LUISS

Dipartimento
di Impresa e Management

Cattedra Informatica

Blockchain & Criptovalute

Prof. Luigi Laura
RELATORE

Matr. 220091
CANDIDATO

Anno Accademico 2019/2020

Blockchain e Criptovalute

INTRODUZIONE

Il seguente elaborato ha come oggetto una nuova e fiorente tecnologia informatica annessa ai suoi primi utilizzatori: la *blockchain* e le criptovalute. Lo scopo finale di esso non è solo quello di elencarne le varie caratteristiche di base, ma l'intento è il voler fornire un documento scritto che abbia anche un valore formativo sui temi discussi. Come da indice, nella prima parte dell'elaborato, si prenderanno in considerazione le caratteristiche e le novità che la *blockchain* ha portato con sé all'interno del mondo informatico, sottolineando, inoltre, i suoi sviluppi e le sue possibili problematiche. Per converso, nella seconda parte, si proseguirà con un'analisi delle *digital currency*, non solo da un punto di vista meramente finanziario, ma anche tecnologico. Auguro a tutti una buona e gradita lettura.

La tecnologia *blockchain* deve le sue origini a *Satoshi Nakamoto*, pseudonimo assegnato all'individuo o al gruppo di individui, non ancora identificati, che nel 2008-2009 hanno rilasciato la prima criptovaluta al mondo: *Il Bitcoin*[1]. La stessa moneta ha, nei suoi primi anni, messo assolutamente in ombra la struttura che le faceva da spina dorsale: la *Blockchain*. Solo grazie al boom riconducibile all'anno 2016, ben otto anni dopo dalla sua prima pubblicazione, grazie ad un'impennata del valore di Bitcoin, si iniziò a prendere in considerazione cosa effettivamente vi fosse dietro la criptovaluta. Venne alla luce il potenziale della *Blockchain*. Le caratteristiche più interessanti, che avevano in particolare incuriosito gli utenti, riguardavano proprio la sua trasparenza e tracciabilità. Vennero successivamente svolti numerosi studi per sfruttare tale tecnologia in settori tradizionali come quello agricolo o come quello politico. Vennero fuori, inoltre, differenti possibilità sulle molteplici destinazioni d'uso, di cui, di seguito, alcuni esempi. Negli ultimi periodi la *blockchain* è stata protagonista di varie sperimentazioni come quella della *ballotchain*[2]. Detto in parole povere si è voluta implementare la catena di blocchi come "gestionale" per delle elezioni. In sintesi è possibile:

- Tracciare, costantemente ed in modo sicuro, le evoluzioni di una votazione elettorale;
- Evitare, inoltre, la possibilità di una doppia votazione, che è assimilabile al problema del *double spending* di *Bitcoin* che sarà trattato successivamente;
- Risparmiare tempo e denaro[2].

Un esempio pratico viene dal nostro stesso Stato, o meglio dal nostro ministero dello sviluppo economico, intenzionato ad implementare la *blockchain* per la tracciabilità del made in Italy[3]. Anche qui i vantaggi sono similari ai precedentemente elencati. Un altro settore che si è interessato a questa tecnologia è quello sanitario. Si andrebbe, dunque, ad implementare la "catena" per l'identificazione dei pazienti, per la tracciabilità delle prescrizioni e per la corretta applicazione dei protocolli sanitari. Ultime, ma non per importanza, le grandi aziende. Esse potrebbero facilmente adottare nel loro circuito una *blockchain* "centralizzata" capace di tenere traccia di: dipendenti, stipendi, spedizioni, acquisti e vendite. Questo breve *excursus* ci ha anticipato una delle caratteristiche principali della *blockchain*: *la programmabilità.* La capacità, dunque, che questa magnifica tecnologia ha di essere potenzialmente programmata e sfruttata per gestire in un modo più economico ed efficiente un processo gestionale classico. Non è infatti assolutamente da considerare la catena di blocchi un meccanismo esclusivo delle *digital currency.*

[1] <https://it.wikipedia.org/wiki/Bitcoin> Ultima consultazione aprile 2020
[2] <https://www.reply.com/it/content/ballotchain> Ultima consultazione aprile 2020
[3] <https://www.mise.gov.it/index.php/it/blockchain/blockchain-per-il-made-in-italy> Ultima consultazione aprile 2020

Blockchain definizione

La *blockchain* (letteralmente "catena di blocchi") è una struttura di dati condivisa[4]. Quest'ultima è alla base delle più o meno conosciute criptovalute. In termini più tecnici possibile rappresenta un registro digitale in cui sono memorizzati dei *record*, che per semplificare chiameremo *"transazioni"*. È un sistema sicuro, verificabile e permanente[4]. Una volta scritto un dato su di un blocco non sarà possibile procedere ad una sua modifica senza che vengano alterati i blocchi successivi ad esso. Siamo di fronte ad una lista di transazioni che vengono rese sicure mediante l'uso della *crittografia*. Ogni blocco può includere una o più transazioni, ed immagazzina un *hash* del blocco precedente. Ogni transazione, a sua volta, viene verificata da un comune *meccanismo di consenso.* Procedendo con l'analisi dettagliata della catena mi preme elencarne le caratteristiche principali, riassumibili in:

- *Sicurezza*
- *Programmabilità*
- *Trasparenza*
- *Immutabilità*
- *Consenso*
- *Decentralizzazione*[5]

definiremo le seguenti caratteristiche lungo tutto l'elaborato.

Blockchain Decentralizzazione

Il concetto di *decentralizzazione* introdotto dalla *blockchain* è di fondamentale importanza. Per poterne descrivere le caratteristiche potremmo prendere come esempio un classico ente "centralizzato": la nostra BCE. L'ente gestisce, verifica, e monitora tutti i movimenti della valuta FIAT europea: l'euro. Conseguentemente tutti i "clienti" della BCE (banche e Stati) dovranno sempre rispettare e mantenere i "vincoli" imposti dalla stessa. Tutto ciò può avvenire grazie all'importanza del ruolo stesso della BCE che ad oggi è considerato come Nucleo centrale garante della "fiducia" da parte degli enti sottostanti. Possiamo tradurre nel nostro mondo informatico il rapporto della BCE come *uno-a-tanti,* divenendo una sorta di *centralized ledger (*Libro mastro centralizzato). Il libro mastro servirà a registrare tutti i dati risultando come documento *unico e privato*. Si occuperà quindi la stessa BCE di gestirne ed inserirne i dati all'intero, anche grazie alla "fiducia" fornitagli dagli enti-clienti. Partendo da questa breve spiegazione possiamo ricondurci alla definizione di *Decentralized Ledger*. Siamo di fronte ad un insieme di *satelliti* che mantengono il rapporto *uno-a-tanti* relazionandosi, a

[4] <https://it.wikipedia.org/wiki/Blockchain> Ultima consultazione aprile 2020
[5] <https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante> Ultima consultazione aprile 2020

loro volta, tra di loro, sempre con un rapporto *uno-a-tanti*. Non vi è più, quindi, la presenza di un unico ente centrale, ma un insieme di piccoli nuclei centrali che interagiscono tra loro. Anche qui il concetto di fiducia risulta essere di fondamentale importanza poiché, differentemente da un *centralized ledger*, ci saranno un insieme di *satelliti* che non risponderanno direttamente ad un nucleo centrale, ma risponderanno direttamente ad un altro *satellite centrale secondario* più vicino ad esso. Un esempio pratico per comprendere questo processo è l'autonomia che le regioni hanno rispetto allo stato. Quindi, in caso di particolari "materie", sarà la stessa regione ad occuparsi di monitorare, verificare e processare la richiesta, divenendo un vero e proprio *nucleo centrale secondario*, secondo una struttura basata anche qui sulla "fiducia". Avremo quindi *satelliti* più piccoli, province e comuni, che non andranno ad interfacciarsi con un unico nucleo centrale (lo stato), ma con il *satellite di rappresentanza* più vicino. La *blockchain* è andata oltre, poichè aveva la necessità di mantenere il concetto di "fiducia" che l'ente centralizzato garantisce, ma, allo stesso tempo, di lasciare la massima autonomia ad ogni *satellite* sia piccolo che grande. Si è così dato origine alla *distributed ledger*. Con il libro mastro distribuito non si ha più un ente centrale o più enti centrali secondari più piccoli ma, tanti *satelliti*, che chiameremo *nodi,* alla cui base vige un nuovo concetto di fiducia. È qui che interviene il *meccanismo di consenso,* comune a tutta la catena di blocchi. La prima notevole differenza riguarda proprio *il libro mastro*. Quest'ultimo, differentemente da un sistema centralizzato, non è più unico e privato ma, *pubblico e autentico*. Ogni utente ha la sua copia del libro mastro, e può inviare o ricevere transazioni. Per ogni transazione il rapporto di fiducia verrà condiviso da tutti i *nodi,* che avranno la possibilità di visionare il libro mastro aggiornato della stessa transazione. Tali caratteristiche definiscono anche il concetto di *trasparenza* già citato nel paragrafo precedente.

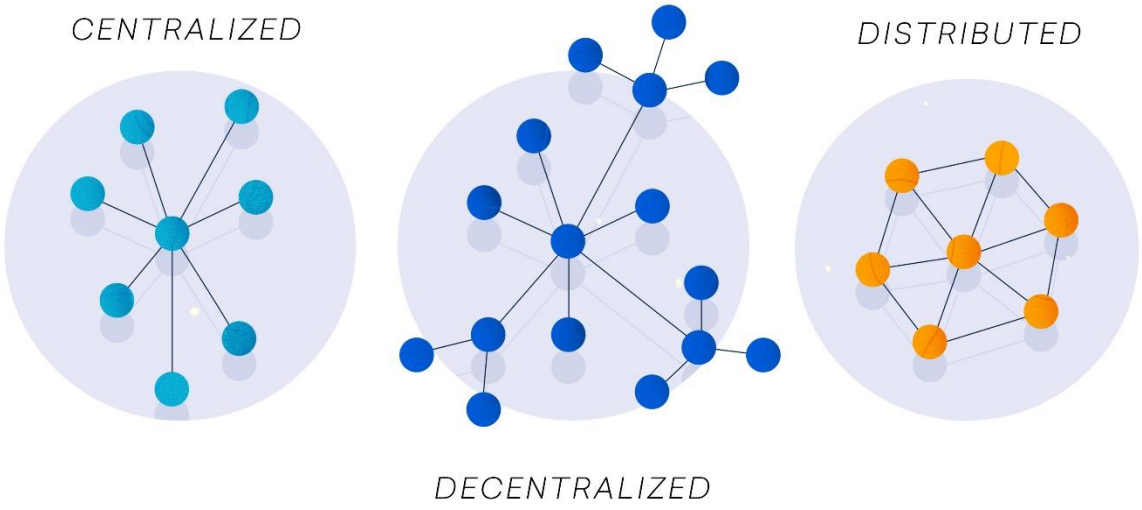

Figura 1 Rappresentazioni del collegamento dei nodi tra i vari tipi di ledger. Fonte[6]

[6] <https://www.cryptopostgazette.com/centralized-vs-decentralized-vs-distributed-network/> Ultima consultazione aprile 2020

Blockchain *immutabilità*

Ritorniamo a parlare di un classico *centralized ledger*. Esso verrà aggiornato ed eventualmente modificato direttamente dal nucleo centrale, in quanto ne ha autorità. Il criterio di *immutabilità,* regola fondamentale della *blockchain*, sottolinea come, nessuno, pur possedendo una copia del libro mastro e pur partecipando alla catena, possa modificare quest'ultima in modo illecito e/o senza modificare l'intera sequenza di blocchi successiva alla eventuale modifica. C'è però una possibilità, sempre previo consenso comune di tutti i partecipanti alla *blockchain*, di "tornare indietro" con la catena ed eventualmente modificare un intero blocco o un'intera transazione. Questo processo è estremamente raro, ed è in particolare utilizzato per la risoluzione di eventuali violazioni sulla catena stessa, come nel caso di un possibile *double spending.* Questo evento non risulta assolutamente comune poiché, un adeguato sistema di consenso, non ne permetterebbe la fattibilità, ciononostante rimane un *topic* del mondo delle criptovalute, con un riferimento particolare a *blockchain* che possiedono strutture piccole e meno complesse. Vedremo successivamente di cosa si tratta. Fortunatamente, grazie alla stessa caratteristica della *trasparenza,* è possibile rendersi conto in modo più o meno rapido di una violazione simile e correre ai ripari. Ricordiamo, inoltre, che la *blockchain* possiede una sorta di *governance* ed un insieme di regole ben definite, mantenute in piedi dal concetto di fiducia, che fungono, da filtro, anch'esse, contro le violazioni. Una violazione effettuata da un nodo non rispetterebbe il concetto di fiducia e le regole di base, mettendo in cattiva luce la stessa catena. In automatico le caratteristiche peculiari verrebbero meno, svalutando anche l'eventuale *token* o *digital currency*. Di conseguenza ci sarà un deprezzamento che renderà controproducente qualsiasi violazione. Si tende perciò ad evitare eventi simili considerando le possibili conseguenze, economiche e di notorietà, sulla criptovaluta. Gli utilizzatori della *community* della *Blockchain* operano come nella realtà e le violazioni e le irregolarità, ovviamente, vengono condannate ed evitate grazie al senso civico della maggior parte dei cittadini.

Sicurezza: Crittografia asimmetrica

C'è da premettere che di base la nostra *blockchain* sfrutta un sistema di connessione *peer-to-peer.* Il sistema *blockchain* garantisce la sua *sicurezza* grazie all'uso della *crittografia asimmetrica*, la quale si basa sull'utilizzo di una coppia di chiavi, *una privata ed una pubblica*. Per poter comprenderne meglio il funzionamento, effettuiamo un esempio di trasferimento di informazioni crittografate da un personaggio A, ad un personaggio B. Nel caso in cui A volesse inviare un file di testo a B e volesse esser sicuro che solo e soltanto B abbia la possibilità di leggerlo, la procedura sarebbe la seguente:

- A Produrrà il file di testo
- A cripterà il file di testo con la *chiave pubblica* di B

- B riceverà il file di testo criptato che decripterà con la sua *chiave privata*

Figura 2 Procedura Grafica di invio file crittografato da A a B. Fonte[7]

Dalla figura deduciamo come una volta criptato il file di testo, solo una ed una sola chiave privata permetterà di sbloccare e di leggere il file.

Facendo un giro contrario vediamo come B invia un file ad A.

Figura 3 Procedura Grafica di invio file crittografato da B ad A. Fonte[7]

In questo caso il file di testo in mano a B dovrà essere criptato con la chiave pubblica di A che, una volta ricevuto il file criptato, avrà la possibilità di decriptarlo con la sua chiave privata. Il sistema di *crittografia asimmetrica,* su elencato, ci garantisce un livello di *sicurezza* elevato, in caso di invio di documentazioni/transazioni importanti.

[7] <https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html> Ultima consultazione aprile 2020

Questa medesima procedura è adottata dalla *blockchain* per trasferire quantitativi di moneta virtuale da un portafoglio ad un altro.

Blockchain Struttura del blocco

Un blocco è composto da due parti principali: *un Header ed un body*[4]. Nell'*Header* sono presenti 7 campi di gestione dello stesso, mentre nel *body* sono racchiuse le transazioni. I sette campi di gestione risultano essere:

- *Versione*[4]*:* numero di versione del software utilizzato;
- *Prevhash*[4] *(Hash del blocco precedente): hash* di 256 bit, legame del nostro blocco al precedente;
- *Merkleroot*[4]*:* hash degli hash di tutte le transazioni che possiamo trovare all'interno del blocco;
- *Timestamp*[4]*:* marchio temporale dell'ultima transazione che utilizza però un algoritmo già conosciuto.
- *Bits*[4]*:* campo che risulta essere di fondamentale importanza poiché esso identifica il valore target: il valore dell'hash dell'header di un blocco deve essere obbligatoriamente uguale se non minore a questo valore target affinché il blocco venga "verificato" ed accettato dalla rete;
- *Nonce*[4]*:* campo direttamente in stretto contatto con l'hash del blocco e con il valore target, poiché risulta essere un valore ad 8 byte, capace di influenzare la funzione di hash facendola variare fino a fare risultare il valore dell*'hash* minore di quello target. Vedremo come esso viene gestito dal meccanismo di consenso;
- *Numero transazione:* va semplicemente ad indicare il numero della transazione.

Di seguito un'immagine[8] di un blocco della blockchain con i relativi valori:

[8] <https://www.blockchain.com/btc/block/000000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501> Ultima consultazione aprile 2020

hash	00000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501
conferme	483
timestamp	2020-03-04 22:10
Altezza	620208
Minatore	F2Pool
Numero di transazioni	2.392
Difficoltà	15.486.913.440.292,87
Radice di Merkle	731af657f676d7c4db69a092a1f54905ac6ead7d03021ffdfacf6c6f82618351
Versione	0×20800000
bits	387.067.068
Peso	3.998.618 WU
Taglia	1.332.656 bytes
nonce	1.833.475.282
Volume delle transazioni	4107.84315750 BTC
Block Reward	12.50000000 BTC
Premio tariffa	0.12933880 BTC

Figura 4 Esempio di Struttura di un blocco della Blockchain di Bitcoin. Fonte[8]

Blockchain nodi

I nodi come abbiamo già anticipato, sono fondamentali per lo sviluppo e per il mantenimento della *distributed ledger;* qualsiasi utente che, tramite pc, si collega all'interfaccia Bitcoin è considerato un nodo. I funzionamenti principali sono il monitoraggio delle transazioni e l'aggiunta dei blocchi convalidati dal mining alla catena. Vari i tipi[9] di nodi:

- *Full nodes*
- *Mining node*
- *Super nodes*

[9] <https://www.binance.vision/it/blockchain/what-are-nodes> Ultima consultazione aprile 2020

- *Client lightweight (svp)*
- *Masternodes*

I *full nodes* sono i più importanti per la blockchain e forniscono stabilità e sicurezza. Sono definiti anche come *full validating nodes* poiché partecipano alla verifica delle transazioni e dei blocchi, secondo il meccanismo di consenso. Per poter attivare e mettere online un nostro *full node* di Bitcoin, possiamo avvalerci dell'utilizzo di *Bitcoin core,* ma attenzione ai requisiti minimi. Al di là dell'avere un sistema operativo aggiornato il nodo richiede non poco spazio di archiviazione. Attualmente sono necessari di base uno spazio di circa 200GB ed una ram di sistema di almeno 2GB. Di fondamentale importanza è la connessione internet che dovrà necessariamente essere illimitata, poiché si dovrà scambiare un numero elevato di dati con l'esterno. Sarà, dunque, obbligatorio avere una base di connessione anche in Upload. Si consiglia un minimo di 50 kb/s, molto bassa e facilmente gestibile dalle connessioni casalinghe tradizionali. Tutto questo perché un *full node* mensilmente è capace di trasferire in upload più di 200GB e in download più di 20GB. La necessità è di tenere acceso il *full node* per almeno 6 ore al giorno, ma sicuramente è sempre meglio tenerlo online 24/7. Il numero di nodi attualmente sulla rete bitcoin e più di 6000, alcuni risultano visibili ed altri no. I *super node,* anche conosciuti come *listening node,* sono dei nodi visibili pubblicamente, ossia, condividono informazioni con la community. Possono essere un importante ponte di informazioni e di fonti. Chiaramente questi ultimi risultano essere nodi molto grandi e stabili, quindi connessi 24/7 alla rete e richiedenti una potenza di calcolo più grande. Sarà molto probabile che un ipotetico *full node* gestito da noi risulti un nodo nascosto e quindi non pubblico e non utilizzabile da tutti come un listening node. I *miner nodes* sono necessari al sostentamento del mining e quindi del calcolo del protocollo di consenso che tratteremo successivamente. I *client lightweight,* meglio conosciuti come *simplified payment verification client,* partecipano alla rete bitcoin ma non sotto forma di *full node.* Questi ultimi non aiutano la sicurezza e non contribuiscono al sostentamento della *blockchain*. Da questi client è quindi possibile verificare se alcune transazioni sono state inserite o meno nel blocco e quindi validate. Le informazioni vengono direttamente acquisite e fornite da un *super node.* Molto spesso questi sistemi vengono utilizzati da diversi wallet per criptovalute. Ultimi, ma non per importanza sono i *masternode.* Questi nodi sono particolari di alcune *blockchain* come per Dash, un'importante *altcoin,* che utilizza la tecnologia dei *masternode* per gestire l'intera catena di blocchi; esso è facilmente assimilabile ad un *full node* ma con la peculiarità di ricevere *reward.* Si aggiunge, pertanto, alla solita lista dei protocolli di consenso, il cosiddetto *proof of service.* I *masternode* possiamo dunque catalogarli come un ibrido tra un mining node classico basato sul *proof of work* e il meccanismo di consenso *proof of stake;* infatti noi andremo a gestire un vero e proprio *full node* che dovrà necessariamente essere connesso 24/7 e dovrà essere collegato ad un portafoglio che include un esatto quantitativo della moneta. Questo nodo si occuperà di gestire, confermare e convalidare i blocchi ricevendo dei *reward* per il lavoro svolto.

Blockchain distributed ledger

La *distributed ledger* ha dato origine a due diversi generi: la *permissionless ledger*[5] e *la permissioned ledger*[5]. La prima come quella della *Blockchain Bitcoin* è un registro pubblico e di conseguenza aperto, non ha una "proprietà" specifica e nasce proprio per non essere controllata, pertanto potrebbero essere utilizzata come database globale con dati all'interno immutabili nel tempo. La seconda, altrettanto interessante, è riconducibile alle possibili destinazioni d'uso che abbiamo già trattato nella parte iniziale e risulta caratterizzata da una "proprietà". Il controllo, dunque, sarà solo concesso agli autorizzati. Ritornando al settore sanitario come esempio, il controllo non può essere autogestito dai pazienti stessi, poiché incompetenti sull'argomento, sarà quindi necessario avere una proprietà alla base che monitori il giusto funzionamento della catena. Pur avendo, dunque, un'impostazione distribuita, ci sarà una proprietà che si occuperà del controllo. Qui di seguito una tabella riepilogativa dei vari *Distributed ledgers.*

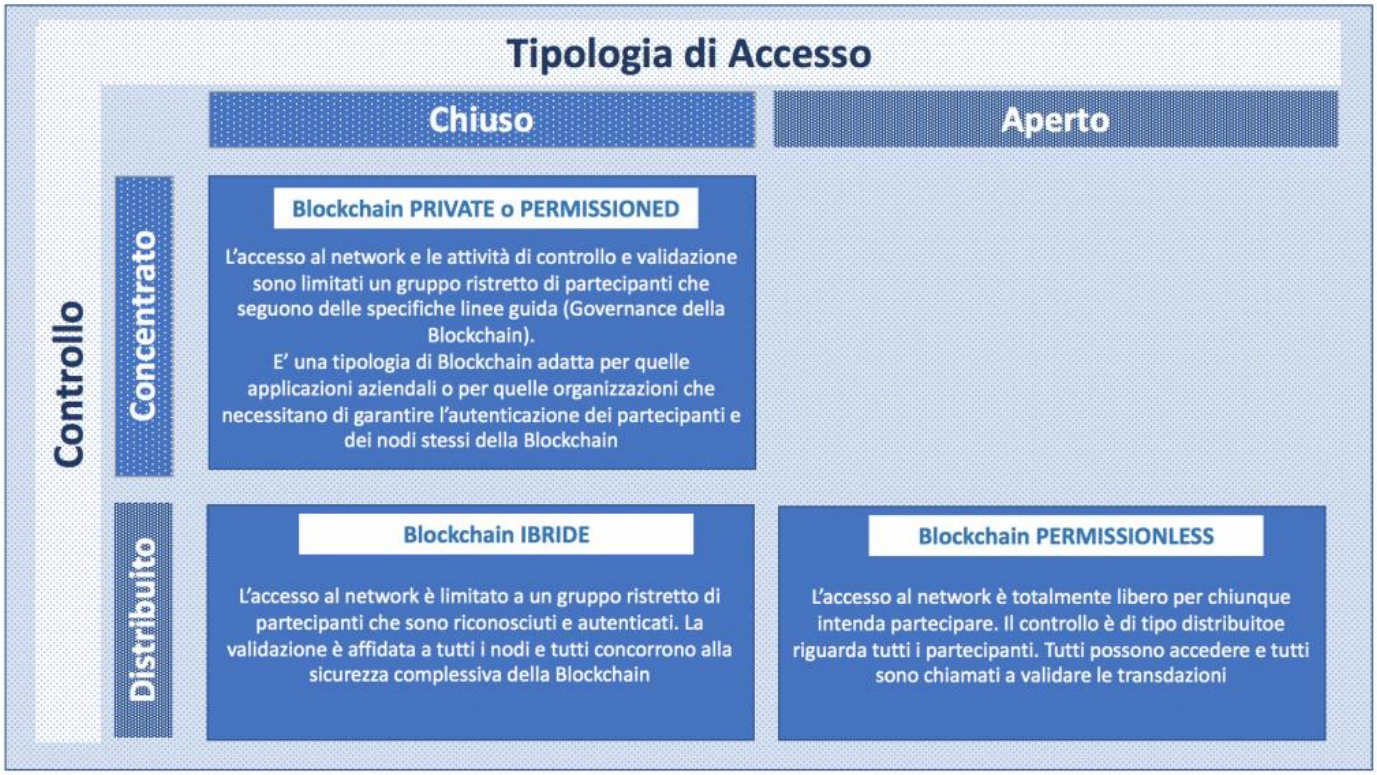

Tabella 1. Tabella riassuntiva tra i vari tipi di distributed ledger. Fonte[5]

Ritorniamo ancora a parlare di un ente centralizzato. Laddove il consenso all'elaborazione di un libro mastro avverrà per mezzo dello stesso ente. Sappiamo che nella *distributed ledger* non vi è più un ente centrale che ha la massima autorità su tutto, ma tutti i nodi si trovano allo stesso livello. Si ha bisogno dunque di un sistema di consenso distribuito o decentralizzato, che abbia la capacità di verificare le *transazioni* della catena. La prima *blockchain,* quella di *Bitcoin,* ha risolto questo problema sfruttando un meccanismo di consenso denominato *proof-of-work (POW)*[10], sistema nasce dall'idea di due informatici, Cynthia Dwork e Moni Naor, che hanno applicato il protocollo ad *Hashcash*[11]. *Hashcash* nasce con l'intento di scoraggiare gli attacchi informatici, facendo eseguire dei calcoli verificabili da un hardware corrispondente alla nostra CPU. Generalmente i più comuni attacchi informatici risultano essere i DOS (Denial of service[12]). Un attacco simile, infatti, causerebbe un intasamento di un *Client,* grazie all' invio di una grande mole di *spam mail,* che metterebbe fuori uso le risorse di sistema, causando un *crash* del servizio primario. Potrebbe questo essere il caso di un server su cui viene *hostato,* ossia gestito, un sito web che, di fronte ad una mole di numerose *spam mail,* non riesce a funzionare adeguatamente. *Hashcash* interviene risolvendo il problema con l'inserimento un piccolo calcolo nella intestazione delle e-mail. Inizialmente il mittente imposterà nell'intestazione un valore di base per il calcolo dell'*hash*. Quest'ultimo successivamente verrà calcolato prendendo in considerazione un algoritmo *sha-1* a 160 bit, per cui avremo 2^{160} soluzioni possibili. Da qui affinché l'intestazione risulti valida, sarà necessario che i primi 20 *bits* corrispondano a zero. In caso contrario si dovrà procedere al ricalcolo. Le soluzioni valide del calcolo risultano essere 2^{140} su 2^{160}. Mediamente, quindi, il mittente sarà costretto a "tentare" il calcolo 2^{20} volte, prima di trovare un risultato valido. Il tutto sembrerebbe richiedere una quantità di tempo non indifferente, invece, considerando un semplice *PC desktop* comune, basterà semplicemente circa un secondo per trovare un risultato. Considerando che chi fa spam ha la necessità di inviare più mail contemporaneamente e nella maggior quantità possibile, anche questo semplice secondo di calcolo per ogni mail, disincentiva l'operato dello *spammer*. *Bitcoin* ha deciso di adottare un sistema similare, sfruttando sempre un hash, ma basandosi sull' algoritmo *sha-256,* quindi su di un protocollo a 256 *bit.* La criptovaluta ha sfruttato la competitività creando così il *mining.* Nel nostro caso un *miner,* per mezzo dei *nodi* che raccolgono le *transazioni* non verificate, raggruppandole tutte in un blocco, si occupa di trovare il giusto *nonce* adatto a quel blocco, ossia un numero arbitrario che una volta inserito nel blocco restituisca un *hash* con tanti zeri *bit* quanti quelli necessari al valore target di rete in quel momento. Una volta trovato il *nonce,* il blocco verrà aggiunto alla catena, ed il suo *hash* diventa la sua impronta univoca. Il meccanismo di consenso

[10] <https://it.wikipedia.org/wiki/Proof-of-work> Ultima consultazione aprile 2020
[11] <https://it.wikipedia.org/wiki/Hashcash#Come_funziona> Ultima consultazione aprile 2020
[12]<https://it.wikipedia.org/wiki/Denial_of_service> Ultima consultazione aprile 2020

distribuito, che in questo caso è il *proof-of work,* garantisce la validazione dei blocchi e dunque anche delle transazioni.

