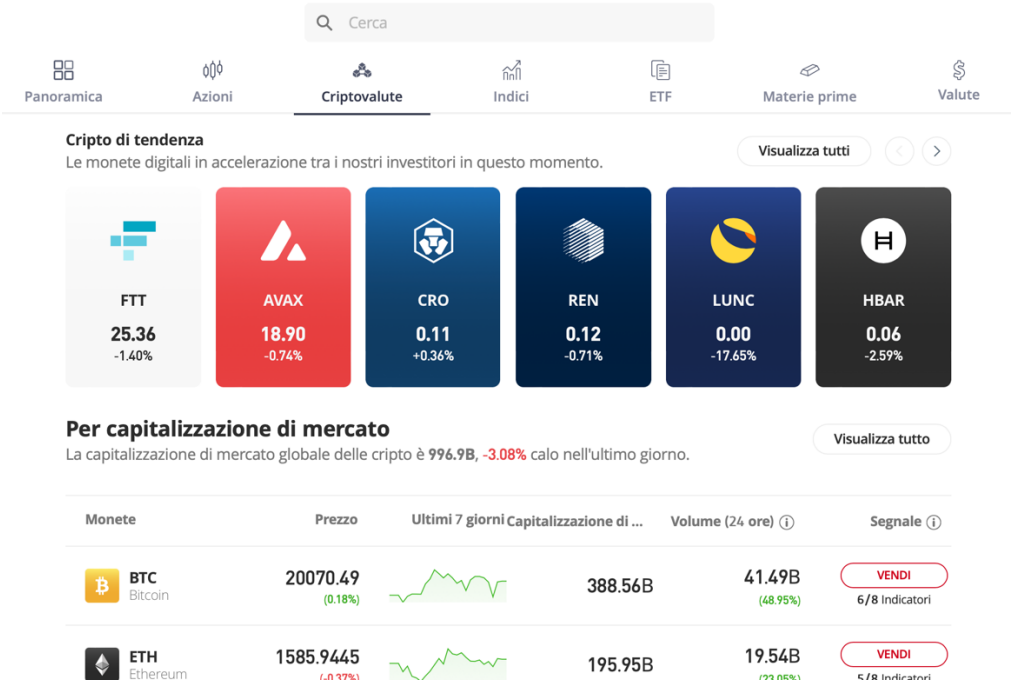
Il primo passo per poter effettuare una transazione su una determinata blockchain consiste nella creazione di un wallet cripto, che ci permetta, poi, di poterla svolgere. Nel mio caso, disponendo, per interessi personali, della piattaforma eToro.com, ho deciso di creare un account su eToro money, un mobile wallet. Quest'ultimo corrisponde ad un wallet cripto, offerto gratuitamente agli utenti della piattaforma stessa. Al fine della creazione, la quale risulta molto intuitiva, è necessario accedere all'app da mobile "eToro Money" e seguire l'autenticazione a due fattori. Il nome utente e la password utilizzati per l'accesso al wallet sono i medesimi che permettono l'accesso al suddetto exchange.

Nel momento in cui si effettua il login, si visualizzano tre schede: la prima, a sinistra, indicante il saldo, inteso come quantità di criptovalute detenute nel portafoglio; la seconda contiene, invece, le transazioni effettuate nella sezione investimenti di eToro; la terza, infine, indica la disponibilità, ossia il denaro FIAT di cui si dispone all'interno del wallet. Viene concessa la possibilità, non solo di trasferire criptovalute all'interno del wallet, ma anche di acquistarle al prezzo corrente, usufruendo dell'exchange di riferimento.

Per lo svolgimento di questa prova pratica, ho effettuato l'accesso alla mia area personale di eToro e, successivamente, mi sono recato nella sezione "Criptovalute", in cui possiamo visualizzarne più di 120 tipi.

Tutte le immagini inserite in questo capitolo corrispondono a screenshots effettuati da me medesimo.

Figura 10: Sezione Criptovalute di eToro.



