POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Matematica

Tesi di Laurea Magistrale

Analisi comparativa delle maggiori criptovalute: Protocolli e Blockchain

Relatori:

Prof. Danilo Bazzanella

Alexandru Stefan Gheban

Candidato:

Laura Barbera

ANNO ACCADEMICO 2019/2020

Indice

Introduzione **1**

1 Bitcoin-mania ฿ **3**

1.1 Nascita e motivazioni storiche 3

1.2 Funzione hash 7

1.2.1 SHA-256 10

1.2.2 RIPEMD-160 13

1.3 Firma digitale 14

1.3.1 ECDSA- Elliptic Curve Digital Signature Algorithm 16

1.4 Transazioni 19

1.5 Proof-of-Work & Mining 22

1.5.1 Difficoltà e target 25

1.6 Blockchain 29

1.7 Incentivi 31

2 Altcoin **35**

2.1 Mercato delle criptovalute 35

2.2 Litecoin 37

2.2.1 Scrypt 38

2.3 Ethereum 41

2.3.1 Transazioni 41

2.3.2 Funzione hash 44

2.3.3 Merkle Patricia Tree 49

2.3.4 Ethash 53

2.4 Ripple 55

2.4.1 XRP Ledger Consensus Protocol 56
2.5 Stellar 59
2.5.1 Stellar Consensus Protocol 60
2.6 Algorand 64
2.6.1 Pure Proof-of-Stake 65
2.6.2 Dettagli tecnici 71
2.6.3 Moneta e Applicazioni 74

3 Analisi comparativa **77**
3.1 Bolle speculative 79
3.2 Analisi comparativa dati storici 83
3.2.1 Ritorno dell'investimento 84
3.2.2 Volatilità 86
3.3 Correlazioni 90
3.4 Valutazione delle criptovalute 99
3.4.1 Price-to-earnings 99
3.4.2 Network-Value-to-Transactions 100
3.4.3 Price-to-Utility 102
3.5 Confronto sicurezza delle criptovalute 106
3.5.1 Sicurezza Proof-of-Work 106
3.5.2 Sicurezza XRP LCP 110
3.6 Privacy 113
3.6.1 Pericoli 114
3.6.2 Possibili soluzioni 116

4 Stablecoin **120**
4.1 USD Coin 122
4.1.1 Centre 123
4.1.2 Volatilità 125
4.2 PAX Gold 126
4.2.1 Volatilità 129
4.3 MakerDAO 130

4.3.1 Partecipanti interni ed esterni 131
4.3.2 Vault 133
4.3.3 Auctions 134
4.4 Decentralized Finance 136
4.4.1 Maker 137
4.4.2 Compound 140

Conclusioni **142**

Appendice **144**

Bibliografia **152**

Introduzione

La prima parola che viene associata alla tematica *criptovalute* è, senza dubbio alcuno, *Bitcoin*. Non stupisce poi se con molta probabilità, il pensiero vada subito dopo a Satoshi Nakamoto, pseudonimo di chi ha diffuso nel mondo molto più che una semplice innovazione. Sono queste le più famose parole e tematiche che hanno dato il kick-off ad un nuovo paradigma.
Ci si può chiedere però quale sia stato il contesto, il terreno che abbia permesso nel tempo la diffusione, evoluzione e la continua attenzione di un pubblico sempre più vasto.
La letteratura sta trattando tali tematiche in maniera crescente negli ultimi anni. Questo impegno sottolinea un interesse non meramente informativo, ma una netta propensione alla formazione di figure professionali competenti in materia e che abbiano la giusta sensibilità sia socio-economica che tecnico-matematica.
L'attualità e dinamicità del mondo delle criptovalute rende Internet la più grande fonte di informazione con nuovi articoli, post *Twitter* dei fondatori, siti web aggiornati continuamente, forum di confronto e divulgazione.

L'evoluzione di Bitcoin è storia.
E' storia presente, studiata, discussa, attaccata, elogiata e riproposta. E' una pagina di storia che si sta scrivendo e che è chiaro segnerà il futuro in maniera non solo imprevedibile ma straordinaria. Il mondo della finanza osserva e si muove per inseguire un cambiamento epocale. In questo contesto così entusiasmate e dinamico si colloca **Young Platform**, un'azienda tutta italiana, giovane e competente che dal 2017 lavora con un'idea chiara in mente: rendere il mondo delle criptovalute semplice ed accessibile per tutti.

Dunque non solo *exchange* delle principali valute *Bitcoin, Ethereum, Ripple, Litecoin*, ma anche una piattaforma dove imparare a conoscere tutti gli elementi utili in maniera chiara, semplice. E ancora altre idee fresche come l'*utility token Young* e *Stepdrop*, che ripaga proporzionalmente ai passi effettuati.
"Non è la specie più forte o la più intelligente a sopravvivere, ma quella che si adatta meglio al cambiamento", afferma nel 1963 Leon C. Megginson, professore universitario e saggista statunitense, riferendosi alle tesi di *Charles Darwin* in *Origin of Species*. Suona così attuale oggi se si pensa che sei giovani ragazzi siano riusciti a raccogliere in crowdfunding oltre 780 000 euro per rendere operativa la loro idea.

Il seguente lavoro di tesi si è svolto in partnership con questa azienda; ciò necessita un caloroso ringraziamento e i più sinceri complimenti con profonda ammirazione.

Lo sviluppo del seguente lavoro di tesi si pone l'obiettivo di indagare da un punto di vista tecnico gli strumenti crittografici che hanno permesso a Bitcoin prima (Capitolo 1) e alle successive valute poi (Capitolo 2), una rapida e sicura ascesa. Senza la loro solidità e maturità storica i protocolli sarebbero stati facilmente attaccati e nessuno si sarebbe sentito sicuro ad affidarvi il proprio investimento.
La seconda parte (Capitolo 3) tratta argomentazioni di tipo statistico/economico cercando di far luce su aspetti interni al mercato delle criptovalute che, ad onor del vero, sono per gran parte oscuri a tutti gli interessati. Se così non fosse e qualcuno nel mondo avesse conoscenza di come si muovono i mercati, avrebbe una ricchezza enorme da dover gestire.
Nell'ultima sezione (Capitolo 4) si trattano le *Stablecoin*, una differente prospettiva per l'utilizzo di cripto-asset come mezzo di pagamento giornaliero fino a giungere alla *DeFi*, la nuova strada per gestire le proprie finanze in maniera indipendente, senza intermediari e con grandi benefici.

Capitolo 1

Bitcoin-mania ₿

1.1 Nascita e motivazioni storiche

Il 31 Ottobre 2008 è una data fondamentale nella storia delle criptovalute: Satoshi Nakamoto scrive [1] il *White Paper* dal titolo **Bitcoin: A Peer-to-Peer Electronic Cash System**.
Il documento è semplice nella sua struttura, una lettura consigliata a chi vuole conoscere il funzionamento di Bitcoin e, ancora di più, a chi aspira a cogliere la forte esigenza sentita dal/dai creatori. Si legge *"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party"*.
E' probabilmente questo il punto saliente e di grande innovazione, ripreso con forza da chiunque difenda e persegua la strada delle criptocurrency.

Nakamoto nel suo paper sottolinea la debolezza di un sistema che, sebbene permetta pagamenti elettronici per il commercio su Internet, sia ancora estremamente legato ad un modello basato sulla fiducia in un'autorità terza che regoli le dispute e sofferente di costi di mediazione. Sono inevitabili, nel sistema di pagamento in vigore, una certa quantità di frodi e, sebbene lo scambio di moneta fisica possa permettere di ridurle, poco si può fare per i pagamenti su Internet.

[1] Il White Paper verrà diffuso da Nakamoto a Novembre dello stesso anno tramite diverse mail list crittografiche.

La sua idea è chiara e coincisa: propone la soluzione al problema con una versione puramente *peer-to-peer* di denaro elettronico che permetta di effettuare pagamenti online senza un'istituzione finanziaria.
Risulta particolarmente evidente l'influenza di Wei Dai, ingegnere informatico che dieci anni prima di Nakamoto aveva ideato *b-money*; Satoshi non ne fa mistero e difatti il primo riferimento bibliografico del White Paper Bitcoin è proprio al Paper di **b-money**, 1998 [5].

Wei Dai: b-money

Il suddetto testo pone le sue basi nel *Crypto Anarchist Manifesto* di **Timothy C. May**, un documento che profetizza gli effetti di quella che viene chiamata "crypto anarchy".
La tecnologia informatica, scrive, è sul punto di proporre soluzioni crittografiche finalizzate alla protezione dell'anonimato negli scambi, comunicazioni e più genericamente alla libertà personale, con garanzia *quasi perfetta* contro qualsiasi manomissione.
Una vera e propria rivoluzione, dice May nel 1988, sia sul piano sociale che economico, basata sui metodi crittografici a chiave pubblica, zero-knowledge proof e protocolli di autenticazione e verifica, ben conosciuti dal punto di vista teorico già da decenni.

L'attenzione di Wei Dai si focalizzò sull'eliminazione permanente di un governo ed in particolare, conscio della necessità delle comunità di cooperare con un mezzo di scambio che renda valida una forma contrattuale fra individui, descrive due protocolli affinché non sia più necessaria la presenza di istituti promossi dal governo per validare gli scambi economici.
L'idea di base di entrambi è quella di dotare ogni partecipante, identificato con uno pseudonimo, di database separati in cui si ha informazione di quanti soldi possiede ogni individuo e che vengano aggiornati da tutti. I cinque passaggi fondamentali sono: creazione e trasferimento di denaro; stipulazione, conclusione, applicazione di contratti. Ritenendo che sia irrealizzabile la partecipazione collettiva globale, il

secondo protocollo si differenzia dal primo solo per il numero di *server* interessati che sarà ridotto; un meccanismo di controllo è la richiesta di una certa quantità di denaro utilizzabile per multare eventuali comportamenti scorretti da parte dei server stessi. Sono questi ultimi a doversi impegnare per la creazione di denaro e controllare che i database pubblicati siano correttamente aggiornati.
Il punto di maggiore difficoltà per *b-money* è sicuramente la *creazione del denaro*. Una prima soluzione proposta è quella di ripagare con unità monetaria in proporzione allo sforzo computazionale compiuto per risolvere un problema di calcolo.
La difficoltà nell'accordarsi sulla complessità di calcolo effettiva e l'avanzo rapido della capacità di calcolo, portarono da subito Dai a non essere convinto che questa potesse essere la giusta strada. Propone un'alternativa in cui i server decidono l'ammontare di b-money da creare in ogni periodo con un costo che viene determinato da un'asta. Si susseguono quattro fasi:

1. Pianificazione della moneta necessaria per il periodo successivo. Ci può essere o meno l'accordo fra i partecipanti;

2. Offerte da chiunque voglia creare b-money specificandone la quantità e il problema irrisolto di costo computazionale pubblicamente concordato;

3. Effettuare i calcoli e trasmettere le soluzioni;

4. Creazione del denaro e aggiornamento dei conti di coloro i quali hanno risolto il problema computazionalmente più costoso.

Wei Dai non è convinto che l'inventore di Bitcoin sia stato influenzato dal suo paper, al contrario sostiene che probabilmente lo abbia letto solo successivamente.
Eppure l'affinità con il modello proposto qualche anno dopo da Satoshi Nakamoto è particolarmente evidente sia nell'obiettivo finale, sia nell'idea di creare valuta sfruttando uno sforzo computazionale che i partecipanti devono compiere. Il lavoro di Satoshi è certamente più completo e applicabile, a differenza di b-money che è rimasta solo una proposta. Tuttavia la grande somiglianza ha portato nel tempo a ritenere un possibile candidato per l'anonima figura di Satoshi Nakamoto proprio lo stesso Wei Dai.

Il giusto clima

Non stupisce come, ma soprattutto perchè, il mondo accolse con così tanto entusiasmo la nascita delle criptovalute da quel Novembre 2008 in poi.
A differenza di venti anni prima (con la crypto anarchy di May) o di dieci (con la proposta *b-money*), lo *sviluppo tecnologico* aveva raggiunto dei livelli nettamente superiori di diffusione ed utilizzo. Si stima che il numero di host internet negli anni sia cresciuto in maniera esponenziale, passando da qualche centinaia di migliaia negli anni '80, a quaranta milioni a fine degli anni '90, fino ad oltre 625 milioni nel 2008. Da lì in poi il numero di utilizzatori di internet continuò a crescere e oggi viene stimato da diversi report che oltre il 50% della popolazione acceda ad internet.
Questo ha portato inevitabilmente ad una maggiore diffusione non solo di conoscenza, ma anche di fiducia in un mezzo tanto potente e fino a pochi decenni prima sconosciuto. Un numero sempre più grande di curiosi da tutto il mondo si è dunque avvicinato e ha seguito con passione la nascita e lo sviluppo delle criptovalute, l'espressione di quella esigenza di "anarchia economica" che probabilmente era già sentita da tempo ma che necessitava di maggiore divulgazione. Non è un mistero che i movimenti precedenti a Bitcoin non furono accolti così positivamente dalle istituzioni che di certo non ne promossero la diffusione.
Parallelamente anche i protocolli crittografici applicati all'elettronica dei calcolatori, che saranno da base al modello proposto da Satoshi, avevano raggiunto una maturità e conoscenza maggiore.

Altro fattore favorevole alla diffusione del "fenomeno criptovalute", fu sicuramente la grave situazione in cui versava l'economia globale in quegli anni: dal 2007 la *grande recessione* iniziò a manifestarsi in un mondo né pronto a reagire, né conscio di quali sarebbero state le conseguenze da affrontare. Non passò molto che banche, investitori finanziari ed istituti di credito, furono additati come i principali responsabili di un dissesto incontrollabile.
In questo contesto la proposta concreta di una valuta alternativa a quelle controllate dagli Stati, autonoma e indipendente da qualsiasi autorità centrale, che allo stesso tempo fosse sicura tanto quanto (e magari di più, a detta di Satoshi) gli allora attuali

metodi di pagamento su Internet, fu un richiamo fortissimo per appassionati e non da tutto il mondo.

Come ogni innovazione, non si può certo pensare che sia stata di immediata diffusione; la prima transazione nel mondo reale che abbia utilizzato Bitcoin come valuta di scambio è avvenuta il 22 Maggio 2010 quando un programmatore di Jacksonville, in Florida, propone dieci mila bitcoin per acquistare due pizze. Da lì a poco la capitalizzazione del bitcoin cambierà notevolmente e non si potrà più dire che sia stato un acquisto vantaggioso.

Senza ombra di dubbio, la madre di tutte le criptovalute è **Bitcoin**. Per questo motivo non si può prescindere da una sua conoscenza approfondita prima di approcciarsi alle sue numerose "figlie".
Tutti i punti salienti e i meccanismi alla base della criptovaluta Bitcoin sono espressi in maniera sintetica ma esaustiva nel White Paper. Negli anni, una letteratura sempre più ricca e completa ha aperto ad una comprensione più profonda del protocollo. Si analizzano a seguire tutti gli strumenti che ne permettono il corretto funzionamento.
Dal punto di vista crittografico, erano già diffusi da tempo l'utilizzo della *funzione hash* e della *firma digitale*, strumenti indispensabili nel protocollo Bitcoin.

1.2 Funzione hash

Definito Σ l'alfabeto e Σ^* l'insieme di tutte le parole di lunghezza arbitraria ottenibili da Σ, si definisce una **funzione pre-hash**

$$h : \Sigma^* \longrightarrow \Sigma^n$$

con n fissato, tale che un testo di lunghezza arbitraria venga mandato in un testo di dimensione fissata.

Nelle applicazioni digitali, l'alfabeto in questione è quello dei bit $\{0, 1\}$ ed n può

variare in base all'esigenza, così da ottenere potenze di due.
Non qualsiasi funzione *pre-hash* che rispetti queste caratteristiche può essere una valida funzione *hash*. L'utilità di questa, infatti, è poter avere un'impronta, un *digest*, del messaggio originale in uno di dimensione più piccola, che quindi necessiti di minor memoria per essere trasmesso.
Per essere considerata valida, una funzione pre-hash deve soddisfare le proprietà di *resistenza alle collisioni*, *resistenza alla seconda pre-immagine*, *unidirezionalità*.