Blockchain Mining

Abbiamo già anticipato nel paragrafo precedente il funzionamento del mining, ma non ci siamo soffermati in dettagli su alcune caratteristiche fondamentali di quest'ultimo. Abbiamo compreso che Il mining è il nostro ente che verifica le transazioni e convalida i blocchi, per aggiungerli successivamente alla catena. Volendo dare una definizione tecnica, il mining è un processo di *brute forcing* che ricerca il valore (*nonce)* adatto, da inserire nel blocco, tale da originare un *hash* del blocco corrispondente al valore target di quel momento. Essendo basato su di un algoritmo *sha-256,* il numero di zeri bit iniziali, affinché il blocco sia valido, non deve necessariamente sempre corrispondere ai primi 36 bits, ma questo valore varia in base alla *difficoltà di rete.* La difficoltà del mining è un valore fondamentale poiché più è alta, più saranno necessari "tentativi di calcolo" da parte degli hardware utilizzati per il mining per convalidare un blocco. Prendendo come riferimento la *blockchain di Bitcoin* noteremo che essa è un sistema progettato nei minimi dettagli tanto da reimpostare la difficoltà di rete, in modo tale da convalidare ed aggiungere un blocco alla catena con un intervallo di 10 minuti. Ciò significa che, nel caso in cui oggi la difficoltà di rete sia 1 e stessi minando unicamente io con il mio *hardware,* riuscirei a convalidare da solo un blocco ogni 10 minuti. Se subentrassero nella rete nuovi miner, per esempio altri 10, con *hardware* della stessa potenza di calcolo della mia, automaticamente riusciremo a convalidare un blocco in un tempo inferiore ai 10 minuti, tutto ciò se non aumentasse proporzionalmente la difficoltà di rete. La potenza di calcolo che noi offriamo alla rete può essere calcolata in *hash per secondo.* Un'ultima variabile che manca all'appello, ma fondamentale alla chiusura del cerchio per quanto riguarda il tema del consenso, è il *reward.* Il processo di mining, dunque, viene "ricompensato" per un ammontare fisso di un certo quantitativo di *digital currency,* fungendo automaticamente sia da incentivo, sia da forma possibile di guadagno. Per ogni blockchain ci saranno criteri di difficoltà di rete e di tempi di convalida di blocco differenti. Per esemplificazione utilizzeremo sempre la *blockchain di Bitcoin*.

Blockchain rewards

Il guadagno venuto fuori dal mining e di conseguenza, da ogni convalida di blocco, assume diverse forme in ogni tipo di *blockchain*. Per ogni blocco "minato" e convalidato spettano al *miner* 12.5 *Bitcoin*. Ipotizzando per assurdo di essere gli unici a minare nella *blockchain di Bitcoin,* guadagneremo ogni 10 minuti, 12,5 *Btc,* cifra considerevole, considerando il prezzo attuale sul mercato della moneta stessa. Sfortunatamente ciò non è assolutamente plausibile, o meglio, la rete *Bitcoin* è fitta di *miners* che con la loro enorme potenza di calcolo

raggiungono una potenza attiva totale, definita come *net hashrate*, di 117.000.000 *Tera Hash al secondo*[13]. Questo valore è molto importante poiché non solo al suo aumentare, aumenta la difficoltà di rete, ma fa capire quanta competitività c'è nella *blockchain di Bitcoin*. I *rewards* dunque avranno un particolare vincitore. Intuitivamente possiamo facilmente comprendere come sia necessaria un'enorme potenza di rete prima di riuscire a generare anche un solo Bitcoin al giorno.

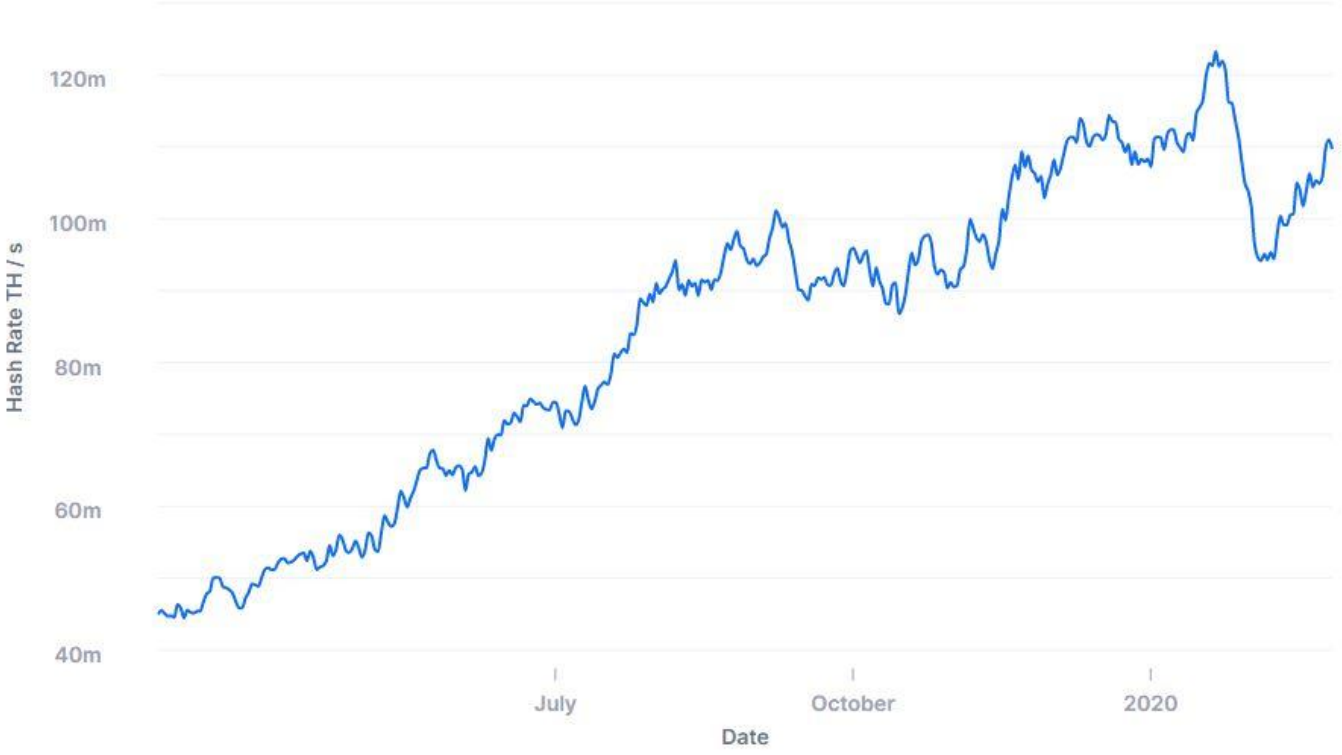

Figura 5 Chart Hashrate mondiale della Blockchain Bitcoin. Fonte[13]

Blockchain Halving

La questione *rewards* riserva altre sorprese. La *blockchain* è strutturata in modo tale da dimezzare il *reward* per blocco ogni tot numero di blocchi convalidati. In data marzo 2020 per ogni blocco convalidato viene distribuita una ricompensa di 12,5 BTC. Al raggiungimento del blocco numero 630.000 avverrà il cosiddetto

[13] <https://www.blockchain.com/charts/hash-rate> Ultima consultazione aprile 2020

"*halving*[14]" un vero e proprio dimezzamento dei *rewards* per blocco che passeranno da 12,5 a 6,25. *Satoshi Nakamoto* ha inserito questo protocollo per garantire una possibile stabilità del prezzo della criptovaluta, evitando il fenomeno inflattivo comune a tutte le monete FIAT che, differentemente dalle criptovalute, possono essere infinitamente stampate. Il seguente *halving*, dunque, dimezzerà anche le entrate di tutti gli attuali miner, che dovranno rimboccarsi le maniche ed eventualmente acquistare nuovi *Hardware* per mantenere una *revenue* adeguata. I *rewards* iniziali della *blockchain di Bitcoin* corrispondevano a 50 Btc per blocco. Fino a marzo 2020 abbiamo assistito esclusivamente a due halving, il primo che ha fatto dimezzare il reward per blocco a 25 ed il secondo che ha fatto dimezzare il reward per blocco da 25 a 12,5. La tabella[14] qui in basso mostra le date dei prossimi halving ed i rispettivi dimezzamenti del *reward.*

Halving	Est. Data	Altezza Blocco	Ricompensa Blocco (BTC)
0	N/A	0	50
1	28/11/2012	210.000	25
2	09/07/2016	420.000	12,5
3	2020	630.000	6,25
4	2024	840.000	3,125
5	2028	1.050.000	1,5625

Tabella 2 Riepilogo dati Halving Bitcoin Fonte[14]

Considerando come periodo indicativo sempre marzo 2020 e trovandosi all'altezza del blocco 620,216 con molta probabilità l'halving avverrà intorno ai primi giorni di maggio[15] 2020. È previsto, di base, un halving ogni 210.000 blocchi. In figura non sono presenti tutti gli *halving* predisposti sulla *blockchain di bitcoin* che ha in programma un totale di 32 *halving*, al cui termine, non sarà più possibile generare altri *bitcoin.* È possibile seguire il *Countdown* del prossimo Halving di Bitcoin direttamente dal sito web *Bitcoinblockhalf*[15]

Figure 6 Countdown Halving presente sul sito web. Fonte[15]

[14] <https://www.binance.vision/it/halving> Ultima consultazione aprile 2020
[15] <https://www.bitcoinblockhalf.com/> Ultima consultazione aprile 2020

Il processo di *mining* è particolarmente importante nelle *Blockchain*. In mancanza di esso difficilmente la stessa catena riuscirebbe ad essere autogestita. In Molti, interessati alle criptovalute si avvicinano anche questo processo, soprattutto per una questione di profittabilità. "Iniziare a fare *mining*" non è cosa semplice, considerando che attualmente esistono macchinari specializzati per queste operazioni. La particolarità è che ad oggi abbiamo la possibilità di adottare due strade: il *solo mining* ed il *pool mining. Il solo mining* consiste letteralmente nell'iniziare a minare autonomamente dal proprio pc senza collegarsi ad un servizio di terze parti. Sarà necessario il possedere un *wallet* ed un *config file* che ci permetteranno di essere reindirizzati al server per svolgere attività di calcolo computazionale. Per facilitare il processo di connessione alla rete anche alcune pool hanno iniziato ad offrire una "connessione rapida" tramite la loro piattaforma nonostante il *solo mining* rimanga una modalità obsoleta quasi per tutte le *Digital Currency* disponibili sul mercato, a causa della forte "competitività". In sostituzione a questo subentra il classico *pool mining.* In questo caso saremo noi direttamente a connetterci ad un "bacino comune" con il nostro hardware ed insieme ad altri *miners* a tentare la convalida dei blocchi. Generalmente la seconda strada la si preferisce poiché di più facile lettura, con una richiesta di *setup* più intuitivo e rapido. La potenza generale di rete, in particolare di Bitcoin, è suddivisa attualmente in poche pool che si dividono i premi della convalida del blocco. Avremo quindi a discapito di un *solo mining* un guadagno più stabile e sicuro. La figura 7 ci mostra a grandi linee come era suddivisa la potenza di calcolo mondiale tra le varie pool in base alla percentuale di blocchi minati fino a maggio 2019.

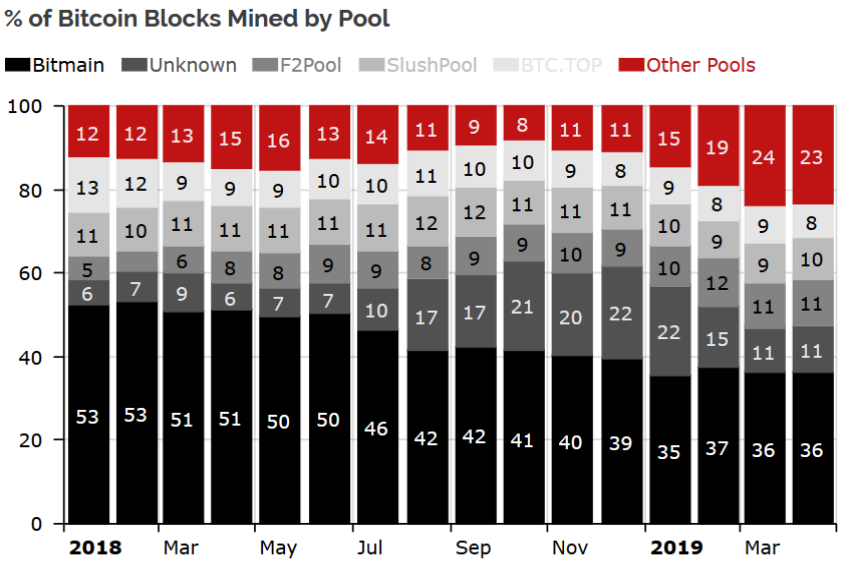

Figura 7 Grafico raffigurante le percentuali di Blocchi minati dalle varie Pool. Fonte[16]

[16] < https://it.cointelegraph.com/news/diar-bitcoin-mining-hashrate-is-becoming-more-distributed-among-pools> Ultima consultazione aprile 2020

Il servizio però fornito richiederà una *fee* di gestione corrispondente a circa l'1%-3% del minato. Le modalità di pagamento delle *pool* sono di vario genere. Le più conosciute ed utilizzate sono *PPS*[17] e *PPLNS*[17]. Per PPS si intende *pay per share*. In questo caso riceveremo un *payout* fisso e sicuro in proporzione allo *share*, ovvero alla potenza di calcolo offerta sulla *pool*. Ipotizziamo di offrire il 10% di share su un totale di 100% della *pool*. In questo caso anche se il blocco minato è convalidato da un'altra *pool*, riceveremo comunque un *payout* in rapporto alla potenza di calcolo offerta, ossa il 10%. Nel caso in cui il nostro miner dovesse trovare lo *share* adeguato e convalidare il blocco non riceveremmo il totale guadagno dalla convalida, 12.5 Btc, ma tutto in proporzione al 10% di *share*. Introduciamo dunque una nuova variabile; la *luck;* infatti la convalida di un blocco non spetterà a tutti i miner, ma ad uno in particolare che trova il giusto *nonce*. C'è da considerare anche, che per ogni convalida ci sarà un numero di *share* variabile. Quindi potenzialmente potremmo con il *solo mining* convalidare un blocco e guadagnare 12.5 btc. Questa risulta però essere un'ipotesi molto remota, se non impossibile, poiché la nostra potenza di *solo mining* andrebbe a "scontrarsi" con le potenze delle più grandi *pool* che solitamente in base alla *luck* si girano a "turno" la convalida dei blocchi. Proprio per questo motivo le *pool* stesse hanno la possibilità di garantire un pagamento fisso e stabile ai miner connessi con il metodo del *PPS*. Per PPLNS indichiamo il *pay per last N share.* In questo caso però ogni convalida del blocco viene definito un numero fisso N di *share* che comprendono tutti gli *share* possibili di tutti i miner sulla rete. Solitamente questo valore N viene impostato al doppio della difficoltà di rete e, essendo fisso, non è strettamente correlato alla *luck*. La *pool* in questo caso pagherà solo ed esclusivamente se viene trovato un blocco e, di conseguenza, pagato per tutti quanti gli *hash* che vengono personalmente minati. Entrambi sistemi risultano essere estremamente efficienti. C'è la possibilità di guadagnare molto di più o molto di meno con il metodo PPLNS in cui subentra una buona dose di casualità. Mettendo in rapporto i due metodi noteremo che una *pool* con il metodo *PPS* si assumerebbe un forte rischio poiché in caso di mancata convalida dei blocchi sarà comunque costretta a pagare una somma fissa e proporzionale ai miner, andando a sottrarre questo pagamento direttamente dal proprio bilancio. Questo sistema, infatti, è alla base delle più grandi *pool*, con potenze capaci di fare la differenza e di convalidare statisticamente un tot numero di blocchi al giorno. Le *fee* richieste, oltre ad essere un sistema di guadagno, servono proprio a bilanciare le uscite fisse dei miner, anche quando non si convalida un blocco.

[17] <https://medium.com/luxor/mining-pool-payment-methods-pps-vs-pplns-ac699f44149f> Ultima consultazione aprile 2020

Nei primi anni dall'uscita di *Bitcoin* la facilità di calcolo permetteva di "minare moneta" direttamente per mezzo dei propri pc, in particolare per mezzo della CPU. Vedremo di seguito i vari generi di mining che prendono il loro nome direttamente dal tipo di *Hardware* utilizzato per il calcolo computazionale. Il primo genere di mining può essere classificato, pertanto, come *cpu mining.*

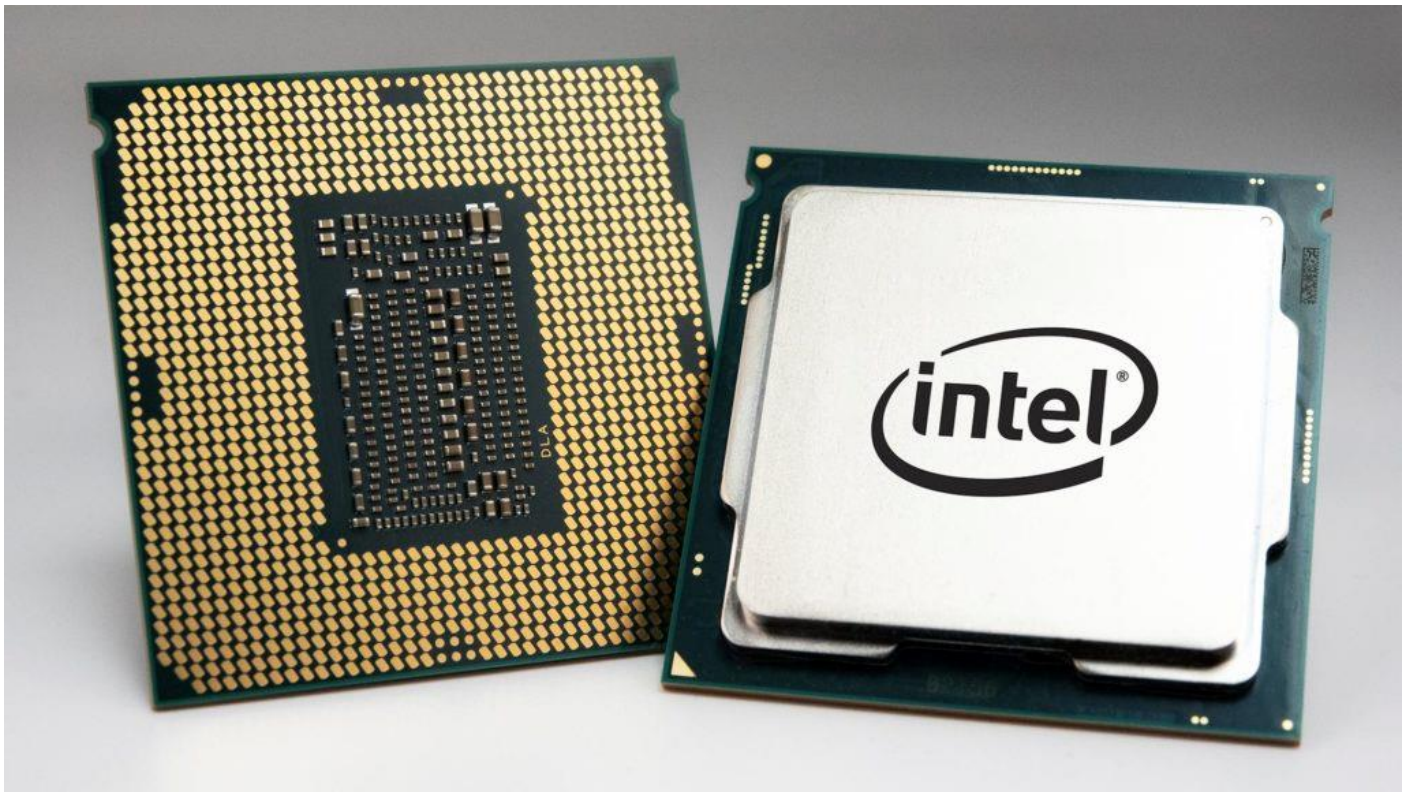

Figure 8 Esempio di una CPU. Fonte[18]

La mancata conoscenza della moneta, una conseguente mancanza di competitività e la difficoltà bassa rendevano i guadagni paradossalmente nulli. Pur avendo un *reward* per blocco di 50 Btc, ai tempi, la moneta valeva pochi centesimi e quindi il *mining* risultava più hobby che un guadagno. In molti iniziarono a minare semplicemente per il desiderio di partecipazione ad una *community* senza per nulla considerarne il risvolto economico. Attualmente la difficoltà è aumentata a tal punto da non poter più utilizzare un personal computer come *hardware*. Sono ormai numerose le aziende che si occupano di produrre *hardware* dedicati capaci di erogare potenze, per *Bitcoin*, intorno alle 100 *Tera Hash per secondo.* Tali dispositivi sono chiamati *ASIC miner.*

[18] < https://giochipertutti.org/perdite-della-data-di-rilascio-di-intel-comet-lake-prestazioni-della-cpu-a-10-core-e-prezzo/> Ultima consultazione aprile 2020

Figura 9 Esempio di ASIC Miner. Fonte[19]

L'acronimo *asic*[20] sta per *Application specific integrated circuit*, un circuito, quindi, dedicato, per risolvere dei calcoli specifici. Proporzionalmente alla potenza di calcolo, sono saliti i consumi energetici, classificabili nei comuni *watt*, e costi di acquisto, che hanno raggiunto prezzi oltre le migliaia di euro. Si è dato origine ad un vero e proprio business intorno al mondo del *mining*. Pur essendo queste macchine molto efficienti nel loro lavoro non sono "programmabili" o meglio non permettono un utilizzo su tutte le *blockchain*. Gli Asic, infatti, vengono classificati in base all'algoritmo. Ogni macchinario lavora su un unico algoritmo e di conseguenza il miner lavorerà sulle *blockchain* e criptovalute che adottano il sistema *proof of work* simile e con uno specifico algoritmo. Nel *world wide web* non esiste solo *Bitcoin* e non esiste solo l'algoritmo *sha-256*. Sono nate nuove monete digitali con algoritmi di base differenti. Ciò non ha di certo fermato il mercato degli ASIC che continua ad essere fiorente, ma ha introdotto nuove modalità di mining con differenti *hardware*. Tra i più comuni annoveriamo: le *graphics card. Ethereum* ne è stata la prova, facendo impazzire il mercato delle GPU qualche anno fa. Colossi come *AMD* e *NVIDIA* non riuscivano a sostenere le richieste del mercato che aveva interesse di acquistare stock enormi per il mining. Nell'anno 2017 anche una scheda *mid-level* permetteva dei guadagni giornalieri intorno ai 4-5 dollari. Il *gpu mining* è differente dall'*asic mining*. L'architettura delle gpu permette una applicabilità di calcolo su più algoritmi e di conseguenza di minare più monete. Ogni particolare modello possiede migliori o peggiori *hashrate* in base all'algoritmo. Ogni utente utilizza una *Test benchmark* per

[19] <https://shop.bitmain.com/product/detail?pid=00020200226232356122Y0FHc2rQ0657> Ultima consultazione aprile 2020

[20] <https://it.wikipedia.org/wiki/Application_specific_integrated_circuit> Ultima consultazione aprile 2020

decretare qual è l'algoritmo e conseguentemente la moneta più adatta alla propria gpu. Nel 2017 la scarsità sul mercato di queste ultime ne ha fatto schizzare i prezzi, ma allo stesso tempo ha sollecitato una parte della community a migliorarne le efficienze; per esempio da l'utilizzo di sofisticati sistemi di raffreddamento ad acqua a modifiche *firmware.* Un esempio pratico, che ha fatto storia, è la *gpu RX470,* la gpu dei minatori per eccellenza. Alcuni programmatori erano riusciti a modificare *i bios* e conseguentemente *memory clock e core clock* di base per passare da una potenza di calcolo di 21 *mega hash al secondo a* circa 30 *mega hash al secondo,* riducendone anche il consumo elettrico. Sono state prodotte *motherboard* e *Case* esclusivi per il *gpu mining,* che successivamente hanno preso il nome di *mining rigs.*

Figura 10 Esempio di Mining Rig composta da 6 schede grafiche. Fonte[21]

Tramite una *mining rig* si possono gestire fino a 12 schede grafiche in contemporanea, *driver* permettendo. Da notare le gli *hashrate* di un ASIC da 100 tera ed una gpu da 30 mega la differenza è sostanziale, ma come già anticipato, i macchinari operano su *blockchain* differenti e le grandezze non rispecchiano assolutamente la profittabilità finale. Alcune gpu potrebbero quindi essere più profittevoli di alcuni asic. Una menzione va fatta

[21]< https://www.massmux.com/an-efficient-6-gpu-ethereum-rig/> Ultima consultazione aprile 2020

anche per le *fpga*[22] e per l'*hdd mining*. Per *fpga* si intende *Field Programmable Gate Array* corrispondente ad un singolo dispositivo logico "programmabile". Ne Esistono due versioni: quelle programmabili un'unica volta, e quelle programmabili più volte. La struttura di queste fpga è costituita da una matrice di blocchi logici denominati CLB[22], *configurable logic block*, che sono connessi tra di loro. Nelle parti esterne, invece, abbiamo blocchi IOB[22], *input/output block*, che gestiscono i trasferimenti di dati dall'interno all'esterno e viceversa. Tralasciando la struttura dettagliata possiamo con questi pochi dati già inserire le fpga nel mezzo tra gpu e asic.

Figura 11 Esempio di FPGA Miner. Fonte[23]

[22] <https://it.wikipedia.org/wiki/Field_Programmable_Gate_Array> Ultima consultazione aprile 2020
[23] < https://cryptomining-blog.com/10766-blackminer-f1-mini-is-an-upcoming-single-chip-fpga-miner/> Ultima consultazione aprile 2020

Questi particolari hardware hanno a loro favore la programmabilità e il basso consumo delle gpu, ma una potenza superiore, comunque non comparabile con gli asic. Essi Non hanno fatto "fortuna" rimanendo sempre nell'ombra a causa del loro mercato di base di nicchia e per l'alto costo, ed anche perché sfruttati per calcoli complessi di elaborazione. Ultimamente stanno prendendo piede in particolare per il mining di *altcoins* poco conosciute o di nuova fattura. Siamo di fronte ad un *hardware* programmabile che, supportando più algoritmi, potrebbe rosicchiare mercato sia al *gpu mining* che all'*asic mining*. L'unico lato negativo è rappresentato proprio dalla programmazione stessa. Infatti, in questo caso l'*hardware* ha la necessità di essere programmato *ad hoc* per ogni algoritmo ed *altcoin*. Tutto ciò ha dato origine ad un piccolo commercio di *bitstreams,* file di programmazione, capaci di sfruttare i processori logici delle fpga per minare criptovalute. Se ad un utente interessa acquistare un fpga dovrà anche essere pronto ad acquistare un *bitstream* per utilizzarla. Manca all'appello *l'hdd mining*, praticamente in disuso, ma che aveva incuriosito qualche anno fa grazie alla facile reperibilità del comparto hardware: i nostri *hard disk.* L'idea nasce da *Burstcoin,* un *altcoin* che aveva la possibilità di essere "minata" direttamente con i propri hard disk. Bastava "*plottizzare"* e quindi riempire lo spazio di archiviazione tramite un *software* dedicato con *hash* dell'algoritmo *shabal-256* da cui poi poter convalidare i blocchi. Una nicchia che non ha avuto molto successo tanto da quasi scomparire. Tramite un piccolo schema mi preme raggruppare i generi di mining menzionati con i vantaggi, gli svantaggi e caratteristiche trattate.

Hardware	Algoritmo	Vantaggi	Svantaggi
Asic	Unico	Maggiori prestazioni.	Consumi elevati, costo di acquisto elevato.
Fpga	Configurabile	Molto efficiente.	Mercato molto ristretto, molto costosi, setup impegnativo.
Gpu	Configurabile	Facilmente reperibile sul mercato, Consumi ridotti, mina più di un algoritmo.	Efficenza ridotta.
Cpu	Configurabile	Facilmente reperibile sul mercato, Consumi ridotti, mina più di un algoritmo.	Bassa efficienza.
Hdd	Configurabile	Hardware poco costoso e con con consumi ridotti.	Guadagni tendenti allo zero, Obsoleto.

Tabella 3 Raccolta vantaggi/svantaggi vari tipi di miner.

Blockchain Setup

Non resta che analizzare come iniziare a minare. Per una questione di semplificazione, verranno spiegate le stringhe di configurazione per collegarsi ad una *pool mining.* Per poter iniziare a minare, oltre gli hardware su citati, avremo bisogno di un *software* che sia capace di gestire i calcoli e di una connessione *internet*. I software classici di mining sono *cgminer* e *bfgminer* la cui programmazione delle stringhe è molto simile ed intuitiva. Nel caso di *Cpu mining* e *gpu mining* i seguenti *software* collegheranno gli *hardware* alla *pool* mostrando una finestra di prompt dei comandi direttamente sul PC.

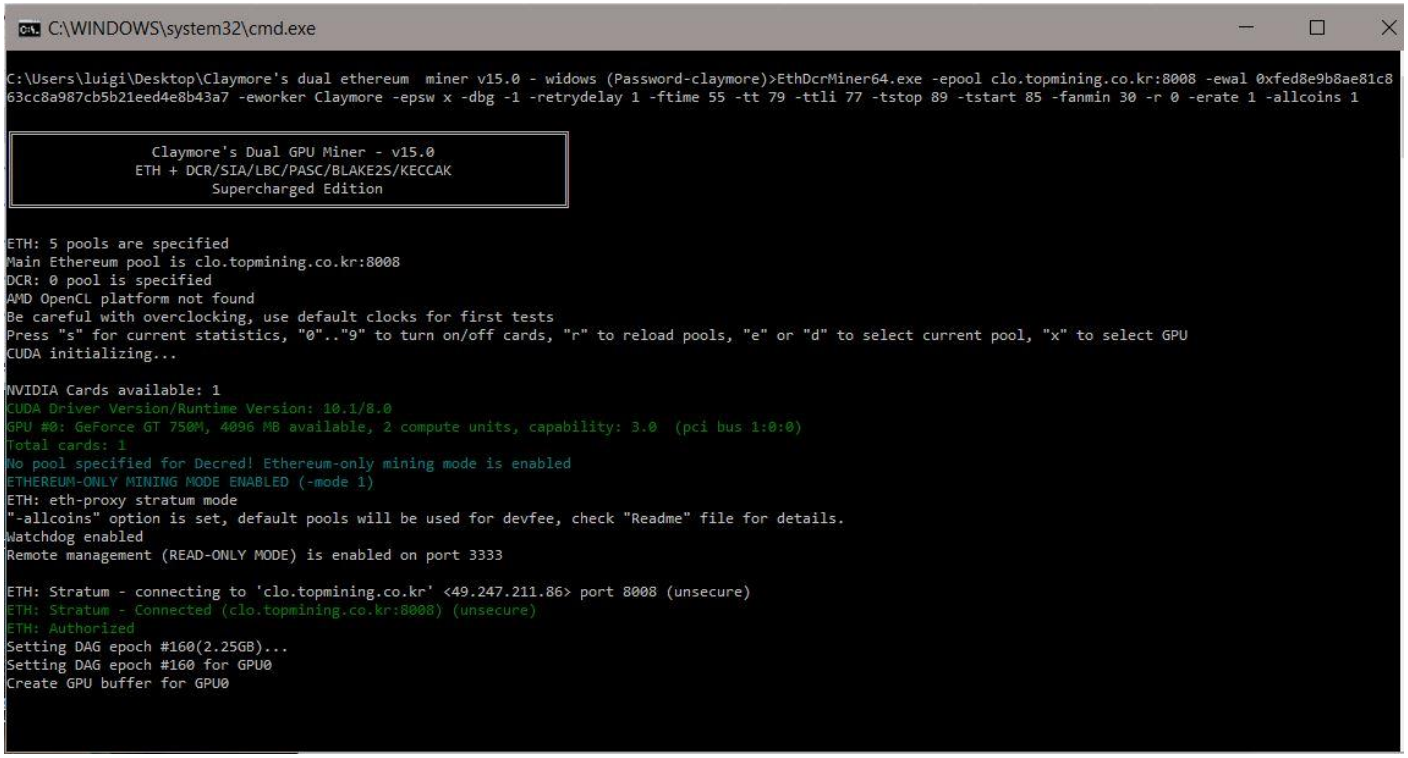

Figura 12 Dashboard Software Claymore da prompt dei comandi.