Ho deciso di acquistare il token “ADA”, cryptovaluta scambiata sulla blockchain Cardano, e, attraverso un investimento di $51, ne ho acquistato 107.12 unità. Il prezzo pagato, per ogni unità, è stato 0.4761 dollari.

L’investimento è stato reso immediatamente visualizzabile all’interno della sezione “Portafoglio”, della mia area riservata. Cliccando, successivamente, sulla voce “dettagli dell’acquisto”, interna a tale sezione, appare una schermata in cui vengono indicati il prezzo di acquisto dell’asset, la quantità acquistata, la data e l’orario di acquisto. Inoltre, sotto al numero di quantità acquisite appare la dicitura “trasferisci al mio wallet”; cliccandoci sopra, ho trasferito le coin detenute dall’exchange al portafoglio precedentemente creato. Prima che il trasferimento si completi, appare una pagina in cui vengono indicate le unità che si intendono trasferire e le commissioni che saranno poi applicate da eToro per lo svolgimento dell’operazione, che nel mio caso sono state pari a poco più di 2 ADA ($1).

Le fees di eToro per il trasferimento di cripto dall’exchange ai wallet corrispondono al 2%, con un minimo di $1 e un massimo di $100. Per depositi superiori a $5000 di valore, la commissione massima sarà sempre pari a $100.

L’operazione viene successivamente sottoposta ad una fase di verifica, durante la quale la piattaforma preleva i token dal nostro exchange e ne controlla la validità. Nel caso di esito positivo, verranno accreditate le criptovalute all’interno del nostro wallet e potremmo visualizzarle nella sezione “Saldo”.

È importante ricordare che all’interno dei wallet non sono contenute le coin, ma, solamente, le chiavi private, che ci permettono di fruirne. Il portafoglio, infatti, permette di visualizzare il valore degli unspent transaction output di cui disponiamo all’interno di ogni diverso registro distribuito. Di conseguenza, nel momento in cui decideremo di effettuare una transazione, non invieremo effettivamente i token, ma firmeremo le operazioni che ci permettono di spenderli. Come affermato precedentemente, infatti, ogni criptovaluta possiede la relativa blockchain di riferimento e, di conseguenza, deteniamo tante chiavi private, quanti sono i registri distribuiti in cui operiamo. Difatti, le transazioni sono caratterizzate da codici identificativi che differiscono tra di loro in base alla blockchain a cui appartengono.

Nel mio caso, è possibile notare il valore complessivo dei token di cui dispongo sulla blockchain ADA:

Figura 11: Saldo Wallet.

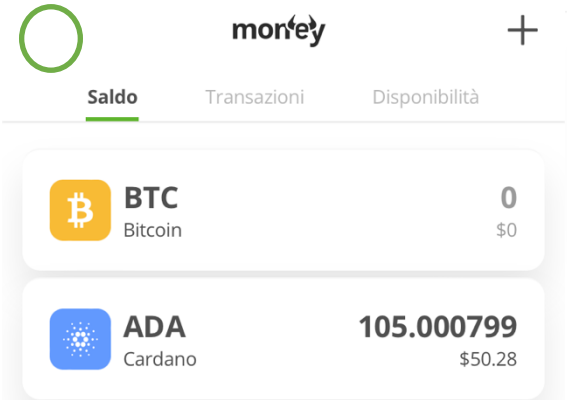
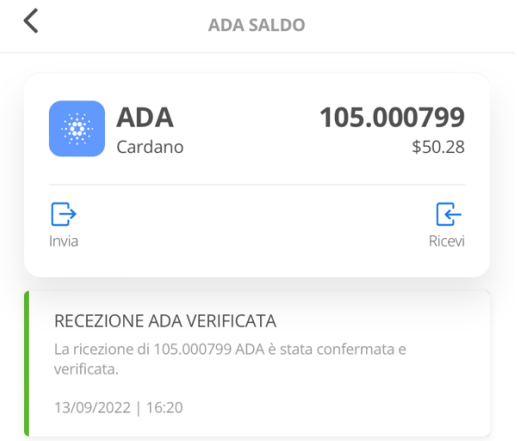


Figura 12: Saldo ADA.