Definizione 1.2.1. *Siano* $a, b \in \Sigma^*$, $a \neq b$, $h : \Sigma^* \longrightarrow \Sigma^n$ *una funzione pre-hash. Se* $h(a) = h(b)$*, allora si è trovata una collisione.*

Non deve però essere possibile, o più concretamente deve essere computazionalmente molto difficile, trovare collisioni, coppie di parole qualsiasi nell'alfabeto, diverse fra loro, che abbiano la stessa immagine per la funzione considerata.
Inoltre devono essere verificate anche le successive definizioni.

Definizione 1.2.2. *Sia* $a \in \Sigma^*$, $h : \Sigma^* \longrightarrow \Sigma^n$ *una funzione pre-hash resistente alla seconda pre-immagine se trovare* $b \in \Sigma^*$, $b \neq a$ *tale che* $h(a) = h(b)$ *è computazionalmente infeasible.*

Definizione 1.2.3. *Sia* $h : \Sigma^* \longrightarrow \Sigma^n$ *una funzione pre-hash,* $z \in \Sigma^n$ *tale che* $h(x) = z$ *per qualche* $x \in \Sigma^*$*.* h *è unidirezionale se il calcolo di* x *è computazionalmente infeasible.*

L'unico modo per trovare x deve essere forza-bruta, ossia provare tutti i possibili input fino a quando si trova corrispondenza.
Non per ultimo, un algoritmo per essere accettato deve fare in modo che sia verificato il cosiddetto *effetto a valanga*: se due input differiscono anche per un singolo bit, gli output corrispondenti devono essere notevolmente differenti fra loro.
Solo sotto queste ipotesi si può definire h una **funzione hash**.

Dagli anni '90 l'agenzia americana *NIST- National Institute of Standards and Technology* ha indetto delle competizioni pubbliche per la ricerca di adeguati protocolli di funzioni hash che potessero essere condivisi a livello mondiale. La prima versione di **Secure Hash Standard SHA** viene pubblicata nel 1993, soppiantata due anni

dopo da un aggiornamento SHA-1. Nel 2001 viene pubblicato SHA-2, sostituendo il protocollo precedente essendosi trovate delle collisioni. Nel 2006 l'ultima competizione indetta ha portato alla pubblicazione di *Keccak* SHA-3.
Tutta la comunità scientifica può partecipare proponendo un algoritmo o provando ad attaccare quelli selezionati, così da scartare quelli non sicuri.

Una buona funzione hash risulta necessaria nell'applicazione Bitcoin e difatti Satoshi Nakamoto ne fa largamente uso. Ad esempio ogni scambio di bitcoin deve contenere:

- l'hash dell'intera transazione, al fine di poterla identificare univocamente;
- l'hash della transazione che precedentemente aveva coinvolto il mittente che vuole spedire bitcoin.

Se si potessero trovare transazioni diverse fra loro ma con lo stesso digest, nel caso Bitcoin ad esempio, l'identificazione della transazione stessa potrebbe non essere univoca. Inoltre un attaccante del sistema potrebbe sfruttare a suo favore la facilità di trovare collisioni per legare mittente e destinatario delle transazioni a propria scelta. Si comprende dunque la necessità di una funzione hash *collision-resistant*.
L'unidirezionalità della funzione è uno dei meccanismi di sicurezza del protocollo: sebbene il calcolo degli hash è deterministico e abbastanza veloce, così da non rallentare il processo, tornare indietro non lo è e dunque eventuali modifiche risulterebbero *infeasible*.
Analogamente, l'importanza dell'effetto a valanga è evidente: se così non fosse, la ricerca degli input, a partire dall'hash, sarebbe molto più semplice e i tentativi *brute-force* da fare molto inferiori, potendo muoversi in direzioni "privilegiate" quando si trova qualcosa simile all'output cercato.
Bitcoin ha scelto di utilizzare due funzioni crittografiche hash: prima SHA-256 e poi RIPEMD-160. Le due funzioni sono state sviluppate da enti diversi: i primi dal NIST, i RIPE da ricercatori che vogliono trovare alternative ai classici algoritmi digest proposti negli anni. L'utilizzo di entrambi fortifica il sistema da eventuali attacchi.

1.2.1 SHA-256

Il protocollo SHA-256 è uno fra le quattro varianti di SHA-2, insieme a SHA-224, SHA-384 e SHA-512. Il funzionamento è il seguente.

Al messaggio originale vengono aggiunti bit fino a quando la sua lunghezza è congruente a 448 mod 512. Viene poi aggiunto un intero di 64 bit contenente la lunghezza del messaggio originale, così da avere una dimensione multipla di 512. Il messaggio viene dunque diviso in blocchi di 512 bit $M^1, \cdots, M^N$. Ad uno ad uno, i blocchi vengono processati partendo da un valore fissato di hash iniziale $H^{(0)}$ costituito da una sequenza di 8 parole da 32 bit

$$H_1^{(0)} = 6a09e667 \quad H_2^{(0)} = bb67ae85 \quad H_3^{(0)} = 3c6ef372 \quad H_4^{(0)} = a54ff53a$$

$$H_5^{(0)} = 510e527f \quad H_6^{(0)} = 9b05688e \quad H_7^{(0)} = 1f83d9ab \quad H_8^{(0)} = 5be0cd19$$

e applicando l'espressione:

$$H_j^i = H_j^{i-1} + C_{M^i}(H_j^{i-1}) \tag{1.1}$$

con $i \in \{1, \cdots, N\}$; $j \in \{1, \cdots, 8\}$; C è la **funzione di compressione** e l'hash del messaggio sarà H^N.

La funzione di compressione è un algoritmo *cipher block* di 256 bit, con chiave il blocco M^i del messaggio.

Ogni blocco M^i di lunghezza 512 bit è la concatenazione di 16 parole di lunghezza 32 bit, così che il messaggio originale può essere visto come:

$$M_0(0), M_0(1), \cdots, M_0(31), \cdots, \cdots, \cdots, M_{15}(31)$$

Ognuna di queste, viene espansa in una parola w di lunghezza 64 tale che:

$$\begin{cases} w(j) = M_j(i) & j = 0, 1, \cdots, 15 \\ w(j) = A_1(w(j-2)) + w(j-7) + A_0(w(j-15)) + w(j-16) & 16 \leq j \leq 63 \end{cases} \tag{1.2}$$

dove A_0 e A_1 sono funzioni logiche su parole di 32 bit definite, congiuntamente alle altre utilizzate, come segue:

$$Ch(X, Y, Z) = (x \cap Y) \oplus (\overline{X} \cap Z)$$

$$Maj(X, Y, Z) = (X \cap Y) \oplus (X \cap Z) \oplus (Y \cap Z)Y$$

$$S_0 = S^2(X) \oplus S^{13}(X) \oplus S^{22}(X)$$

$$S_1 = S^6(X) \oplus S^{11}(X) \oplus S^{25}(X)$$

$$A_0 = S^7(X) \oplus S^{18}(X) \oplus R^3(X)$$

$$A_1 = S^{17}(X) \oplus S^{19}(X) \oplus R^{10}(X)$$

con R^n shift destro di n bit; S^n shift ciclico destro di n bit.

E' utile vedere l'espansione graficamente:

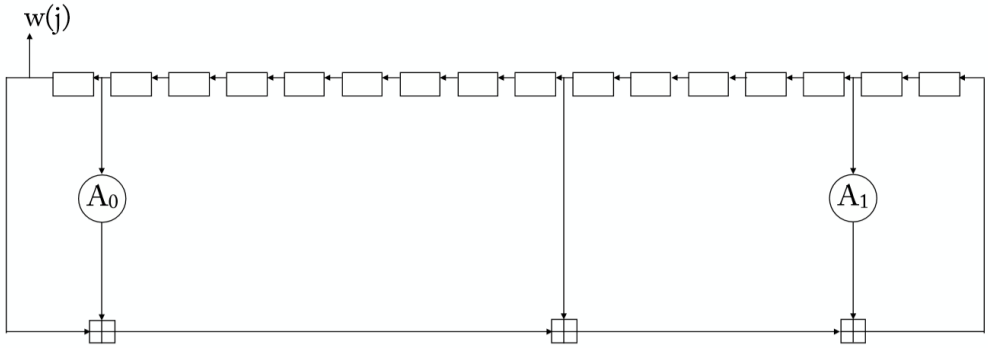


Figura 1.1: Espansione parole del blocco M_i.

Per procedere con il calcolo della funzione di compressione, e poi il valore finale dell'hash, occorre calcolare:

$$a = H_1^i \quad b = H_2^i \quad c = H_3^i \quad d = H_4^i \quad e = H_5^i \quad f = H_6^i \quad g = H_7^i \quad h = H_8^i$$

$\forall i = 1, \cdots, N$.

Anche il calcolo della funzione di compressione è più esplicativo se visto graficamente:

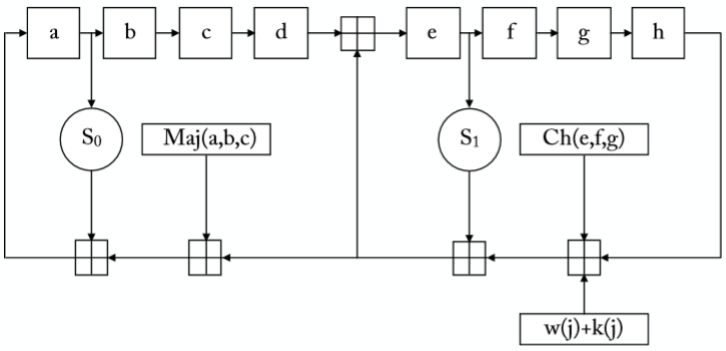


Figura 1.2: Funzione di compressione SHA-256.

specificando che:

$$\begin{cases} T_1 = h + S_1(e) + Ch(ef, g) + k(j) + w(j) \\ T_2 = S_0(a) + Maj(a, b, c) \end{cases} \tag{1.3}$$

aggiornando come segue:

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

e con $k(j)$ valori costanti tabulati.

Infine, applicando 1.1, si costruisce l'hash del messaggio:

$$H^N = (H_1^N, H_2^N, \cdots, H_8^N)$$

$H_1^i = a + H_1^{i-1}$

$H_2^i = b + H_2^{i-1}$

$H_3^i = c + H_3^{i-1}$

$H_4^i = d + H_4^{i-1}$

$H_5^i = e + H_5^{i-1}$

$H_6^i = f + H_6^{i-1}$

$H_7^i = g + H_7^{i-1}$

$H_8^i = h + H_8^{i-1} \qquad \forall i = 1, \cdots, N$

L'output in uscita avrà una lunghezza di 256 bit.

Il successivo passaggio in Bitcoin è applicare la seconda funzione hash.

1.2.2 RIPEMD-160

Sviluppato dal progetto European RIPE con l'obiettivo di proporre algoritmi differenti da quelli del NIST, è più forte delle versioni precedenti e ci si aspetta che sia sicuro per i prossimi dieci anni, o più. La sicurezza di una funzione hash è valutata dall'assenza di collisioni trovate dal mondo accademico e non solo. Quanto riportato in seguito è spiegato nel paper [2] dagli autori.

Il messaggio, l'output di SHA-256, dunque di 256 bit, viene aggiornato con un padding così che la sua lunghezza sia di 16 blocchi da 32 bit, parole su cui opera l'algoritmo.

Vengono inizializzati dei valori costanti di 32 bit in esadecimale h_0, h_1, h_2, $h_3\, h_4$ e i rispettivi valori :

$A := h_0,\ B := h_1,\ C := h_2\ D := h_3\ E := h_4,$

$A' := h_0,\ B' := h_1,\ C' := h_2\ D' := h_3\ E' := h_4.$

Segue la funzione di compressione che in cui ogni round si può rappresentare graficamente:

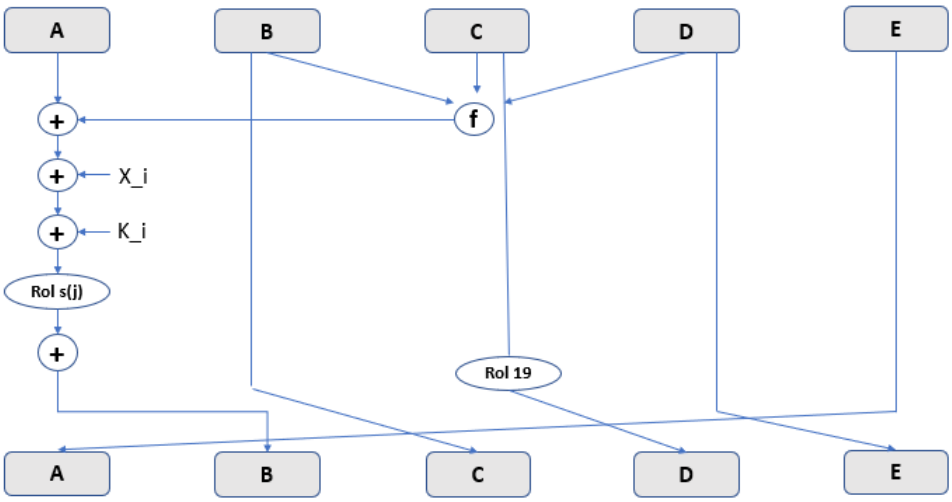


Figura 1.3: Funzione di compressione RIPEMD-160. Fonte pagina LinkedIn *Joe Christensen*, ingegnere informatico.

Lo pseudo-codice della funzione fa comprendere bene come l'algoritmo operi effettuando gli 80 round in cascata. Esso rappresenta la precedente figura e si articola come segue:

for $j := 0$ *to* 79 *{*

$T := rol_{s(j)}(A \boxplus f(j, B, C, D) \boxplus X_i[r(j)]) \boxplus K(j)) \boxplus E;$

$A := E; \quad E := D; \quad D := rol_{10}(C); \; C := B; \quad B := T;$

$T := rol_{s'(j)}(A' \boxplus f(79 - j, B', C', D') \boxplus X_i[r'(j)]) \boxplus K'(j)) \boxplus E';$

$A' := E'; \quad E' := D'; \quad D' := rol_{10}(C'); \; C' := B'; \quad B' := T;$

}

ricordando che $\boxplus$ è l'addizione modulo 2^{32}. Le funzioni non lineari, le costanti, le rotazioni sinistre rol di un certo s o s' sono riportate in Appendice A.
Segue l'aggiornamento di T e degli h_i:
$T := h_1 \boxplus C \boxplus D'; \quad h_1 := h_2 \boxplus D \boxplus E'; \quad h_2 := h_3 \boxplus E \boxplus A';$
$h_3 := h_4 \boxplus A \boxplus B'; \quad h_4 := h_0 \boxplus B \boxplus C'; \quad h_0 := T.$

Qui si è ipotizzato che il messaggio fosse costituito da un unico blocco di 16 parole, ma si può estendere al caso in cui ci sono t di questi blocchi iterando per tutti i blocchi.

1.3 Firma digitale

Analogamente alla firma nella vita reale, la firma digitale serve a garantire il mittente di un messaggio o, più genericamente, a garantire l'identità di chi compie una certa operazione.

Nei sistemi a chiave pubblica, sebbene venga evitato il problema di scambiare le chiavi crittografiche, sorge la difficoltà di autenticare il mittente del messaggio.
Siano A e B mittente e destinatario di un messaggio M, ognuno dotato di (f_i, f_i^{-1}) coppia di chiavi pubblica e privata, $i = \{A, B\}$, si può introdurre la struttura logica alla base di ogni protocollo di firma digitale.

Schema generale di firma digitale:

- *A invia a B un messaggio M utilizzando la chiave pubblica di B* $f_B(M)$

- *A certifica la propria identità con la sua chiave privata f_A^{-1} inviando la coppia:*

$$(f_B(f_A^{-1}(s_A)), s_A)$$

con s_A informazioni utili quali timestamp, data/ora o l'indirizzo IP.

- *Si può far dipendere la firma dal messaggio, così che B non si possa spacciare successivamente per A:*

$$(f_B(f_A^{-1}(s_A \,||h(M))), s_A)$$

con $h(M)$ digest del messaggio.

Negli anni lo studio dei protocolli di firma digitale è stato intenso e ricco di risultati. I più noti sono: *RSA, PGP, ElGamal, DSA, ECDSA.*
Ognuno di questi riproduce lo schema generale con caratteristiche peculiari, più o meno applicabili in contesti reali, in base alla difficoltà con cui possono essere "rotti" da un'attaccante esterno.
I diversi metodi sono stati testati dalle più importanti agenzie che si occupano di sicurezza tecnologica e attualmente quelli che a parità di sicurezza offerta utilizzano chiavi con un minor numero di bit sono quelli implementati sulle *curve ellittiche* e saranno oggetto della successiva sezione[2].