Sarà possibile monitorare l'andamento del mining direttamente dalla suddetta finestra.

Generalmente i *software* sono scaricabili gratuitamente, ma molto spesso essi hanno delle *fees*, sempre intorno all'1% 2%, sebbene opzionali. Tramite un comando da includere nelle stringhe di comando sarà possibile annullare la tassa a discapito, però, dell'efficienza generale del proprio hardware. Il *software* viene direttamente gestito da un file *.bat* modificabile, per mezzo del quale si può configurare il programma a proprio piacimento. Vediamo come:

All'interno del file *batch* bisogna inserire:

- *Stratum*: variabile necessaria alla connessione con la *pool.* Si dovrà inserire un indirizzo web con 4 cifre finali corrispondenti alla porta *tcp* di rete. Un esempio: "*stratum+tcp://eu.stratum.slushpool.com:3333"*
- Algoritmo: voce che varia in base all'algoritmo ed al software utilizzato, basterà indicare un'abbreviazione dell'algoritmo desiderato.
- Indirizzo di ricezione: si tratta della voce che permetterà di ricevere i guadagni direttamente nei propri "portafogli virtuali"
- Potenza: la potenza da dedicare al mining può essere selezionata a seconda dei *software*. Nel caso di un cpu mining, ad esempio, si considera il numero dei processori logici del nostro hardware, di conseguenza, data una cpu *quad core,* avente 4 processori fisici ed in totale 8 logici, ipotizzando di voler dedicare il 50% al mining, si imposterà la stringa con un unico valore corrispondente a "3" o secondo la seguente formula {0, 1, 2, 3}. Ricordiamo che la numerazione parte dallo zero incluso, quindi, per richiamare l'ultimo processore dobbiamo inserire il valore "7" e non "8".

Le suddette variabili sono le più importanti, ma il file *batch* richiede ulteriori stringhe. Prendendo come esempio il software Claymore[24], che si occupa di gestire il mining, prevalentemente delle gpu, andiamo ad analizzare le sue stringhe di setup.

EthDcrMiner64.exe -epool eu1.ethermine.org:4444 -eworker YOUR_RIG_NAME -ewal YOUR_WALLET ADDRESS -epsw x

Il primo richiamo è del file *.exe* dello stesso *software*, obbligatorio al fine di far partire il processo. Per ogni comando sarà necessario lasciare un solo spazio e includere dei comandi predefiniti del programma stesso. -*epool* è il richiamo allo *stratum* che ci permetterà quindi di connetterci alla *pool mining.* In questo caso abbiamo una forma "abbreviata" corrispondente agli indirizzi web e alle porte: *eu1.ethermine.org:4444*. La scelta tra *stratum* in forma completa o non in forma abbreviata dipende dalle condizioni di base del *software.* -*eworker* ci indicherà lo spazio in cui inserire il nome personalizzato che si assegna all*'hardware mining*. Esso è importante, in quanto ci permetterà di analizzare i dati delle singole prestazioni direttamente dai siti web delle rispettive pool. -*ewal* richiama il nostro indirizzo pubblico; Si dovrà quindi inserire il nostro indirizzo pubblico di ricezione per garantire la ricezione dei guadagni del *mining*. Ultima, ma non per importanza, è -*epsw* che va a richiamare una possibile password di sicurezza. Solitamente per una questione di rapidità viene lasciato di default x, poiché una password complessa non garantirebbe nessuna sicurezza maggiore nel mining. La stringa sopra elencata è una versione standard a cui vanno aggiunti altri dati come i seguenti:

setx GPU_FORCE_64BIT_PTR 0

setx GPU_MAX_HEAP_SIZE 100

setx GPU_USE_SYNC_OBJECTS 1

setx GPU_MAX_ALLOC_PERCENT 100

setx GPU_SINGLE_ALLOC_PERCENT 100

Le seguenti stringhe sono personalizzabili come le sopra citate nella sezione potenza. In questo caso si potranno settare le percentuali di potenza che la propria o le proprie eventuali gpu devono dedicare al mining. Una nuova versione completa di stringa può risultare la seguente:

EthDcrMiner64.exe -epool eu.clo.epool.io:8008 -ewal 0xfed8e9b8ae81c863cc8a987cb5b21eed4e8b43a7 -eworker Claymore -epsw x -dbg -1 -retrydelay 1 -ftime 55 -tt 79 -ttli 77 -tstop 89 -tstart 85 -fanmin 30 -r 0 -erate 1 -allcoins 1

[24] <https://claymoredualminer.com/> Ultima consultazione aprile 2020

pause

La stringa risulta essere evidentemente più complessa. I setup di base che vengono utilizzati nel Cpu mining e nel gpu mining sono prevalentemente questi. Per quanto concerne L'ASIC mining, il setup si complica nella fase iniziale. Molto spesso si avrà a che fare con macchinari non direttamente connessi con il proprio personal computer e di conseguenza sarà necessario essere provvisti di un *ip scanner*.

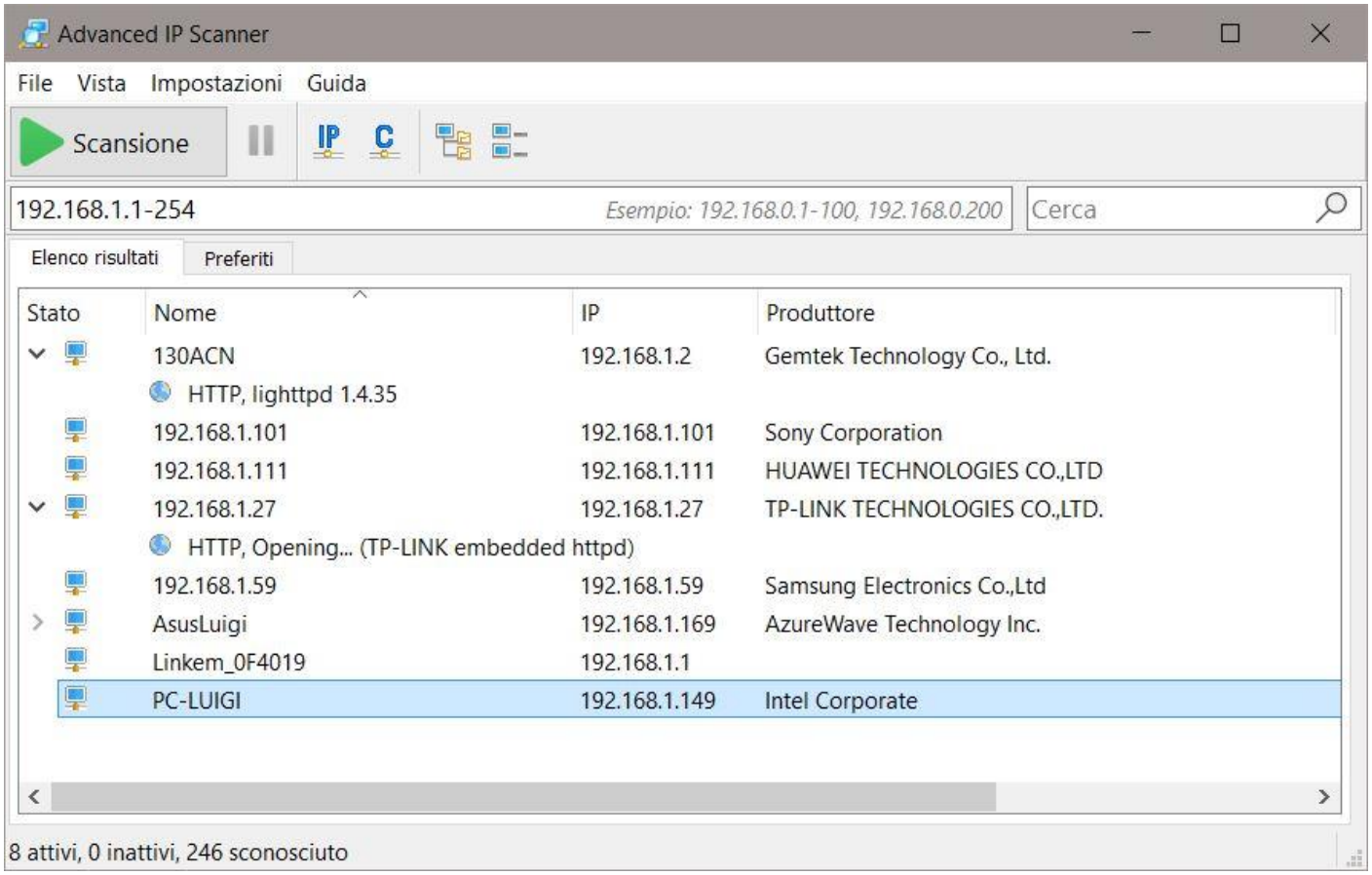

Figura 13 Esempio di software Ip-scanner in funzione.

Una volta connesso il proprio hardware per mezzo di un classico cavo ethernet alla connessione internet domestica, tramite il suddetto software si potrà cercare l'*ip automatico* assegnato al nostro macchinario. Generalmente, in caso non siano state fatte delle modifiche alla rete tradizionale, dovrebbe essere assegnato un ip *192.168.1.x* con la x che varierà a seconda del numero di dispositivi connessi. Ipotizziamo che venga assegnato un ip 192.168.1.34, quest'ultimo dovrà essere digitato sui motori di ricerca per poter entrare nella cabina di comando del nostro *Hardware mining*.

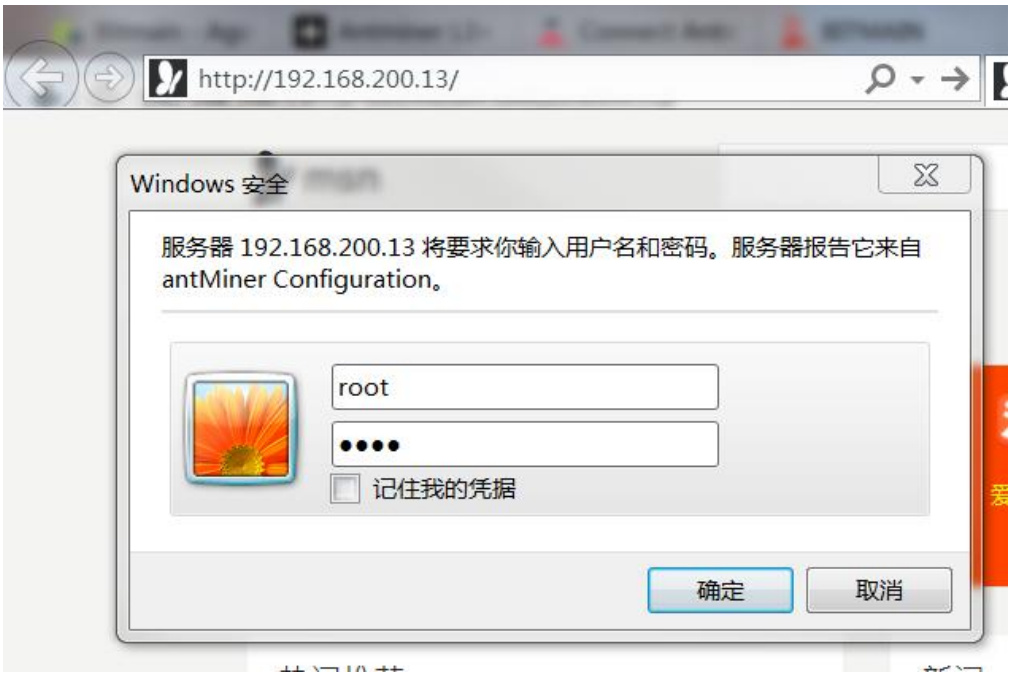

Figura 14 Esempio di finestra di login per visualizzare la dashboard di un ASIC miner. Fonte[25]

All'interno della dashboard, che sarà visualizzabile solo dopo aver inserito un username ed una password (generalmente le credenziali standard sono root/root), si potranno inserire i dati necessari per il collegamento alla pool. I sistemi ASIC necessitano l'inserimento esclusivo di uno o più *stratum* ed il semplice indirizzo di ricezione nelle loro apposite sezioni.

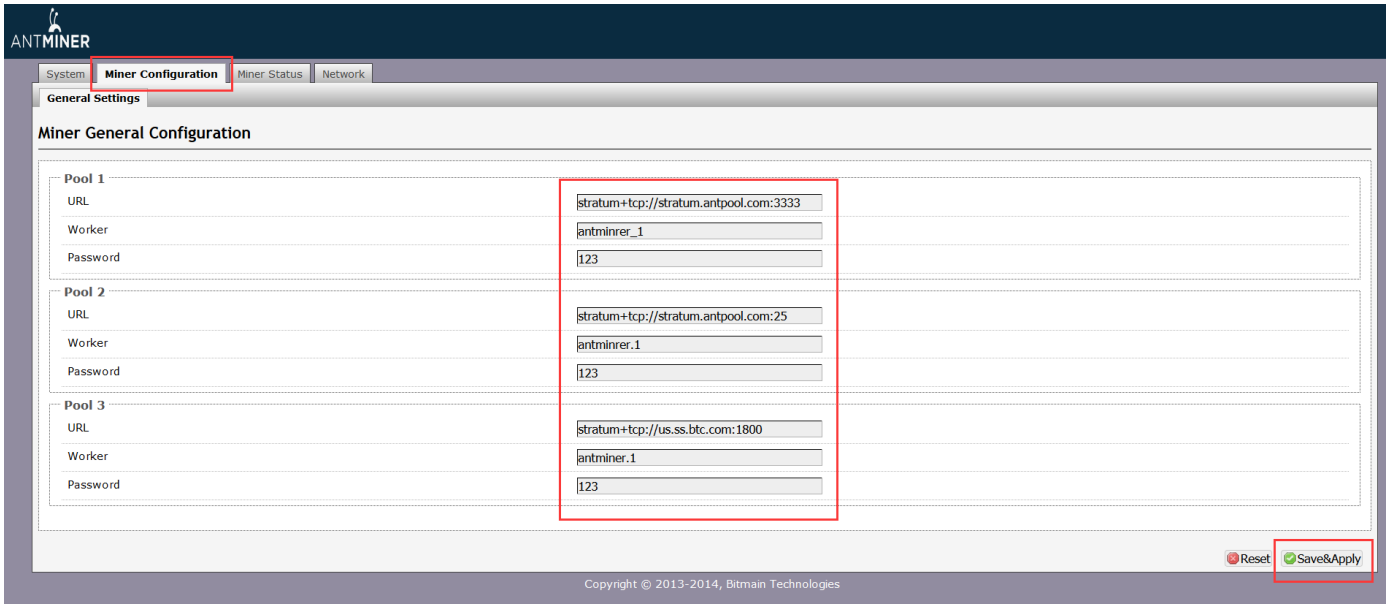

Figure 15 Esempio di Dashboard ASIC miner. Fonte[25]

[25] < https://support.bitmain.com/hc/en-us/articles/115000211774-Connect-Antminer-S9i-S9-T9-S7-to-Pools-Antpool-BTC-com> Ultima consultazione aprile 2020

Solitamente viene richiesta una password che viene lasciata anche qui standard. Manca la sezione del name worker sopra citata. Sarà possibile aggiungere un nome personalizzato, nell'apposita sezione, semplicemente aggiungendo un punto ed il proprio nickname successivamente all'indirizzo pubblico di ricezione. Ecco un esempio:

34F7w4L8J9xkUfSL664pjM9ZGS2kSX68NT.Rig1

La prima parte è rappresentata dalla chiave pubblica mentre "rig1" è il nome che abbiamo assegnato all'*hardware*.

Questione ambientale

Riprendendo il valore attuale del *net hashrate* totale del *mining* di *Bitcoin* e facendo una media per macchinario noteremo che sono connesse alla rete più di due milioni di macchine. Concretamente le macchine attive sono nettamente superiori poiché risultano essere ancora utilizzati macchinari di vecchia data capaci di erogare solamente 14-15 TH/s e con consumi elevati. Ipotizzando la presenza del doppio dei macchinari attivi, quindi circa 5 milioni, basterà fare un semplice calcolo per capire che questo settore consuma un quantitativo di energia elettrica considerevole. Il consumo si attesta oltre i 70 *terawatt*[26] solo contando il settore del *mining* di *Bitcoin*. La questione ha toccato gli ambientalisti, che hanno criticato aspramente questa tecnologia, accusandola di essere una delle più inquinanti al mondo. È indubbio che i consumi siano elevati, considerando anche come numerosi investitori da anni approfittino di agevolazioni e discrepanze di costi dell'energia elettrica, creando le *farm mining*, capannoni saturi di ASIC miner.

[26] <https://cryptonomist.ch/2019/09/15/mining-consumo-di-energia/> Ultima consultazione aprile 2020

Figura 16 Esempio di mining farm. Fonte[27]

Il problema ambientale potrebbe negli anni essere preso in considerazione, ma allo stesso tempo comparando i consumi di tutto il mondo del *world wide web ed* il mining, rimane in rapporto, ancora un valore molto basso. Una possibile soluzione potrebbe essere la proibizione del mining in particolari stati. Ciò non causerebbe assolutamente un collasso del sistema poiché, come già spiegato, la difficoltà di rete potrà bilanciare la convalida dei blocchi mantenendo la media dei 6 blocchi l'ora; l'unico pericolo deriverebbe da una diminuzione della stessa decentralizzazione. Portando in mano a pochi *miners* la convalida dei blocchi.

[27] < https://scienews.com/it/bitcoin/3964-nella-regione-di-krasnoyarsk-vogliono-creare-mining-farm-per-3-miliard.html> Ultima consultazione Aprile 2020

Blockchain POW vs POS

Nelle varie blockchain non è soltanto presente il classico sistema di consenso *proof of work* già ampiamente trattato e spiegato. *Ethereum* a breve implementerà un protocollo di consenso differente, denominato *proof of stake*[28]. Questo meccanismo di consenso non è nuovo al mondo delle criptovalute. Una delle prime *altcoin* a sfruttare questo protocollo è stata *Peercoin.* La principale differenza sta nel mezzo che viene usato per il consenso. Abbiamo abbondantemente analizzato come per il proof of work sia necessario un hardware per operare un calcolo. Nel caso del *proof of stake* "basterà" possedere un determinato quantitativo di moneta e si passerà a sfruttare i portafogli digitali come "miners". Insieme alla selezione *randomica* per quale *hash* convalida i blocchi, viene introdotto il concetto di "anzianità". I fondi dei portafogli più prosperosi, che NON sono stati spesi per almeno 30 giorni, concorreranno alla creazione del blocco successivo. Una volta che quel quantitativo è riuscito a convalidare un blocco ripartirà con un "anzianità zero". L'anzianità massima verrebbe raggiunta ai 90 giorni quando c'è una certezza massima di convalida del blocco. La ridistribuzione dei *rewards* verrà comunque operata, ma per una valutazione dei rendimenti; in questo caso non vi è una potenza di calcolo ma tutto dipende dalla grandezza del portafoglio e da un eventuale *annual yield.* Ipotizzando di possedere un portafoglio in *staking* con all'interno 100 *Ethereum* con un *annual yield* del 5% ricaveremo annualmente 5 *Ethereum*. Un vantaggio sicuramente sarà la riduzione notevole dei consumi elettrici, ma soprattutto una più remota possibilità di effettuare il double spending, poiché rispetto ad un sistema di *proof of work,* si richiede un maggiore impiego di denaro.

Blockchain Stale block, blocco orfano e Uncle block

La *blockchain*, come già anticipato, potrebbe subire delle modifiche o avere alcuni problemi. Risulta, di base, essere un protocollo enormemente stabile, ma come quando un server va in tilt o la nostra rete internet va in *crash*, anche la *blockchain* ha, alle volte, la necessità di essere "spenta e riaccesa". Per esser più chiari durante l'allungamento della catena ci potremmo "perdere" dei blocchi. Andiamo a vedere in dettagli cosa si intende per *Stale block*[29]. Questo evento è assimilabile al, già ampiamente citato, mondo del *mining*. Precisamente questo "errore" è dovuto ad un disallineamento del calcolo del *mining*. Ricordiamo che il *timestamp* e la durata dei blocchi sono fondamentali per un adeguato funzionamento della catena. Nel momento in cui più miner connessi a diverse pool condividono potenza di calcolo, la rete potrebbe subire un *delay,* anche solo per pochi secondi, nel trasferimento di dati, dando origine a due differenti blocchi con una stessa "altezza". Si avranno quindi due blocchi validi per la catena che però non vengono istantaneamente accettati dai nodi. Si avranno

[28] <https://www.ilbitcoin.news/pow-e-pos-cosa-sono-e-quali-sono-le-differenze/> Ultima consultazione aprile 2020
[29] <https://bitcoin.org/en/glossary/stale-block> Ultima consultazione aprile 2020

dunque, considerando di trovarci poco dopo il blocco numero 500, due blocchi numero 501. In questo caso solo e soltanto uno dei due blocchi minati verrà aggiunto alla catena, e solitamente vi corrisponde quello che ha un seguito, cioè che ha la catena più lunga attaccata/minata, mentre l'altro viene per così dire "perduto". C'è da considerare però che lo *stale block*, pur non continuando la catena, ha portato con sé delle informazioni e delle transazioni che potrebbero essere perse. Il più delle volte ciò non accade poichè la manciata di transazioni che sono all'intero dello *stale block* vengono reimmesse nel blocco successivo della catena principale, non facendo verificare nessuna problematica e nessun fenomeno di *double spending*. Per riportare un esempio[30] pratico, si è avuto uno *stale block* al blocco numero **619970** verificatosi proprio a causa di un disallineamento temporale di due pool di appena 4 secondi. L'evento risale ai primi giorni del marzo 2020, ma non si tratta assolutamente di un fenomeno rarissimo, di fatti seguendo le testate giornalistiche interessate all' argomento potremmo ricevere aggiornamenti a riguardo. Per quanto riguarda il blocco orfano[31] la situazione non è estremamente differente. In questo caso il blocco risulta, differentemente dallo *stale block*, non completamente validato poiché i suoi blocchi parenti non sono stati precedentemente processati dai nodi. Un esempio visivo per comprendere meglio le differenze è il seguente:

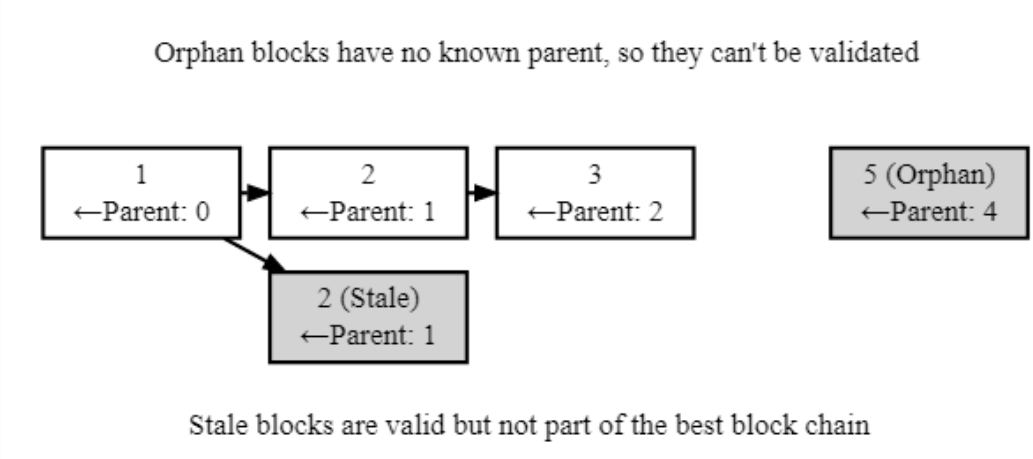

Figura 17 Rappresentazione grafica di un blocco orfano ed uno Stale. Fonte[29]

Riepilogando, il blocco orfano non verrà mai validato, mentre lo *stale block* sarà valido, ma non farà parte della miglior catena e quindi non si collegherà alla *best blockchain.* In *Ethereum* i blocchi orfani vengono denominati come *uncle block*[32] e differentemente dalla catena di Bitcoin hanno un *reward.* Anche i blocchi *stale* su *Ethereum* possono essere inclusi nella catena come *uncle*, ricevendo un *reward* massimo del 75% rispetto ad un totale.

[30]<https://cryptonomist.ch/2020/03/03/bitcoin-altro-stale-block/> Ultima consultazione aprile 2020
[31]<https://bitcoin.org/en/p2p-network-guide#orphan-blocks> Ultima consultazione aprile 2020
[32] <https://www.cryptohelper.it/glossario/blocchi-orfani-e-blocchi-uncle/> Ultima consultazione aprile 2020

Blockchain Fork

Durante la propria vita la *blockchain* potrebbe subire degli aggiornamenti nella sua struttura. Molto spesso un aggiornamento della catena dipende da un aggiornamento delle regole di consenso. Nel momento in cui vengono introdotte nuove regole potrebbero esserci dei *nodi*, non aggiornati, che continuano a seguire le vecchie regole e *nodi* che invece seguiranno le nuove regole. Da qui potrebbero venire fuori due scenari[33]:

- Un blocco, seguendo le nuove regole, verrà convalidato dai nodi aggiornati ma non da quelli NON aggiornati.
- Un blocco viola le nuove regole e quindi non sarà accettato dai nodi aggiornati ma potrebbe essere aggiunto dai nodi non *updated.*

Nel primo caso, il rifiuto dei vecchi nodi richiama il *software mining* che prende informazioni dalla *blockchain* che, in automatico, si rifiuta di basarsi sulla stessa catena agganciandosi agli *updated nodes.* Si dà origine in questo caso ad un *hardfork*[33] cioè una divergenza permanente della catena. La prima catena, generalmente chiamata *legacy,* manterrà i nodi non aggiornati con le solite regole, la seconda verrà gestita dai nodi aggiornati. Nel secondo caso la situazione è differente. Il rifiuto dei blocchi da parte dei nodi aggiornati potrebbe far virare la catena su questi ultimi, nel caso in cui essi controllino la maggior parte dell'*hashrate.* Ciò accade perché i nodi non aggiornati continueranno a convalidare tutti i blocchi sia quelli che seguono le nuove regole sia quelli che le violano. I nodi aggiornati, essendo maggiori, possono costruire una catena più forte che verrà conseguentemente accettata come *best valid blockchain.* Si darà origine in questo caso ad un *soft fork*[33]. La *Bitcoin blockchain* ha subito numerosi fork che possono essere riassunti tramite la seguente immagine[34]:

[33] <https://bitcoin.org/en/blockchain-guide#consensus-rule-changes> Ultima Consultazione aprile 2020
[34] <https://scenarieconomici.it/cripto-un-riassunto-degli-hard-fork-di-bitcoin-per-capire-cosa-e-successo-e-puo-succedere/> Ultima consultazione aprile 2020

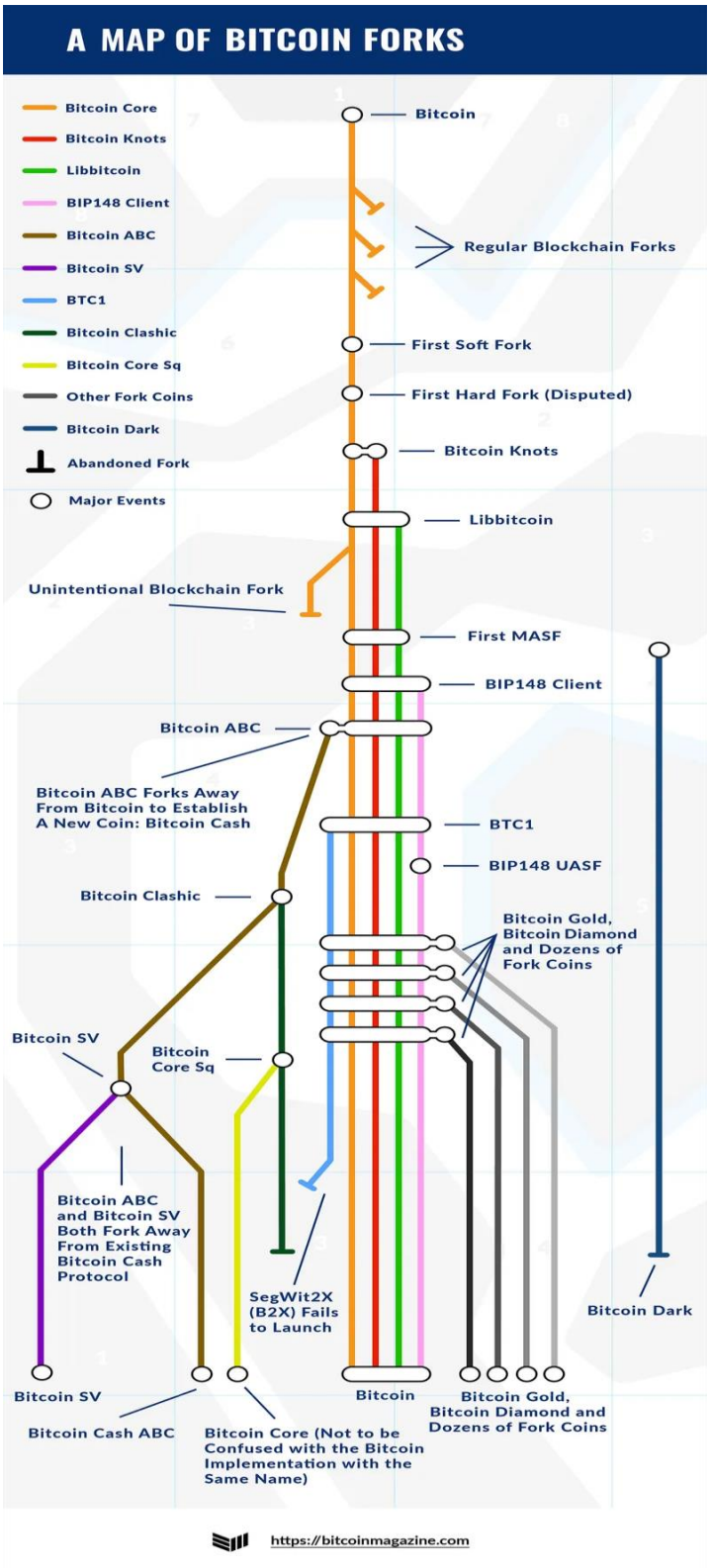

Figure 18 Riepilogo grafico dei fork su catena Bitcoin. Fonte[34]

Dalla figura possiamo notare che molti *hard fork* hanno fatto derivare vere e proprie nuove monete virtuali che hanno introdotto nuove regole rispetto alla catena *legacy*. I *soft fork* risultano essere, paradossalmente, inferiori in quanto in caso di cambiamenti complessi della catena, quale potrebbe essere il ridimensionamento dei blocchi da 1 Megabyte a 512 kilobyte, viene sempre utilizzato un *hardfork*. La motivazione risiede proprio

nel consenso, infatti, molto spesso questi grossi cambiamenti vengono accettati dai nodi e quindi aggiornati, poiché forniscono un miglioramento all'interno del sistema; sarebbe stupido non aggiornare un nodo, anche perché poi ne deriverebbe anche un forte indebolimento. Meno nodi non aggiornati, meno struttura, meno interesse, meno applicazione del vecchio protocollo, che automaticamente rischia di divenire obsoleto ed inutilizzato.