Come si può osservare nella figura 11, nella sezione “Saldo” è presente sia la dicitura “BTC” sia “ADA”. Ciò significa che, nel mio wallet, sono state archiviate due chiavi pubbliche e due private: una coppia funzionante nella blockchain Bitcoin e una in Cardano.

Per quanto riguarda il saldo di ADA, cliccando sopra l'icona, possiamo visualizzare la quantità di token in nostro possesso e, inoltre, il giorno e l'orario in cui è avvenuta la transazione verificata, che ha portato alla ricezione. Successivamente, selezionando "RICEZIONE ADA VERIFICATA", navighiamo all'interno dell'explorer della blockchain in questione, Cardano, e abbiamo la facoltà di verificare una serie di dati su di essa, come l'ID dell'operazione e la numerazione del blocco in cui è contenuta.

Trattando, ora, in concreto, il trasferimento dei token ad un altro wallet, mi sono servito, per l'esecuzione della transazione, di quello posseduto da un compagno di studi, offerto da Coinbase. Ciò a dimostrazione del fatto che la diversità del provider del wallet non condiziona l'esecuzione e il compimento dell'operazione, ma ne modifica solamente l'interfaccia visualizzata.

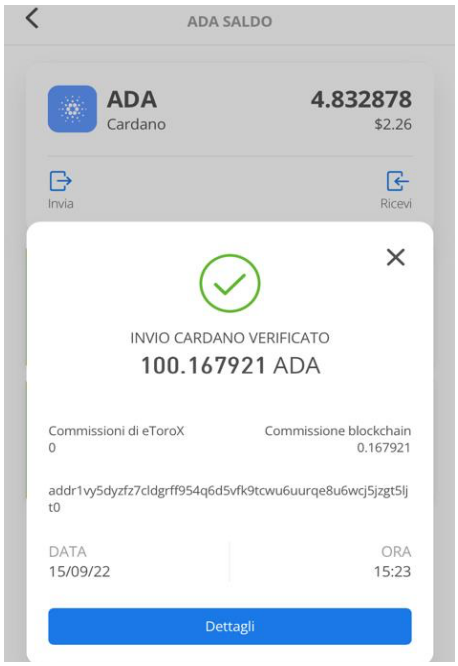
Dopo essermi fatto comunicare l'address pubblico della blockchain Cardano, ho predisposto la transazione, inserendo i dati richiesti, e, successivamente, cliccando sulla voce "invia", selezionando 100 unità di criptovaluta, le ho inoltrate all'indirizzo: 'addr1vy5dyzfz7cldgrff954q6d5vfk9tcwu6uurqe8u6wcj5jzgt5ljt0'.

È, immediatamente, apparsa la quantità di fees richieste dalla blockchain per il completamento dell'operazione: 0.167921 unità di ADA, al tasso di conversione attuale corrispondenti a circa $0.079.

Nel momento in cui si decide di inviare una transazione, il wallet richiede una verifica dell'identità, la quale può consistere in un codice pin sul telefono o in una conferma tramite Face ID, a seconda del tipo di portafoglio utilizzato.

A questo punto, bisogna attendere solamente la convalida definitiva da parte del network. Una volta ricevuta, il nostro saldo sarà decurtato dei token inviati e visualizzeremo una notifica relativa all'invio.

Figura 13: Transazione verificata.



Cliccando sulla voce “Dettagli” della figura 13, possiamo visionare tutti i dati della transazione, come è illustrato dalla figura 14.

Figura 14: Cardano blockchain explorer.

Il numero del blocco di riferimento corrisponde ad uno dei dati più importanti, in quanto attraverso questo, chiunque, in qualsiasi momento, entrando nella blockchain Cardano

e inserendo l'ID della transazione, può verificare l'effettivo spostamento delle criptovalute.