Tutti si basano sulla difficoltà, o presunta impossibilità, di risalire alla chiave privata data la condivisione della chiave pubblica. Se si dovessero trovare algoritmi efficienti di risoluzione per i problemi matematici [3] di base, l'intero schema di firma crollerebbe.
Nel perseguire l'obiettivo di realizzare una versione di denaro elettronico fra gli utenti, un passo necessario è quello della firma digitale della transazione. Questo chiaramente non viene visto da Nakamoto nel suo Paper come un fattore di novità, tanto che non viene nemmeno citato l'algoritmo scelto. Risulta però importante, al fine di una valutazione e comparazione della sicurezza del protocollo, analizzarlo nel dettaglio.

[2]Sul sito [23] è possibile osservare un confronto diretto fra metodi differenti.

[3]Dato G gruppo di ordine n generato da g, $\forall y \in G$, $y = g^x$. Calcolare x a partire dai dati precedenti è il problema del logaritmo discreto.

1.3.1 ECDSA- Elliptic Curve Digital Signature Algorithm

Analogo del DSA ma su curva ellittica, l'algoritmo venne accettato nel 2000 fra gli standard del NIST. Fornisce lo stesso livello di sicurezza di altri algoritmi ma con una lunghezza della chiave nettamente inferiore.
E' utile ricordare che:

> Sia $p > 3$ un primo. Una curva ellittica di Weierstrass E su $\mathbb{F}_p$ è definita da un'equazione della forma
>
> $$y^2 = x^3 + a\ x + b$$
>
> dove $a, b \in \mathbb{F}_p, \quad 4a^3 + 27b^2 \not\equiv 0\,(mod p)$.
>
> L'insieme degli elementi in $\mathbb{F}_p$ che soddisfano l'equazione, insieme a $\mathcal{O}$ punto all'infinito, costituiscono i punti della curva $E(\mathbb{F}_p)$.

La curva ellittica scelta, e divenuta famosa proprio per la sua applicazione a Bitcoin, è

$$y^2 = x^3 + 7$$

identificata dal nome **Secp256k1**, sul campo $\mathbb{Z}_p$, con $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ un primo molto grande. Le coordinate dei punti x, y, sono interi di 256 bit mod p.

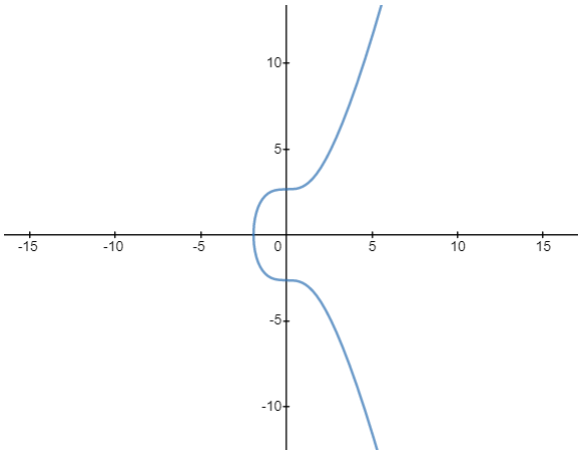


Figura 1.4: Rappresentazione sul piano reale della curva Secp256k1.

E' necessario poter svolgere agevolmente addizioni sulla curva cioè, dati P e $Q \in E(\mathbb{F}_p)$, trovare $R = (x_R, y_R) \in E(\mathbb{F}_p)$.
Considerazioni di tipo grafico (*regola della tangente*) e analitico, portano alle formule:

- somma P+Q:

$$x_R = m^2 - x_P - x_Q$$

$$y_R = m(x_P - x_R) - y_P$$

  con $m = \dfrac{y_Q - y_P}{x_Q - x_P}$

- duplicazione P+P:

$$x_R = m^2 - 2x_P$$

$$y_R = m(x_P - x_R) - y_P$$

  con $m = \dfrac{3x_P^2 + a}{2y_P}$

Fra i parametri di dominio per ECDSA, vi è anche il *punto base* G in $E(\mathbb{Z}_p)$ generatore del gruppo dei punti della curva e l'*ordine* del gruppo. Per Bitcoin questi sono:

$x_G = 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D9$
$59F2815B16F81798$
$y_G = 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A6855419$
$9C47D08FFB10D4B8$
$n =$Ordine del gruppo: $FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE$
$BAAEDCE6AF48A03BBFD25E8CD0364141$

L'obiettivo è preservare *autenticità, confidenzialità, integrità* dei partecipanti e delle informazioni. Per far ciò, deve essere generata una coppia di chiavi, una privata per firmare le transazioni per spendere bitcoin, quella pubblica per riceverli. Quest'ultima è comunicata tramite l'applicazione delle due funzioni hash precedentemente descritte alla chiave pubblica: *bitcoin address*. Anche in questo caso, essendo funzioni *one-way*, non si può risalire alla chiave pubblica. Il bitcoin address viene rappresentato con una codifica nota come *Base58Check* in 58 caratteri pensati ad hoc per evitare errori, così da renderne più semplice l'utilizzo agli utenti.

Figura 1.5: Chiave pubblica, chiave privata, bitcoin address.

La chiave privata è un numero casuale fra 1 ed $n-1$; affinché abbia lunghezza 256 bit viene calcolato l'output SHA-256$= d$, controllando che sia minore di $n-1$. La chiave pubblica corrispondente è il punto sulla curva $P = dG$ di cui si salva solo la coordinata x, per risparmiare memoria. Bisogna però ricordare il segno della coordinata y: la simmetria della curva rispetto all'asse delle ascisse ci assicura che esiste il punto specchiato corrispondente; per farlo, viene aggiunto un prefisso alla chiave pubblica: 02 se y è positivo, 03 altrimenti.
Il calcolo della chiave pubblica a partire da quella privata è abbastanza veloce, ma computazionalmente molto difficile da invertire. E' il noto *ECDLP- elliptic curve discrete logarithm problem*: l'impossibilità di risalire a d è ciò che rende sicuro, ad oggi, questo metodo.

Protocollo di firma digitale ECDSA:

- *il mittente calcola l'hash del messaggio* $h = h(M)$
- *sceglie un valore casuale* $k \in \mathbb{Z}_n$
- *calcola il punto della curva* $kG = (x, y)$
- *fissa* $r = x \bmod n$ *e calcola* $s = (h + rd)/k \bmod n$
- *allega al messaggio la coppia* (r, s).

La scelta di un valore casuale fa in modo che la firma sia sempre differente.
L'utente che deve ricevere il pagamento [4] può controllare l'esito del precedente protocollo come segue.

[4] Anche tutti gli altri utenti del network possono e devono verificare la correttezza delle transazioni in modo da garantire una catena non fraudolenta.

Verifica della firma digitale (r, s):

- *calcolare l'inverso del secondo termine della firma, determinando* $w = s^{-1} = k/(h + rd))$
- *calcolare* $u = wh$ *e* $v = wr$
- *calcolare il punto* $Q = uG + vP$*, con* $P = dG$ *chiave pubblica del mittente*
- *la firma è considerata valida solo se la prima coordinata del punto* Q*, mod* n*, coincide con* r*.*

Uno degli standard irrinunciabile del modello bancario tradizionale è la privacy garantita alle parti coinvolte. Bitcoin non può fare altrettanto perché tutte le transazioni saranno pubbliche e, come specificato in seguito, condivise. Ciò che viene però fatto è mantenere l'anonimato: si può vedere che qualcuno sta inviando della valuta a qualcun' altro, ma non si deve risalire all'utente. Perché ciò sia vero, deve essere *generata una nuova coppia di chiavi per ogni transazione.* Se così non fosse, se ad esempio Alice ricevesse dei bitcoin da Bob, ricondurrebbe a lui la chiave pubblica e, tutte le volte in cui ritrova questa in transazioni successive, saprebbe ricondurla a Bob, divenendo totalmente a conoscenza delle sue attività.
Generatori e contenitori di chiavi private sono i *wallets*, i quali utilizzano algoritmi di tipo deterministico oppure randomico.

1.4 Transazioni

L'idea di Satoshi Nakamoto è quella di una valuta elettronica gestita su una catena di blocchi in cui "scrivere" **transazioni**, cioè il passaggio di un certo numero di bitcoin da un proprietario ad un altro. Il problema di eliminare un'autorità fiduciaria centrale è principalmente quello del *double-spending* e dunque nasce la necessità di un protocollo che assicuri al beneficiario che il proprietario precedente non abbia già speso la stessa moneta, volendo fare un parallelismo con il mondo reale.
Ogni transazione ha uno o più *input*, debiti relativi a degli account, e uno o più *output*, crediti aggiunti ad uno o più account. La somma degli input è leggermente

superiore alla somma degli output perchè è presente una *transaction fee*, pagamento per l'utilizzo del servizio.

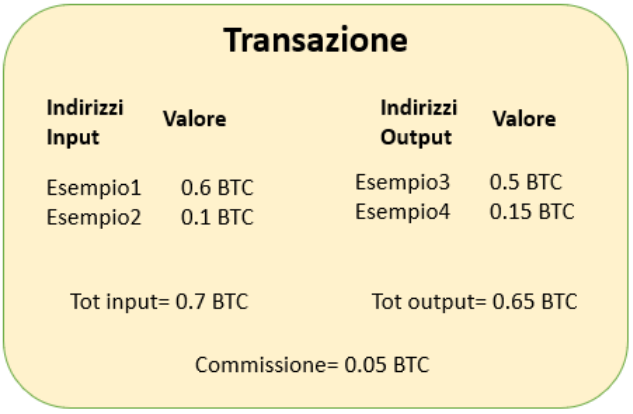


Figura 1.6: Esempio di transazione.

Ogni transazione è caratterizzata anche da *metadata*, informazioni relative alla grandezza, numero di input, numero di output.

Unendo gli strumenti precedentemente analizzati, si può adesso definire la catena delle transazioni come segue: chi vuole trasferire valuta firma digitalmente un hash della transazione precedente aggiungendo il bitcoin address del proprietario successivo. La catena di proprietà può essere agevolmente verificata come scritto in precedenza con il protocollo di *verifica di firma digitale*.

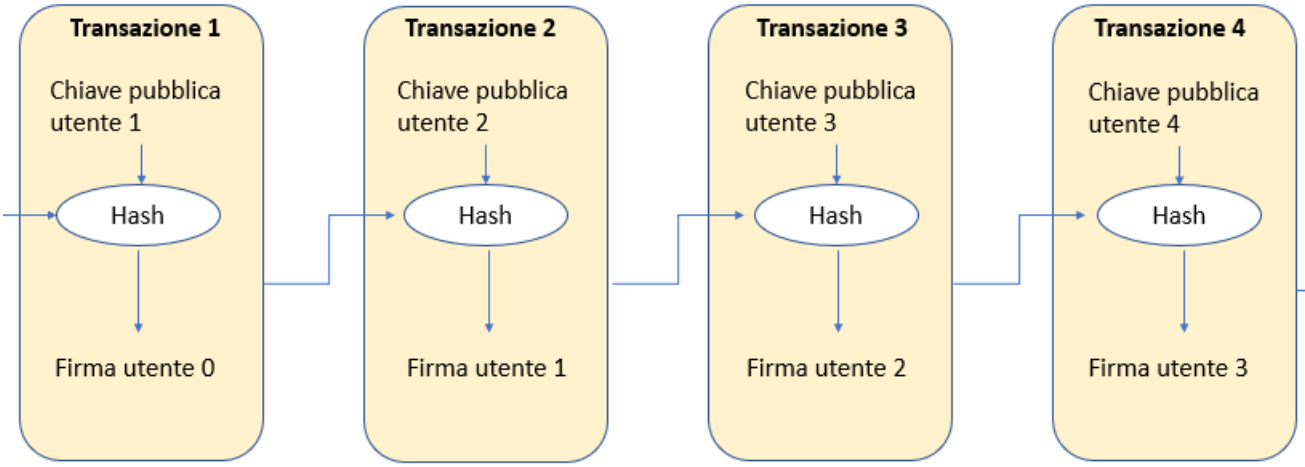


Figura 1.7: Catena di transazioni; la firma dell'utente i viene effettuata con la sua chiave privata e solo lui può verificarla.

Un **blocco** è una struttura che contiene un insieme di transazioni che devono essere validate dalla rete. Esso è costituito dal *block header* e da una lista di transazioni.

Block Header

E' costituito da un insieme di tre insiemi di metadata.
In primis, il block header precedente viene legato facendone due volte SHA-256. Seguono *difficoltà, nonce*, concetti che verranno ripresi nel seguito poichè legati al *mining*, e il **timestamp**, il momento in cui viene creato il blocco espresso in secondi a partire dal 1/1/70 (convenzione Unix Epoch).
Il *timestamping* viene citato da Nakamoto nel suo Paper in quanto è la sua soluzione al problema del **double-spending**. Infatti, una delle caratteristiche principali del denaro è che la stessa banconota non può essere spesa due volte "dalla stessa persona"; la stessa cosa deve avvenire con la valuta virtuale. La volontà di non far riferimento ad un'autorità centrale che regoli la questione, ha portato alla soluzione proposta di accettare la *transazione che per prima venga verificata*. Il Timestamping serve proprio a tale scopo, allegando 4 byte all'hash di un blocco prima che venga diffuso e includendo il timestamping del blocco precedente.
Il terzo elemento è un *merkle tree root*, una struttura che sintetizza tutte le transazioni del blocco.
Merkle Tree: conosciuto anche come *binary hash tree*, permette di sintetizzare efficientemente una grande quantità di dati. L'algoritmo crittografico di hash è il doppio SHA-256. In Bitcoin vengono utilizzati questi alberi per controllare rapidamente se una transazione è inclusa in un blocco.
L'approccio che viene utilizzato è bottom-up: partendo dalle singole transazioni, si calcola ad esempio

$$H_A = SHA\,256(SHA\,256(Transazione\,A))$$

ottenendo i nodi foglia.
Si concatenano poi coppie consecutive di nodi foglia in nodi più alti e si applicano nuovamente le funzioni hash. Si itera ancora fino a quando non si ottiene un unico nodo, il *Merkle root*. Questo unico noto permette di identificare tutte le transazioni del blocco. Se il numero iniziale di nodi non fosse pari, viene duplicato l'ultimo.

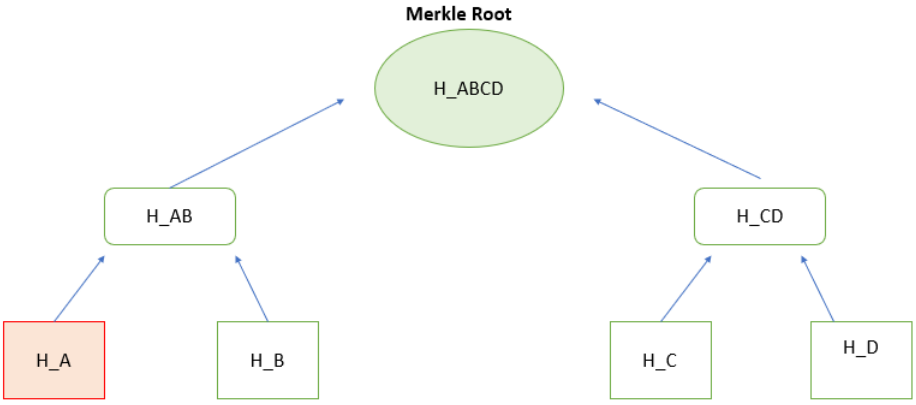


Figura 1.8: Esempio *Merkle Tree*; $H_AB = Hash(H_A + H_B)$.

Per verificare che una transazione è presente nel blocco, un nodo deve effettuare il calcolo di $\log_2(N)$ funzioni hash per ricostruire un cammino che porti alla radice. L'efficienza di questi alberi è più evidente man mano che il numero di transazioni aumenta; dato che in Bitcoin spesso ne vengono aggiunte anche migliaia, l'utilità è molto alta.

Se è vero che il *timestamp* permette un ordine cronologico dei blocchi, nulla fin qui assicura che un attaccante non possa voler modificare la catena di blocchi impropriamente. Per spiegare perché ciò non può avvenire, bisogna introdurre come, da chi e secondo quali regole, questi vengono aggiunti.