Blockchain funzionamento

Siamo giunti al termine della sezione riguardante la spiegazione della *blockchain*. Facendo nostre tutte le informazioni acquisite, riepiloghiamone il funzionamento. La catena è formata da blocchi, come i seguenti[35]:

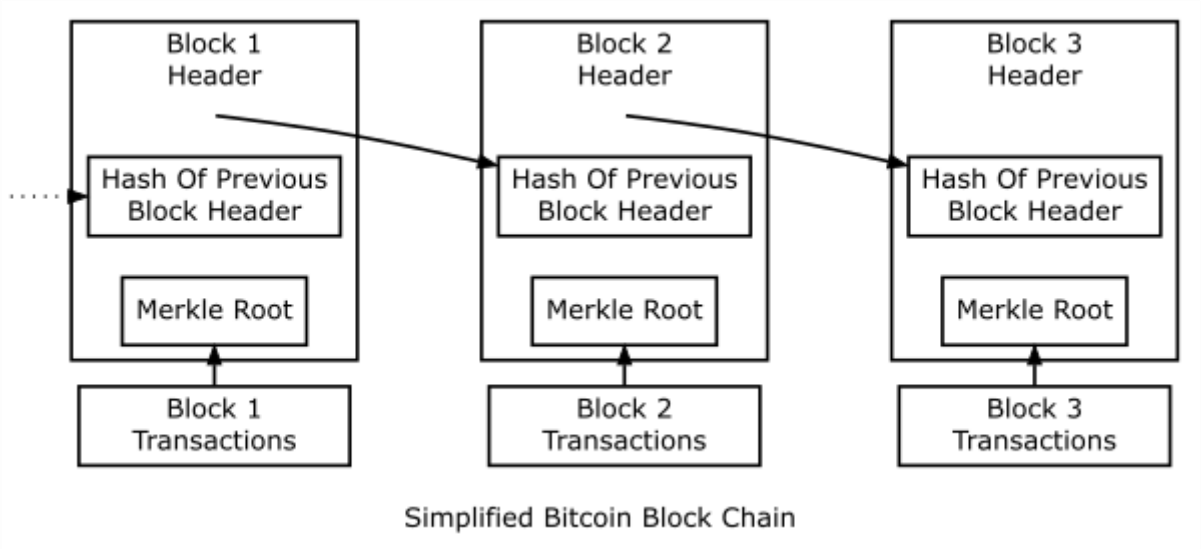

Figure 19 Rappresentazione Grafica sequenza di blocchi. Fonte[35]

Nei blocchi abbiamo delle sezioni specifiche, ogni blocco racchiude le transazioni che vengono svolte sulla rete tramite un protocollo P2P. I nodi della distributed ledger, in particolare i full node, raccolgono le transazioni e le raggruppano in blocchi, i miner nodes si occupano di convalidare i blocchi tramite il protocollo di consenso POW. I miner nodes tramite il calcolo computazionale trovano il giusto *nonce* per definire l'*hash* di ogni blocco. Subentrano di nuovo i *full node* che selezionano i blocchi validi e li ricollegano alla catena. Tale processo è continuo 24/7 per il mantenimento ed il controllo della catena *blockchain.*

[35] <https://bitcoin.org/en/blockchain-guide#introduction> Ultima Consultazione aprile 2020

La storia attorno al mondo delle *digital currency* percorre in parallelo il percorso storico descritto nella *blockchain*. *Bitcoin* viene creato e pubblicato nel 2009. Ad oggi il suo valore, ancora molto volatile, si attesta sulle 6-7 mila dollari. C'è da considerare che la valuta è partita con un valore pressoché nullo, ma l'interesse della comunità ed il suo "valore intrinseco" ne hanno fatto lievitare il prezzo fino a gennaio 2018 quando si è registrato il picco massimo mai raggiunto dalla moneta, che equivale ad oltre $20.000. Ancora oggi viene festeggiato un particolare episodio rimasto nella storia: "Il Bitcoin pizza day."[36] Il 22 maggio 2010, ossia un anno dopo l'uscita di *Bitcoin*, un programmatore di nome Laszlo Hanyecz chiese all'interno di un forum di farsi inviare presso il proprio domicilio due Pizze al "modico" prezzo di 10.000 BTC. Sono evidenti le motivazioni del perché un episodio simile venga ricordato. Facendo due calcoli rapidissimi se il nostro programmatore non avesse pagato in BTC quelle due pizze, attualmente si ritroverebbe in tasca più di 60 milioni di dollari. Tornando al discorso prezzo, allego delle charts riguardanti la storia del Btc sin dalla sua nascita.

Figura 20 Grafico andamento prezzo BTC rispetto al dollaro. Fonte[37]

[36] <http://www.bitcoinita.it/news/oggi-bitcoin-pizza-day/> Ultima consultazione aprile 2020
[37] <https://coinmarketcap.com/currencies/bitcoin/> Ultima consultazione aprile 2020

Figure 21 Grafico andamento prezzo btc da anno 2017. Fonte[37]

Il primo grafico rappresenta tutta la storia del prezzo di Btc. Nel secondo vediamo gli ultimi 3 anni, protagonisti di oscillazioni estremamente frequenti. Non solo, possiamo evidenziare come queste ultime siano, in alcuni casi, molto ampie (+/- 30%). Ne è un esempio pratico un crash di prezzo avvenuto a metà marzo 2020 quando *Bitcoin* nel giro di poche ore ha perso più del 30% del suo valore.

Figure 22 Rappresentazione Grafica del Crollo repentino del 12 Marzo. Fonte[38]

[38] <https://it.tradingview.com/chart/?symbol=GEMINI%3ABTCUSD> Ultima consultazione aprile 2020

Come si pió dedurre anche dalle candele successive, a seguito del primo crollo, nella notte si è registrato un valore minimo intorno alle 3700$. Le analisi su questo crash sono state ampissime, si è considerata anche una eventuale correlazione con i mercati tradizionali ed il suo, per così dire, alter ego fisico: l'oro. In effetti notiamo un crash generale in quella giornata, dovuto probabilmente alla diffusione del co-VID 19 a livello mondiale. Ciò ha fatto tremare tutti i mercati e gli investitori hanno agito di conseguenza, chiudendo posizioni in cerca di liquidità. Proseguendo la nostra analisi storica vediamo come si sia creato nel tempo un vero e proprio mercato "digitale" parallelo a quello tradizionale. La tecnologia è stata studiata ed implementata su nuove valute come *Ethereum* già menzionato più volte nell'elaborato. *Bitcoin ed Ethereum*, infatti, risultano essere solo la punta dell'iceberg dell'enorme mercato digitale delle criptovalute. Si registrano attualmente più di 5000 monete, sebbene *Bitcoin* mantenga ancora il primato di moneta con la più alta capitalizzazione, diventando a una vera e propria direttrice del mercato: quando è in rosso difficilmente le altre monete verranno trovate al cambio in positivo. Molto probabilmente questo dipende anche dalla non possibilità di convertire in modo rapido la nostra valuta fiat in una qualunque altra criptovaluta. La *Bitcoin dominance,* evidenzia questa tale "potenza", mettendo in rapporto la percentuale di capitalizzazione esclusiva di *Bitcoin* rispetto alla totale di tutte le altre monete digitali. Si attesta attualmente una *Bitcoin dominance* di oltre il 50%, confermando come sia considerata ancora la *Currency* più solida e richiesta del settore. Come facilmente deducibile non è mai stato ritenuto, sin dall'inizio, uno strumento "sicuro e valido" da parte degli investitori tradizionali. Tanto meno le banche hanno visto e vedono di buon occhio questa tecnologia. Le motivazioni sono ben deducibili dalle informazioni fin qui fornite. La *blockchain* è capace di eliminare del tutto il lavoro bancario, automatizzando e garantendo la medesima sicurezza al sistema. Sappiamo che le banche forniscono molto spesso dei "prestiti" bancari, strumento fondamentale all'equilibrio del mercato finanziario ed imprenditoriale. Fino a pochi anni fa non era ancora possibile gestire il servizio prestiti nel mondo delle monete virtuali, ma la soluzione è arrivata ed è chiamata *DeFi*, di cui ne parleremo più approfonditamente in una fase successiva. In conclusione di questo breve *excursus* sulla storia del prezzo di *Bitcoin*, procederei con la spiegazione sul come si effettua una transazione.

Criptovalute: Transazioni

Analizziamo una transazione in *Bitcoin* dal punto di vista crittografico. Posto che si abbia intenzione di passare una somma di denaro da utente ad un altro assicurandoci che solo e soltanto quest'ultimo riceva quel quantitativo di denaro, la procedura consisterà nel "criptare" la nostra somma di *Bitcoin* con la chiave pubblica del ricevente che chiameremo, in questo caso, B. Ci si può aiutare con le immagini già inserite nella sezione "crittografia" aggiungendo alcuni dettagli (rif. pag. 11). Prima di analizzare l'intero processo dobbiamo considerare che le transazioni che effettueremo verranno eseguite da un portafoglio virtuale. Vedremo

successivamente di cosa si tratta. Importante ora fare la distinzione tra chiave pubblica e chiave privata. Un esempio di chiavi pubbliche che chiameremo da ora "indirizzo pubblico" è:

"34F7w4L8J9xkUfSL664pjM9ZGS2kSX68NT"

"bc1qvtxh2trqfswyhprejtm9ur73sf092jst4gmrs7"

La seconda è leggermente differente alla prima in quanto essa è conseguenza di un *fork (Segwit),* di cui si è già ampiamente parlato. L'indirizzo è gestito da una catena aggiornata in cui tutte le chiavi inizieranno prevalentemente con "bc1". Rimane di base la compatibilità di quest'ultima catena con gli indirizzi *legacy* come il primo. Ad ogni chiave pubblica corrisponde una più complessa chiave privata che non dovrà in alcun caso essere condivisa con nessuno. Questi, insieme al portafoglio, sono gli strumenti che servono per effettuare una transazione. Ritornando alle fasi già citate nella prima parte, durante l'esecuzione della transazione, al fine di inviare il nostro quantitativo di *Bitcoin,* cripteremo il saldo con l'indirizzo pubblico del ricevente B. Alla transazione verrà assegnato un hash di riferimento e successivamente il ricevente decripterà il saldo con la sua chiave privata. Questo procedimento ci permette di garantire che il saldo, da noi inviato, sia esclusivamente disponibile, utilizzabile e visualizzabile nel portafoglio di B. Qui di seguito il procedimento grafico.

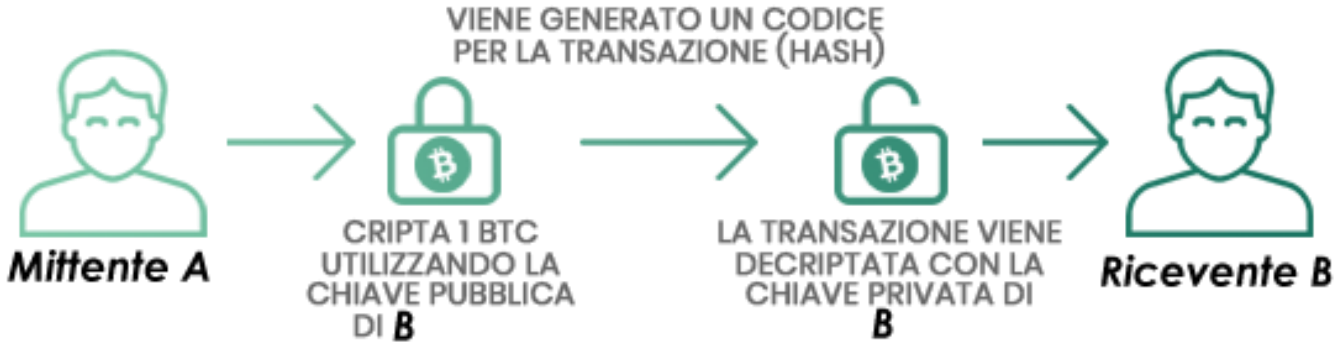

Figure 23 Rappresentazione Grafica Transazione BTC. Fonte[7]

Consideriamo che il processo non è istantaneo. La transazione avrà necessità di esser "verificata" dai nodi, aggiunta ad un blocco che, a sua volta, dovrà essere aggiunto alla catena di blocchi.

Criptovalute: Portafoglio

Dopo aver approfondito il tema "transazioni" è doveroso comprendere il funzionamento e la gestione dei portafogli. Un *Wallet* è un ibrido virtuale tra una banca, il nostro portafoglio fisico e la nostra cassaforte. Da esso immagazziniamo, gestiamo, proteggiamo, riceviamo ed inviamo moneta virtuale. È un elemento la cui presenza è imprescindibile se si vuole "investire" in criptovalute. Generalmente, essendo virtuale, si ha la

necessità di configurarne uno direttamente sul nostro PC. Ma procediamo nella nostra analisi innanzitutto fare con il classificare i vari tipi di portafoglio presenti sul mercato. Un primo distinguo potrà esser fatto tra *single-currency* e *multi-currency*. Un *Wallet Single currency* permetterà di gestire una sola criptovaluta come il più tradizionale *Bitcoin core*, per converso, un *Wallet multi currency* permetterà di gestire due o più valute. Una successiva distinzione può esser legata all'hardware utilizzato. Avremo dunque un *desktop wallet*, ossia un portafoglio standard installabile su pc, come quello già sopra citato, o un *hardware wallet*, una periferica esterna, distaccata dal nostro standard laptop; esso è accompagnato da un proprio software, installabile su pc o su smartphone, dal quale sarà possibile gestire i propri saldi di moneta virtuale. Ne è un esempio il *ledger nano x*.

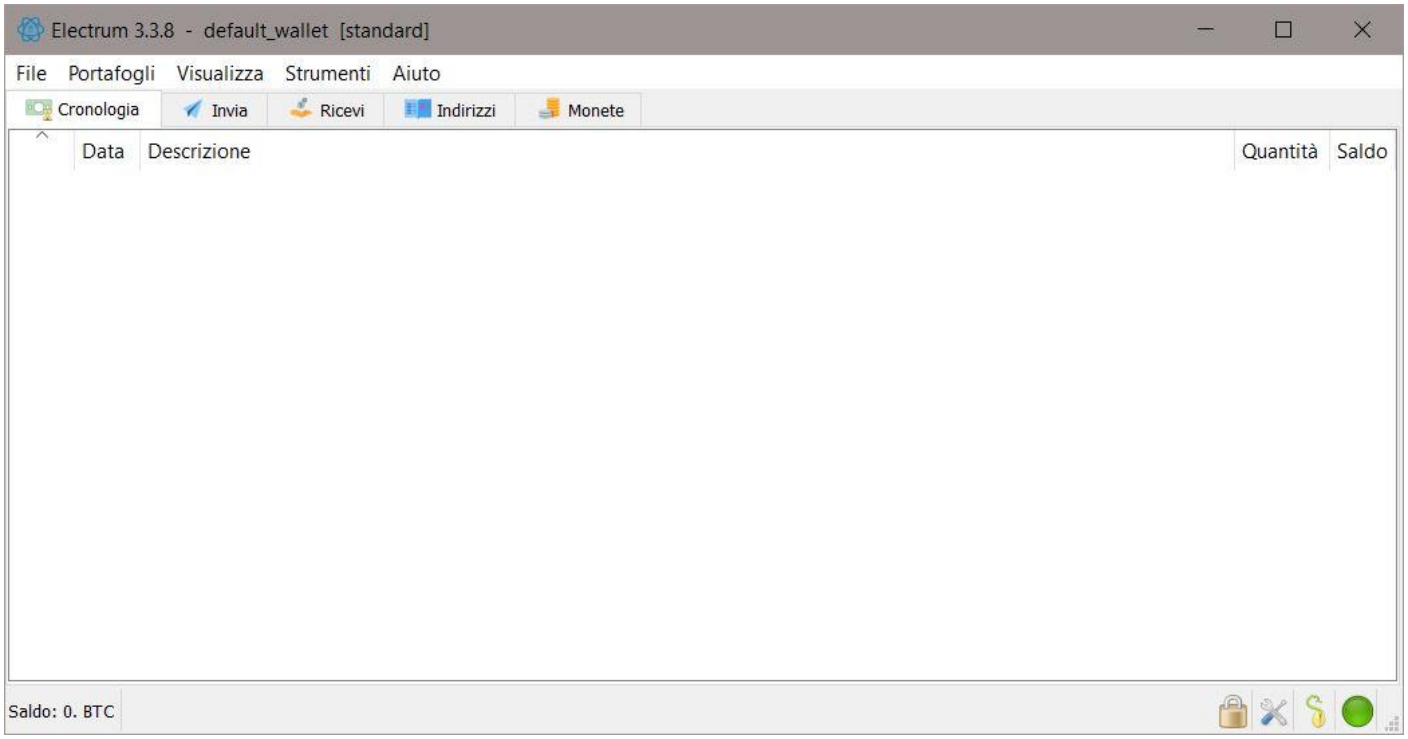

Figure 24 Esempio di desktop Wallet: Electrum Wallet. Fonte[39]

La differenza sostanziale dipende proprio da dove sono contenute e protette le criptovalute. Nel primo caso i dati sono salvati ed immagazzinati sul pc, nel secondo i saldi sono salvati sull' *hardware*, periferica esterna, che si avvale di un *software* semplicemente per l'invio e la ricezione di criptovalute. Pertanto, la differenza essenziale è la sicurezza. Immagazzinare un saldo in criptovaluta su un hard disk o un pc fisso non è sempre la soluzione più sicura, poiché le componenti potrebbero rompersi o eventualmente essere anche rubate. Con una periferica esterna potremmo avere la certezza di mantenere il dispositivo sempre al sicuro, magari in cassaforte, ed utilizzarlo solo in caso di necessità.

[39] <https://electrum.org/#download> Ultima consultazione aprile 2020

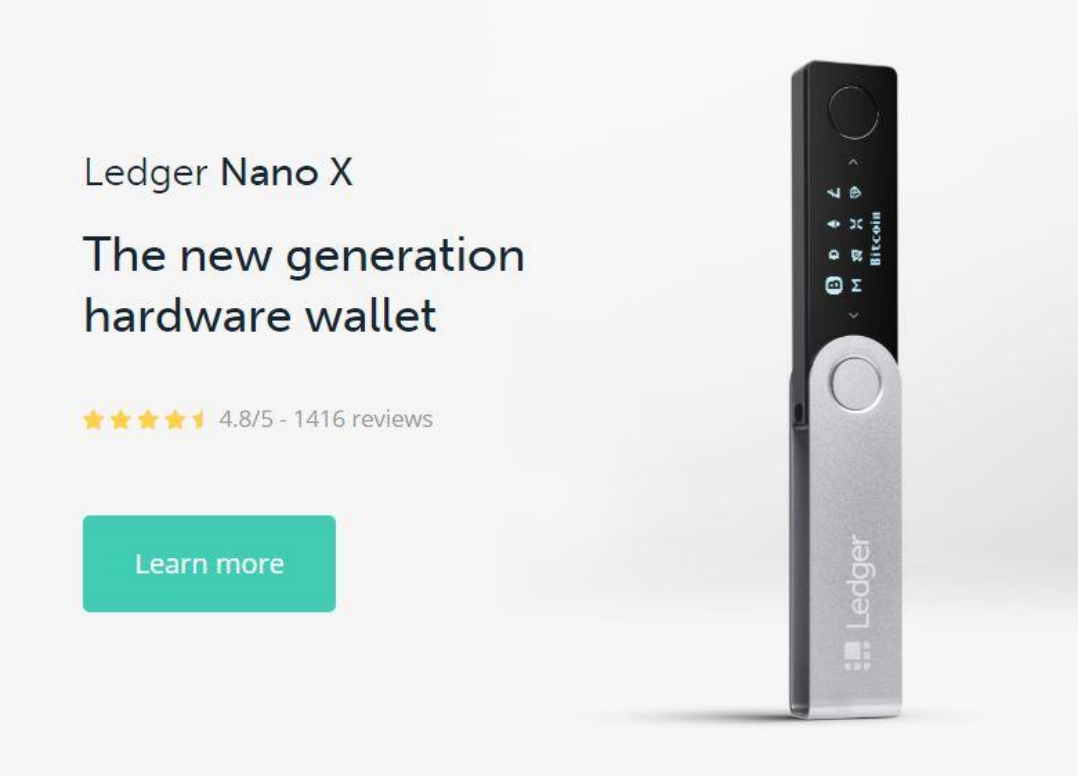

Figure 25 Esempio di Hardware wallet: Ledger Nano X. Fonte[40]

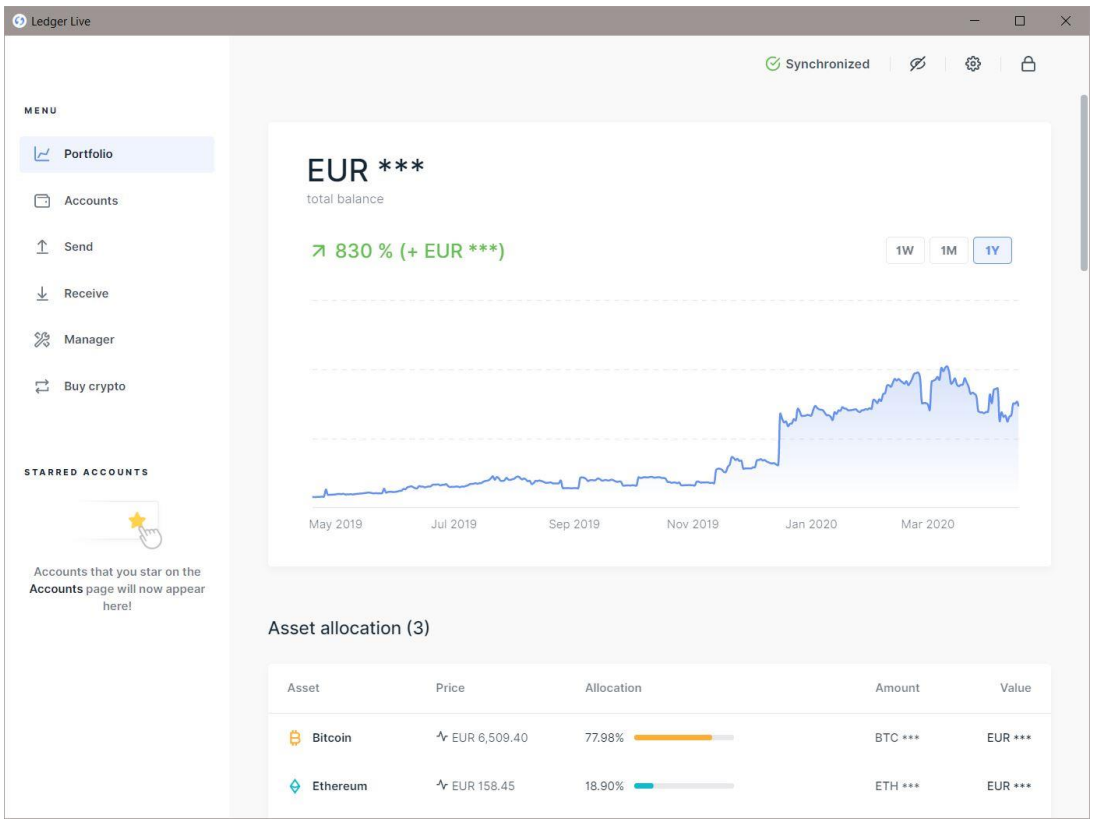

Figure 26 Esempio di Software di gestione Hardware wallet: Ledger Live

[40] <https://www.ledger.com/> Ultima consultazione aprile 2020

Sempre più utilizzati di recente, rientrano in una categoria a parte i *mobile wallet*; con essi si riesce a gestire tutto il portafoglio per mezzo del proprio *smartphone.* La sicurezza di tali portafogli lascia un po' a desiderare riscontrando similarità con quella *desktop*, anche in maniera più accentuata, essi risultano più soggetti a rotture o ad eventuali furti.