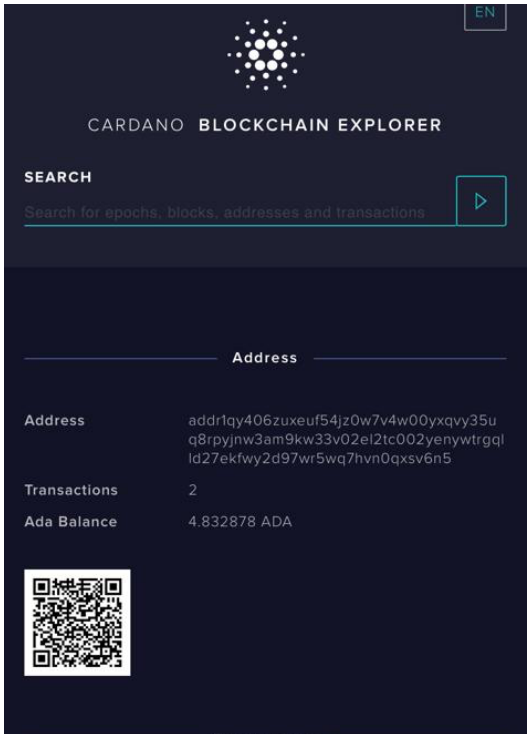
Dal mio personal wallet l'importo totale inviato corrisponde a 100.167921 ADA, mentre il total output risulta pari a 104.832878 ADA, maggiorato di una transaction fee, trattenuta dalla blockchain, di 0.167921 ADA. Sorge spontaneo chiedersi: perché sono stati compresi anche i 4.832878 ADA, che si trovavano nel portafoglio?

Come affermato precedentemente, nel capitolo 1.2, nel momento in cui si effettua una transazione, a meno che il valore non sia pari a quello delle nostre unspent transaction, se ne genereranno due. Una di queste a favore del portafoglio del beneficiario, l'altra, che prende il nome di "change", invece, di ritorno nel wallet dell'emittente.

Approfondendo questo concetto, nel momento in cui ho inviato 100 ADA, la blockchain ha utilizzato la mia transazione unspent di 105.000799 ADA. I token in questione sono transati tutti all'interno della blockchain CARDANO: 100 di questi sono stati inviati al destinatario, 0.167921 prelevati, invece, come commissione e i restanti 4.832878 mandati nuovamente al mio wallet.

Come spiegato in precedenza, ciò corrisponde ad un modo per rendere completamente verificabile che le coin detenute dipendano esclusivamente da transazioni non ancora spese o porzioni di esse.

Figura 15: Il Change.



Il tutto è illustrato nella figura 14, nella quale il portafoglio che ha effettuato la transazione, non solo è riportato come mittente, ma è, anche, affiancato a quello del beneficiario, tra i riceventi. Infatti, si otterrà, un flusso di ritorno pari al saldo disponibile a seguito della transazione. È possibile equiparare il nostro wallet ad un motore di ricerca come Google o Firefox, i quali permettono agli utenti di navigare attraverso i vari siti: in questo caso, è concessa la possibilità alla community di visulizzare le diverse blockchain.

Effettuare transazioni attraverso questi portafogli non è affatto complicato, in più, le commissioni che la blockchain applica per il compimento delle operazioni sono relativamente basse. Fondamentale rimane la scelta del wallet nel quale si verseranno i propri fondi, al fine di una valutazione della convenienza relativa all'acquisto di criptovalute.

CONCLUSIONI

Ho deciso di redigere questo elaborato per illustrare, in modo sintetico, il funzionamento della blockchain, strumento a mio avviso rivoluzionario. Ritengo sia inopinabile il fatto che, a partire dal 2008, anno in cui è nata, abbia cambiato la vita di molte persone.