1.5 Proof-of-Work & Mining

Il primo blocco di questa catena, noto come *Genesis Block*, è stato creato il 3 Gennaio 2009 alle ore 18:18. Il suo hash è noto a tutti i partecipanti della rete come un punto di partenza, una *secure root* per tutti i successivi.
All'interno dell'unica transazione presente è contenuto un testo:

"The Times 03/Jan/2009 Chancellor on brink of second ballout for banks".

Non solo il modo per fissare chiaramente la data di inizio, ma anche un monito per sottolineare l'importanza di una moneta indipendente in un periodo in cui gli istituti finanziari stanno vivendo una fortissima crisi monetaria.

Decentralizzazione

Uno degli aspetti cardine di Bitcoin è, come già visto, l'allontanamento da un sistema centralizzato. Questo si rispecchia anche a livello architetturale: non è più previsto un (o più) grande server centrale controllato da chi detiene l'autorità, che verifica tutte le transazioni richieste. Al contrario, il sistema è decentralizzato, tutti i nodi hanno l'autorità e fungono da server per la catena di blocchi che, dunque, sarà opportunamente duplicata su ogni nodo della rete. Si deve dunque raggiungere quello che viene chiamato con *emergent consensus*, l'approvazione comune non perché decisa da un'ente esogeno, ma frutto dell'interazione di migliaia di nodi indipendenti che seguano le stesse regole.
I criteri da verificare sono fissati e mirano al controllo della correttezza e completezza delle informazioni, il rifiuto di transazioni duplicate e la conferma di requisiti tecnici (la lista completa in Appendice B.)

Aggiunta di nuovi blocchi

Ci si chiede come si possa tecnicamente creare questo sistema di server distribuito *peeer-to-peer* con marcatura temporale, evitando il più possibile attacchi informatici. La risposta è nel *proof-of-work*, un protocollo di verifica liberamente inspirato (e Satoshi lo dice esplicitamente) dall'*Hashcash* di Adam Back.

Hashcash: nel 1997 si comincia a diffondere lo *spam*, un problema su Internet ed in particolare legato all'ambito della posta elettronica . Questo termine indica l'invio di messaggi non desiderati, e spesso dannosi, ad una grande quantità di indirizzi. Gli obiettivi dello spamming sono vari, da semplice pubblicità, alle proposte di acquisto di materiale spesso illegale, fino all'organizzazione di vere e proprie truffe.
Per arginare questo problema l'idea di Adam Back è di aggiungere un costo computazionale all'invio di un email. Tecnicamente deve essere aggiunto un codice testuale all'intestazione, unico per ogni destinatario perché ne deve contenere anche l'informazione relativa all'indirizzo email: il mittente, impostando un valore casuale come contatore fa l'hash del testo con un'opportuna funzione crittografica (la proposta iniziale è stata SHA-1). Dovrà essere modificato il valore del contatore fino a quan-

do non si ottenga un output con un numero di bit iniziale di zeri concordato. Questo numero va scelto in modo da rendere questo lavoro complesso quanto occorre per scoraggiare l'invio massivo di email. Il destinatario calcola l'hash del testo inviato con la stessa funzione e, se non rispetta la condizione imposta, rifiuta l'email. Questa operazione chiaramente richiede molto meno tempo.

Lo stesso "gioco" verrà richiesto ai *miner* della rete, un sottoinsieme di tutti i nodi che decidono di partecipare mettendo a disposizione la loro potenza di calcolo, per aggiungere blocchi alla catena e, come vedremo, per generare nuovi bitcoins.
Quando un blocco di transazioni viene aggiunto, ricomincia la competizione fra i miner. Ognuno costruisce un nuovo blocco con un certo numero di nuove transazioni e viene modificato progressivamente o secondo una scelta arbitraria il ***nounce***, un contatore numerico di 4 bytes presente nel Block header fino a quando l'hash dell'header (doppio SHA-256) sarà un numero inferiore al valore *target* fissato.
Come noto, una buona funzione di hash deve preservare l'effetto a valanga, dunque una piccola modifica del *nounce* (anche una sola cifra) ci aspettiamo comporti grandi cambiamenti nell'output. Questa proprietà è fondamentale nel network: se così non fosse vorrebbe dire che, una volta trovato un valore del nounce per cui l'hash è vicino al valore target, potrebbe bastare modificarlo poco per ottenere l'output voluto. Questo però allontanerebbe da una ricerca realmente *brute-force* intaccando la sicurezza stessa del protocollo.

Dimensione (bytes)	Campo
4	Versione del software
32	Hash del blocco precedente
32	Merkle Root
4	Timestamp
4	Difficulty target
4	Nonce

Figura 1.9: Esempio Block Header.

Nella rara ipotesi in cui tutti i 2^{32} possibili tentativi per il nounce nell'header non abbiano portato ad un output inferiore al valore target, i miner passano alla mo-

difica del nounce nella **Coinbase**, la prima transazione di ogni blocco che regola il pagamento a chi riesce a risolvere il problema per primo.
L'input di questa prima transazione è un valore casuale, il nounce della Coinbase; come input *null* perché non si lega a nessuna transazione precedente ma *vengono creati nuovi bitcoins* ed immessi nella rete come ricompensa allo sforzo computazionale svolto. Questo è l'unico modo con cui viene creata valuta.
Dato che la modifica del nounce nella prima transazione comporterebbe modifiche per l'intero Merkle tree, viene effettuata solo quando tutti i tentativi precedenti hanno fallito.
Da quanto detto emergono degli aspetti interessanti:

- i miners non lavorano tutti sullo stesso blocco: possono decidere quante transazioni aggiungere, da quale nounce partire nella coinbase, come effettuare la ricerca. L'indirizzo che specificano per l'eventuale accredito di bitcoin è differente, quindi differente è il Proof-of-work da risolvere;

- il livello di difficoltà dipende dalla capacità dei calcolatori che, come noto, aumenta continuamente. Per mantenere tempo medio di mining di circa un blocco ogni 10 minuti deciso da Satoshi, risulta necessario settare periodicamente la difficoltà. Nello specifico, per Bitcoin questo avviene ogni 2016 blocchi secondo la formula:

$$next_difficulty = previous_difficulty \cdot \frac{2016 \cdot 10\,minutes}{time\,to\,mine\,last\,2016\,blocks} \tag{1.4}$$

1.5.1 Difficoltà e target

La precedente formula 1.4 esprime che, se il tempo per gli ultimi blocchi è stato inferiore rispetto all'obiettivo, la difficoltà deve aumentare; viceversa la difficoltà va diminuita. Con "difficoltà più alta" si intende che il *Difficulty Target* sarà un numero più piccolo, così che stare sotto quel valore richiederà, mediamente, più sforzo computazionale.

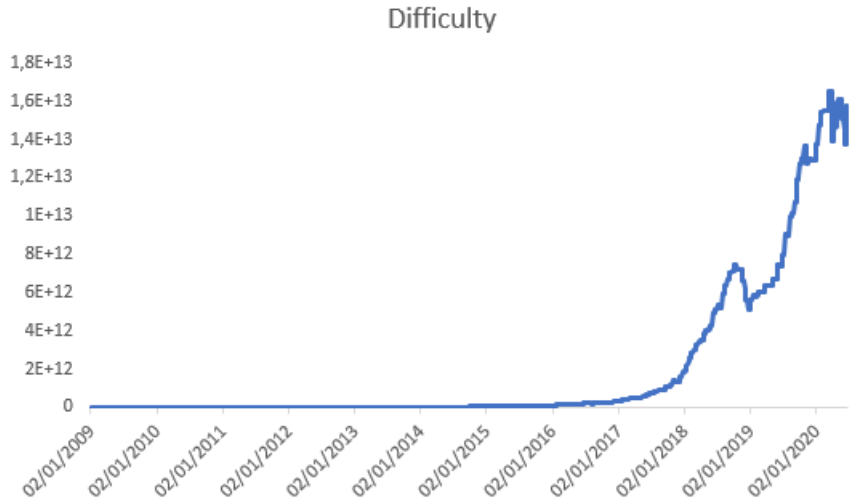


Figura 1.10: Dal 3/01/2009 (D=1) al 2/03/2020 (D=15 milioni), fonte [9].

Il target massimo Bitcoin, ovvero la difficoltà più bassa di creazione di un blocco, è fissato a

$$t_max = 0x00000000FFFF0000000000000000000000000000000000000000000000000000$$
$$= 0x00000000FFFF \cdot 2^{208} = 65535 \cdot 2^{208}$$

e corrisponde a difficoltà $D = 1$. In generale la difficoltà è il rapporto fra il target massimo e il target corrente t: $D = \frac{t_max}{t}$. Come atteso, più il target diminuisce, più la difficoltà aumenta.
L'aumento così elevato della difficoltà, dell'ordine di grandezza di 10^{13}, non può essere spiegato solamente con l'aumento della capacità di calcolo dei computer negli ultimi anni. Senza dubbio questo ha influenzato notevolmente, se si considera come i cosiddetti "SuperComputer" sono passati da 1 $Pflop/s = 10^{15}$ operazioni al secondo nel 2008 a sfiorare 1 $Eflop/s = 10^{18}$.

Se è vero che nulla ci assicura che i computer utilizzati da i miners abbiano prestazioni paragonabili ai TOP500, è pur vero che risulta lecito attendersi che le variazioni in ordine di grandezza siano in ogni caso paragonabili. Vanno aggiunte considerazioni relative ai costi per l'acquisto di $Gflop/s$, ridotti in maniera considerevole negli anni in questione: nel 2007 il costo approssimativo per $Gflop/s$ è stimato intorno ai 50 dollari e già nel 2017 era sui 3 centesimi di dollari. Si intuisce come a parità di denaro investito, i miner necessariamente hanno acquisito sempre più capacità di

calcolo. In più, l'interesse sempre crescente nei confronti dei Bitcoin mette in luce sicuramente investimenti maggiori in tale ambito. Ne sono un esempio i **mining pool**, collaborazioni di miners che condividono energia e mezzi per amplificare i ricavi. Proprio per questo assetto, non è semplice sapere esattamente quanti sono i miners che ogni giorno partecipano. Può però rendere l'idea osservare come un grande pool, ad esempio *Poolin*, ne conta 670000; una più piccola come *Mining city*, circa 20000.

Dalla figura 2.4, si può osservare che ben poco spazio viene lasciato a miners indipendenti.

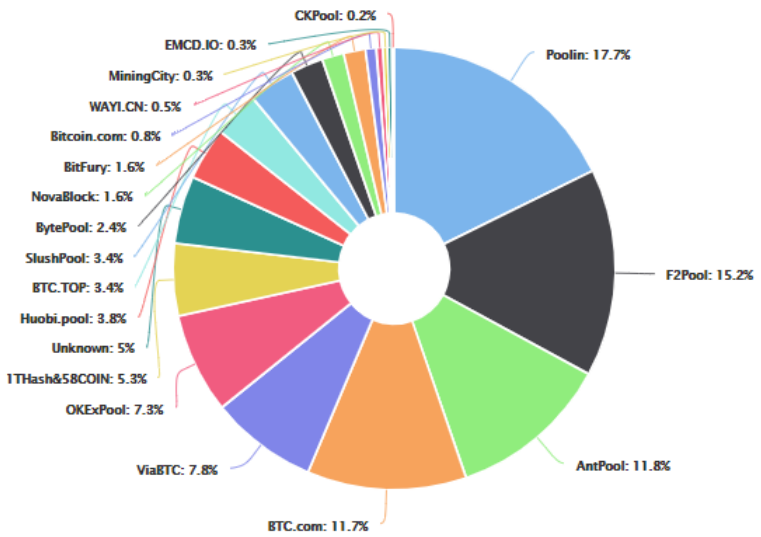


Figura 1.11: Distribuzione capacità di Hash, 04/03/2020, fonte [9].

Una questione attualmente molto diffusa in ambito Bitcoin è proprio quella legata alla massiccia presenza di *mining pool* rispetto ai singoli *miners*. Ciò che desta preoccupazione è il rischio della perdita di decentralizzazione a favore di un potere nuovamente nelle mani di poche e potenti organizzazioni.

Il perchè questo assetto abbia lentamente sostituito lo scenario di individui indipendenti può essere presentato attraverso la seguente dimostrazione di come le *mining pool* permettano stessi guadagni in media ma con una variabilità notevolmente inferiore rispetto al *mining* autonomo.

Approccio probabilistico:

Fra tutti i 2^{256} possibili valori dell'hash, si raggiunge un numero inferiore al valore

target t con probabilità:

$$p(t) = \frac{t}{2^{256}}$$

Per un singolo miner occorrerebbero in media un numero di tentativi pari a

$$n(t) = \frac{2^{256}}{t}$$

Per un generico livello di difficoltà D, il target corrispondente sarà D volte più piccolo di quello corrispondente a $D = 1$:

$$t_D = \frac{0XFFFF \cdot 2^{208}}{D}$$

dunque il numero atteso di hash per trovare un blocco con difficoltà D sarà

$$n_D = \frac{D}{0XFFFF \cdot 2^{208}} \cdot 2^{256} = \frac{D \cdot 2^{48}}{0XFFFF} = \frac{D \cdot 2^{48}}{2^{16} - 1}$$

Si può equivalentemente dire che il valore target è stato scelto affiché ogni computazione porti alla validazione di un blocco con probabilità

$$p = \frac{2^{16} - 1}{2^{48}\, D} \equiv \frac{1}{2^{32}\, D}$$

Le validazioni del blocchi possono essere definiti come τ_1, τ_2, τ_3, $\cdots$, variabili esponenziali indipendenti ed identicamente distribuite, visti come tempi di interarrivo. Sia $T_n = \tau_1 + \tau_2 + \cdots + \tau_n$ tempo di convalida nell'$n - esimo$ blocco.
Dunque un singolo miner con *hashrate* h in un periodo di tempo t troverà un numero di blocchi che è modellizzabile come un **Processo di Poisson** $N(s)$ di parametro $\frac{h}{2^{32}\, D} = \lambda$

$$\begin{aligned} N(s) &= \text{numero di blocchi fino al tempo s} \\ &= max\{n \geq 0 : T_n \leq s\} \end{aligned}$$

Dato che

$$N(t+s) - N(s) \sim Poisson(\lambda\, t)$$

ne segue che, per il numero di blocchi trovati, *valore atteso*$=$ *varianza*$= \lambda\, t$.
Chiamando B i bitcoin ricavati dal blocco,

$$payout \;\; atteso = \frac{h\, t\, B}{2^{32}\, D}$$

Quando diversi miners lavorano insieme per aggiungere nuovi blocchi alla catena, l'hashrate complessivo diventa H. Le considerazioni precedenti si possono ripetere perché la *mining pool* agisce come singolo, trovando valore medio e varianza$= \frac{H\,t}{2^{32}\,D}$. Ogni miner parteciperà con una certa quota $h = qH$, $0 \leq q \leq 1$, ed in base a quella sarà ricompensato ottenendo mediamente lo stesso ricavo che se lavorasse da solo

$$q\,\frac{H\,t\,B}{2^{32}\,D} = \frac{h\,t\,B}{2^{32}\,D}$$

Quella che cambia considerevolmente è la varianza individuale Poisson e di conseguenza del payout:

$$q^2\frac{H\,t}{2^{32}\,D} = q\,\frac{h\,t}{2^{32}\,D}$$

cioè q volte la varianza del singolo miner.
La minore distanza dal valore atteso è un vantaggio tutt'altro che indifferente: un partecipante individuale potrebbe dover aspettare anche parecchi mesi prima di avere un guadagno, magari sostanzioso, ma che ha richiesto notevoli spese hardware e di energia. Un guadagno meno variabile, a parità di valore atteso, rappresenta un vantaggio talmente grande da aver spazzato via, di fatto, i singoli miner dal mercato.

Guadagni più omogenei portano ad investire sempre più in calcolatori, così da aumentare l'hashrate del pool H e portare più guadagni. Di conseguenza la difficoltà dovrà essere aumentata per mantenere i tempi medi di mining.
Ecco come il grande sviluppo tecnologico unito all'interesse dei miner organizzati in pool, sono i fattori che possono spiegare perché negli anni la difficoltà sia cresciuta così tanto.