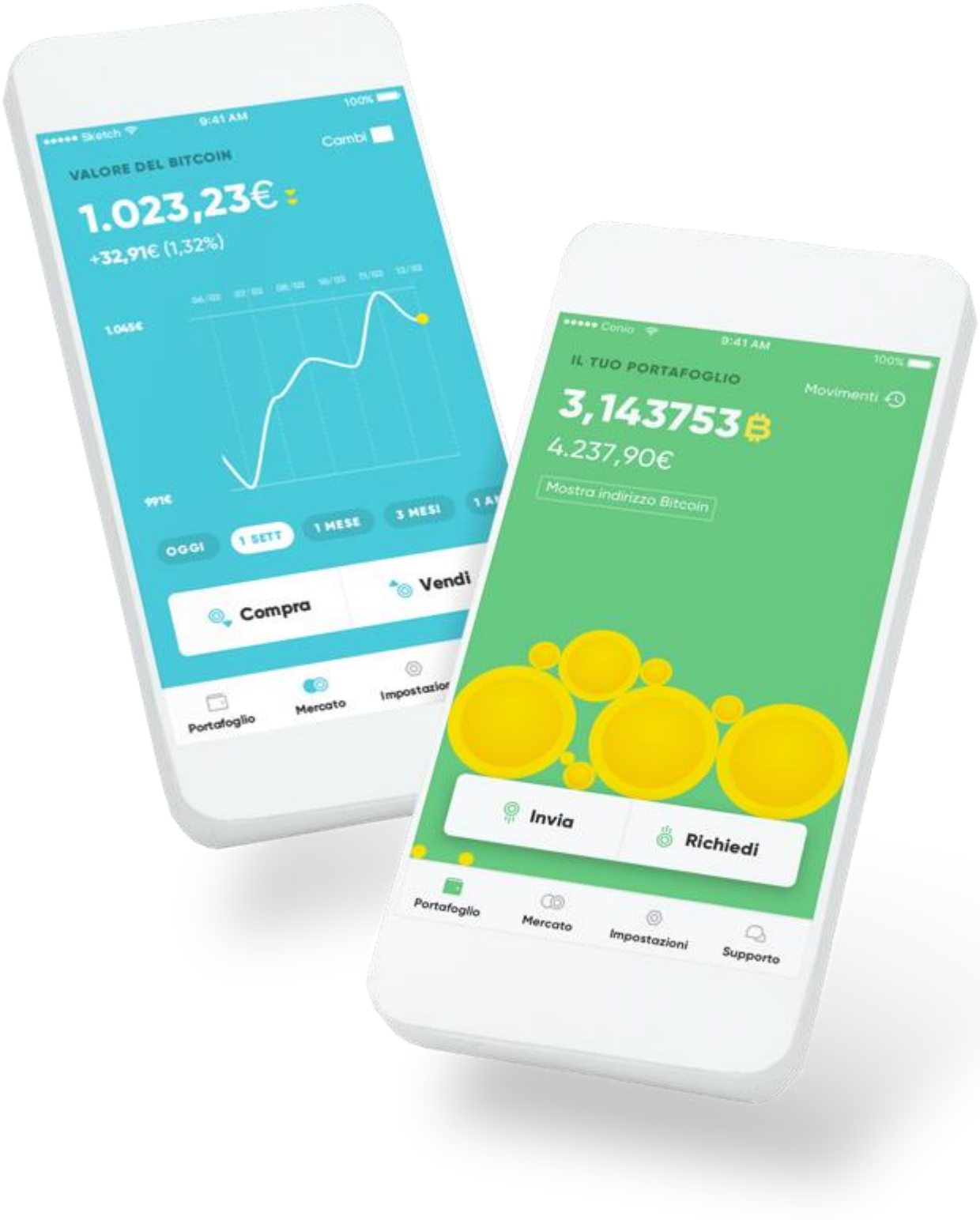

Figure 27 Esempio di mobile Wallet: Conio. Fonte[41]

[41] < https://www.conio.com/it/> Ultima consultazione aprile 2020

Una piccola citazione deve esser fatta anche sui *paper wallet*, portafogli a mono indirizzo, con lo stesso funzionamento dei precedenti. In particolare, tramite un *software* sarà possibile generare una chiave privata ed una pubblica utilizzabili a tutti gli effetti. I dati verranno salvati inizialmente su un foglio stampabile, potendo sfruttare i *qr-code* presenti su di esso come nella immagine[42] di esempio:

Figure 28 Esempio di paper wallet. Fonte[42]

Alcune piattaforme come *Blockchain.com*[43] permettono di importare le chiavi del *paper wallet* direttamente nella loro applicazione, permettendone anche un utilizzo come *web wallet* o *mobile wallet.* Un'ultima categoria è il *web wallet*. Si tratta di portafogli gestibili interamente online, che non sempre offrono un livello di sicurezza consono, basti pensare che, in caso di un down dei server di gestione della piattaforma online, non si riuscirà ad entrare nel proprio account ed eventualmente tirare fuori i saldi in moneta virtuale; in aggiunta, eventuali falle nella gestione delle credenziali, potrebbe esporci ad un furto di dati. Con gli anni sono stati aggiunti nuovi sistemi di sicurezza quali la doppia autenticazione ed il *Seed* che hanno reso tutti i tipi di portafogli citati più stabili e sicuri. Per poter operare una scelta tra un portafoglio ed un altro, in modo adeguato, bisogna sempre controllare le caratteristiche di base, analizzare gli eventuali sistemi di sicurezza utilizzabili, e soprattutto gli eventuali sistemi di *recovery.*

[42] <https://valutevirtuali.com/cose-si-usa-un-paper-wallet/> Ultima consultazione aprile 2020
[43] < https://www.blockchain.com/ > Ultima consultazione aprile 2020

Online/offline wallet e cold storage

In aggiunta alle prime classificazioni dei portafogli operate, vediamo cosa si intende per *online/offline wallet e cold storage*. Dobbiamo fare una distinzione tra i *web wallet* e gli *online/offline wallet*. Non sono assolutamente la stessa cosa. Sulle caratteristiche dei primi ci siamo già soffermati nel paragrafo precedente di contro è opportuno analizzare il concetto di *online/offline wallet*. La definizione non deriva dal tipo di piattaforma utilizzato, ma dal metodo di connettività con i nodi e la *blockchain*. I portafogli per poter operare necessitano, generalmente, di connessione e quindi di essere "online" per effettuare un invio, o per ricevere una transazione. Prendendo in considerazione un portafoglio come *Bitcoin core* classificabile come *desktop wallet,* accompagnato molto spesso da un *full node*, possiamo classificarlo come portafoglio "sempre acceso". Si avrà quindi una esposizione più elevata sia per il saldo che per i dati. Ovviamente con una adeguata configurazione sarà possibile gestire la connettività, sempre ricordando che sarà necessario avere un grande spazio per contenere l'intero *distributed ledger*. Prendendo, invece, come esempio, un portafoglio *electrum, wallet* per *Bitcoin,* la sua struttura si avvicina ad un efficace *online/offline wallet*. La prima considerazione da fare è che wallet simili si avvalgono dei già anticipati *client lightweight o spv*, di conseguenza non occuperanno molto spazio di archiviazione sul nostro pc e non fungeranno da *full node,* quindi, non collaboreranno alla verifica ed al monitoraggio delle transazioni. Con il metodo *spv*[44], acronimo che sta per *simple payment verification,* è permesso ad un client *lightweight* di verificare transazioni evitando di scaricare l'intero libro mastro, andando a fare il download esclusivamente dell'header del blocco richiesto. *Electrum* andrà "online" ogni qualvolta noi lo chiameremo in causa, mentre rimarrà offline quando spento e non utilizzato. Il vantaggio esclusivo è che non si potrà mai inviare un saldo quando "disattivo", ma esclusivamente riceverlo. Qualunque malintenzionato dovrà necessariamente inserire la password del portafoglio e accedervi direttamente dal nostro pc per poter "rubare" della moneta virtuale. Eventuali gateway di rete non potranno essere sfruttati. Per poter inviare un saldo ad un portafoglio "offline" sfrutteremo sempre gli indirizzi pubblici. La transazione sarà gestita interamente dalla *blockchain* che assegnerà il saldo inviato all'indirizzo pubblico del ricevente. Dunque, non è necessario che il portafoglio del ricevente sia costantemente online per ricevere, sarà invece necessario che il portafoglio del mittente sia attivo ed online in fase di invio. Un'evoluzione di questa procedura è il *cold storage*[45] [46] utilizzato per lo più dai "cassettisti" e quindi da chi fa *Hodling* di *Bitcoin*. Con esso si creerà uno *storage,* quindi un magazzino, in cui andremo ad inviare della moneta virtuale. La caratteristica fondamentale è che quest'ultimo è "congelato" ossia mai "online". Sarà possibile ricevere bitcoin al portafoglio e, tramite una particolare procedura offline, anche inviare un saldo. La caratteristica peculiare

[44] < https://electrum.readthedocs.io/en/latest/spv.html> Ultima consultazione aprile 2020
[45] < https://electrum.readthedocs.io/en/latest/coldstorage.html> Ultima consultazione aprile 2020
[46] < http://www.bitcoinquotidiano.com/mettere-bitcoin-al-sicuro-cold-storage-guida-electrum/> Ultima consultazione aprile 2020

di un *cold storage* è pertanto l'estrema sicurezza che possiede il portafoglio stesso, essendo costantemente offline e facendo diventare *electrum* una opzione economica dei più conosciuti e già citati *hardware wallet*. Per poter creare un *cold storage* con *electrum* avremo bisogno di due dispositivi, di cui, uno online ed uno offline. Inizialmente dovremo andare a creare un portafoglio standard sul primo hardware che potrebbe tranquillamente essere un *raspberry pi* (offline). Una volta eseguito questo primo passaggio dovremo configurare il dispositivo online. Per fare ciò avremo la necessità di copiare il cosiddetto *master public key* dal portafoglio offline ed utilizzare quest'ultimo per configurare un secondo portafoglio sull'hardware online in modalità "*watch only".* Sarà possibile quindi visionare tutte le transazioni ricevute ed inviate al portafoglio offline. In questo modo si avrà, non solo il proprio portafoglio protetto all'interno del *raspberry*, ma si potrà anche "monitorarlo" dal proprio hardware online. Gli *hardware wallet* sono abitualmente strutturati di base come *cold storage wallet*. Basti pensare che l'hardware non è connesso direttamente ad internet ma si avvale del software di supporto per gestire i dati. Ad oggi, gli *hardware wallet* risultano essere la soluzione più sicura per proteggere e gestire una o più criptovalute.

Seed e recovery wallet

Abbiamo finora discusso sui differenti portafogli presenti sul mercato, sulle varie ed eventuali caratteristiche che possiedono, ma non ci siamo soffermati ad analizzare situazione, spiacevoli e purtroppo non cosi rare quali la rottura, il furto o la perdita di un *hardware wallet* o del dispositivo su cui era installato un tradizionale portafoglio virtuale. Molti sistemi attuali sono riusciti a risolvere il problema aggiungendo nella configurazione iniziale del portafoglio il cosiddetto *Seed*[47]. Si tratta di un certo numero di parole casuali che dà la possibilità di recuperare tutti i dati del proprio portafoglio, chiavi pubbliche e private. Si raccomanda all'inizio della prima configurazione, di solito, di stampare in cartaceo più copie della *passphrase* di modo tale da avere sempre una sorta di backup del vostro portafoglio. Il *seed* sarà l'unico codice che ci permetterà in qualunque evenienza di recuperare il proprio saldo in criptovaluta. Ma facciamo molta attenzione, potrebbe risultare un'arma a doppio taglio, se dovessimo perderlo o farcelo rubare, non ci sarà più nessuna possibilità di recuperare i dati. Alla base di tale procedura vi è il noto *portafoglio deterministico gerarchico*[47], che dall'insieme delle parole su citate ed apparentemente senza un senso logico, fa derivare una *master key* da cui deriveranno e verranno sbloccate in maniera gerarchica tutte le altre chiavi. Il *portafoglio deterministico gerarchico* si affida a dei protocolli chiamati BIP 32,39,44[47]. Sarebbero presenti anche altri protocolli, ma i più utilizzati dagli attuali portafogli sul mercato, sono proprio questi. Li differenzia principalmente la lunghezza della *passphrase* che sappiamo partire da un minimo di 12 parole fino ad arrivare ad un massimo di 24. Interessante è la prerogativa del BIP 44[47] ossia quella di dare la possibilità di creare account multipli

[47] <https://cryptonomist.ch/2019/06/01/bip32-bip39-bip44-differenze-seed-wallet/> Ultima consultazione aprile 2020

per la gestione dei saldi con un solo *seed*. Essendo protocolli standard è permessa non solo la compatibilità tra portafogli di vari sistemi ma anche tra portafogli di diverse monete. Si potrebbe quindi tentare di recuperare dei dati di un portafoglio *electrum* caricando il *seed* durante la procedura di *recovery wallet*, ma su un'altra piattaforma purché abbiano entrambe lo stesso protocollo BIP di funzionamento. Inoltre, come già anticipato, con un unico *seed* potremmo recuperare anche più di un portafoglio di monete diverse. Un esempio è il caso di *ledger nano x* che dà la possibilità di recuperare più portafogli, essendo un *hardware wallet multi currency*, con unico *seed.*

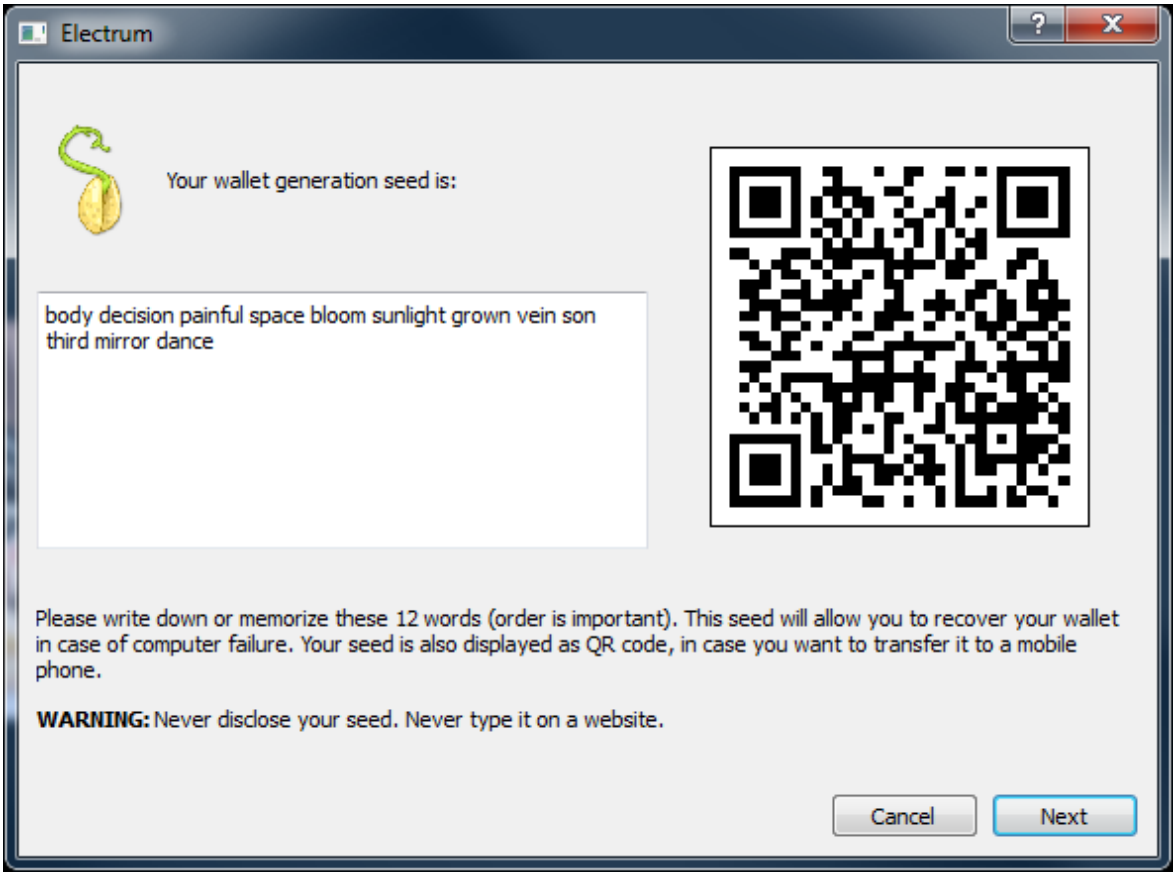

Figure 29 Esempio di Seed di un wallet. Fonte[48]

Privacy e illegalità

La questione privacy era stata approssimativamente trattata nei paragrafi precedenti, ma necessita di una disamina più approfondita in quanto non è mai da sottovalutare, considerando soprattutto quali potrebbero essere i vantaggi nel rispetto di essa o i danni che potrebbe arrecare un non rispetto delle sue norme. I portafogli personali ed i propri saldi sono essenzialmente riconducibili ad un *seed*, una *master key* ed un insieme di chiavi pubbliche e private. Non sarà mai assegnato un nome o un *alias* direttamente al proprio portafoglio o al proprio

[48] <https://edge.app/blog/why-a-12-word-mnemonic-is-an-insecure-bitcoin-wallet-backup/> Ultima consultazione aprile 2020

indirizzo. Si potrebbe tranquillamente trasferire quantitativi di criptovaluta ad un indirizzo pubblico senza sapere chi si cela dietro di esso. Questa peculiarità è stata molto spesso sfruttata negli acquisti e vendite di prodotti "illeciti" presenti nel *Deep-web*. Non sarà infatti necessario conoscere nome e cognome del venditore, ma semplicemente il suo indirizzo pubblico. Nei primi anni, Bitcoin è stato ingiustamente attaccato e accusato di essere una vera e propria moneta "illegale" o strumento di riciclaggio di denaro sporco. La situazione è ben differente, la struttura di Bitcoin inizialmente permetteva un traffico di denaro, presumibilmente illegale, grazie alle caratteristiche della sua privacy come nell'esempio del *deep-web* sopra citato, ma la definizione di moneta illegale risulta essere inopportuna così come la questione riciclaggio che assume una problematica inesistente. Considerando che alla base di Bitcoin vi è una *distributed ledger* e dunque un libro mastro comune, tutti hanno la possibilità di visionare e monitorare le transazioni. Tra transazioni periodiche con gli stessi indirizzi ed un intreccio di dati personali, si può, ad oggi, giungere al soggetto che vi è dietro un particolare indirizzo. Tramite un monitoraggio della catena sarà quindi possibile scoprire eventuali traffici illeciti o un eventuale riciclaggio di denaro. Ciò è anche possibile grazie al fatto che le conversioni da moneta fiat in btc e viceversa avvengono principalmente presso gli *exchange*, piattaforme online di conversione. È facilmente deducibile che per l'acquisto sarà necessario uno strumento elettronico per il trasferimento di euro o dollaro che siano. Un eventuale account di conversione possiederà tanti dati personali dell'utente e quindi risulterà tracciabile. Questo importante vincolo conferma quanto il miglior strumento per il riciclaggio non risulti assolutamente essere il *Bitcoin*, ma lo stesso denaro contate, più facilmente gestibile e non tracciabile all'interno di una economia sommersa. La stessa analisi può essere fatta per acquisti "illegali" che saranno sempre preceduti da un acquisto della moneta su di una piattaforma monitorata. La verità è nel mezzo. *Bitcoin*, non richiedendo per una transazione, come in un bonifico sepa, dati personali, iban, codici *Swift/Bic*, sia del mittente che del ricevente, gode di una privacy teoricamente molto elevata, ma grazie agli exchange, ai vari portafogli, al libro mastro pubblico, con un intreccio di dati si può risalire, senza non poca fatica, al proprietario della transazione. Il livello di privacy attuale di Bitcoin è medio. Esistono attualmente monete che hanno un livello di privacy estremamente elevato come *Monero*[49]. Quest'ultima è diventata strumento di pagamento preferito dei creatori di *ransomware*, virus capaci di bloccare file o cartelle nei nostri pc, chiedendo un riscatto per lo sblocco dei dati. Nel 90% dei casi è sempre più conveniente pagare il "riscatto" che rischiare di perdere file importanti. *Monero nasce* da un *fork* della moneta *Bytecoin* da cui eredita un protocollo base denominato *CryptoNote*[50]. Per garantire una *privacy* ancora più forte sono stati affiancati al protocollo *cryptonote* altrettanti sistemi[49] come:

- *Ring Signature:* processo di verifica che consiste nel far firmare a nome del gruppo di appartenenza degli individui tutte le transazioni.

[49] <https://cryptonomist.ch/2019/08/11/monero-xmr-criptovaluta-anonimato/> Ultima consultazione aprile 2020
[50] <https://it.wikipedia.org/wiki/CryptoNote> Ultima consultazione aprile 2020

- Protocollo modificato di *diffie-hellman:* per ogni transazione effettuata gli indirizzi verranno automaticamente rigenerati.
- *Ring CT e Kovri:* evoluzione della Ring Signatures che non permette a nessuno se non mittente e destinatario di verificare quanto saldo è stato trasferito.

Monero non è l'unica *private cripto* sul mercato, ma è certamente la più utilizzata e famosa.

Double spending e 51% mining attack

La problematica del *Double spending*[51] è ancora oggi, in molte *blockchain*, un grosso problema, principalmente nelle più deboli. La problematica vien fuori nel momento in cui un "malintenzionato" voglia effettuare una doppia spesa, ossia quando si vuole effettuare una doppia transizione verso indirizzi differenti con uno stesso ammontare. Si invierà dunque uno stesso saldo a due persone diverse avente un *hash* o numero seriale uguale. Le due transazioni dovranno essere successivamente confermate dai nodi ed implementate nella catena. Prendendo una sana e strutturata *blockchain* di esempio come quella di *Bitcoin*, durante questa fase, considerando che siamo in una *distributed ledger*, ci saranno migliaia di nodi che controlleranno la transazione, ergo in molti riusciranno a notare l'illegalità compiuta ed eventualmente tornare indietro nella catena ed aggiustare la transazione. Tutto ciò andrebbe ad intaccare il concetto di *immutabilità*, ma sappiamo anche che l'intera comunità legata a *Bitcoin* può intervenire, in questi casi, per la risoluzione del problema, come già anticipato nella prima parte. Nel momento in cui gli utenti sono tanti e i nodi saranno altrettanti, ed il mining sarà ben distribuito, le problematiche derivanti da un'eventuale *double spending* saranno minime, se non nulle. Una più grande preoccupazione deriverebbe da un eventuale attacco mining del 51%[52]. Queste due problematiche solitamente viaggiano a braccetto. Sappiamo che il mining è il meccanismo di consenso che permette di avere un monitoraggio e una adeguata gestione delle transazioni, rendendo la catena di blocchi un sistema "antifrode". Per assurdo, noi potremmo gestire il 50 o più % della potenza di calcolo, avendo possibilità di avere un controllo sulle verifiche dei blocchi quasi totale. Chi eventualmente detiene il 51% potrebbe senza problemi eludere le regole alla base del consenso ed eventualmente convalidare anche un *double spending*. Di recente è accaduto sulla blockchain di *Ethereum classic*, con un attacco sulla potenza di calcolo in cui, in un lasso di tempo breve, è stato verificato un enorme quantitativo di blocchi confermando anche un voluto *Double spending.* A rendersene conto molti osservatori costanti delle blockchain ossia gli *exchange*, che hanno visualizzato movimenti anomali sulla catena. La situazione è stata risolta e monitorata, ma ha destato non poche preoccupazioni, considerando che ETC è una delle cryptocurrency più conosciute. Le cause sono attribuibili a dei test di nuove macchine (ASIC) che hanno iniettato nella "piccola" *blockchain* di *ethereum classic* una potenza enorme, tanto da poter superare il 51% della potenza totale della rete. La

[51] Materiale del corso di informatica
[52] <https://www.crypto51.app/about.html> Ultima consultazione aprile 2020

"facilità" di esecuzione è stata aiutata dal piccolo *environment* della moneta. Per farsi un'idea sulla fattibilità di un attacco simile, sarà possibile calcolare il costo di un eventuale attacco tramite svariati siti web. Un esempio è *Bitcoin*: per attaccare la rete per una sola ora "basterebbero" circa 600 mila dollari[53].

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$128.26 B	SHA-256	122,010 PH/s	*$599,063*	0%
Ethereum	ETH	$18.79 B	Ethash	176 TH/s	*$99,942*	3%
BitcoinCashABC	BCH	$4.20 B	SHA-256	1,797 PH/s	*$8,824*	18%
BitcoinSV	BSV	$3.52 B	SHA-256	1,562 PH/s	*$7,667*	21%
Litecoin	LTC	$2.73 B	Scrypt	158 TH/s	*$13,569*	6%
Dash	DASH	$706.95 M	X11	6 PH/s	*$2,517*	6%
EthereumClassic	ETC	$625.16 M	Ethash	9 TH/s	*$4,959*	63%
Zcash	ZEC	$345.08 M	Equihash	5 GH/s	*$8,668*	2%
BitcoinGold	BTG	$170.12 M	Zhash	3 MH/s	*$662*	55%
Ravencoin	RVN	$95.50 M	X16Rv2	37 TH/s	*$27,288*	1%

Figure 30 Esempio di classifica Costi per un'ora di attacco mining. Fonte[53]

Il valore risulta essere abbastanza fittizio, poiché difficilmente le piattaforme online e le *pool* permettono di acquistare tutta quella potenza di calcolo anche solo per un'ora. Servirebbe una organizzazione non da poco per gestire tutto l'attacco ed eventualmente comprare direttamente un quantitativo di *miners* elevatissimo. Tra gestione e costi, non ne varrebbe assolutamente la pena. Un'ultima variabile è data dal valore intrinseco che hanno le monete digitali, esso verrebbe meno in caso di continui attacchi e *double spending*, riducendone la fiducia ed anche i guadagni. In conclusione, il problema e la possibilità c'è, ma la struttura e la piattaforma di consenso rende il tutto estremamente difficile, poco economico, e di conseguenza poco profittevole.

[53] <https://www.crypto51.app/> Ultima consultazione aprile 2020

Exchange

Per *exchange* si vuole intendere una qualsiasi piattaforma che ci permette di "convertire" moneta FIAT in moneta digitale. L'importanza di queste strutture è di facile comprensione, poiché senza di essere sarebbe molto difficile comprare e vendere *cryptocurrencies.* Potremmo classificare queste piattaforme come degli "intermediari finanziari" all'interno di un "mercato dei cambi". In quest'ultimo, nella sua versione tradizionale, vengono messe in rapporto le varie monete mondiali (euro, dollaro, sterlina, ecc.). Da qui si avrà la possibilità di convertire i nostri euro in altre valute, in base ad un determinato tasso di cambio. Nel caso in cui noi avessimo una determinata liquidità, ad esempio dieci mila euro, e volessimo sfruttare l'intero saldo per "acquistare" dei dollari, sarà necessario interfacciarsi con degli intermediari finanziari all'interno del mercato dei cambi di riferimento. Ipotizzando un cambio sull'euro/dollaro di 1,15 acquisiremo, con la liquidità sopra citata, 11500 dollari, a cui vanno aggiunti i vari costi di conversione. Gli intermediari sono presenti nei vari mercati proprio per abbattere i costi, che diventerebbero estremamente elevati nel caso in cui si volesse direttamente, come privati, andare ad investire una piccola somma. I più conosciuti *exchange* sono *Coinbase, Karen, Binance, The Rock Trading e Huobi.* Pochi rispetto all'elenco totale. Per poter comprendere il loro funzionamento è opportuno partire da piattaforme più intuitive come *Coinbase*. All'interno di quest'ultima l'acquisto e la vendita di criptovaluta sono molto rapidi. Per potersi registrare a piattaforme simili saranno necessarie non solo il nostro nome e cognome e una mail, ma ulteriori dati personali. Si richiedono spesso informazioni molto dettagliate: se si è lavoratori autonomi o dipendenti, da dove provengono i flussi di denaro fiat che verranno utilizzati per l'acquisto di moneta, quale è il nostro stato sociale attuale e così via. Questa maggiore richiesta di dettagli personali è stata aggiunta per la conformità al *KYC, Know your customer,* una procedura di riconoscimento dei clienti da parte delle aziende. È principalmente adottata in piattaforme online, non solo da parte degli *exchange*, ma anche da parte delle banche, ad oggi sempre più tecnologiche, che la richiedono per fornire ai clienti i servizi online come *l'home banking*. All'interno degli *exchange* prima di poter operare, verranno richieste ulteriori documentazioni addizionali per la verifica dell'identità e residenza, sempre per il rispetto delle conformità (*Kyc).* Sarà quindi necessario caricare una copia fronte retro del proprio documento di riconoscimento (carta d'identità, passaporto, patente di guida). Solitamente questa prima verifica sbloccherà i "primi" limiti del conto. Si potrà iniziare ad acquistare cripto, ma con specifici metodi di pagamento e con dei limiti di acquisto. Per "sbloccare" interamente il nostro *account* si dovrà verificare anche il nostro indirizzo di residenza. Dovranno essere utilizzati, anche qui, dei documenti ufficiali (come un estratto conto bancario o una bolletta) dove siano presenti il proprio nome e cognome ed il proprio indirizzo di residenza. Dopo questa fase i limiti al conto verranno eliminati e si potrà procedere all'acquisto con più libertà. Da *Coinbase* avremo la possibilità di acquistare del BTC o altre *altcoin* direttamente con la nostra carta di

credito o debito personali, basterà fare un rapido collegamento dei dati della carta. Ecco un'immagine[54] della finestra di Gateway per l'acquisto di *Bitcoin* su *coinbase:*

Figure 31 Esempio di finestra rapida di Compravendita Bitcoin su COINBASE. Fonte[54]

Tramite questa finestra si potrà in pochi secondi comprare al prezzo di mercato i nostri btc. La piattaforma offre interfacce molto intuitive, ma permette di acquistare *bitcoin* esclusivamente solo al prezzo di cambio attuale. Nel caso in cui il prezzo di cambio fosse €6000 per BTC nel momento di acquisto, il cambio della nostra liquidità avverrà in rapporto a quella cifra. Considerando come liquidità 9mila euro, vorrà dire che verranno accreditati sul conto 1,5 BTC, a cui vanno aggiunti sempre i costi di transazione. Una versione più professionale di *Coinbase*, assieme alle piattaforme *Binance* e *Kraken* dà la possibilità di piazzare veri e propri ordini di richiesta, che possono discostarsi anche dal prezzo di mercato attuale.

[54] <https://www.coinbase.com/dashboard> Ultima consultazione aprile 2020

Prezzo di mercato

Per quanto riguarda il prezzo di mercato del *Bitcoin* esso assume un profilo non tanto similare al mercato dei cambi quanto più a quello azionario. Siamo di fronte a delle forti oscillazioni del valore anche nel breve periodo. Il prezzo della moneta viene fuori da una classica intersezione tra due curve: la curva della domanda e quella dell'offerta. Il punto di intersezione corrisponderebbe al prezzo di cambio o di mercato della valuta digitale. Questo punto varia rapidamente spostandosi all'interno del grafico stesso a seconda anche di come la curva di offerta e di domanda si muovono. Per fare un esempio semplice, considerando in un mercato azionario classico una notizia su di un positivo trimestre dell'azienda "Tal dei tali", la più probabile conseguenza sarà il rialzo del valore azionario della stessa azienda, poiché la domanda delle azioni aziendali salirà, mentre l'offerta rimarrà la stessa. Di contro se la notizia fornita evidenzia un trimestre negativo probabilmente la domanda si abbasserà mentre l'offerta aumenterà facendo abbassare il prezzo di equilibrio. Bitcoin nei suoi primi anni ha subito molte oscillazioni di prezzo anche a causa di notizie o giudizi nei confronti della moneta espressi da importanti personaggi o testate giornalistiche. Ultimamente le variazioni di prezzo dipendono da delle variazioni vere e proprie di liquidità nel mercato cripto. Un grande volume di ordini di vendita farebbe pian piano scendere il prezzo della moneta, mentre una grande iniezione di liquidità all'acquisto farebbe salire il prezzo di equilibrio. *Gli exchange* sono assimilabili quindi ad un intermediario finanziario ibrido tra i vari mercati tradizionali. Ci sono talmente tante sfumature che risulta quasi non adeguato fare una comparazione. Rimane comunque necessario fare un paragone approssimativo per comprendere meglio il concetto che c'è dietro queste piattaforme.

#	Nome	Prezzo	Variazione	Capitalizzazione di mercato
1	Bitcoin BTC	6.459,88 €	+4,77%	119.4B €
2	Ethereum ETH	157,50 €	+10,05%	17.6B €
3	XRP XRP	0,17 €	+3,82%	7.7B €
4	Tether USDT	0,92 €	-0,02%	5.9B €
5	Bitcoin Cash BCH	212,74 €	+5,48%	3.9B €
6	Bitcoin SV BSV	180,73 €	+3,42%	3.3B €

Figure 32 Esempio di elenco di prezzi di mercato criptovalute. Fonte[55]

[55] < https://www.coinbase.com/price> Ultima consultazione aprile 2020

Come già anticipato vi è la possibilità con piattaforme più professionali, come questa in foto[56], di operare con più libertà direttamente nel mercato digitale.