È corretto e, quanto meno, necessario trattare questo argomento associandolo alle criptovalute, soprattutto a Bitcoin, ma è fondamentale tenere a mente che questo non corrisponde all'unico possibile ambito di applicazione. In pochi anni, infatti, ha la possibilità di rendere più agevoli le operazioni in svariati settori: finanziario, sanitario, assicurativo e non solo. Questi ultimi, difatti, condividono la conservazione permanente dei registri e l'elaborazione efficiente delle transazioni finanziarie e informative, aree in cui la blockchain può notevolmente semplificare i processi attuali. La varietà di situazioni in cui potrebbe essere implementata questa tecnologia non concerne solamente gli ambiti suindicati, ma anche i contratti, le proprietà e tutte le transazioni dei mercati finanziari.

L'invenzione di questo strumento rappresenta un enorme cambiamento tecnologico che porta con sé opportunità interessanti e tangibili. Tuttavia, permangono diverse minacce. Le autorità centrali, principale nemico del sistema della blockchain, risolvono non solo il problema della fiducia nella certificazione delle transazioni di valore, ma forniscono una supervisione essenziale sul processo stesso, ad esempio garantendo un livello ragionevole dell'asimmetria informativa tra le parti che stipulano qualsiasi tipo di contratto, soprattutto nel mondo finanziario. Consentire alle persone di trasferirsi direttamente valore oppure permettere alle aziende di raccogliere facilmente capitali può incrementare l'efficienza finanziaria, ma offre, anche, spazio a frodi e comportamenti scorretti.

Oggigiorno, le aziende interessate a raccogliere fondi, attraverso strumenti innovativi, come il crowdfunding, oppure tramite enti tradizionali, come i mercati finanziari pubblici, sono tenute a divulgare le informazioni rilevanti e a essere sottoposte ad un profondo processo di verifica. Le autorità di regolamentazione dovrebbero garantire lo stesso livello di controllo sulle società, che raccolgono fondi tramite offerte iniziali di token o altri tipi di offerte presenti su blockchain. Ritengo che il primo passo verso una regolamentazione equa di questa tecnologia sia la comprensione del suo impatto sulla società in un futuro prossimo. Indubbiamente stare al passo con la rapida evoluzione di questi strumenti può risultare complesso, ma, prima le organizzazioni faranno proprie queste tecnologie, più probabilmente saranno in grado di integrarle nei processi aziendali, traendone enorme vantaggio.

Non è possibile prevedere facilmente il panorama tecnologico futuro e come in questo si inserisca esattamente la blockchain, ma, all'orizzonte, sono visibili buoni segnali che lasciano desumere un ipotetico sviluppo esponenziale. Nell'epoca attuale, caratterizzata da crisi e scandali, causati dalla poca trasparenza dei mercati, la blockchain può aumentare la fiducia dei partecipanti al mercato finanziario, presentandosi come un registro distribuito e non modificabile. Ulteriori benefici sarebbero riscontrabili nello snellimento dei processi e delle tempistiche, nonché nell'aumento della liquidità dei mercati.

In un futuro non molto lontano potrebbe essere possibile trovare Bitcoin, Ethereum o qualsiasi altra criptovaluta all'interno del bilancio di qualche Banca Centrale. Dopotutto, se anche aziende come Tesla, Microstrategy e Square hanno deciso di detenere Bitcoin all'interno del loro stato patrimoniale, forse non si tratta di uno scenario così improbabile. Sicuramente, è necessario tener conto del fatto che queste valute sono nate proprio per cercare di essere indipendenti dal sistema bancario ordinario. Finora, questa tendenza si è trattata, per la maggior parte, di un approccio unidirezionale, in quanto non mi sento di affermare che il sistema bancario abbia generalmente cercato di ostacolare l'avvento di questa tecnologia.

Infatti, esistono, già ora, diversi gruppi bancari che accettano Bitcoin e altre criptovalute, dunque, forse è proprio vero il detto "se non puoi sconfiggere il tuo nemico, unisciti a lui".

BIBLIOGRAFIA

Ammous, S. (2018). *Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley & Sons, Incorporated, John.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.