1.6 Blockchain

Tutto il processo precedentemente descritto permette la formazione di una lunga *catena del consenso* in cui sono scritte in maniera irreversibile tutte le transazioni.
I blocchi sono validati ed aggiunti sequenzialmente, secondo la scelta presentata da Nakamoto nel suo Paper: il sistema prevede che venga inserito mediamente un blocco ogni dieci minuti.
Questo limite pone sicuramente delle difficoltà nell'utilizzo della valuta come metodo

di pagamento per l'assenza di immediatezza e sarà ampiamente discusso dai seguaci Bitcoin.

Un fenomeno da ridurre è quello delle **forks**, ossia biforcazioni dovute all'aggiunta quasi contemporanea di due blocchi.

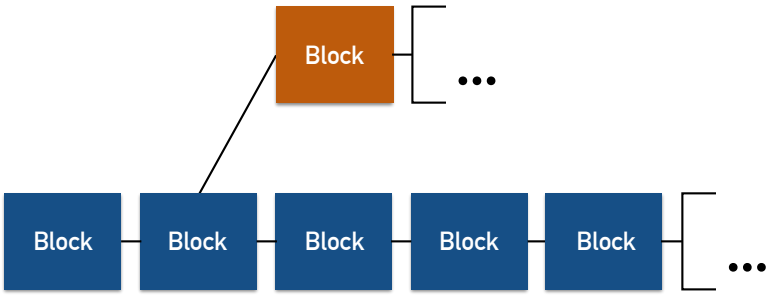


Figura 1.12: Esempio di fork su Blockchain.

Nel Proof of Work, infatti, può capitare che avvenga una convalida quasi sincrona di due blocchi differenti. A quel punto i miners continueranno a lavorare su nuovi blocchi, scegliendo quale catena seguire fra le due possibili. Solo quando una delle due è sufficientemente lunga da potersi considerare solida, le transazioni contenute all'interno dei blocchi sono realmente aggiunte alla blockchain e i miners ricompensati.

La decisione di settare la difficoltà in modo che la velocità di inseritmento dei blocchi sia quella indicata, è legata essenzialmente alla riduzione di possibili forks della catena.

I blocchi contenuti nel fork che viene abbandonato vengono definiti *orfani* e le transazioni al loro interno andranno nuovamente nell'elenco di quelle da aggiungere alla blockchain.

Questa situazione è sicuramente svantaggiosa per tutti i partecipanti. Nei primi anni di vita di Bitcoin il fenomeno non si presentò; i partecipanti al network erano in numero basso e la probabilità della contemporaneità minima. Con il tempo invece i casi diventarono di più e sono state applicate tecniche specifiche per evitare che ciò accadesse, fino ad essere praticamente assenti oggi. La comunità è molto attenta ed evidenzia da subito possibili fork, che però non superano il singolo blocco.

La fork più lunga non è mai stata comunque più lunga di 7 blocchi.

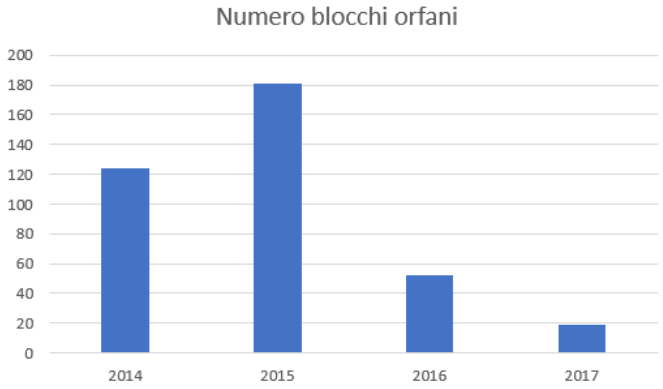


Figura 1.13: Distribuzione del numero di blocchi orfani registrati, fonte [9].

Quest'idea di una forma tutta nuova di organizzazione del consenso sta lasciando il segno in numerosi ambiti.

Immutabilità, Tracciabilità, Decentralizzazione

sono le parole chiave di un'innovazione che pian piano coinvolgerà settori ed applicazioni differenti.

1.7 Incentivi

Rimane ancora la questione aperta su come evitare che si possa attaccare il sistema modificando un blocco passato. Perché ciò avvenga, sarebbe necessario che venisse rifatta la proof-of-work di quel blocco e di tutti quelli successivi sorpassando il lavoro dei nodi onesti.
In quest'ottica risulta chiave l'importanza di un sistema in cui i protagonisti siano *incentivati a perseguire un comportamento corretto*. Le misure previste sono, come già spiegato, le nuove monete "coniate" e il pagamento delle *transaction fees*.

Nakamoto ha esplicitato come dovesse avvenire l'emissione di nuova moneta. Era necessario dare un buon incentivo iniziale per far sviluppare il network, così è stato fissato a 50 bitcoin per blocco aggiunto alla catena. Le transazioni da convalidare erano poche, essendo pochi gli utenti interessati a scambiarli, e dunque quasi nullo il compenso derivante dalle fees.

Ogni 210 000 blocchi aggiunti alla catena, circa quattro anni [5], il compenso si dimezza dando al miner che risolve la POW un numero di bitcoins pari a 25, 12.5, 6.25 ...

Il numero massimo di bitcoin coniato sarà 21 milioni, teoricamente modellizabile dalla serie geometrica:

$$210000 \cdot 50 \cdot \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k = 210000 \cdot 100 = 21000000$$

Nella pratica, non avverrà che il numero di bitcoin tenderà asintoticamente alla cifra di 21 milioni, bensì ci sarà un momento in cui la ricompensa sarà zero e l'unico beneficio si avrà dalle transaction fees.

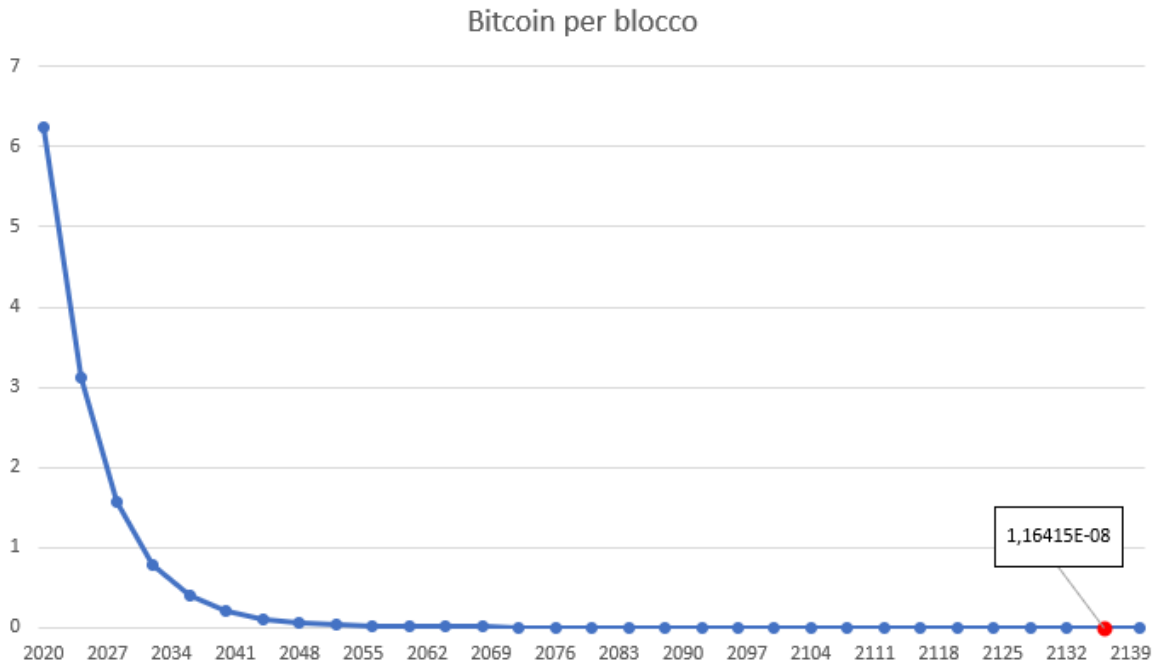


Figura 1.14: Ricompensa di bitcoin per blocco in base ai successivi dimezzamenti previsti.

Oggi sono stati minati oltre 18 milioni di bitcoin e il prossimo dimezzamento è previsto a Maggio 2020[6], passando ad una ricompensa di 6,25 bitcoin per blocco. In figura 1.14 si osserva che proseguendo con tale andamento, la ricompensa nel 2136

[5]Tempo stimato dal fatto che la velocità di mining viene settata periodicamente affinché venga aggiunto un blocco ogni dieci minuti.

[6]Halving avvenuto l'11 Maggio 2020.

sarà di $1,164 \cdot 10^{-8}$ bitcoin per blocco, soglia ancora accettabile in quanto la più piccola unità scambiabile è

$$1\, satoshi = 10^{-8} BTC$$

Il dimezzamento successivo a $5,82 \cdot 10^{-9}$ non sarà invece possibile. Da quel momento in poi non sarà più coniata nuova valuta e sarà scambiata solo quella esistente.

E' notevole osservare come il sistema stia effettivamente seguendo il modello voluto. Non è così banale se si pensa a difficoltà oggettive che nel tempo possono sorgere: mancanza di miner interessati a partecipare al gioco o di domanda da parte del mercato, malfunzionamenti che avrebbero potuto bloccare il sistema oppure renderlo incontrollabile, attacchi esterni. Tutto ciò non è avvenuto e si stima che per oltre il $99,98\%$ del tempo, dal 2009 ad oggi, Bitcoin abbia funzionato correttamente e senza interruzioni.

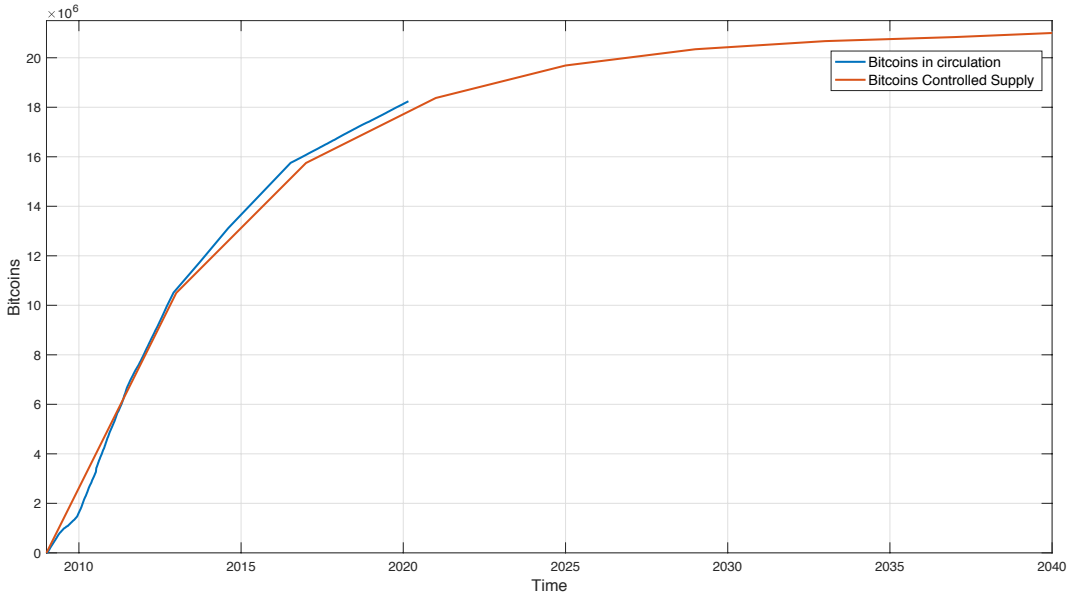


Figura 1.15: Distribuzione bitcoin desiderata VS Bitcoin in circolazione.

Non stupisce che nel primo periodo il mining dei blocchi fosse difficile da mantenere elevato: pochi utenti a conoscenza del protocollo, pochi convinti di spendere energia per dei bitcoins. E' possibile osservarlo dalla figura 1.16 dal fatto che i valori reali sottostavano quelli desiderati.

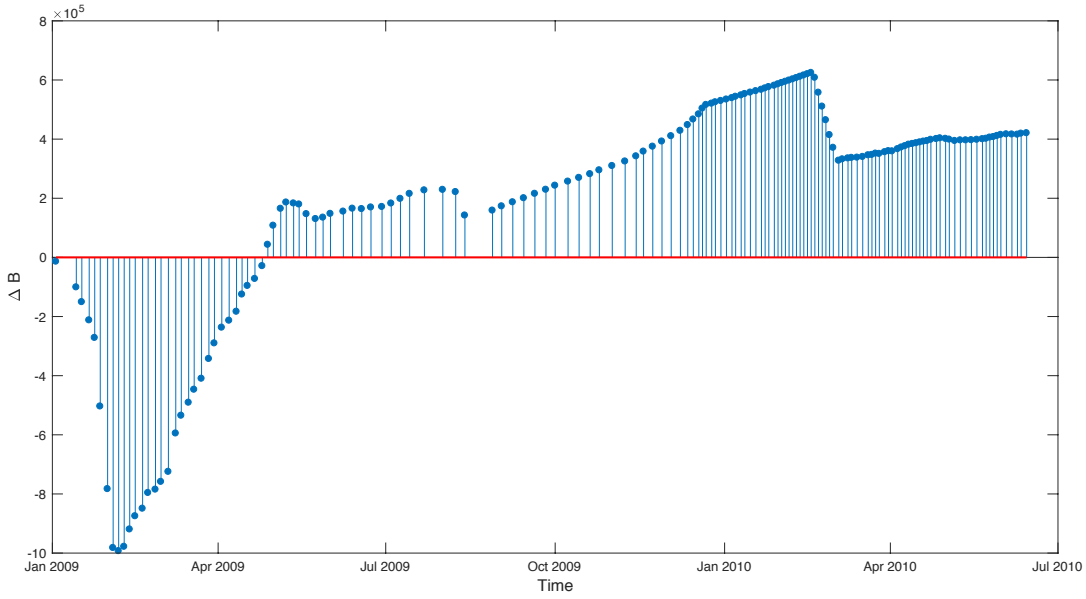


Figura 1.16: Delta fra "Bitcoins in circulation" e "Bitcoin Controlled Supply"

Passò poco prima che la tendenza si invertisse (intorno a Maggio dello stesso anno) e che fosse necessario un set continuo del livello di difficoltà per non far esplodere la curva.

Per il futuro ci si può aspettare un andamento simile alla previsione in figura 1.15 se continua la partecipazione e fiducia in Bitcoin, la domanda di mercato rimane elevata e i nodi partecipanti prediligono la correttezza. Che tutto ciò rimanga in perfetto equilibrio per centoventi anni è forse poco realizzabile.

Capitolo 2

Altcoin

2.1 Mercato delle criptovalute

2.675 *cryptocurrencies*, $ 268.140.662.115 di Market Cap, 22.739 mercati coinvolti. Questi sono solo alcuni dei valori riportati in data 14/06/2020 da *CoinMarketCap*, uno dei più citati website informativi in ambito *criptocurrency*.
Cifre talmente grandi da sorprendere forse anche lo stesso Satoshi Nakamoto, o forse no. Ad undici anni dal lancio della sua valuta, il mondo non solo sembra avergli dato fiducia, ma sta provando a replicare la sua impresa in tanti modi differenti.
Sono note con l'appellativo di *Altcoins*, *alternative coins*, tutte quelle valute alternative successive al lancio e alla diffusione di Bitcoin, con un pattern simile ma con network e blockchain specifici.

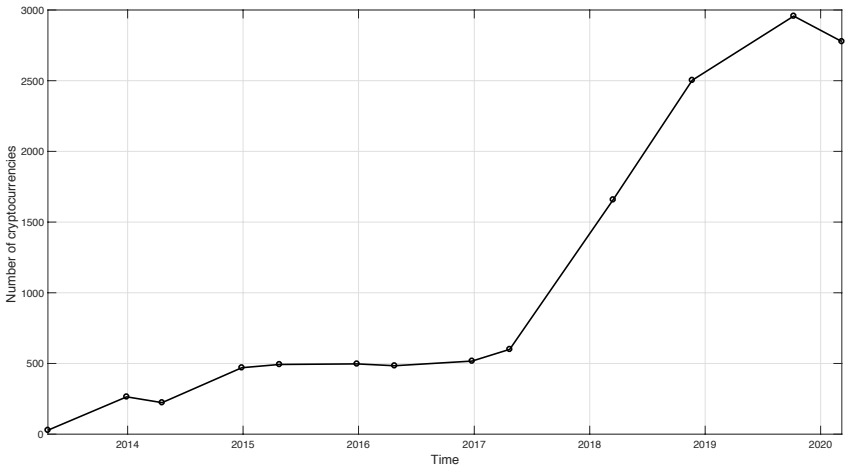


Figura 2.1: Numero di token, dal 2013 ad oggi.