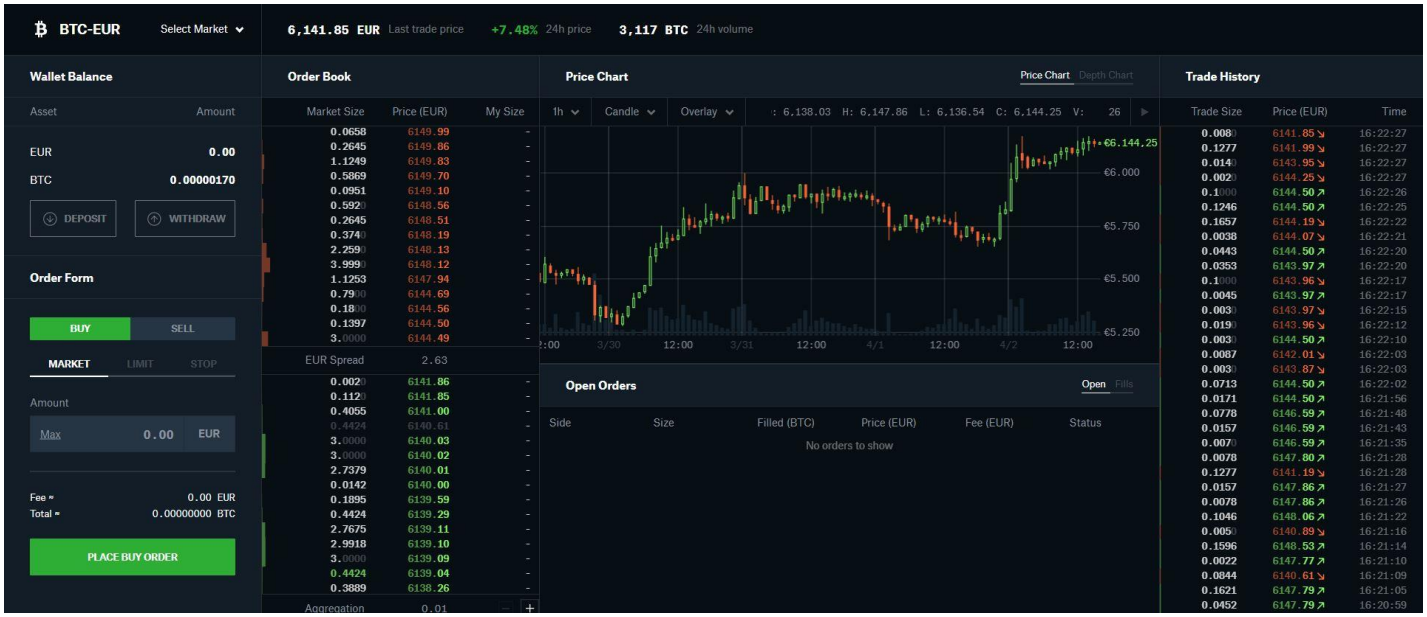

Figura 33 dashboard Coinbase pro. Fonte56

La dashboard e le modalità di acquisto e di vendita in questo caso non sono intuitive come quelle già analizzate. Vengono fornite più opzioni all'utente. Di fatti, oltre alla possibilità di acquistare e vendere a prezzo di mercato, sarà inoltre possibile inserire nel mercato nuovi "ordini". Molto semplicemente si tratta di richieste che vengono inviate nel mercato, limitato alla piattaforma, in cui si è disposti a pagare o vendere il proprio saldo ad un prezzo di cambio differente da quello di mercato attuale. Osservando i dati in foto noteremo una colonna sulla sinistra diviso in due elenchi: l'*order book*. La prima colonna in rosso, nella parte superiore, rappresenta gli ordini ed i volumi di vendita immessi nel mercato, mentre, la colonna posta in basso di colore verde rappresenta gli ordini ed i volumi di acquisto. Nel mezzo tra le due colonne è presente il cosiddetto "spread" che non ha in alcun modo a che vedere con quello tradizionalmente conosciuto, bensì sta ad indicare la quantità in euro di differenza tra l'ordine con il prezzo di vendita più basso e l'ordine con il prezzo di acquisto più alto. Nella parte centrale è ben visibile un grafico a candele dell'andamento attuale della coppia che si sta analizzando, nel nostro caso il rapporto BTC/EUR visualizzabile in alto a sinistra. Nell'ultima colonna sulla destra sono presenti in ordine cronologico ed in tempo reale tutti gli ordini completati: il *Trade history*. Siamo di fronte alla piattaforma *Coinbase Pro* versione differente dal classico *Coinbase*.

[56] <https://pro.coinbase.com/> Ultima consultazione aprile 2020

Order Book

Market Size	Price (EUR)	My Size
4.0000	6461.91	-
3.9525	6461.90	-
1.2608	6461.29	-
0.2955	6460.83	-
0.5920	6460.69	-
1.4277	6460.10	-
2.3000	6459.71	-
0.1800	6459.69	-
6.2287	6459.68	-
0.2021	6459.36	-
1.2000	6459.35	-
0.4283	6458.81	-
0.0784	6458.80	-
EUR Spread	4.80	
0.0104	6454.00	-
0.0363	6452.00	-
0.1200	6450.83	-
0.9620	6450.81	-
0.9618	6450.58	-
0.1801	6450.33	-
0.0850	6450.31	-
1.2000	6450.29	-
0.2955	6450.28	-
0.0362	6450.00	-
0.4283	6449.60	-
0.0312	6448.00	-
0.8090	6446.55	-
0.1200	6446.54	-
1.1040	6446.49	-
0.7137	6446.13	-

Figure 34 Order book ed Eur spread. Fonte56

Trade History

Trade Size	Price (EUR)	Time
0.0014	6455.43 ↘	19:13:52
0.0486	6456.46 ↘	19:13:45
0.3300	6461.93 ↗	19:13:41
0.2003	6461.93 ↗	19:13:37
0.0225	6461.93 ↗	19:13:35
0.1060	6456.46 ↘	19:13:34
0.0049	6457.73 ↘	19:13:34
0.0325	6461.93 ↗	19:13:28
0.3771	6461.93 ↗	19:13:28
2.2182	6461.94 ↗	19:13:27
1.2000	6461.93 ↗	19:13:27
0.1800	6461.92 ↗	19:13:27
1.2000	6461.91 ↗	19:13:27
0.5657	6461.91 ↗	19:13:27
0.0321	6457.73 ↘	19:13:18
0.0014	6463.06 ↗	19:13:16
0.0016	6455.61 ↘	19:13:13
0.0222	6463.08 ↗	19:13:13
0.0163	6463.08 ↗	19:13:12
0.0103	6462.13 ↗	19:13:05
0.0025	6462.13 ↗	19:13:05
0.1000	6461.68 ↗	19:13:01
0.0149	6461.70 ↗	19:13:00
0.0028	6463.14 ↗	19:12:55
0.0034	6463.14 ↗	19:12:54
0.6963	6457.73 ↘	19:12:50
0.0739	6457.74 ↘	19:12:50
0.0671	6457.75 ↘	19:12:50
0.1406	6463.18 ↗	19:12:48
0.0111	6463.18 ↗	19:12:45
0.1109	6463.18 ↗	19:12:41
0.0074	6463.19 ↗	19:12:35
0.0074	6463.17 ↗	19:12:30

Figure 35 Trade History. Fonte56

Le altre piattaforme già citate assumono un'impostazione simile a questa in foto, rendendo non sempre estremamente facile l'acquisto di criptovaluta. Per poter piazzare un ordine, magari nel nostro caso uno di acquisto, dovremo utilizzare L'*order form* sulla parte sinistra della schermata. Inseriremo il prezzo di cambio, differente o uguale a quello di mercato attuale, ed il quantitativo di liquidità che li vogliamo assegnare. Siamo disponibili, ad esempio, a comprare 1 BTC al prezzo di cambio di €6500. Inseriremo quindi un prezzo di cambio di €6500. Queste impostazioni sono a nostra discrezione. Generalmente, nei valori da inserire, viene richiesta la quantità di btc da acquistare, quindi quanti euro si vogliono spendere ed il prezzo di cambio. Una

volta inseriti, prima della "apertura" dell'ordine vengono riepilogati i costi di conversione, che si pagheranno nel caso in cui l'ordine andasse a buon fine ed il quantitativo di *euro* che spenderemo per l'acquisto.

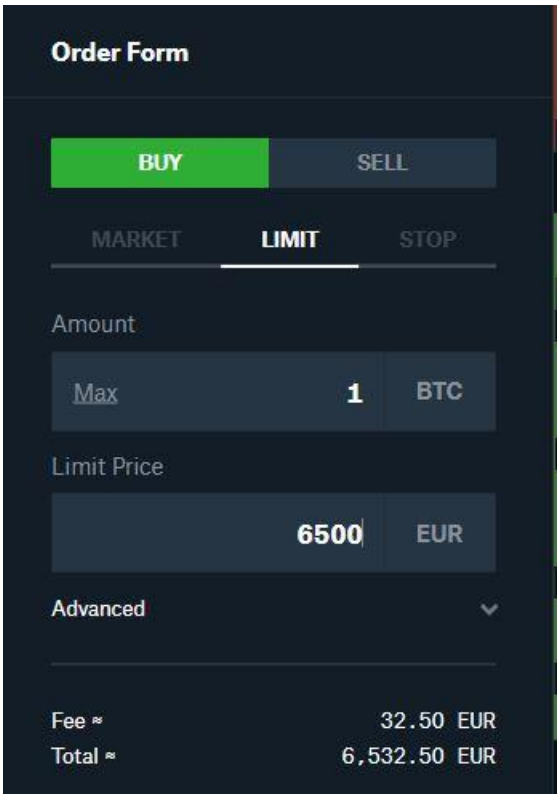

Figure 36 Order form con dati di esempio. Fonte56

Ordini aperti, chiusi e *filled*

Per poter comprare o vendere criptovaluta dovremo "aprire" un ordine. Questo termine indica la messa sul mercato (limitato all'*exchange* di riferimento) della richiesta, come quella compilata in precedenza. Attenzione però, la richiesta se si dovesse discostare molto dall'attuale prezzo di mercato non verrebbe "processata" immediatamente, ma rimarrebbe "aperta" fin quando non sarà presente un ordine "opposto" sul mercato con medesimi volumi e stesso prezzo di cambio. Quindi se riuscissimo a piazzare un ordine di vendita, dovrà essere presente un opposto ordine di acquisto con medesimo prezzo di cambio e simil volume per poter essere "completato". Nel momento in cui dovesse essere presente un ordine "opposto" ma con un diverso volume, e nel caso in cui quest'ultimo fosse inferiore al volume d'ordine da noi impostato, il nostro verrà *partially filled* quindi sarà processato parzialmente. Mentre, nel momento in cui l'ordine "opposto" avesse un volume maggiore, il nostro ordine verrebbe *filled* e quindi processato interamente. Di contro, l'ordine "opposto" risulterà, in quest'ultimo caso, *partially filled.* Sia nel caso contemplato precedentemente, sia in questo caso, gli ordini *partially filled* verranno "completati" da altri ordini che in ordine cronologico verranno "aperti". Nel caso in cui avessimo aperto un ordine e quest'ultimo non venisse né *partially filled* né *filled* avremmo la possibilità di "chiudere" l'ordine manualmente e quindi annullare la richiesta ed è un caso molto frequente poiché non è mai facile analizzare gli andamenti del mercato. Si potrebbe aprire un ordine ad un prezzo

leggermente inferiore rispetto all'attuale prezzo di mercato, ma potrebbe non essere mai completato perché essendo il mercato in positivo, difficilmente saranno disponibili degli ordini "opposti" capaci di completare il nostro.

Market Maker o taker

In stretto collegamento con la gestione degli ordini, c'è la scelta su come operare all'interno dell'*Exchange*, se come *market maker*[57] *o taker.* Per poter definire il primo, possiamo utilizzare come esempio un mercato monopolistico. All'interno di questo mercato ci sarà una ed una sola azienda che produrrà un determinato bene o servizio da rivendere al pubblico, questa qualità permette all'impresa stessa, in mancanza di concorrenza, di operare come *price maker*, sarà quindi lei a decidere il prezzo di vendita di quel bene. Nel caso in cui noi operassimo in un *exchange*, come descritto nei paragrafi precedenti, tramite gli esempi numerici, saremmo dei price *maker:* decideremmo noi il prezzo di cambio tra btc ed euro che saremmo disposti a pagare. Nel caso in cui noi dovessimo invece accettare il prezzo di mercato opereremmo come dei *taker,* accettando, dunque, il prezzo di mercato è quindi disposti a pagare a quel prezzo di cambio. Questa differenza è molto importane da comprendere poiché, sulle varie piattaforme, c'è una notevole differenza di costi di conversione, ne vedremo un esempio nella sezione dedicata. Si aggiunge un altro vantaggio all'utilizzo di strutture professionali in quanto si ha la possibilità di procedere con un ordine *limit*, in cui è quindi possibile operare da *maker* e decidere il prezzo.

Comandi Comuni

- *Limit buy/sell*[58]*:* ordine di acquisto o di vendita con prezzo "limite" di cambio. Avremo la possibilità di impostare un prezzo di cambio differente da quello di mercato;
- *Good till canceled*[58]: l'ordine rimarrà "aperto" fino ad un eventuale completamento o cancellazione manuale dell'utente;
- *immediate or cancel*[58]*:* l'ordine verrà "aperto" ma, se non completato nell'immediato, sarà automaticamente cancellato dalla piattaforma;
    - *Market order*[58]*:* l'ordine verrà aperto al prezzo di cambio di mercato attuale.

[57] < https://etherevolution.eu/differenza-maker-taker/?cn-reloaded=1> Ultima consultazione aprile 2020
[58] <https://help.coinbase.com/en/pro/trading-and-funding/orders/overview-of-order-types-and-settings-stop-limit-market.html> Ultima consultazione aprile 2020

Costi di conversione

Le piattaforme di certo non operano senza guadagno. Le entrate vengono generate principalmente dai costi di conversione. Per ogni ordine d'acquisto o di vendita verrà attribuita una percentuale di costo in proporzione percentuale al volume d'ordine inserito. Quindi per ogni ordine aperto e "fillato" verrà sottratta una percentuale variabile a seconda della piattaforma e del metodo di pagamento. Ipotizzando un costo di conversione del 2% su un volume di €5000 d'ordine ed un prezzo di cambio di €5000 spenderemo €100 di costi di conversione. L'intera transazione verrà a costare €5100 euro ed avremo convertito quella somma in un 1 BTC. Gli *exchange* in cui l'acquisto è più semplice e rapido come il classico Coinbase, hanno lo svantaggio di possedere costi di conversione molto più alti, raggiungendo percentuali 3-4 volte più grandi di un *exchange* in cui è possibile operare come *maker*. Tutte le piattaforme più professionali hanno ideato differenti strutture dei costi per spronare gli investitori ad immettere sempre più liquidità e ad operare come *maker*, come per *Coinbase Pro* o *Kraken*. Nel caso, invece, di *Huobi* e *Binance* le strutture dei costi dipendondo da quanti *token* di loro proprietà si possiedono sulla piattaforma. Cercando di riassumere e comparare brevemente i dati sulle commissioni tra gli *exchange Coinbase Pro* e *Kraken* ho ideato questa rapida tabella riepilogativa:

	Volume su 30 Giorni in $	Maker	Taker		Maker	Taker
Coinbase Pro	0- 10k	0,50%	0,50%	**Kraken**	0,16%	0,26%
	10k-50k	0,35%	0,35%		0,16%	0,26%
	50-100k	0,15%	0,25%		0,14%	0,24%
	100k-250k	0,10%	0,20%		0,12%	0,22%
	250k-500k	0,10%	0,20%		0,10%	0,20%
	500k-1M	0,10%	0,20%		0,08%	0,18%
	1M-2,5M	0,08%	0,18%		0,06%	0,16%
	2,5M-5M	0,08%	0,18%		0,04%	0,14%
	5M-10M	0,08%	0,18%		0,02%	0,12%
	10M-50M	0,05%	0,15%		0,00%	0,10%
	50M-100M	0,00%	0,10%		0,00%	0,10%
	100M-300M	0,00%	0,07%		0,00%	0,10%
	300M-500M	0,00%	0,06%		0,00%	0,10%
	500M-1B	0,00%	0,05%		0,00%	0,10%
	1B+	0,00%	0,04%		0,00%	0,10%

Tabella 4 Riepilogo percentuali commissioni in rapporto a volume. Fonte[59] [60]

[59] < https://www.kraken.com/it-it/features/fee-schedule> Ultima consultazione aprile 2020
[60] < https://help.coinbase.com/en/pro/trading-and-funding/trading-rules-and-fees/fees.html> ultima consultazione aprile 2020

Sicurezza

Gli *exchange* ad oggi immagazzinano un'enormità di fondi e di informazioni. Per quanto queste grandi piattaforme siano sicure, non si può mai essere sicuri al 100%. Abbiamo già trattato la questione online wallet, classificandoli come non estremamente sicuri. Molto spesso i primi provider che offrono portafogli online sono gli stessi *exchange* poiché la conversione tra valuta fiat e monete virtuali avviene direttamente al loro interno. Nel momento in cui convertiamo in nostri euro in *Bitcoin*, questi ultimi vengono accreditati nel nostro portafoglio online, ma nella piattaforma. Pur avendo massima libertà di gestire il saldo e le chiavi, dobbiamo comunque considerare che si tratta di portafogli online e controllati da una piattaforma. Le *private key* del portafoglio, che teoricamente dovrebbero essere detenute esclusivamente e personalmente, saranno condivise con la piattaforma. Nessuno purtroppo garantisce che la piattaforma da un giorno all'altro non chiuda e non fugga con i nostri fondi all'interno. Per questo motivo è sempre consigliato immagazzinare il saldo, post conversione, su portafogli *hardware*. L'analisi in questione è stata fatta considerando un eventuale mala fede delle piattaforme che, ad onor del vero, non otterrebbero nessun guadagno con un'azione simile. Da considerare è anche l'eventualità di attacchi *hacker*. Episodi simili, purtroppo, sono già avvenuti in passato, come la piattaforma *Mt.Gox fi* che nel 2014 scomparve nel nulla e che attualmente ha posto il saldo rimanente in fase di liquidazione. In quell'anno la piattaforma gestiva circa il 70% delle transazioni *Bitcoin*, in totale 850mila btc sono andati persi. Sono stati nel tempo ritrovati in totale "solamente" 200 mila btc. Sembra che le cause siano riconducibili a furti perpetrati nel tempo dall'anno 2011. Di recente anche *Cryptopia, exchange* che deteneva un volume importante di criptovalute, ha subito un attacco, perdendo gran parte dei saldi in *Ethereum* ed i relativi *Token*. Il caso è ancora in via di risoluzione con una prima *tranche* di liquidazioni.

Vantaggi e Svantaggi Bitcoin

Il primo vantaggio implicito è la stessa struttura. La *blockchain* è una tecnologia innovativa che porta con sé una gestione più controllata e minori spese di gestione. Da non sottovalutare anche il concetto di "libertà[61]". La non presenza di un ente centralizzato che gestisce e monitora l'intero *environment,* permette l'abbassamento dei costi sopra citati. L'alta portabilità[61], ossia la facilità e la rapidità di trasferimento anche di grosse somme di denaro, rende la criptovaluta uno strumento con una efficienza molto elevata. Mettendo a confronto gli eventuali costi e la velocità di trasferimento tra un semplice bonifico ed una transazione Bitcoin non ci sono quasi paragoni. Di recente le banche hanno implementato come servizio il cosiddetto "bonifico istantaneo" capace di inviare in pochi minuti il saldo che si vuole "bonificare". Molto spesso, essendo un servizio extra,

[61] <https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin> Ultima consultazione aprile 2020

ha dei limiti e costi di transazione molto elevati. Per poter trasferire anche "solo" €5000 i costi in media oscillano tra i €2,5 e €5. Per contro con Bitcoin potremmo trasferire in pochi minuti milioni di euro o dollari ad un costo inferiore. È disponibile online *whale alert*[62] una piattaforma con varie pagine social, che condivide in tempo reale le più grandi transazioni che vengono effettuate nel mercato cripto. Ne è un esempio un trasferimento in BTC di oltre 700 milioni di dollari con un costo totale di transazione di soli 0,26 centesimi di dollaro. Attenzione, i costi di transazione in questione non sono gli stessi trattati nei paragrafi precedenti, bensì costi di gestione dell'*environment blockchain.* Le commissioni sono teoricamente facoltative e non presenti in alcune *blockchain*, poiché sono un incentivo per i *miner* ad includere la transazione nel blocco. Solitamente dai propri portafogli si ha la possibilità di decidere quante commissioni dedicare alla transazione. Il calcolo[63] viene fatto in base al peso della transazione: X *Satoshi per 1 Byte*. Considerando che una transazione media occupa 224 *byte* pagheremo x *Satoshi* per 224 *Byte*. Satoshi è una grandezza congruente a 0.00000001 *Bitcoin.* Ipotizzando che in questo momento il rapporto migliore tra velocità di trasferimento e risparmio sia di 25 *Satoshi per 1 Byte* pagheremo, per una transazione, circa 5600 *Satoshi* (0.00005600 BTC). La piattaforma *bitcoin fees*[64], che ci consiglia qual è la giusta commissione del momento, può esserci di aiuto ma bisogna fare attenzione. Non tutti i portafogli permettono di gestire le commissioni; in particolare gli exchange impostano commissioni, ulteriori ai loro costi di conversione, nel momento in cui si ritirerò il proprio saldo in criptovaluta. Di solito, non è però permesso dalle piattaforme, l'impostare un costo per byte. Considerando gli svantaggi che la criptovaluta porta con sé, la questione legale rientra sicuramente tra di essi. Essendo uno strumento nuovo e, come già anticipato, con un livello di privacy medio-alto, molto spesso risulta difficile da regolamentare. Molti governi a livello mondiale sono alla ricerca di una soluzione per la convivenza tra moneta tradizionale e digitale. Gli investitori si ritrovano molto spesso a combattere con il fisco proprio perché non si riesce a collegare le cripto a nessun genere di reddito esistente. Rimangono ancora delle forti lacune nella risoluzione del problema, ma c'è chi attualmente considera le monete virtuali come "plusvalenze" o come un eventuali "dividendi". È indubbio che la questione chiavi perdute rimanga un grosso svantaggio. Infatti, come già ampiamente discusso, ipotizzando il caso in cui si dovessero perdere chiavi o i *Seed* dei portafogli, non sarebbe in alcun modo possibile recuperare i risparmi. La volatilità[61] rappresenta un ulteriore svantaggio poichè fin quando assisteremo a dei forti sali scendi, la "fiducia" delle criptovalute non sarà mai elevata, ed un impiego di massa, sarà conseguentemente remoto.

[62] <https://whale-alert.io/> Ultima consultazione aprile 2020
[63] <https://coinlist.me/it/glossario/commissione/> Ultima consultazione aprile 2020
[64] <https://bitcoinfees.earn.com/> Ultima consultazione aprile 2020

Introduzione ad Ethereum e smart contract

La criptovaluta *Ethereum*[65] apre le porte ai successivi argomenti. La sua prima versione venne pubblicata nel luglio 2015 grazie a *Vitalik Buterin* con l'intento di creare una moneta digitale che fosse capace non solo di competere con *Bitcoin*, ma soprattutto di creare un sistema molto più efficiente e performante. Il sistema presenta un grande potenziale: costruire altri asset sulla sua stessa *blockchain*. Avremo quindi a disposizione un *EVM, Ethereum Virtual machine*, da cui è possibile generare uno *smart contract*[66]. Quest'ultimo risulta essere un vero e proprio contratto digitale da compilare tramite codice. I linguaggi attuali più popolari per scrivere uno *smart contract* sono *Solidity e Vyper.* Il primo è una fusione tra i linguaggi *c++, javascript e python* mentre il secondo è interamente basato sul linguaggio *Python.* Dalla creazione di uno *smart contract* è possibile generare un proprio *Token.* Affinché tutto il progetto vada a buon fine sarà necessario possedere un saldo in *Ethereum* ed un indirizzo. Il saldo in particolare è fondamentale poiché per reggere l'intera struttura dello *smart contract* è necessario un fondo capace di gestire il cosiddetto *gas* risultante essere una grandezza per il calcolo dei costi di transazione.

Token

All'interno dell'environment *Ethereum* sono presenti attualmente innumerevoli *token.* Essi possono essere considerati come dei veri e propri "gettoni" digitali che vengono acquistati o distribuiti. I primi *token* sulla piattaforma erano retti da un *ERC20*[67]*:* uno standard di *Ethereum* classificabile come un template di base per la creazione. In fase di progettazione grazie a questo "protocollo" si conoscevano in anticipo gli eventuali comportamenti del *token*. Alcuni *developers Ethereum* sottopongono all'analisi della community gli *Ethereum Improvement proposals*, meglio conosciuti come *EIPs*[67]. Una volta commentati e revisionati, nel caso in cui questi venissero accettati dalla community stessa, si trasformerebbero automaticamente in un *ERC*[67]*, Ethereum Request for Comments.* Quello sopra citato ne è un esempio. Nel tempo sono spuntati alcuni bug sullo standard *ERC20,* in particolare uno riguardante il trasferimento dei *token.* Non utilizzando una giusta funzione si potrebbe vedere sul portafoglio una transazione avvenuta con successo, ma senza però ricevere alcun saldo. Attualmente, si continua ad usare l'*ERC20,* ciononostante, per ovviare ai problemi sollevati in precedenza, sono stati sviluppati due nuovi ERC*:* il 223 ed il 777. Si vorrebbe, con questi due nuovi standard, migliorare la struttura degli smart contract evitando, in caso di un errato invio, di perdere definitivamente *Token,* cosa che in alcuni casi causerebbe anche un'ingente perdita di denaro. Il più aggiornato risulta essere proprio

[65] <https://it.wikipedia.org/wiki/Ethereum> Ultima consultazione aprile 2020
[66] <https://ethereum.org/developers/#getting-started> Ultima consultazione aprile 2020
[67] <https://101blockchains.com/erc20-vs-erc223-vs-erc777/> Ultima consultazione aprile 2020

l'ultimo, il 777[68] che manterrebbe la compatibilità con il primo standard *ERC20,* ma migliorerebbe in modo considerevole *l'environment* degli *smart contract.* Unica pecca: una maggiore efficienza richiederebbe anche dei costi di *gas* più elevati.

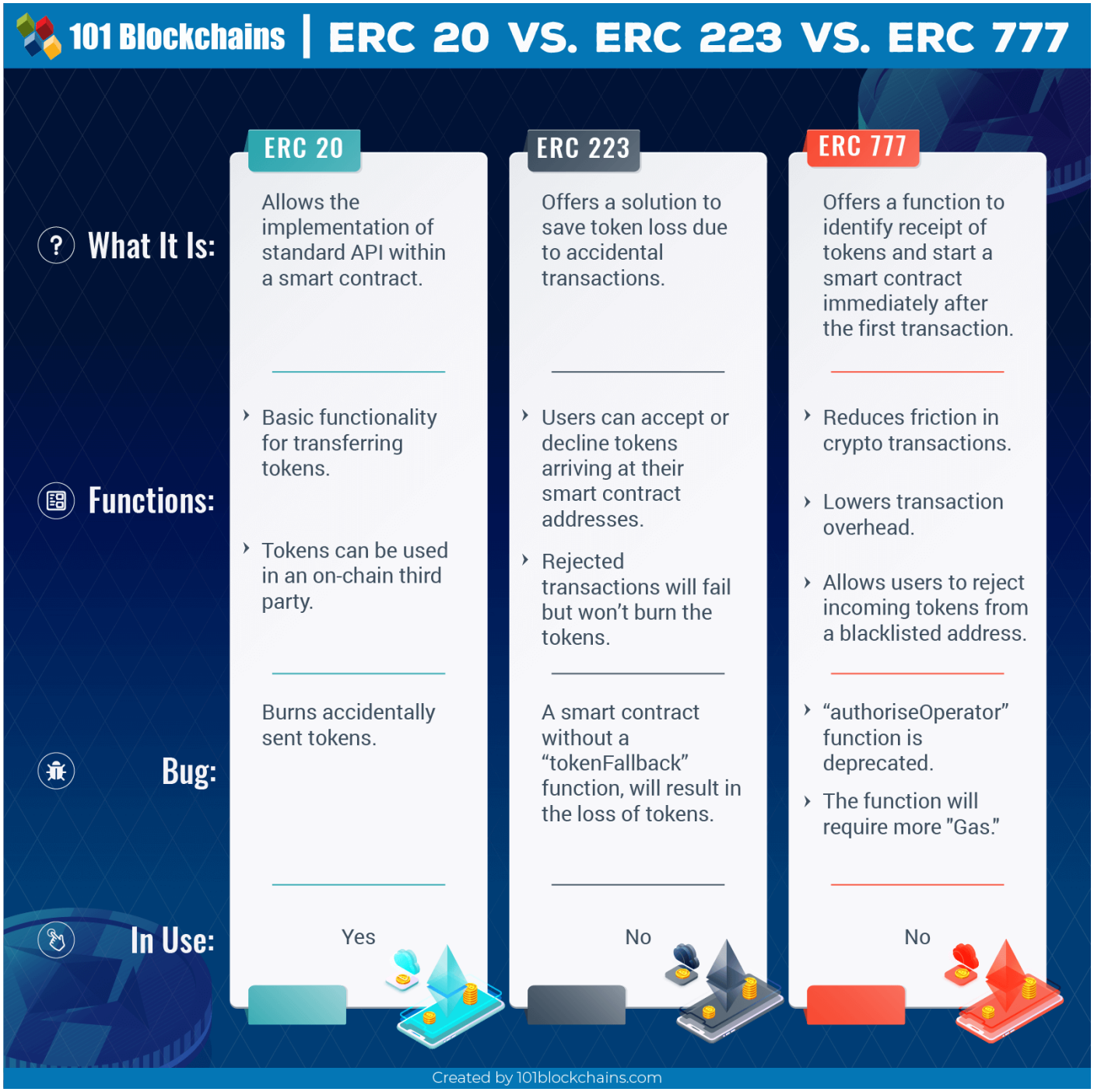

Figura 37 Riepilogo differenze miglioramenti tra i vari ERC. FONTE[67]

[68] <https://cryptonomist.ch/2019/06/12/erc777-vs-erc20-standard/> Ultima consultazione aprile 2020

ICO

Prima di passare alla definizione ed al significato di *ICO, Initial coin offering,* è importante parlare delle *IPO, Initial public offering,* fortemente utilizzate nel mercato tradizionale per finanziare una attività od un progetto. Esse rappresentano letteralmente la prima quotazione di una società nel mercato regolamentato. Molto spesso, intervengono in questa prima fase i cosiddetti *Private angels,* investitori informali che partecipano all'equity aziendale, divenendo soci dell'impresa, e sottoscrivendo gran parte delle prime azioni distribuite. Ci sarà, anche da parte loro, una partecipazione al rischio aziendale. Soggetti simili all'interno del progetto non solo garantiscono una notevole quantità di fondi, ma immettono nel circuito aziendale conoscenze, esperienza e contatti di terze parti. Con le *ICO,* si è voluto emulare un po' il funzionamento delle *IPO,* sfruttando quindi un'offerta iniziale per acquisire liquidità. La differenza essenziale è che da una sottoscrizione di quote azionarie, agli investitori verranno distribuiti Token, derivanti da uno *Smart Contract*. L'anno 2018 è stato il boom delle *ICO,* grazie anche al sempre più sviluppato e forte *Environment* di *Ethereum,* ma all'aumento di popolarità ed interesse, non sono di certo mancati problemi. Molti progetti hanno avuto vita breve, facendo perdere tempo e denaro a molti investitori, tanto che, le *ICO* stesse, sono state successivamente viste, da una gran fetta della community, come frodi vere e proprie. Sostanzialmente con la sostituzione delle quote azionarie con i *Token* sono stati esposti gli investitori ad un rischio maggiore. In molti si sono avvicinati alle *ICO per* motivi speculativi e non perché credessero fermamente in un idea o progetto. La promessa di notevoli guadagni, l'aggiunta di facilità di pubblicizzazione, di acquisto, e di distribuzione dei *Token,* hanno favorito l'avvicinamento anche di piccoli speculatori rendendo sempre più instabile tutto lo scheletro del progetto. Le *ICO,* comunque, non sono tutte uguali e non devono essere considerate a priori ingannevoli. È consigliabile dunque studiare ed informarsi molto bene sul progetto, prima di fare un qualsiasi investimento. Sarebbe opportuno anche, informarsi, come ulteriore analisi, sui possibili grandi investitori o sponsor che partecipano al progetto, avendo cura di fare un controllo dettagliato sulla veridicità dell'accordo in modo bilaterale, quindi controllando non solo la ICO, ma anche la conferma dell'accordo dalla controparte. Facendo alcuni esempi di *ICO* di successo è impossibile non parlare di Eidoo[69]. Il progetto è partito nell' ottobre del 2017 raccogliendo ben 25 milioni di dollari. Inizialmente Eidoo si presentava come un nuovo sistema di portafoglio *Crypto,* con al suo interno una *ICO Engine,* un apparato per aiutare altri progetti a decollare. Un'altra storia di successo è quella di *Zillqa*[69], con un progetto risalente al gennaio 2018 che è riuscito a raccogliere circa 22 milioni di dollari. Alla base vi era l'interesse di risolvere in modo efficiente i problemi di scalabilità su *blockchain*. Da uno studio[70] risalente all'agosto 2019 si è evidenziato come solo il 55% delle top ICO si sia poi trasformato in un vero e proprio successo. Al primo posto *EOS* con ben 4 miliardi di dollari raccolti in un solo anno.