Darie, C., & Brinzarea, B. (2007). *AJAX e PHP: Sviluppare applicazioni web dinamiche*. Packt Publishing.

Giani, D. (2017). *Come le Applicazioni Stanno Cambiando il Mondo: Cosa Devi Fare per Sfruttarle Nel Tuo Business*. Independently Published.

Guan, J., Huang, L., Zheng, G., & Gao, L. (2020). *Ethereum Smart Contract Development in Solidity*. Springer.

Higgins, M. G. (2019). *Cryptocurrency*. Saddleback Educational Publishing, Incorporated.
Rijmenam, M. V., & Ryan, P. (2018). *Blockchain*. Taylor & Francis Group.

SITOGRAFIA

Blockchain cresce, prepara rivoluzione Web3 - Hi-tech.
AgenziaANSA: *https://www.ansa.it/sito/notizie/tecnologia/hitech/2022/01/21/cresce-nel-mondo-blockchain-39-ma-mercato-italia-fermo_599381b6-fac0-43ee-bc77-e1d5fad7176a.html*

Crypto & Blockchain.
Forbes. *https://www.forbes.com/crypto-blockchain/?sh=abc5e4b2b6ee*

Blockchain.
Wikipedia, l'enciclopedia libera. *https://it.wikipedia.org/wiki/Blockchain*

Correspondent, M. S. T. (2022, 15 settembre). Bitcoin rival ethereum cuts power consumption by 99.95%. The Times & The Sunday
Times. *https://www.thetimes.co.uk/article/crypto-cuts-its-carbon-footprint-as-bitcoin-rival-ethereum-slashes-power-consumption-by-99-95-ql5h2g2b6*

Il Sole 24 Ore. (2022, 2 maggio). Come funziona la blockchain?
Il Sole 24 ORE. *https://www.ilsole24ore.com/art/come-funziona-blockchain-AEk3yJOB*

Blockchain Definition - Investing.com.
Investing.com. *https://www.investing.com/education/terms/blockchain-200408966*

Criptovalute - MilanoFinanza.it.
Milano Finanza. *https://www.milanofinanza.it/news/mytech/criptovalute*

Mercato crypto - Prezzi e capitalizzazione di mercato.
Young Platform | Compra Bitcoin, è semplice. *https://youngplatform.com/exchange/*

Basile, M. (2021, 15 novembre). Il mistero di Satoshi Nakamoto: una causa da 64 miliardi potrebbe smascherare il vero padre del bitcoin.

Repubblica. *https://www.repubblica.it/economia/2021/11/15/news/il_mistero_di_satoshi_nakamoto_una_causa_da_64_miliardi_potrebbe_smascherare_il_vero_padre_del_bitcoin-326514556/*

Lopp, J. (2016, 9 aprile). Bitcoin and the Rise of the Cypherpunks.
CoinDesk: Bitcoin, Ethereum, Crypto News and
Price. *https://www.coindesk.com/markets/2016/04/09/bitcoin-and-the-rise-of-the-cypherpunks/*

Introduzione agli Smart Contract | ethereum.org
Ethereum.org. *https://ethereum.org/it/developers/docs/smart-contracts/*
https://www.ibm.com/topics/smart-contracts

Bloomberg - Are you a robot?
Bloomberg. *https://www.bloomberg.com/news/articles/2022-09-15/ether-miners-are-piling-up-losses-after-shifting-to-altcoins*

Frankenfield, J. (2017, 3 maggio). What Does Proof-of-Stake (PoS) Mean in Crypto?
Investopedia. *https://www.investopedia.com/terms/p/proof-stake-pos.asp*

Borsa Italiana. *https://www.borsaitaliana.it/borsa/glossario/proof-of-work.html*

Blockchain Explained: The rise of private blockchains | Euromoney Learning.
The leading authority for the world's banking and financial markets |
Euromoney. *https://www.euromoney.com/learning/blockchain-explained/the-rise-of-private-blockchains*