Negli ultimi anni ne sono nate moltissime, alcune sviluppatesi con successo, altre della durata di qualche giorno e niente più.

Per un paio di anni, fino a metà del 2011, non ci fu alcuna valuta sul mercato. Poi nacque *NameCoin* e dal 2013 il fenomeno è cresciuto considerevolmente.

Sebbene interessante osservare come il numero sia cresciuto negli anni, seguendo anche la grandissima crescita del valore di Bitcoin fra il 2017 e il 2018, oggi (15/06/2020) più dell'85% della capitalizzazione è riconducibile alle Top 10 criptovalute.

Questo inevitabilmente sposta su di loro l'attenzione, sebbene va sempre tenuta in mente la dinamicità del settore, per cui chi riesce a prevederne i cambiamenti riesce ad avere guadagni oltre ogni previsione possibile.

Ciò che è certo è che queste vantano, come riportato, una capitalizzazione di mercato così grande da non poter passare inosservate.

Figura 2.2: Market Cap globale in milardi di dollari, dal 2013 ad oggi. Fonte [11].

Inoltre, l'innovazione di Satoshi Nakamoto sta pian piano entrando in ogni ambito della nostra vita: dall'*e-voting* alla musica online, dal *car sharing* alla compravendita immobiliare, alle assicurazioni. Non sono escluse sanità, *supply chain* e varie applicazioni in ambito giuridico. Ma questi sono solo alcuni ambiti in cui aziende di tutto il mondo, ma anche italiane, stanno puntando per rinnovarsi in ottica *blockchain*. Una vera e propria *digital trasformation* sta crescendo annualmente a ritmi molto sostenuti, aumentando sempre più i dispositivi connessi ad internet e fra di loro; in questo contesto la blockchain con le sue caratteristiche sta diventando lo

strumento prescelto per le comunicazioni di sistema. Spesso è opportuno che il protocollo si adatti all'applicazione, subendo modifiche anche strutturali, ma nessuno toglie mai a Satoshi la paternità di tale invenzione.

Oggetto della successiva trattazione sarà tuttavia il primo, e ancora ad oggi il più rivoluzionario, fra gli ambiti: **il mercato delle criptovalute.** Le sue ripercussioni in ambito finanziario, economico e sociale sono oggi più potenti che mai.
Di seguito saranno analizzate le più influenti attuali altcoin, trattate da *Young Platform* e disponibili per i suoi utenti: *Litecoin, Ethereum, Ripple, Stellar.* Nell'ultimo paragrafo viene infine presentata *Algorand*, recente blockchain oggetto di grande interesse internazionale.

2.2 Litecoin

Considerata da molti come la prima *altcoin*, fu lanciata il 7 Ottobre del 2011 da Charlie Lee, ex dipendente Google appassionatosi fin da subito al mondo Bitcoin, che ha lasciato il suo ruolo da programmatore per seguire totalmente la strada *criptocurrency.*
Tutte le altcoin sono state lanciate negli anni con uno specifico obiettivo; quello di Lee è ben chiaro: creare una moneta digitale sicura, decentralizzata e con tempi di validazione delle transazioni molto più veloci rispetto al modello Bitcoin.
La sua idea non è mai stata quella di competere, piuttosto affiancare ed essere complementare [17] a quello che per lui è un modello fondamentale.

"I wanted to create something that is kind of silver to Bitcoin's gold."

E' effettivamente un ostacolo all'utilizzo dei bitcoins come possibile metodo di pagamento nelle transazioni di tutti i giorni l'attuale lentezza nell'approvazione delle transazioni: come già esplicitato, i blocchi vengono minati ogni 10 minuti e, per la possibile presenza di biforcazioni, bisogna attendere la convalida di altri 5/6 blocchi per poter essere certi che la propria richiesta sia stata approvata. Questo ovviamente presenta delle difficoltà non banali e sarebbero necessari accordi più complessi per poter utilizzare i bitcoins per pagamenti veloci.

La visione di Lee è proprio quella di usare Litecoin come mezzo di pagamento per gli acquisti di ogni giorno (si pensi all'hashtag da lui lanciato sui social *#PayWithLitecoin*).
I punti di distacco da Bitcoin sono essenzialmente tre: protocollo di hashing, il tempo di transazione per blocco, numero totale di monete emesse. Per il primo punto è necessario una trattazione approfondita e dettagliata, affrontata nel successivo paragrafo **Scrypt**. Le ultime due sono considerazione di tipo qualitativo ed essenzialmente di continuità rispetto al protocollo Bitcoin.

Tempo di transazione e Numero di monete

La difficoltà di mining viene settata in modo tale che venga convalidato un blocco ogni 2.5 minuti circa. Inoltre, ogni blocco elabora un numero più elevato di transazioni, così da venire incontro all'esigenza di una criptovaluta adatta maggiormente alle transazioni correnti.
In analogia al rapporto di 1:4 nei tempi di mining *Litecoin* : *Bitcoin*, il numero di monete massimo in circolazione sarà quattro volte più grande, per l'appunto 84 milioni.

2.2.1 Scrypt

L'obiettivo iniziale di Litecoin era quello di evitare di centralizzare la potenza di calcolo in mano alle grandi *mining pool*, rendendo accessibile il mining solo da CPU. Bisogna però osservare che questo proposito da lì a poco venne meno, escludendo ancora una volta i singoli miner dal mercato.
Lo *Scrypt* è un alternativo protocollo di hashing e prevede diversi step (Fig.2.3):

1. dato il messaggio iniziale P a cui applicare lo Scrypt e S una stringa randomica, si calcola l'output di **PBKDF2**. In output si avranno p blocchi.

2. I blocchi vengono mixati fra loro e al loro interno con la funzione **ROMix** applicata un numero di volte pari ad N.

3. I blocchi in uscita vengono concatenati e utilizzati come S applicando nuovamente la funzione PBKDF2 su P.

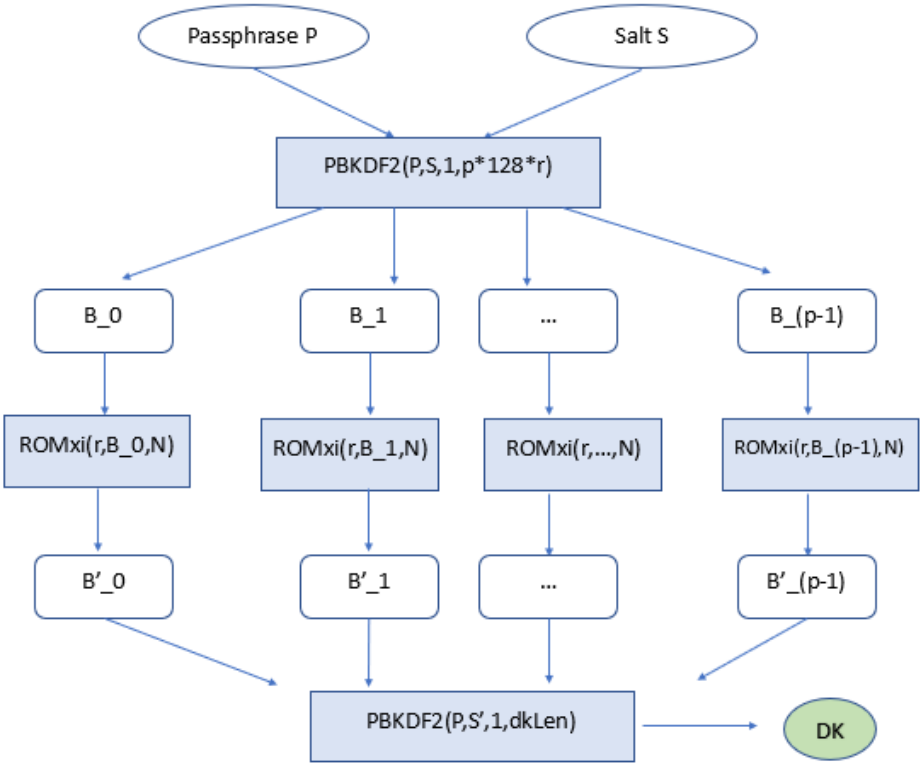


Figura 2.3: Diagramma Scrypt; $S' = B_0^{'}||B_1^{'}||\cdots||B_{p-1}^{'}$

Le due funzioni crittografiche erano già da tempo consolidate nella cultura crittografica e possono essere sintetizzate dai passaggi-chiave.

PBKDF2: una funzione crittografica che serve a ridurre la vulnerabilità dell'input iniziale da attacchi forza bruta generando una stringa della lunghezza desiderata.
Occorre definire prima cos'è *HMAC*.

Un algoritmo *MAC-Message Authentication Code* riceve una chiave segreta e un messaggio da autenticare restituendo un *tag*.
Una modalità per realizzare l'algoritmo è tramite l'applicazione di una funzione hash:

$$HMAC_K(M) = H((K' \oplus Opad)||(H(K' \oplus Ipad)||M))$$

K chiave, K' chiave adeguata alla lunghezza necessaria; Ipad e Opad costanti.

A questo punto è possibile esplicitare i passaggi della funzione PBKDF2.

$U_1 = HMAC_{256}(Password, Salt||INT_32_BE(i))$

$\vdots$

$U_c = HMAC_{256}(Password, U_{c-1})$

$T_i = F(Password, Salt, c, i) = U_1 \oplus \cdots \oplus U_c$

con $INT_32_BE(i)$ trasmissione di interi 32 bit in modalità big-endian (dal byte più significativo al meno significativo); c numero di iterazioni richieste; *dklen* la lunghezza desiderata; *hlen* la lunghezza dell'output della funzione F; $i \in \{0, \cdots, p-1\}$.

Infine si ricava la Derived key DK

$$T_1||T_2||\cdots||T_{dklen/hlen}$$

ROMix: ogni blocco in output dalla funzione PBKDF2 ha lunghezza $128 \cdot r$ bytes. Ognuno di questi viene visto come un array $[B_0, \cdots, B_{2r-1}]$ inizializzando $X = B_{2r-1}$. Per tutti i blocchi si aggiorna il valore di X [1]

$$X = Salsa20/8\,(X \oplus B_i)$$

$$Y_i = X$$

così da ottenere

$$X' = Y_0||Y_1||\cdots||Y_{2r-1}$$

Questi passaggi (*BlockMix*) vengono ripetuti tante volte quanto i passi di iterazione voluti. Seguono poi altrettante iterazioni in cui

$$j = Integerify(X')\, mod N$$

$$X = BlockMix(X' \oplus V_j)$$

con *Integerify* una funzione biettiva da $\{0,1\}^k$ a $\{0, \cdots, 2^k - 1\}$; V_j la $j - esima$ iterazione del *BlockMix*.

[1] Salsa20/8 è una variante de cifrario di flusso Salsa20 riducendo i cicli da 20 ad 8.

2.3 Ethereum

Nel 2013 lo scopo del giovanissimo programmatore di origini russe *Vitalik Buterin*, allora diciannovenne e impegnato attivamente nel mondo Bitcoin, era quello di modificarne il protocollo rendendolo più flessibile ed adatto ad un gran numero di differenti applicazioni decentralizzate: *dApps* [12].
Per rendere operativo il suo progetto, viene lanciata una pre-vendita di valuta *ether*; in quarantadue giorni sono stati raccolti 31 591 bitcoin [2].
La prima critica mossa agli *script* di Bitcoin è la seguente: sebbene il linguaggio di programmazione alla base può supportare diverse operazioni (schemi a soglia per firme digitali, forme di scambio fra criptovalute), c'è una grande famiglia impossibile da implementare: i **loop**. La scelta è stata presa appositamente per evitare che si potessero avere cicli infiniti nelle transazioni che potrebbero bloccare la rete. Contrariamente, Ethereum nasce come un linguaggio di programmazione **Turing-complete**, senza alcun limite nella scrittura degli *smart contracts*, bytecode di basso livello che elaborano in maniera deterministica il risultato in base alle informazioni raccolte dalle parti interessate e alle regole precedentemente definite. Possono riguardare tematiche differenti e da qui la duttilità del protocollo.
L'idea di base di Buterin era quella di non creare un nuovo sistema tutte le volte che occorre qualcosa, bensì un protocollo che può supportare qualsiasi tipo di applicazione, sostenuto da una criptovaluta.

2.3.1 Transazioni

Il modello Ethereum è costituito da *account* che mutano il loro *stato* attraverso le transazioni.
Ogni account è caratterizzato da un indirizzo di 160 bit e contiene quattro valori:

- *nonce*, contatore relativo alle transazioni effettuate dall'indirizzo;
- *bilancio* attuale di valuta **ether**, usata come commissione per le transazioni;
- *contract code* se presente, in particolare ne viene riportato l'hash;

[2] Rispetto al tasso di cambio di quel periodo, il valore era di circa 18 milioni di dollari.

- *storage*, vuoto di default.

I tipi di account sono due: quelli gestiti da chiavi private e quelli "da contratto", ossia controllati dal codice che viene eseguito quando sollecitati.
Come già introdotto, i codici non impediscono preliminarmente la presenza di loop. Questo di per sé è un problema in quanto un contratto potrebbe potenzialmente essere eseguito "per sempre". E' stato dimostrato da Alan Turing [3]che non esiste un algoritmo che possa dire a priori se vi sarà un loop nel codice, dato un determinato input così da scartarlo eventualmente. La soluzione proposta da Buterik è quanto segue.

Ogni **transazione** deve contenere le seguenti informazioni:

1. indirizzo del destinatario;
2. firma digitale del mittente, con lo stesso protocollo di Bitcoin ECDSA su SECP256K1;
3. quantità di ether da trasferire;
4. campo opzionale;
5. **start gas:** il numero massimo di step computazionali che la transazione può eseguire;
6. **gas price:** quanto deve essere pagato per unità di gas consumato.

Una transazione atta alla creazione di un contratto contiene anche un ulteriore campo **init**: un array contenente la porzione di codice che serve per inizializzare la procedura e che restituisce il **body**, frammento del codice che sarà eseguito quando richiamato. Ogni transazione ha un costo fisso di 21 000 gas.
Si aggiungono altri costi, come specificato nel Paper: ogni step computazionale

[3]Il *Teorema di Turing* afferma che esistono problemi non decidibili, per i quali cioè non ci sono algoritmi che riescano a dare risposte in tempi finiti. Uno fra questi è il *problema della terminazione*: capire se un algoritmo termina o continua la sua esecuzione all'infinito, dando un input finito.

solitamente costa 1 gas, ad eccezione di alcune operazioni più onerose (ad esempio il calcolo di SHA-3 costa 20 gas).
L'idea quindi è che fare seguire istruzioni deve essere oneroso, così che attaccanti esterni siano scoraggiati dal voler bloccare la rete con loop infiniti, pericolo reale in Bitcoin se non si fosse bloccata tale pratica.
Il gas price è scelto in maniera autonoma dai miners, analogamente alle transaction fee di Bitcoin.

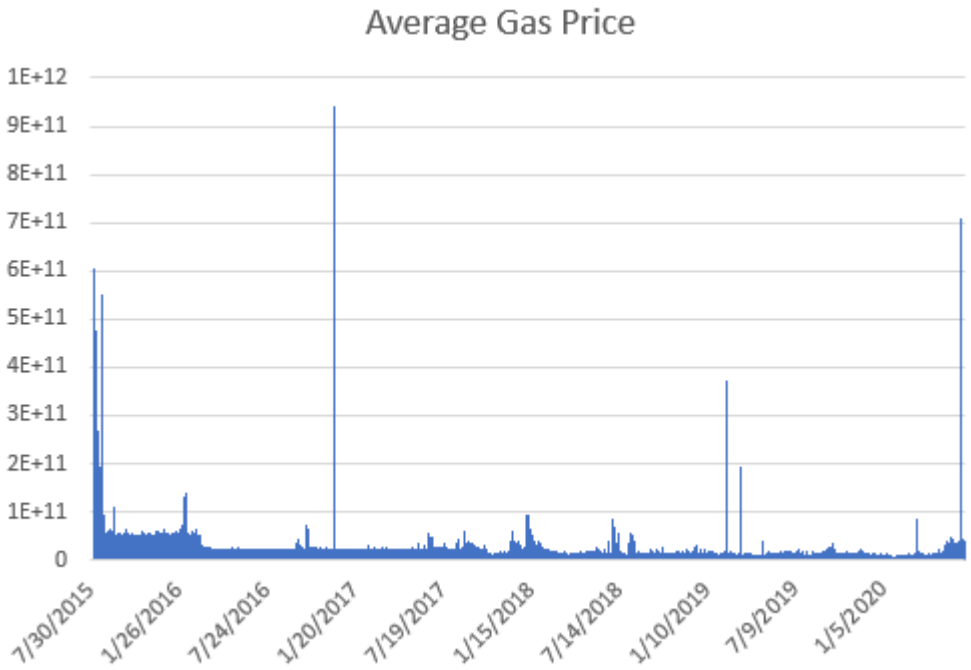


Figura 2.4: Average Gas Price in Gwei. Default 50 GWei$= 5 \cdot 10^{-8}$ ether $\sim 3 \cdot 10^{-10}$ bitcoin per unità di gas.