[69] <https://cryptonomist.ch/2018/03/28/sei-ico-di-successo/> Ultima consultazione aprile 2020
[70] <https://eng.ambcrypto.com/45-of-the-icos-met-their-maker-the-rise-and-fall-of-the-ico-era/> Ultima consultazione aprile 2020

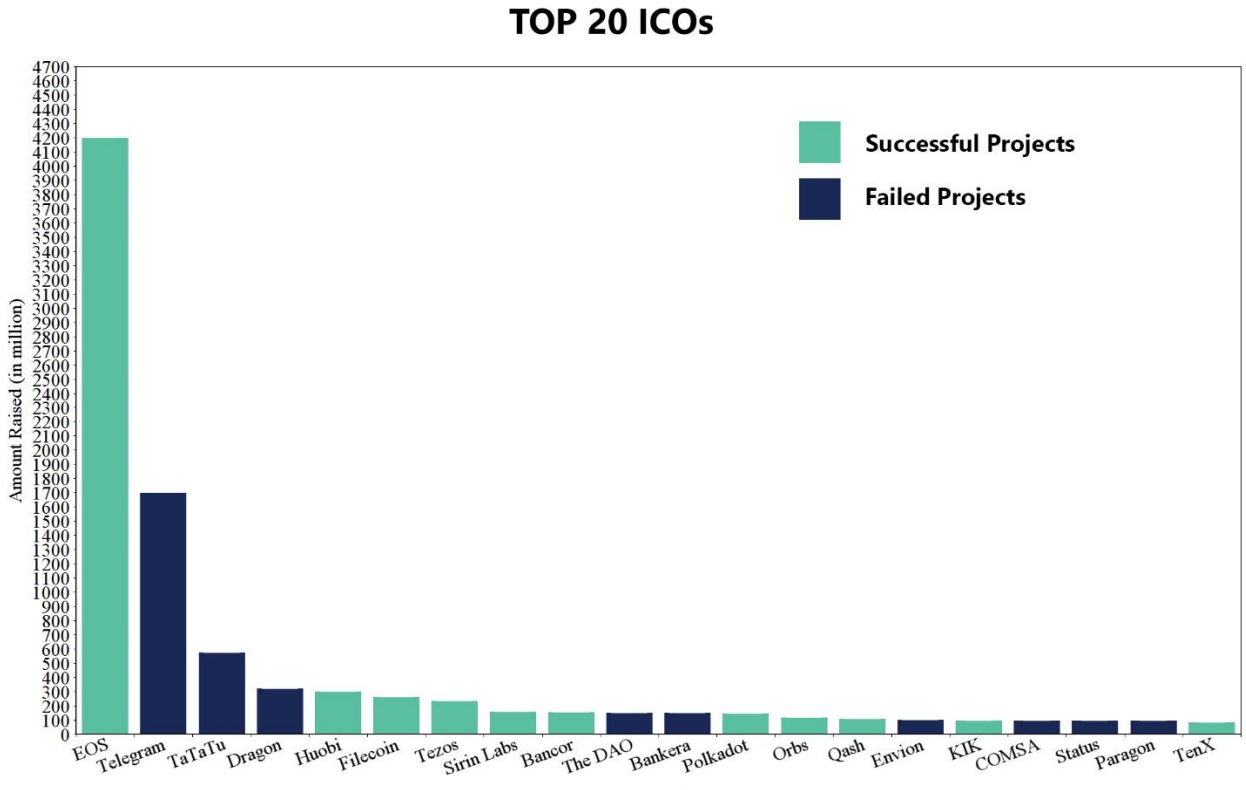

Tabella 5 Rappresentazione grafica tra progetti ICO di successo e non con relativo quantitativo di denaro raccolto dati aggiornati ad agosto 2019. Fonte[70]

Come non parlare anche di quelle *ICO*, che come da grafico, pur avendo raccolto milioni di dollari non sono riuscite per nulla a decollare. È evidente come il progetto più fallimentare di tutti sia stato quello di *Telegram*, da sempre incuriosito ed interessato al mondo cripto tanto da voler creare un proprio *Token.* Dopo una prima ondata di raccolta fondi, Telegram sembrerebbe, come da grafico, esser fallito, ma negli ultimi mesi le notizie fanno pensare ad uno standby e non ad un fallimento, il tutto dovuto a dei conflitti di regolamentazione.

IEO e STO

In aggiunta alle *ICO* sono spuntate *IEO* e *STO*. *IEO* è l'acronimo di *Initial Exchange Offering.* In questo specifico caso i progetti e "le raccolte fondi" vengono direttamente gestiti da delle piattaforme preesistenti: gli *Exchange*. Il concetto di base è lo stesso, cambia il target di potenziali investitori e la solidità del progetto. Dovremo comunque avere un nostro progetto con alla base uno *smart contract.* Differentemente da quello che accade con le ICO, un po' più autonome, invieremo tutte le documentazioni all'*exchange* prescelto per la IEO, che successivamente lo revisionerà, approvandolo nel caso in cui lo ritenga valido. Una volta passata questa fase, il progetto verrà direttamente gestito sulla piattaforma che si occuperà di condividere e consigliare ai

propri clienti la "raccolta fondi". La scelta della IEO porta certamente dei vantaggi[71], sia agli ideatori che agli eventuali investitori. C'è una maggiore sicurezza e affidabilità più o meno garantita dallo stesso *Exchange* di supporto al progetto. Da non sottovalutare anche come eventuali nuovi e piccoli investitori si sentano più tutelati e sicuri nell'impiegare del denaro in progetti gestiti direttamente da una piattaforma in cui sono già registrati. Non mancano però alcuni svantaggi, principalmente per coloro che abbiamo chiamato ideatori. Affidarsi ad una piattaforma significherebbe limitare un po' il proprio target di clientela, poiché con molta probabilità molti non utilizzatori, a meno che non venga fatta una adeguata campagna pubblicitaria, non verranno a conoscenza del progetto, per non parlare dell'eventualità in cui un potenziale investitore non abbia alcuna intenzione di registrarsi su di un nuova piattaforma. Un esempio di *IEO* di successo è *BitTorrent*, *token* che viaggia sulla *blockchain* di *Tron*. Passando alle *STO*[72], acronimo che sta per *Security Token Offering,* la linea di confine con le IPO si fa sempre più sottile. Nel mercato tradizionale le *Securities* sono degli strumenti finanziari che possiedono un particolare valore monetario, ad esempio titoli, azioni ed obbligazioni. Solitamente come nelle IPO questi strumenti vengono gestiti e scambiati "su carta", come per delle sottoscrizioni azionarie. Le STO ne introducono la *tokenizzazzione*. La proprietà del bene verrà confermata tramite una transazione su *blockchain.* Per fare un esempio, una *security token* potrebbe offrire magari il diritto al dividendo o diritto di voto in assemblea. In questo caso dovremmo distaccarci dal pensiero di *Token* come quello delle ICO e considerarlo come una digitalizzazione di uno strumento finanziario. Anche qui i vantaggi non mancano. Basti pensare al notevole snellimento burocratico garantito dalla *blockchain* e dagli *smart contract* ed alla facilità ed alla rapidità di scambio.

Il problema che accomuna un po' queste tre nuove modalità digitali di raccolta fondi è la regolamentazione, ancora oggi un problema molto complesso da risolvere e che fortunatamente da qualche tempo si sta sempre di più tenendo in considerazione.

DeFi

Il mercato delle criptovalute riserva non poche sorprese. Una piacevole novità, nemmeno molto recente, è la *decentralized finance* conosciuta anche come *DeFi*[73]. Già anticipato nel paragrafo sullo storico, all'interno di questo "movimento" sono presenti molte funzioni speculari al mercato tradizionale, come ad esempio la gestione dei prestiti, pagamenti, derivati o investimenti. La cosa che rende tutto estremamente interessante è proprio la *distributed ledger* che vi è alla base. Con il sistema *permissionless* potremmo chiedere un prestito

[71] <https://www.fxempire.it/education/article/cosa-sono-initial-exchange-offering-ieo-in-cosa-differiscono-dalle-ico-152345> Ultima consultazione aprile 2020
[72] <https://blog.yourtarget.ch/cosa-sono-sto-security-token-offering> Ultima consultazione aprile 2020
[73] <https://cryptonomist.ch/2019/09/14/cose-la-defi-decentralised-finance/> Ultima consultazione aprile 2020

senza la presenza di un vero e proprio ente che lo monitori ed eroghi. Per permettere tutto ciò sono nate le *Decentralized Autonomous Organization (DAO),* la più conosciuta ed importante è *Maker DAO*[73]. La gestione dei prestiti avverrà tramite regole matematico-informatiche basandosi su degli *smart contract* presenti su *Ethereum*. Solitamente per poter richiedere un prestito tradizionale si ha bisogno di garanzie, o in alcuni casi di ipotecare un bene per assicurare un rientro alla banca erogatrice in caso di insolvenza. Con la *DeFi* si potrebbe "chiedere un prestito" semplicemente "bloccando" il proprio saldo in criptovaluta. Il saldo che viene bloccato per ricevere il prestito viene chiamato "collaterale". In proporzione percentuale a questo collaterale si otterrà una liquidità o il così chiamato *borrow power*. Quest'ultimo permetterà di ricevere in prestito un determinato ammontare di criptovaluta che, una volta terminato il prestito, dovrà essere restituito con annessi interessi passivi. Il più interessante ed importante nel circuito *DeFi* è il *multi collateral DAI token*, disponibile sulla piattaforma di *MakerDAO*. Esso è una *Stablecoin*, che permette non solo di avere una eventuale liquidità da utilizzare, ma permette, allo stesso modo, chi sia investita ad un altro tasso di interesse annuale. Ricapitoliamo a questo punto quali siano le fasi[74] per ricevere un prestito tramite la *DeFi:*

- Depositeremo un ammontare di ETH sulla piattaforma *DAO* scelta
- Chiederemo un prestito a seconda della massima proporzione rispetto al collaterale (Gli ETH precedentemente depositati);
- Verrà erogato il prestito sotto forma della valuta selezionata, ad esempio il DAI;
- Decorrono gli interessi passivi;
- Restituiremo i *DAI* + gli interessi passivi maturati alla data prestabilita.

Elementi fondamentali della *DeFi* sono gli *oracoli*[75], unico strumento capace di connettere i dati *On-Chain* con i dati relativi all'*environment* esterno. Solitamente gli oracoli sono composti da due parti: una *software* ed una *hardware*. La prima si occupa di acquisire i dati del mondo digitale esterno alla *blockchain* e un esempio possono essere i prezzi degli *stock market*. Mentre la seconda si occupa di connettersi ed informare gli *smart contract* di cosa accade all'esterno. Sono importanti perché si occupano della scelta del "prezzo di riferimento"; un eventuale prezzo che determina se una posizione diventa liquidabile. Ricordiamo sempre che noi abbiamo bloccato un "collaterale" e che questo solitamente corrisponde con certezza al 125%-150% del valore effettivo del prestito. Quindi facendo un calcolo ed ipotizzando che 1 ETH valga €100, se si dovessero bloccare 10 ETH avremmo la possibilità di ricevere un prestito con liquidità €750 (in caso di un tasso di collateralizzazione del 125%). L'oracolo interviene sul prezzo in base all'andamento dei mercati. Nel momento in cui il collaterale assume un valore inferiore alla liquidità offerta + eventuali interessi passivi, il prestito viene automaticamente chiuso.

[74] <https://medium.com/@deepitag/defi-il-mondo-nuovo-della-finanza-b2fa945b3a86> Ultima consultazione aprile 2020

[75] <https://defipulse.com/blog/what-is-an-oracle-how-smart-contracts-see-the-world/> Ultima consultazione aprile 2020

Compound[74] e *MakerDAO*[74] gestiscono gran parte dei fondi destinati alla *DeFi*. Sarà possibile al loro interno chiedere in prestito, prestare, comprare e vendere le valute più utilizzate nella *DeFi*. *Compound* ha, al suo interno, tutti gli strumenti necessari, mentre *Maker* ha la sua sub-piattaforma *Oasis*. Come vedremo successivamente anche per i DEX, per poter operare in tali piattaforme, basterà collegarsi direttamente con i propri portafogli. Le procedure di utilizzo sono simili a quelle già anticipate nei paragrafi precedenti. L'ultimo, ma non per importanza, è *Eidoo*[76]. Tra questi è il più completo. Presenta una multipiattaforma tra *Defi exchange*, *hybrid exchange* e portafoglio. Sarà quindi possibile gestire tutto in una sola applicazione, includendo anche alcune ICO e IEO. Sarà possibile analizzare direttamente sul web le piattaforme con più capitalizzazione[77].

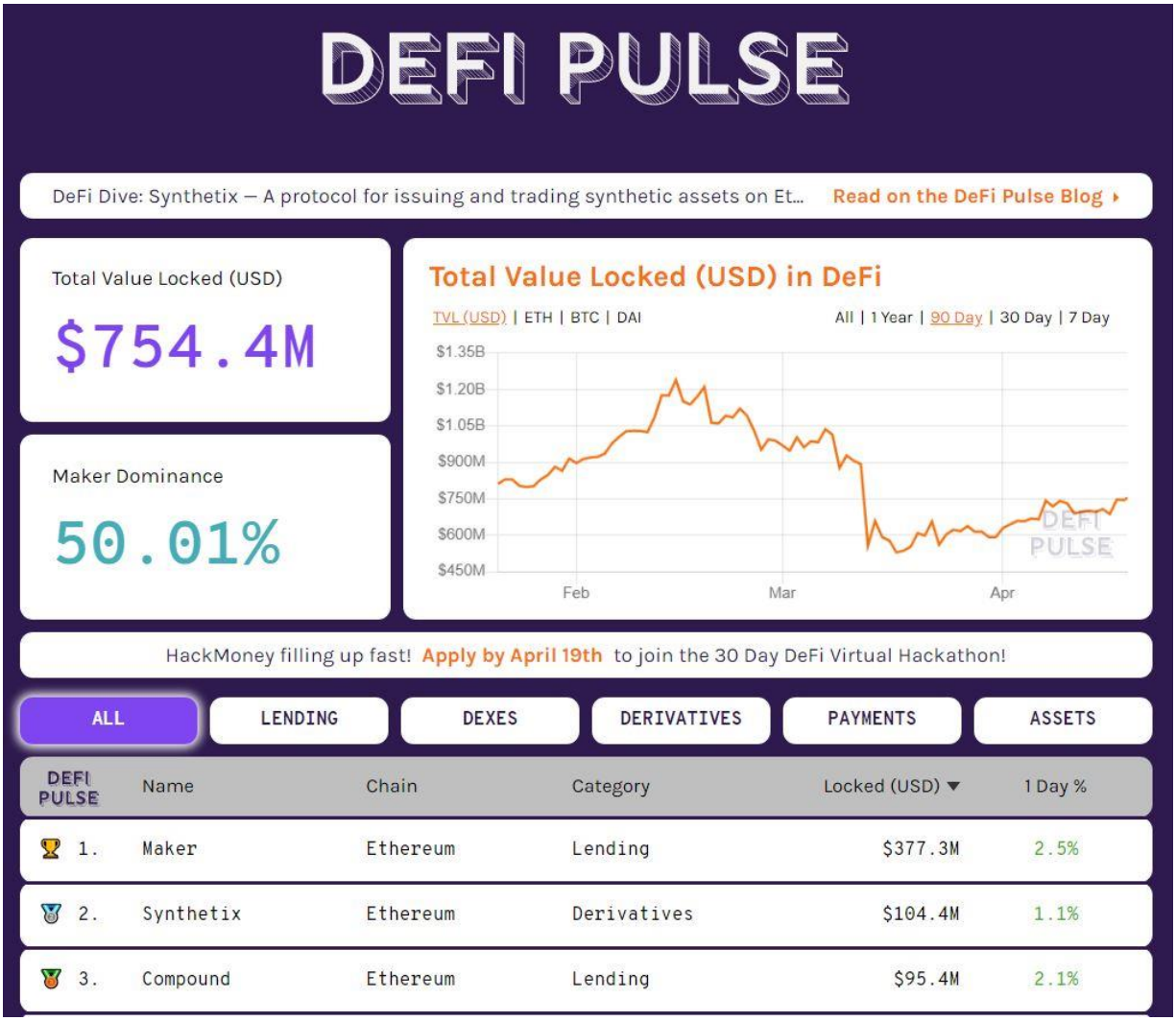

Figura 38 Sito web DEFI PULSE con chart e classifica piattaforme DeFi. Fonte[77]

[76] <https://eidoo.io/> Ultima consultazione aprile 2020
[77] <https://defipulse.com/> Ultima consultazione aprile 2020

Una caratteristica peculiare della *DeFi* è proprio la presenza di *exchange* decentralizzati[78][79]. Differentemente dai precedentemente citati nell'elaborato, sfruttano la decentralizzazione della *blockchain* per operare. Non si avrà più la necessità di pagare costi alti di transazione all'*exchange* o dover necessariamente caricare i propri saldi in criptovaluta su altri portafogli; il che, risulta essere un enorme vantaggio, ed anche una sicurezza in più, poiché tutti gli utenti avranno personalmente in custodia le loro *private key*. Sappiamo bene che lasciare per troppo tempo un saldo su di un exchange classico non è mai consigliabile, con i *DEX*, *decentralized exchange*, questo problema non sussiste, poiché all'interno di queste piattaforme, saranno protagonisti direttamente i nostri portafogli. Non avremo necessità di iscriverci e procedere con il protocollo del *KYC*, ma basterà collegare il proprio portafoglio tra quelli suggeriti dalla piattaforma, Come in foto[80]:

Figura 39 Dashboard dydx. Fonte[80]

I *DEX* risultano essere di fondamentale importanza poiché tramite essi è possibile convertire i principali *Token* di scambio della *DeFi*, come DAI, USDC, WBTC con *Ethereum*, ed è inoltre possibile al loro interno operare con il *margin trading*[81]. Su questi *exchange* si potrà farsi "prestare" dei fondi per investire su di una determinata coppia di valuta. Nel caso si volesse investire $20.000 in criptovaluta, ma sul proprio conto si avessero a disposizione solo $1000, ci si farebbe prestare dei fondi, utilizzando un *leverage* x20. Attenzione bisogna sempre ricordare che il saldo investito che è stato prestato, avrà un eventuale tasso di interesse passivo annuale da pagare, ma si tratterà di somme estremamente basse, considerando che saranno calcolate solo per

[78] <https://cryptonomist.ch/Defi/decentralized-exchange/> Ultima consultazione aprile 2020
[79] <https://defihub.it/exchange-dex-e-la-defi/> Ultima consultazione aprile 2020
[80] <https://trade.dydx.exchange/> Ultima consultazione aprile 2020
[81] <https://defipulse.com/blog/top-3-most-popular-cryptocurrency-margin-trading-platforms-in-defi/> Ultima consultazione aprile 2020

il periodo in cui una posizione è aperta. Quindi se il tasso di interesse per il prestito fosse del 10% annuo, ma avessimo tenuto la posizione aperta per soli 10 giorni, dovremmo pagare il tasso rapportato al numero dei giorni e rapportato al volume prestato in quell'intervallo di tempo. Le posizioni possibili da aprire saranno *Long* o *Short.* Per la prima si "scommetterà" su di un rialzo del prezzo di cambio della coppia scelta, per la seconda su di un ribasso del prezzo. Ipotizziamo di aprire una posizione *Long* con *leverage x10* ed investimento di $1000, su di un eventuale rialzo del prezzo della coppia *ETH-DAI* che in questo momento si trova a $100. Nel caso in cui il prezzo salisse noi otterremmo 10 volte il guadagno rispetto ad un *leverage x1*. Se la coppia passasse da $100 a $110 chiuderemmo la nostra posizione *Long* guadagnando $1000. Questo perché si è immessa una liquidità iniziale di $1000 con una leva 20x. Sarà possibile calcolare un eventuale guadagno con la seguente formula:

$$\frac{Liquidità \times Leverage}{Prezzo\ di\ apertura} \times |Differenza\ tra\ prezzo\ di\ chiusura\ prezzo\ di\ apertura|$$

Sostituendo i dati otterremo:

$$\frac{1000 \times 10}{100} \times |110 - 100| = \$1000$$

Ovviamente verrà fuori un risultato lordo senza considerare i tassi del prestito sopra citati. Il *margin trading* va sfruttato utilizzando sempre le dovute precauzioni, evitando soprattutto di utilizzare grossi *leverage*. Esso rappresenta una pericolosa arma a doppio taglio che potrebbe causare anche una grossa perdita di denaro se l'andamento prendesse direzione opposta a quella "aperta". Negli exchange decentralizzati viene subito fissato il prezzo di liquidazione, prezzo al quale verrà chiusa istantaneamente la posizione e restituito il prestito dovuto rispetto al *leverage.* Le piattaforme più conosciute sono *dydx,* visibile anche nell'immagine, *Fulcrum*[82] e *DDEX*[83]. Con l'avvicinarsi di sempre più utenti alla *DeFi,* non solo nasceranno sempre più piattaforme *DEX,* ma l'intero ecosistema ne andrà a beneficiare, con eventuali miglioramenti.

Stablecoin

Sono considerate *Stablecoin* tutte quelle monete, principalmente *Token,* nate per tenere al minimo la loro volatilità, correlandosi ad un elemento del mercato tradizionale. *Tether,* conosciuta come *USDT,* è una *Stablecoin* legata al prezzo del dollaro statunitense. Nel caso in cui si volesse andare a convertire $100, si riceverebbero quindi 100 *Token USDT.* Nei momenti in cui il mercato delle criptovalute è poco volatile il valore di *Tether* non oscilla, tenendosi stabile a 1 dollaro. Essendo di base un *Token,* in caso di forti

[82] <https://fulcrum.trade/#/> Ultima consultazione aprile 2020
[83] <https://ddex.net/> Ultima consultazione aprile 2020

oscillazioni, il suo prezzo potrebbe leggermente salire o diminuire, sempre rispetto al valore di un dollaro, ma, rispetto alle criptovalute standard, in modo poco significativo. Parliamo di variazioni di prezzo a partire dalla seconda o terza cifra decimale. Nella sua storia il più basso rapporto con il dollaro è stato registrato a $0,91[84] mentre il più alto a $1,21[84]. Queste due registrazioni sono avvenute entrambe nell'anno 2017 in un periodo in cui, con molta probabilità, la fiducia per le *Stablecoin* era ancora ad un livello molto basso. *Tether* è stata protagonista anche di forti accuse, secondo cui le riserve monetarie della prima *governance* non erano abbastanza cospicue per effettuare la conversione in dollari di tutti i *Token* circolanti. Da qualche tempo non si sente più discutere di questa presunta accusa, come se fosse stato trovato un accordo o fosse stato risolto il tutto in modo silente. Non sono mancate le rivali, basti pensare a *USDC, BUSD, Paxos standard,* e *DAI* con l'ultima che si è guadagnata una grande fetta di mercato della *DeFi.* Le *Stablecoin,* finora citate, sono tutte correlate al dollaro statunitense, ma sul mercato ne sono presenti anche altre, come *Pax Gold,* correlate ad altri *stock*. Quest'ultimo *Token* è direttamente connesso con il prezzo dell'oro. La stessa *Paxos*[85]*,* che gestisce la moneta, conserverà per ogni *Pax gold*[86] acquistato, un'oncia fisica d'oro, corrispondente allo stesso valore della *Stablecoin*. *Tether,* di recente, sembra interessata a percorrere la stessa strada, dando origine a *Tether Gold,* prendendo la palla al balzo è facendo leva sulla buona reputazione della materia prima. Non mancheranno in futuro valute rapportate alle altre valute *FIAT* come l'euro o la valuta cinese, sull'impiego delle quali, vari governi si stanno già portando avanti. Come probabilmente già inteso, essendo presente alla base di questi sistemi uno *smart contract,* si avrebbe anche un ente di controllo e di distribuzione dei *Token,* rendendo un po' vano il concetto di decentralizzazione. Anche per *Libra*, *Stablecoin* fortemente voluta da *Mark Zuckerberg* per fornire pagamenti immediati sulle sue piattaforme, ci sono stati problemi, in quanto avrebbe permesso il controllo di numerose somme di denaro da parte dello stesso *CEO*. Bisognerà tener d'occhio le *Stablecoin,* se ne vedranno sempre più sul mercato e rischieranno di divenire anche uno strumento fondamentale e necessario per garantire un *environment* generale delle cripto facilmente raggiungibile ed utilizzabile.

Tron

Tron (TRX) è una *altcoin* di nuova fattura, inizialmente conosciuto come *tronix,* criptovaluta quasi sconosciuta alla community mondiale, che ha assunto, nelle prime battute, un valore intorno ai $0,002. Solo verso la fine dell'anno 2017 le cose sono cambiate[87], anche grazie ad un notevole rialzo del prezzo che successivamente ha toccato i $0,08. Dietro l'intero progetto vi è *Justin Sun*. Non molto conosciuto ai più, ma basterebbe leggere due righe della sua biografia[88] per capire che non è di certo uno qualunque. Al di là dei suoi attuali incarichi di spicco, alle età di 26 anni, è stato scelto da *Jack Ma*, fondatore di *Alibaba*, per studiare alla *Hupan*

[84] <https://coinmarketcap.com/it/currencies/tether/> Ultima consultazione aprile 2020
[85] <https://www.paxos.com/pax/> Ultima Consultazione aprile 2020
[86] <https://www.paxos.com/paxgold/> Ultima consultazione aprile 2020
[87] <https://www.criptovalute24.com/tron/#Tron_%5BTRX%5D_storia> Ultima consultazione aprile 2020
[88] <https://en.wikipedia.org/wiki/Justin_Sun> Ultima consultazione aprile 2020

University; Justin è stato l'unico millennial tra i primi laureati nell'università di Jack Ma stesso. Probabilmente *Jack* aveva già visto in lui qualcosa di unico. L'idea iniziale[89] era quella di creare una piattaforma digitale decentralizzata, tutta dedicata all'intrattenimento. Con il passare degli anni la mission di base ha visto un espansione tale che ad oggi l'obiettivo sarebbe quello di decentralizzare l'intero mondo di internet, introducendo alla base il concetto dello s*haring economy*. Le fondamenta di *Tron* sono state copiate dai codici di *Ethereum* a cui gli sviluppatori hanno aggiunto nuove e differenti funzionalità. Potremmo addirittura classificare *Tron* ed il suo *environment* come un concorrente di *Ethereum*, grazie sicuramente alle sue particolari caratteristiche. Una prima differenza tra le due risiede proprio nel meccanismo di consenso. Sappiamo bene come *Ethereum*, attualmente, stia cercando di implementare il POS. *Tron* è andato oltre, utilizzando il così chiamato *Delegated proof of stake (DPOS)*[90]. All'interno di questo sistema ci saranno niente meno che 27 *super representatives (SRs)* che produrranno blocchi per il network.