Ad eccezione di alcuni outlier, il valore medio del gas price è sostanzialmente stabile e tendente a valori più bassi, rispetto al primo periodo.

Gli *smart contract* possono comunicare fra loro scambiando **messaggi**, oggetti virtuali richiamati da *call* nel codice e caratterizzati dagli stessi campi di una transazione ad eccezione del gas price, in quanto si può considerare una sua sub-esecuzione e ne eredita il valore. In più i messaggi sono caratterizzati dal campo *data*, un array di lunghezza arbitraria che specifica i dati di input.
Richiamando la notazione del *Yellow Paper* [13], recente aggiornamento del primo

documento [12] con un numero maggiore di dettagli tecnici/metodologici, viene introdotta la nozione di ***final state***: insieme di tutte le informazioni utili al sistema quali bilancio di ogni account, dati delle transazioni, accordi di validazione e in genere tutto ciò che viene gestito dagli algoritmi del protocollo.
Le ***transazioni*** sono intese come un "valido arco fra due stati del sistema"; l'aggettivo *valido* riveste un ruolo fondamentale perché solo queste devono essere considerate. Υ è la notazione scelta nel Paper per identificare queste funzioni di transazione fra gli stati; σ la funzione che aggiorna lo *stato* del network, mapping fra gli indirizzi e lo stato degli account.
Lo schema della Blockchain Ethereum viene espresso formalmente:

$$\sigma_{t+1} \equiv \Pi(\sigma_t, B) \tag{2.1}$$

$$B \equiv (\cdots, T_0, T_1, \cdots) \tag{2.2}$$

$$\Pi(\sigma, B) \equiv \Omega(B, \Upsilon(\Upsilon(\sigma, T_0), T_1) \cdots) \tag{2.3}$$

con B blocco costituito da un insieme di transazioni T_i;
Π funzione di transazione applicata a livello di blocco, dunque composizione dell'applicazione della funzione Υ sulle singole transazioni.
In analogia a quanto visto per Bitcoin, ogni blocco contiene diverse informazioni nell'header (elencate in Appendice C) e una versione compressa delle transazioni al suo interno. E' interessante sottolineare non tanto i punti di continuità con Bitcoin, bensì le innovazioni portate al livello crittografico. Le principali sono due e sono trattate dettagliatamente: *funzione hash* e *merkle tree*.

2.3.2 Funzione hash

Un buon protocollo crittografico non può prescindere da un'ottima funzione hash. Mentre nel primo Paper [12] Buterik aveva fatto riferimento a SHA-256, nel lavoro [13], viene aggiornato il protocollo Ethereum con la recentissima innovazione proposta.

SHA 3-Keccak 256: vincitrice della competizione organizzata dal NIST nel 2007 per la ricerca di una nuova funzione crittografica e conclusa nel 2015. Keccak, creata

dal nostro connazionale **Guido Bertoni**[4] insieme a *Joan Daemen, Micheal Peeter, Gilles Van Assche*, fra le cinquanta proposte ritenute valide, è stata la funzione hash selezionata.

L'attacco a SHA-1 presentato nel 2005 dal professore *Wang* ha generato preoccupazione anche fra gli utilizzatori di SHA-2, essendo simile in diversi aspetti al precedente standard ed ereditandone dunque anche debolezze. Si è ritenuto necessario cercare un protocollo differente. Attualmente dunque SHA-3 non sostituisce SHA-2 in tutte le applicazioni, bensì ne fornisce un'alternativa.

La prima differenza sostanziale sta nel fatto che non è semplicemente una funzione hash, ma una **sponge function**: l'input può variare in $\mathbb{Z}_2^*$, ma anche l'output non deve essere di una lunghezza fissata bensì può variare in $\mathbb{Z}_2^n$, con n il valore richiesto. Come scritto in [14], questa scelta avvicina maggiormente al modello crittografico teorico del *random oracle* che ad ogni input fa corrispondere deterministicamente un vero output casuale e della lunghezza richiesta, in cui tutti i bit sono indipendenti ed identicamente distribuiti[5].

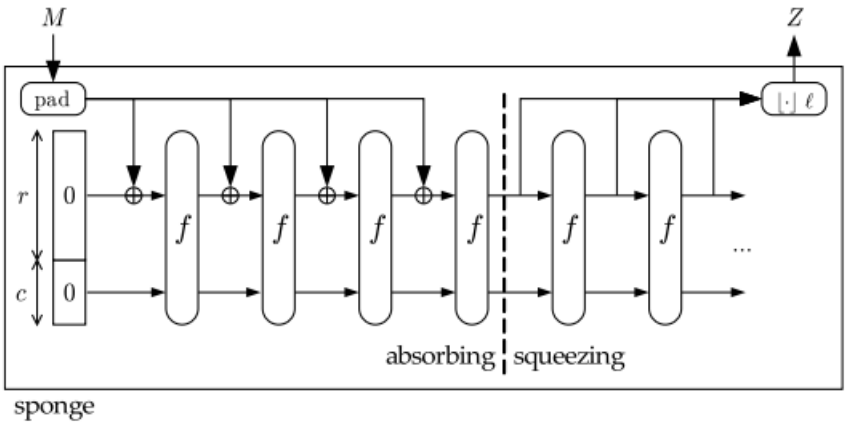


Figura 2.5: **Sponge construction**, Fig. 2.1 da [14]

[4]Guido Bertoni, ingegnere e professore di Crittografia al Politecnico di Milano, è CEO e cofondatore di *Security Pattern*. Inoltre ha partecipato a diversi lavori di ricerca e brevetti in ambito di sicurezza.

[5]Random Oracle è solo un modello matematico di riferimento, non implementabile realmente, preso come riferimento quando si vuole costruire un protocollo di funzione hash.

Come visibile in figura 2.5, la costruzione della funzione F di sponge si articola in due momenti:

1. **fase di assorbimento** in cui viene applicata più volte una funzione f di permutazioni all'output di opportuni XOR con determinati bitstring iniziali per tutti i blocchi del messaggio;

2. **fase di squeezing** in cui si applica più volte la permutazione f in modo da ottenere il numero di bits richiesti in output concatenando una parte dell'output precedente.

Fattori rilevanti del processo in figura 2.5 sono diversi.
Il primo passo è un **padding** adeguato del messaggio originale in una sequenza di blocchi da $r - bit$.

> Una regola di padding è *sponge*-compatibile se non dà mai in output una stringa vuota e se: $\forall n \geq 0$, $\forall M, M' \in \mathbb{Z}_2^* : M \neq M'$ allora
>
> $$M || \, pad[r](|M|) \neq M' || \, pad[r](|M'|) || \, 0^{nr}$$
>
> ovvero, dati due messaggi di lunghezza arbitraria, il padding dei messaggi $M || \, pad[r](|M|)$ ad una sequenza di blocchi da $r - bit$ deve essere differente, anche a meno di concatenazioni successive di blocchi di r $0 - bitstring$: $|| \, 0^{nr}$.

La regola di padding usata da Keccak è *Multi-rate padding*, o $pad10^1$, in cui si concatena un singolo bit 1 seguito da tanti zeri quanti occorrono perché la lunghezza sia il multiplo desiderato.

Contemporaneamente viene inizializzato lo *stato* con b bits uguali a 0. Questi però verranno trattati diversamente, separando i primi $r\,bit$ *rate* o stato esterno, dagli ultimi $c = b - r\,bit$. *capacità* o stato interno.
Tutti gli $r-$ blocchi del messaggio vengono messi in XOR con lo stato e poi concatenati con stringhe 0^{b-r}. Dunque la funzione f aggiorna lo stato e l'algoritmo viene iterato per tutti i blocchi.

Segue la fase di *squeezing* per ottenere una sequenza di lunghezza l.
Fino a quando la lunghezza non è quella richiesta, l'algoritmo continua ad applicare la funzione f, concatenando con i primi r bit dell'output precedente.

Una differenza sostanziale rispetto alle costruzioni hash precedenti sta nel fatto che un ipotetico attaccante vede solo la parte r dello stato, mentre non ha modo di interagire con c alterandola.
Inoltre la funzione f è una permutazione in quanto si conoscono molti risultati su come costruirle e quali livelli di sicurezza si mantengono.
La sicurezza del sistema non è determinato dalla dimensione dell'output, bensì dalla dimensione c della capacità: indipendentemente da quanti bit vengono estratti, un **livello di sicurezza** garantito è di $2^{\frac{c}{2}}$, ovvero non esistono attacchi migliori se non una ricerca esaustiva di tale dimensione.

L'algoritmo, definito dal NIST "elegante nel design" ed estremamente flessibile su diversi dispositivi e per diverse applicazioni, pone la sua forza nella funzione di permutazione **KECCAK-f(b)** f, con $b \in \{25, 50, 100, 200, 400, 800, 1600\}$, parametro precedente. SHA-3 usa $b = 1600$, con $r = 1088$ e $c = 512$; la sicurezza è di 2^{256}.
La funzione **f** è una costruzione iterativa di round nel numero

$$n_T = 12 + 2 \cdot l$$

con $2^l = \frac{b}{25}$. Ogni round, come spiegato nell'articolo [15], è costituito da una sequenza non invertibile di step eseguiti sullo stato in input.
Lo stato viene organizzato in un blocco 5x5 e di profondità w tale che $b = 25\,w$ e dunque $w \in \{1, 2, 4, 8, 16, 32, 64\}$. Lo standard è su 64 bit, ma si può adeguare la scelta all'applicazione desiderata.
Per ogni round si susseguono nell'ordine i seguenti cinque passi invertibili[6]:

[6]L'invertibilità degli step è un grande fattore di novità: rispetto alle costruzioni precedenti all'attaccante viene fornito il modo per invertire, ma questo non lo agevola nel rompere l'algoritmo.

- **Step Θ diffusione:** sia A l'input del round, lo stato settato in precedenza. Lo step prevede le seguenti operazioni in modulo 5

$$C[x] = A[x,0] \oplus A[x,1] \oplus A[x,2] \oplus A[x,3] \oplus A[x,4] \qquad \forall x \in \{0,1,2,3,4\}$$

$$D[x] = C[x-1] \oplus ROT(C[x+1],1) \qquad \forall x \in \{0,1,2,3,4\}$$

$$A[x,y] = A[x,y] \oplus D[x] \qquad \forall (x,y) \in (0,\cdots,4,0,\cdots,4)$$

con $ROT(X,r)$ che indica una rotazione di bit in X di passo r.
E' interessante vederlo graficamente

L'input di Θ viene aggiornato sommandogli i bit della colonna alla sua sinistra e della colonna a destra traslata di una posizione.

- **Step ρ e π dispersione:** i bit dello stato visti per colonna e in profondità e per riga, subiscono delle rotazioni, cambiando l'ordine su queste direzioni rispetto ad un centro fisso.

$$B[x,y] = ROT(A[x,y], r[x,y]) \qquad \forall (x,y) \in (0,\cdots,4,0,\cdots,4)$$

$$A[x,y] = B[y, 2x+3y] \qquad \forall (x,y) \in (0,\cdots,4,0,\cdots,4)$$

con $r[x,y]$ valori tabulati e presentati in Appendice D.

$$A[x,y] = A[(x+3y),x] \qquad \forall (x,y) \in (0,\cdots,4,0,\cdots,4)$$

- **Step χ non linearità:**

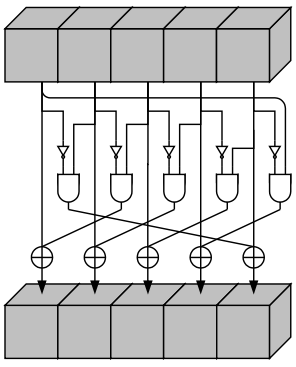


Figura 2.6: Step χ, Fig. da [14]

$$A[x,y] = A[x,y] \oplus ((NOT\, A[x+1,y])AND\, A[x+2,y]) \qquad \forall (x,y) \in (0,\cdots,4,0,\cdots,4)$$

Ogni output è funzione dello XOR fra il bit nella stessa posizione e dell'AND fra il successivo negato e il secondo successivo non negato.
Questa mappa permette di studiare in maniera abbastanza semplice come delle differenze in input si propagano, tenendo presente che è importante che ciò avvenga in maniera massiccia. L'attenta scelta dei parametri utilizzati ha permesso di evitare che l'inverso sia altrettanto semplice.

- **Step l rottura della simmetria:** infine viene aggiornato $A[0,0]$ con le costanti di rotazione RC[i] tabulate in Appendice D, al fine di rompere eventuali simmetrie presenti.

$$A[0,0,z] = A[0,0,z] \oplus RC[z]$$

2.3.3 Merkle Patricia Tree

La seconda differenza con Bitcoin sta nel modo in cui le transazioni vengono conservate all'interno di un blocco. Il problema logico di base è che il sistema non deve semplicemente permettere di aggiungere transazioni ed eventualmente cercarle. In Ethereum è necessario aggiornare frequentemente il valore dello stato (si pensi ad esempio al bilancio).
Il nome esteso è *Modified Merkle Patricia Trie*, noto appunto come Merkle Patricia Tree e rappresenta un modo più efficiente per l'inserimento, ricerca e cancellazione di transazioni.
E' un caso particolare di *radix tree* (figura 2.7), una struttura dati in cui le chiavi sono caratteri, così da memorizzare più agevolmente anche un database molto grande, controllando la presenza di una parola partendo dalla radice e ricostruendo la stringa.
Nel caso di Ethereum però questo sistema non sarebbe efficiente poiché si devono gestire stringhe di lunghezza notevole. Vengono allora apportate delle modifiche per ottimizzare l'algoritmo.
Ogni nodo è identificato dal suo hash (SHA-3). Inoltre, un nodo nell'albero può essere di quattro tipi:

- stringa vuota;

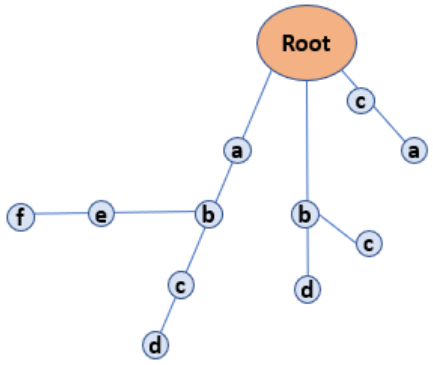


Figura 2.7: Segnalare diversamente i nodi finali serve per la ricerca nell'albero.

- *leaf* nodi con valori [key, value];
- *extension* nodi con due valori [key, value] dove il value è però l'hash di un altro nodo;
- *branch* nodi con lunghezza diciassette in cui i primi 16 elementi corrispondono a possibili caratteri nella chiave in esadecimale e l'ultimo elemento contiene una coppia [key, value]. La chiave è rappresentata dall'univoco indirizzo dell'account.

L'alfabeto utilizzato è l'esadecimale, quindi per ogni nodo avremmo 16 "figli" possibili. Se un flag di terminazione è "on", il nodo che si lega è *leaf* e il valore è quello a cui fare riferimento. Se invece è "off", allora l'hash del valore deve essere cercato nell'albero.