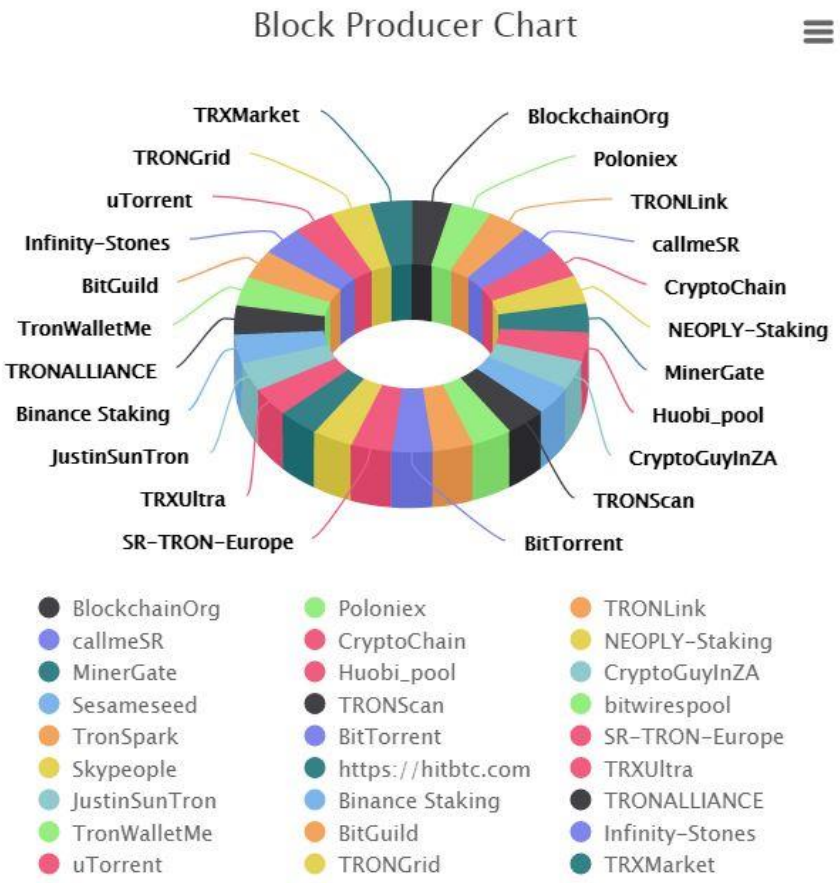

Figure 40 Elenco Dei 27 super representatives. Fonte[91]

I detentori di TRX potranno "freezare" il loro saldo e dare un certo numero di voti ad uno dei 27 SR in modo proporzionale alla quantità di saldo bloccato. Successivamente si riceveranno in modo periodico, ogni due settimane o ogni mese, un certo quantitativo di TRX o *Token* registrati sulla catena. Rispetto ad un protocollo

[89] <https://coinlist.me/it/altcoins/tron/> Ultima consultazione aprile 2020
[90] <https://tron.network/static/doc/white_paper_v_2_0.pdf> Ultima consultazione aprile 2020
[91] <https://tronscan.org/#/blockchain/stats/pieChart> Ultima consultazione aprile 2020

standard *POS* c'è l'aggiunta degli SR che, detto in maniera impropria, fungono da distributori di TRX, ovviamente in proporzione alle quantità di voto offerte. La scelta è libera e personale ed è possibile distribuire i voti anche a differenti SR. Per quanto riguarda invece la struttura della *Blockchain* e dei blocchi, questi ultimi vengono generati ogni 3 secondi ed ogni blocco assegna 32 TRX ai *super representatives*. I nodi nel network di Tron sono classificabili in 3 differenti tipi:

- *Witness Node*: nodi configurati da ogni SR ed i principali responsabili della produzione dei blocchi e della creazione e richiesta di votazione, ritenuti per tanto i più importanti;
- *Full Node*: nodi molto simili agli omonimi della *blockchain* di *Bitcoin* in quanto trasmettono blocchi e transazioni.
- *Solidity Node*: nodi che sincronizzano i blocchi dagli altri nodi.

Una caratteristica molto interessante dell'intera catena è la capacità di gestire fino a 2000 transazioni al secondo rispetto alle 3 al secondo di *Bitcoin* o alle 15 al secondo di *Ethereum*. Anche TRX come ETH ospita al suo interno la possibilità di distribuire *Token*. Avremo quindi anche qui una *virtual machine:* la *tron virtual machine (TVM).* Ogni *Token* avrà alla sua base uno *smart contract*. In sostituzione degli ERC sulla catena di Tron sono presenti i *TRC-10 e TRC-20*. Per gli sviluppatori le differenze essenziali sono le seguenti. I *Token TRC-10* sono accessibili sia tramite *API* sia tramite *smart contracts*, mentre i *TRC-20* che permettono di customizzare l'interfaccia, sono esclusivamente accessibili tramite *smart contract*. A livello di costi le commissioni per le transazioni saranno minori sui Token TRC-10 di circa mille volte rispetto ai 20, ma sono da aggiungere altri costi come la gestione della larghezza di banda per trasferimenti e depositi API. Direttamente dal *whitepaper*[90] è possibile analizzare in dettagli tutte le caratteristiche peculiari dell'intero progetto, avendo anche la possibilità di comprendere meglio il funzionamento di tutti gli elementi che compongo la *Blockchain* di *Tron*. Per fare un rapido esempio di *smart contract* di un *Token TRC-20* ecco un estratto[90] dell'interfaccia:

```
contract TRC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint
balance);
    function allowance(address tokenOwner, address spender) public constant
returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool
success);
    function transferFrom(address from, address to, uint tokens) public
returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint
tokens);
}
```

Figure 41 Esempio di stringhe di codice di smart contract su TRX. Fonte[90]

Tron è in continua evoluzione ed ha tutte le carte in regola per dare filo da torcere a *blockchain* con una struttura simile a quella di *Ethereum* o a quella di *EOS*.

Libra

Brevemente citata nel paragrafo delle *stablecoin*, Libra necessita sicuramente di una spiegazione più approfondita. Nel mese di aprile 2020 è stato aggiornato il *White paper*[92] da cui è possibile trarre tutte le informazioni necessarie alla sua comprensione. Il suo ultimo aggiornamento potrebbe rivoluzionare il mondo cripto, in particolare il gruppo delle *stablecoin.* Il progetto inziale voleva sfruttare la tecnologia *blockchain* con l'intento di creare un moneta digitale singola: *Libra coin* (≈LBR). Questo primo approccio ha, come già anticipato, fatto storcere il naso a tutti gli enti di controllo monetario, preoccupati giustamente per una potenziale delocalizzazione di tutte le transazioni. Con una tecnologia simile, in verità, si potrebbero trasferire velocemente tanti soldi da un continente ad un altro, senza un adeguato controllo. *Libra* ha sempre cercato di mitigare questa questione ritenendo la sua *stablecoin* complementare alla moneta fiat e non *competitor*. Sin dall'inizio ha cercato di collaborare e discutere con organizzazioni, regolatori e *policymakers* per risolvere le problematiche chiave e per il perfezionamento del network. Il salto di qualità è stato sicuramente fatto di recente. Il *network* sembrerebbe esser riuscito a trovare una soluzione più o meno valida per far sfruttare in maniera complementare moneta fiat e criptovaluta. Non si tratterà più di un'unica *Multi currency stablecoin*, ma ad essa saranno affiancate più *single currency stablecoin* una per ogni moneta fiat. Avremo ad esempio *LibraUSD, LibraEUR e LibraGBP*. Il piano sarebbe di aumentare il numero di queste ultime nel corso del tempo. La stessa Associazione che c'è dietro Libra si offre di lavorare insieme alle banche centrali ed ai regolatori per rendere disponibile, nel modo più rapido possibile, la *stablecoin* relativa ad una particolare fiat, sul loro network. Un altro importante step in avanti è quello della gestione delle riserve e della protezione. Libra è nell'attesa di sviluppi di banche centrali digitali, *Central bank digital currencies (CBDCs),* facilmente integrabili con il *network*, per la necessità di gestione delle riserve associate, eliminando rischi di credito e di custodia. La *multi currency* (≈LBR) sarà completamente sostenuta dalle riserve degli asset di ogni *single currency (*≈USD, ≈EUR, ≈GBP ecc.). Grazie a tutto ciò, gli utilizzatori avranno un alto grado di sicurezza nella possibilità di conversione dei loro *Libra coins* in valuta locale. Un grandissimo potenziale riguardo la gestione del rischio, è la volontà di garantire la riserva direttamente con: liquidità, equivalenti o *securities* governative di breve periodo, per un totale uguale, o quasi, al valore facciale totale di ogni Libra Coin in circolazione (rapporto 1 a 1). È stato evidenziato come le riserve fino ad un max dell'80% corrisponderanno a *securities* ed il restante 20% in liquidità, mantenendo la massima trasparenza al pubblico. Si è molto

[92] <https://libra.org/en-US/white-paper/> Ultima consultazione aprile 2020

concentrati nella giusta gestione delle conformità e nella prevenzione delle attività illecite. E' stata quindi definita, in uno schema, la lista dei partecipanti e delle attività di pagamento nel *network Libra*:

- La Associazione ed i suoi sussidiari
- Membri dell'associazione
- Distributori designati
- Virtual asset service provider (*VASPs*)
- Wallet user non gestiti.

Oltre all'Associazione, un ruolo fondamentale verrà assunto dai *VASPs.* Si occuperanno di fare da custodia, *exchange*, o similari servizi finanziari. In aggiunta essi vengono distinti in *regulated o certified.* Rientrano nei primi, i VASPs registrati o che hanno la licenza come membri o entità facenti parte del Gruppo di Azione Finanziaria Internazionale (*Financial Action Task Force, FATF*). Dovranno quindi inviare la richiesta di approvazione all'Associazione con allegati:

- L'attestato di licenza o registrazione al FATF
- La dimostrazione di un programma di conformità e controllo di gestione del rischio ragionevole

I *certified VASPs* sono certificati limitatamente a degli standard dell'Associazione. Con questa certificazione viene permesso ai non membri del FATF di operare e offrire comunque servizi del *Libra Network.* Per quanto riguarda la *Blockchain* l'Associazione ha impostato dei requisiti minimi: una facile scalabilità, capacità di gestire miliardi di account e transazioni con una bassa latenza ed un ottima capacità di *storage*, il mantenere una sicurezza elevata sui fondi ed il mantenere la catena flessibile, permettendo aggiornamenti più rapidi. Per fare ciò è stato impostato un linguaggio di programmazione nuovo, denominato *Move.* Affiancato a questo linguaggio il sistema di consenso sarà il *Libra Byzantine Fault Tolerance (LibraBFT).* Questo protocollo nasce dal problema dei Generali Bizantini[93]; dilemma logico, secondo cui un gruppo di generali bizantini avrebbe sicuramente avuto problemi di comunicazione per le mosse di guerra da seguire. I generali sono situati in posizioni diverse rispetto all'obiettivo e dovranno raggiungere tutti insieme una mossa comune per la buona riuscita dell'azione. Le opzioni sono attaccare o ripiegare, ed una volta presa una decisione, non può essere in alcuno modo convertita. Potendo comunicare esclusivamente tramite messaggio, non sono esclusi dei ritardi, degli smarrimenti o addirittura che il messaggio venga distrutto. Da non escludere vi anche la possibilità per alcuni generali di inviare un messaggio falso. Tutto ciò in una *blockchain*, considerando i generali come dei nodi, con molta probabilità porterebbe ad un fallimento, poiché non si raggiungerebbe un adeguato consenso. Per poter evitare ciò, è necessario che almeno i 2/3 dei nodi o più, siano onesti ed affidabili. Il *LibraBFT* permette di resistere al fallimento o alla frode di un nodo senza che esso destabilizzi l'intero *environment.* Per poter immagazzinare in modo sicuro le transazioni nella *blockchain* di *Libra* essa sarà protetta dai *Merkle trees*, permettenti il monitoraggio di tutte le modifiche sui dati esistenti. Tutti pensavano Libra come un

[93] <https://www.binance.vision/it/blockchain/byzantine-fault-tolerance-explained> Ultima consultazione aprile 2020

qualcosa di fallimentare, non se ne parlava da molti mesi, ma sembrerebbe aver lavorato sodo in questo periodo, in modo silenzioso, trovando delle ottime soluzioni che strizzano l'occhio anche agli enti governativi.

Staking vs lending

La differenza è molto sottile. Da una parte con lo *staking* si può guadagnare semplicemente detenendo nel proprio portafoglio un numero minimo di criptovalute, mentre con il *lending* è possibile guadagnare prestando la propria moneta virtuale in cambio di un tasso di interesse annuale. Per poter effettuare la comparazione dobbiamo considerare non solo il possibile guadagno, ma anche la sicurezza e l'eventuale sviluppo di entrambe. Con lo *staking,* essendo un protocollo di consenso, andremo non solo a guadagnare ma anche ad aiutare la *blockchain* al suo sostentamento. La sicurezza del sistema è elevata, poichè non dovremo fare altro che detenere un fondo nel portafoglio. Il guadagno annuale, invece, è rapportato ad un tasso che varia durante il periodo di detenzione del saldo attivo sullo *staking*. Il *Lending,* agli inizi supportato da alcune piattaforme *exchange* in cui era possibile prestare un saldo in criptovaluta per poi ricevere a fine prestito il totale prestato più un interesse attivo, presenta una sicurezza minore rispetto ad allo *staking*, anche considerando le precedenti informazioni sulle piattaforme. Con la DeFi, sono stati più o meno risolti i problemi di affidabilità, poiché come già visto con i *DEX* e con le varie piattaforme come *Compound*[94] *o Maker DAO*[95], per fare del *lending* basterà connettere direttamente i propri portafogli. Anche in questo caso i guadagni saranno rapportati in base al volume di fondi "investiti" ed in base ad un tasso di interesse annuale variabile. A conti fatti non vi è una soluzione migliore o peggiore, o considerare se convenga o meno operare con lo *staking* o con il *lending*, molto dipenderà dalla gestione del proprio portafoglio, tenendo presente che le criptovalute, con un protocollo di consenso proof of stake, attualmente risultano non ben capitalizzate. Al fine di una più oculata comparazione che prenda in esame tutte le criptovalute che offrono uno *staking* è stata ideata la seguente piattaforma di nome *Staking rewards*[96].

[94] <https://compound.finance/> Ultima consultazione aprile 2020
[95] <https://makerdao.com/> Ultima consultazione aprile 2020
[96] <https://www.stakingrewards.com/ Ultima consultazione aprile 2020

Asset	Price	Reward	Adj. Reward	Market Cap	24h Volume	Total Staked	7d Price Change	Score
Tezos XTZ	$ 2.25 (-2.17%)	5.72%	0.72%	$1,593,792,595	$226,798,962	78.70%		★★★★☆
Cosmos ATOM	$ 2.36 (-5.22%)	8.20%	1.80%	$439,430,497	$112,750,149	72.11%		★★★★☆
Synthetix Netw SNX	$ 0.7248 (-6.78%)	55.39%	0.56%	$67,903,287	$1,939,413	81.52%		★★★★☆
Decred DCR	$ 12.38 (-1.28%)	7.95%	3.73%	$141,179,294	$100,660,537	49.60%		★★★★☆
Livepeer LPT	$ 0.5234 (2.11%)	41.93%	10.68%	$3,363,458	$10,256	67.08%		★★★★☆
Algorand ALGO	$ 0.1873 (-3.84%)	5.45%	0.24%	$137,442,080	$79,337,581	64.37%		★★★★☆
Waves WAVES	$ 1.01 (-1.94%)	5.61%	2.50%	$101,092,098	$49,168,964	56.57%		★★★★☆
ICON ICX	$ 0.2359 (-1.98%)	15.71%	9.71%	$126,702,519	$23,039,344	30.19%		★★★★☆

Figura 42 Elenco riepilogativo presente su staking rewards. Fonte[96]

Conclusioni

Con questo elaborato ho voluto condividere informazioni, conoscenze e passione per un mondo magnifico che accompagna la mia voglia di esplorazione di novità virtuali, dall'età di 14 anni e che spero possa, perché no, trasformarsi in una chance per un progetto di lavoro futuro. Spero, inoltre, di aver quanto meno informato ed incuriosito il lettore sull'enorme potenzialità rappresentata dalla blockchain in quanto mezzo per l'utilizzo di numerose ulteriori vantaggiose applicazioni; senza aver dimenticato le criptovalute che repentinamente, insieme alla *DeFi* e alle *Stablecoin*, saranno sempre più protagoniste nella nostra vita quotidiana. A conclusione dell'elaborato ringrazio il lettore, sperando di aver fatto cosa gradita.

Sitografia e Bibliografia

1. <https://it.wikipedia.org/wiki/Bitcoin> Definizione di Bitcoin, ultima consultazione aprile 2020
2. <https://www.reply.com/it/content/ballotchain> Descrizione Ballotchain, ultima consultazione aprile 2020
3. <https://www.mise.gov.it/index.php/it/blockchain/blockchain-per-il-made-in-italy> Blockchain made in Italy, ultima consultazione aprile 2020
4. <https://it.wikipedia.org/wiki/Blockchain> Definizione Blockchain, ultima consultazione aprile 2020
5. <https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante> Caratteristiche Blockchain e fonte tabella 1, ultima consultazione aprile 2020
6. <https://www.cryptopostgazette.com/centralized-vs-decentralized-vs-distributed-network/> Fonte figura 1, ultima consultazione aprile 2020
7. <https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html> Fonte figure 2 e 3 e 23, ultima consultazione aprile 2020
8. <https://www.blockchain.com/btc/block/000000000000000000090ec83aef111e64d18de540effb87c5209160b4ea4501> Fonte figura 4, ultima consultazione aprile 2020
9. <https://www.binance.vision/it/blockchain/what-are-nodes> I tipi di nodi, ultima consultazione aprile 2020
10. <https://it.wikipedia.org/wiki/Proof-of-work> Sistema Proof of Work, ultima consultazione aprile 2020
11. <https://it.wikipedia.org/wiki/Hashcash#Come_funziona> Funzionamento HashCash, ultima consultazione aprile 2020
12. <https://it.wikipedia.org/wiki/Denial_of_service> Definizione “Denial of Service”, ultima consultazione aprile 2020
13. <https://www.blockchain.com/charts/hash-rate> Fonte figura 5, ultima consultazione aprile 2020
14. <https://www.binance.vision/it/halving> Definizione Halving e fonte tabella 2, ultima consultazione aprile 2020
15. <https://www.bitcoinblockhalf.com/> Fonte figura 6, ultima consultazione aprile 2020
16. < https://it.cointelegraph.com/news/diar-bitcoin-mining-hashrate-is-becoming-more-distributed-among-pools> Fonte figura 7, ultima consultazione Aprile 2020
17. <https://medium.com/luxor/mining-pool-payment-methods-pps-vs-pplns-ac699f44149f> Metodi di pagamento PPS e PPLNS, ultima consultazione aprile 2020
18. <https://giochipertutti.org/perdite-della-data-di-rilascio-di-intel-comet-lake-prestazioni-della-cpu-a-10-core-e-prezzo/> Fonte figura 8, ultima consultazione aprile 2020
19. <https://shop.bitmain.com/product/detail?pid=00020200226232356122Y0FHc2rQ0657> Fonte figura 9, ultima consultazione aprile 2020
20. <https://it.wikipedia.org/wiki/Application_specific_integrated_circuit> Definizione ASIC, ultima consultazione aprile 2020
21. < https://www.massmux.com/an-efficient-6-gpu-ethereum-rig/> Fonte figura 10, ultima consultazione aprile 2020
22. <https://it.wikipedia.org/wiki/Field_Programmable_Gate_Array> Definizione FPGA, ultima consultazione aprile 2020
23. < https://cryptomining-blog.com/10766-blackminer-f1-mini-is-an-upcoming-single-chip-fpga-miner/> Fonte figura 11, ultima consultazione aprile 2020
24. <https://claymoredualminer.com/> Software mining Claymore, ultima consultazione aprile 2020
25. < https://support.bitmain.com/hc/en-us/articles/115000211774-Connect-Antminer-S9i-S9-T9-S7-to-Pools-Antpool-BTC-com> Fonte figure 14 e 15, ultima consultazione aprile 2020
26. <https://cryptonomist.ch/2019/09/15/mining-consumo-di-energia/> Fonte sui consumi di energia del mining, ultima consultazione aprile 2020
27. < https://scienews.com/it/bitcoin/3964-nella-regione-di-krasnoyarsk-vogliono-creare-mining-farm-per-3-miliard.html> Fonte figura 16, ultima consultazione Aprile 2020
28. <https://www.ilbitcoin.news/pow-e-pos-cosa-sono-e-quali-sono-le-differenze/> Differenze tra POS e POW, ultima consultazione aprile 2020

29. <https://bitcoin.org/en/glossary/stale-block> Definizione Stale Block e fonte figura 17, ultima consultazione aprile 2020
30. <https://cryptonomist.ch/2020/03/03/bitcoin-altro-stale-block/> Fonte Stale Block su catena blockchain Bitcoin, ultima consultazione aprile 2020
31. <https://bitcoin.org/en/p2p-network-guide#orphan-blocks> Definizione orphan block, ultima consultazione aprile 2020
32. <https://www.cryptohelper.it/glossario/blocchi-orfani-e-blocchi-uncle/> Definizione uncle block, ultima consultazione aprile 2020
33. <https://bitcoin.org/en/blockchain-guide#consensus-rule-changes> Definizione Hardfork e Softfork, ultima Consultazione aprile 2020
34. <https://scenarieconomici.it/cripto-un-riassunto-degli-hard-fork-di-bitcoin-per-capire-cosa-e-successo-e-puo-succedere/> Fonte figura 18, ultima consultazione aprile 2020
35. <https://bitcoin.org/en/blockchain-guide#introduction> Fonte figura 19, ultima Consultazione aprile 2020
36. <http://www.bitcoinita.it/news/oggi-bitcoin-pizza-day/> Bitcoin pizza Day, ultima consultazione aprile 2020
37. <https://coinmarketcap.com/currencies/bitcoin/> Fonte figure 20 e 21, ultima consultazione aprile 2020
38. <https://it.tradingview.com/chart/?symbol=GEMINI%3ABTCUSD> Fonte figura 22, ultima consultazione aprile 2020
39. <https://electrum.org/#download>Wallet Electrum e fonte figura 24, ultima consultazione aprile 2020
40. <https://www.ledger.com/>Hardaware wallet Ledger e fonte figura 25, ultima consultazione aprile 2020
41. <https://www.conio.com/it/> Mobile wallet Conio e fonte figura 27, ultima consultazione aprile 2020
42. <https://valutevirtuali.com/cose-si-usa-un-paper-wallet/> Paper Wallet e fonte figura 28, ultima consultazione aprile 2020
43. <https://www.blockchain.com/> Piattaforma blockhain.com, ultima consultazione aprile 2020
44. <https://electrum.readthedocs.io/en/latest/spv.html> Definizione spv, ultima consultazione aprile 2020
45. <https://electrum.readthedocs.io/en/latest/coldstorage.html> Definizione coldstorage, ultima consultazione aprile 2020
46. <http://www.bitcoinquotidiano.com/mettere-bitcoin-al-sicuro-cold-storage-guida-electrum/> Definizione coldstorage, ultima consultazione aprile 2020
47. <https://cryptonomist.ch/2019/06/01/bip32-bip39-bip44-differenze-seed-wallet/> Definizione seed, ultima consultazione aprile 2020
48. <https://edge.app/blog/why-a-12-word-mnemonic-is-an-insecure-bitcoin-wallet-backup/> Fonte figura 29, ultima consultazione aprile 2020
49. <https://cryptonomist.ch/2019/08/11/monero-xmr-criptovaluta-anonimato/> Caratteristiche Monero, ultima consultazione aprile 2020
50. <https://it.wikipedia.org/wiki/CryptoNote> Definizione protocollo CryptoNote, ultima consultazione aprile 2020
51. Materiale del corso di informatica
52. <https://www.crypto51.app/about.html> Definizione di un attacco al 51% ultima consultazione aprile 2020
53. <https://www.crypto51.app/> Fonte figura 30, ultima consultazione aprile 2020
54. <https://www.coinbase.com/dashboard> Fonte figura 31, ultima consultazione aprile 2020
55. < https://www.coinbase.com/price> Fonte figura 32, ultima consultazione aprile 2020
56. <https://pro.coinbase.com/> Fonte figure 33, 34, 35, 36, ultima consultazione aprile 2020
57. < https://etherevolution.eu/differenza-maker-taker/?cn-reloaded=1> Definizioni di Price maker e taker, ultima consultazione aprile 2020
58. <https://help.coinbase.com/en/pro/trading-and-funding/orders/overview-of-order-types-and-settings-stop-limit-market.html> Definizioni di comando piattaforma Coinbase Pro, ultima consultazione aprile 2020
59. < https://www.kraken.com/it-it/features/fee-schedule> Fonte tabella 4, ultima consultazione aprile 2020
60. < https://help.coinbase.com/en/pro/trading-and-funding/trading-rules-and-fees/fees.html> Fonte tabella 4, ultima consultazione aprile 2020
61. <https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin> Caratteristiche fondamentali di Bitcoin, ultima consultazione aprile 2020
62. <https://whale-alert.io/> Piattaforma Whale Alert, ultima consultazione aprile 2020
63. <https://coinlist.me/it/glossario/commissione/> Calcolo costi di commissione, ultima consultazione aprile 2020

64. <https://bitcoinfees.earn.com/> Piattaforma Bitcoin fees, ultima consultazione aprile 2020
65. <https://it.wikipedia.org/wiki/Ethereum> Definizione di Ethereum, ultima consultazione aprile 2020
66. <https://ethereum.org/developers/#getting-started> Definizione di Smart Contract, ultima consultazione aprile 2020
67. <https://101blockchains.com/erc20-vs-erc223-vs-erc777/> Definizione token ERC20, ERC223 e ERC777 e fonte figura 37, ultima consultazione aprile 2020
68. <https://cryptonomist.ch/2019/06/12/erc777-vs-erc20-standard/> Definizione ERC777, ultima consultazione aprile 2020
69. <https://cryptonomist.ch/2018/03/28/sei-ico-di-successo/>Ico di successo: Zillqa, ultima consultazione aprile 2020
70. <https://eng.ambcrypto.com/45-of-the-icos-met-their-maker-the-rise-and-fall-of-the-ico-era/>Fonte tabella 5, ultima consultazione aprile 2020
71. <https://www.fxempire.it/education/article/cosa-sono-initial-exchange-offering-ieo-in-cosa-differiscono-dalle-ico-152345> Definizione IEO, ultima consultazione aprile 2020
72. <https://blog.yourtarget.ch/cosa-sono-sto-security-token-offering> Definizione STO, ultima consultazione aprile 2020
73. <https://cryptonomist.ch/2019/09/14/cose-la-defi-decentralised-finance/>Definizione DeFi, ultima consultazione aprile 2020
74. <https://medium.com/@deepitag/defi-il-mondo-nuovo-della-finanza-b2fa945b3a86> Liquidità sulla DeFi, ultima consultazione aprile 2020
75. <https://defipulse.com/blog/what-is-an-oracle-how-smart-contracts-see-the-world/> Definizione Oracoli, ultima consultazione aprile 2020
76. <https://eidoo.io/> Piattaforma Eidoo, ultima consultazione aprile 2020
77. <https://defipulse.com/> Piattaforma DeFipulse e fonte figura 38, ultima consultazione aprile 2020
78. <https://cryptonomist.ch/Defi/decentralized-exchange/> Definizione di Exchange decentralizzato, ultima consultazione aprile 2020
79. <https://defihub.it/exchange-dex-e-la-defi/> Definizione di Exchange decentralizzato, ultima consultazione aprile 2020
80. <https://trade.dydx.exchange/> Exchange dydx e fonte figura 39, ultima consultazione aprile 2020
81. <https://defipulse.com/blog/top-3-most-popular-cryptocurrency-margin-trading-platforms-in-defi/> Il Margin trading, ultima consultazione aprile 2020
82. <https://fulcrum.trade/#/> Exchange Fulcrum, ultima consultazione aprile 2020
83. <https://ddex.net/> Exchange ddex, ultima consultazione aprile 2020
84. <https://coinmarketcap.com/it/currencies/tether/> Definizione e storico di Tether, ultima consultazione aprile 2020
85. <https://www.paxos.com/pax/> Definizione di Pax, ultima consultazione aprile 2020
86. <https://www.paxos.com/paxgold/> Definizione di Pax Gold, ultima consultazione aprile 2020
87. <https://www.criptovalute24.com/tron/#Tron_%5BTRX%5D_storia> Storico di Tron, ultima consultazione aprile 2020
88. <https://en.wikipedia.org/wiki/Justin_Sun> Biografia Justin Sun, ultima consultazione aprile 2020
89. <https://coinlist.me/it/altcoins/tron/> Progetto Tron, ultima consultazione aprile 2020
90. <https://tron.network/static/doc/white_paper_v_2_0.pdf> Delegated Proof of Stake e fonte figura 41, ultima consultazione aprile 2020
91. <https://tronscan.org/#/blockchain/stats/pieChart> Fonte figura 40, ultima consultazione aprile 2020
92. <https://libra.org/en-US/white-paper/> White paper Libra, ultima consultazione aprile 2020
93. <https://www.binance.vision/it/blockchain/byzantine-fault-tolerance-explained> Problema dei generali Bizantini, ultima consultazione aprile 2020
94. <https://compound.finance/> Piattaforma Compound, ultima consultazione aprile 2020
95. <https://makerdao.com/> Piattaforma MakerDAO, ultima consultazione aprile 2020
96. <https://www.stakingrewards.com/ Piattaforma Staking Rewards e fonte figura 42, ultima consultazione aprile 2020