Un esempio può chiarire il procedimento.
Si immagini di voler aggiungere le seguenti transazioni espresse tramite le coppie [key; value] indicanti indirizzo e bilancio. Devono essere memorizzate nel block header facendo l'hash del *root node*.

$$[7c23553; 5.0] \qquad [7c6f134; 11.00]$$

$$[7c6ff93; 2.3] \qquad [7c24397; 0.01]$$

Per prima cosa viene identificata una radice comune alle chiavi da voler salvare, in questo caso "7c". Questa viene poi estesa in un branch node che contiene tutti i

possibili sedici caratteri della chiave. Le chiavi che continuano con "2" si estendono con la stessa logica precedente. Quando non hanno altro in comune quindi diventano leaf node completando la chiave e associando il value. Analogamente per "6". Il prefisso permette di riconoscere i nodi foglia e segue la legenda in Figura 2.8.

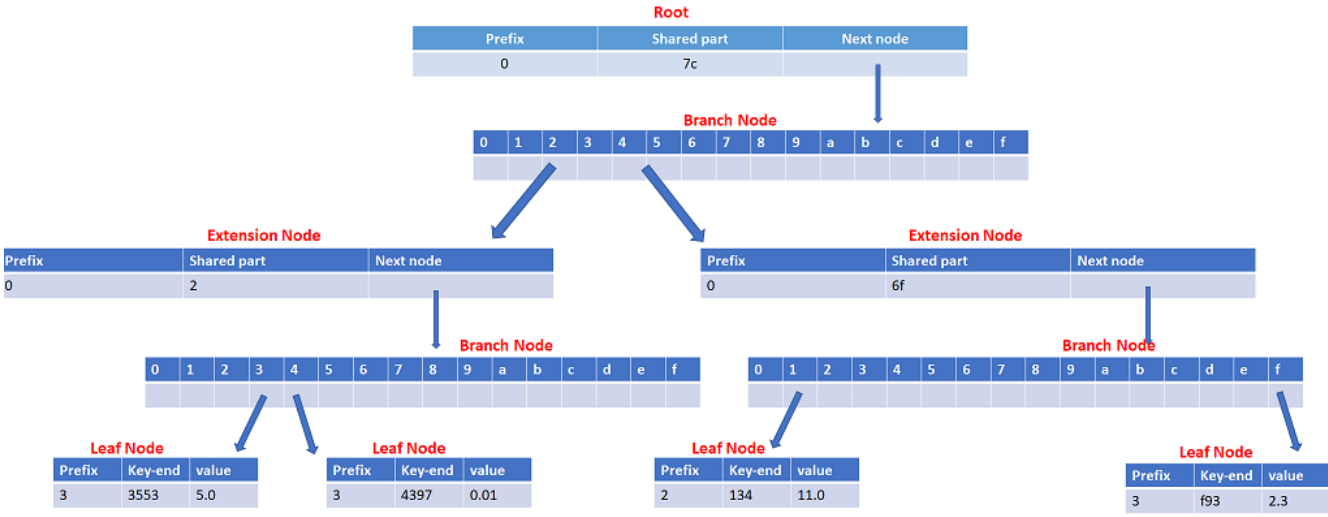


Figura 2.8: Esempio di Merkle Patricia Tree in Ethereum. Prefissi: 0 per Extension node con un numero pari di valori condivisi; 1 per Extension node con un numero pari di valori condivisi; 2 per Leaf Node con un numero pari di valori in comune; 3 per Leaf Node con un numero pari di valori in comune.

In questo modo, procedendo dall'alto, si potrà controllare il bilancio di qualunque di questi indirizzi.
Oltre allo *stateRoot*, il block header tiene traccia tramite Merkle Patricia Tree di *transactionsRoot* e *receiptsRoot* (transazioni ricevute).

Ritornando a [13], la validazione dei blocchi segue fino ad adesso un processo di *Proof-of-Work* simile a Bitcoin ma con alcune inevitabili differenze.
Un blocco B è costituito dal block header H, un insieme di transazioni T e un altro insieme di block header U a lui legati. Gran parte dell'informazione è racchiusa in H, per questo motivo la difficoltà di mining di un blocco viene definita in relazione

al block header H:

$$D(H) = \begin{cases} D_0 & se\, H_i = 0 \\ max(D_0, P(H)_{H_d} + x \cdot \zeta_2 + \epsilon) & altrimenti \end{cases}$$

con:

$D_0 = 131072$ la difficoltà del primo blocco;

$P(H) = KEC(RLP(B_H)) = H_p$ il *parent block's header* del block header H, da cui si ricava $P(H)_{H_d}$ la sua difficoltà;

la funzione *Recursive Length Prefix* RLP è il metodo usato per codificare dei dati binari trasformando in una sequenza di bytes adeguata per essere trasmessa.

$x \equiv \left\lfloor \frac{P(H)_{H_d}}{2048} \right\rfloor$;

ζ_2 parametro settato in modo da mantenere un tempo di mining adeguato;

$\epsilon \equiv \left\lfloor 2^{\lfloor H_i/100000 \rfloor - 2} \right\rfloor$ un tasso che cresce esponenzialmente ogni 100 000 blocchi.

L'aumento di difficoltà, oltre che per mantenere una certa velocità di mining, ha l'obiettivo di passare gradualmente dall'attuale *Proof-of-Work* alla *Proof-of-Stake*, nuovo paradigma di verifica.

Vanno validate ancora le condizioni sul gasLimit H_l:

$$H_l < P(H)_{H_l} + \left\lfloor \frac{P(H)_{H_l}}{1024} \right\rfloor$$

$$H_l > P(H)_{H_l} - \left\lfloor \frac{P(H)_{H_l}}{1024} \right\rfloor$$

$$H_l \geq 5000$$

Il gas usato H_g deve essere minore o uguale al gas limite H_l; il timestamp H_s deve essere maggiore del precedente $P(H)_{H_s}$ e i numeri identificativi del blocco devono essere incrementali $H_i = P(H)_{H_i} + 1$. Gli extraData H_x non possono occupare più di 32 bytes.

Solo dopo la verifica di tutte queste condizioni può essere eseguita la *Proof-of-Work.*

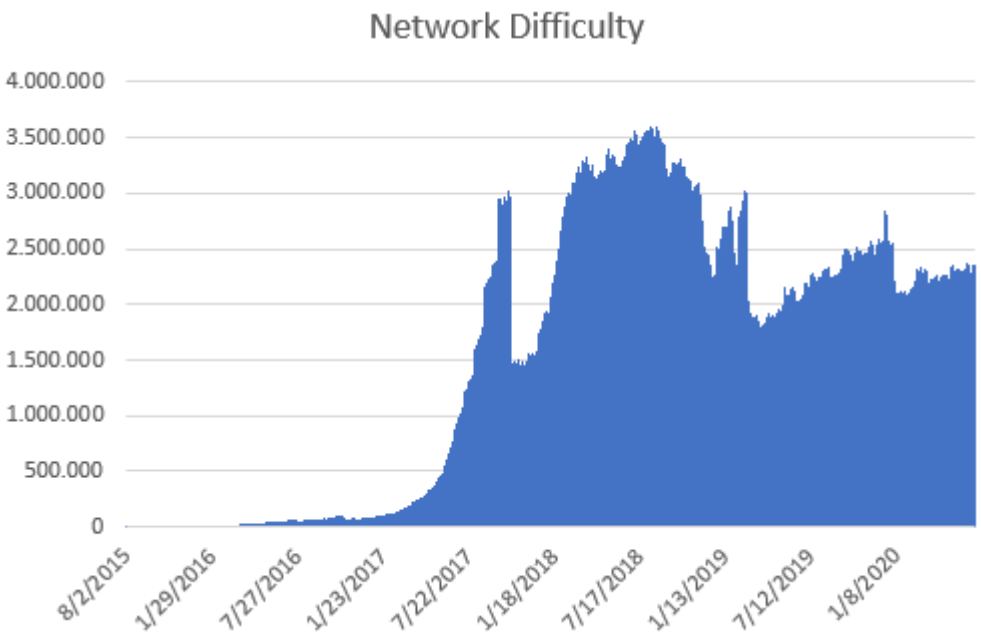


Figura 2.9: Variazione difficoltà nel tempo.

2.3.4 Ethash

Il Proof of Work sulla blockchain Ethereum è noto come **Ethash**. Così come per Bitcoin, i miner partecipano alla risoluzione di un problema matematico impiegando la loro potenza di calcolo. Gareggiano fra di loro per vincere la competizione aggiungendo alla catena un nuovo blocco con un certo numero di transazioni in attesa di approvazione o eseguendo un certo numero di smart contract. Le ricompense che ottengono vengono ancora una volta sia da delle commissioni che dagli attuali due ether per ogni blocco. La difficoltà è settata in modo da validare un blocco ogni 15 secondi.

Ci sono però dei punti di distacco significativi, attuati con l'obiettivo di rendere la validazione più veloce e dunque meno costosa, preservando lo stesso livello di sicurezza. Ulteriore obiettivo è quello di scoraggiare l'esecuzione parallela attraverso circuiti integrati in serie (ASIC), privilegiando i miners indipendenti nella direzione di una blockchain pienamente decentralizzata, rispetto alla centralizzazione che i mining pool stanno avendo nel network Bitcoin negli ultimi anni.
Ethash è un protocollo *memory-hard* caratterizzato da un file DAG *Directed Acyclic Graph*, un dataset aggiornato ogni 30 000 blocchi aggiunti, ossia ogni cinque giorni

circa. Questo periodo temporale è chiamato *epoca*.
La PoW per ogni nodo si articola nei seguenti passi:

1. A partire da un nuovo seme, hash del seme dell'epoca precedente, il miner crea una cache pseudorandom da 16 MB.

2. La cache viene utilizzata per generare il dataset DAG condiviso da ogni nodo.

3. Randomicamente vengono presi dei pezzi dal DAG e ne viene fatto l'hash cercando il nonce vincente per validare il blocco.

Il vantaggio principale è che il processo di controllo e verifica può essere effettuato con una quantità minima di memoria, memorizzando solo il contenuto della cache. In questo modo i grandi miners non hanno vantaggi evidenti rispetto a chi partecipa con una semplice scheda video GPU, in quanto sono stati minimizzati i *translation lookaside buffer*, memorie virtuali che appesantiscono il processo e che avvantaggiavano gli ASIC.
La velocità elevata del sistema, mista al tempo necessario affinché le comunicazioni vengano condivise da tutti i partecipanti al network, pone spesso il problema di blocchi "orfani", che nel caso di Ethereum prendono il nome di *uncle*. Capita spesso infatti che gli utenti continuino a lavorare su un blocco, non sapendo che era stato già validato. Per fronteggiare questo problema, Ethash prevede che i blocchi *uncle*, al più due per ogni blocco validato dalla catena, sono ripagati con 1/32 della ricompensa prevista[7]. Questi non riceveranno il compenso legato alle *fees* e devono avere un un antenato in comune con un "true block" almeno di settima generazione.
In questo modo vengono incentivati i miners che partecipano alla sicurezza della rete, anche se non vincenti, preservando la decentralizzazione.

Parte consistente del protocollo Ethereum risiede negli aspetti legati alle sue applicazioni di natura contrattuale e quindi nello Yellow Paper sono trattati dettagliatamente argomenti quali l'esecuzione delle transazioni, creazione dei contratti, messaggi ed esecuzione dell'*Ethereum Virtual Machine EVM*. Questi aspetti sono più lontani dal mondo criptocurrency.

[7]Fonte in Bibliografia [18].

2.4 Ripple

La quarta criptovaluta che è possibile gestire dai wallet *Young Platform* è *Ripple (XRP)*. Anche in questo caso, l'idea che ha portato alla fondazione dell'azienda e dunque alla diffusione della criptovaluta, è la volontà di rendere il sistema Bitcoin **più veloce**, difatti le transazioni vengono approvate in massimo cinque secondi.
Un'altra differenza sostanziale sta nell'aver reso possibile trattare **asset molto diversi** in maniera diretta, tracciando dunque non solo scambi di bitcoins.
Questo va nella direzione dell'eliminazione dei costi finanziari di intermediazione e la rottura degli schemi tradizionali (si pensi al necessario passaggio dal dollaro per alcuni scambi fra valute) evitando così i rischi e le perdite legate ad essi.
Ulteriore aspetto da sottolineare è che **non viene eseguito mining di valuta** per crearne nuova, bensì tutta la quantità prevista di 100 miliardi è stata già coniata. Ogni mese viene immesso nel mercato un miliardo di Ripple e dunque non è ancora interamente in circolazione.
Inoltre ogni transazione richiede un costo che può variare in base all'impegno del network per approvarla, così da evitare attacchi spam alla rete. Questi costi non sono diretti a nessuno, la valuta viene semplicemente distrutta. Dato che non ne viene coniata di nuova, il conseguente valore di chi detiene ripple aumenta.

Il sistema *Ripple Transaction Protocol RTXP* viene creato nel 2012, parallelamente alla fondazione dell'azienda *Ripple Labs* da parte di *Chris Larsen* e *Jed McCaleb*.
Ancora oggi il sistema è supportato da questa società ed è del tipo **permissioned pubblica**: l'utilizzo della rete è permesso a tutti, ma solo gli individui considerati fidati possono partecipare attivamente al protocollo di consenso.
Questo aspetto è fortemente criticato dai puristi *permissionless*, così come anche la vicinanza negli anni con banche e istituti finanziari. Negli anni *Santander, Union Credit, Axis Bank* e altri hanno investito in *Ripple Labs* dando luogo ad un'inevitabile collaborazione; una posizione troppo distante dalla volontà di eliminare le banche di Satoshi Nakamoto ed i suoi seguaci.

Il protocollo del consenso utilizzato da Ripple ha subito diverse evoluzioni fino alla sua struttura attuale profondamente diversa da quella Bitcoin. Non viene infatti annoverato o ricondotto a nessuna fra le *Proof* diffuse, ma segue un modello ideato negli anni '80 da *Lamport, Shostak, Pease* noto come *"Byzantine Generals Problem"*. L'obiettivo, allora come adesso, era di sviluppare un sistema di consenso condiviso in cui i partecipanti devono agire nello stesso modo evitando problemi nonostante alcuni attori potrebbero essere inaffidabili.

2.4.1 XRP Ledger Consensus Protocol

Così come per le altre criptovalute, l'obiettivo imprescindibile è mantenere un sistema autonomo in cui le transazioni fra gli stati dei partecipanti devono essere validate da tutto il network. Più nello specifico, il protocollo Ripple richiede che solo una determinata parte dei partecipanti debba dare la sua approvazione e questo motiva la maggior velocità del processo rispetto a Bitcoin.
Affinché ciò sia possibile, ogni utente deve definire una **UNL unique node list** di utenti di cui "si fida". Più queste liste si intersecano, più il sistema è sicuro. Inizialmente era stata settata una soglia di sovrapposizione pari al 20%. Successive analisi hanno innalzato tale livello al 40%.
Seguendo la notazione del Paper [21] tipica della teoria dei grafi, si identificano P_i i nodi del network, $\forall\, i$. Ognuno di questi specifica una sua UNL_i. Non viene richiesto che la relazione sia simmetrica, cioè può accadere che i, j tali che

$$P_j \in UNL_i \;\; \wedge \;\; P_i \notin UNL_j$$

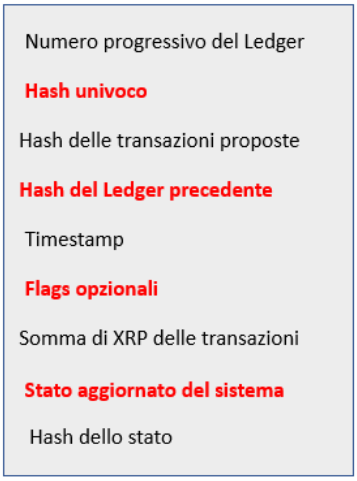
Più un nodo è presente in UNL differenti, più esso sarà influente.
Si definiscono:
$n_i = |UNL_i|$
$q_i = \lceil 0.8 \cdot n_i \rceil$ **quorum** che indica il numero minimo di nodi che devono dare il consenso affinché il nodo P_i possa prendere una decisione;
Si suppone $t_i \leq n_i - q_i$ nodi **Byzantine**, ossia *non onesti*.
Tutti i messaggi che P_i riceve dalla sua UNL sono autenticati con lo stesso algoritmo di firma digitale di Bitcoin *ECDSA* sulla curva secp256k1, ma il sistema è in grado

di adattarsi anche ad altri algoritmi, proprietà tutt'altro che banale. Si pensi all'avvento dei computer quantistici e alla possibilità che questi riescano ad attaccare i classici protocolli; la flessibilità ad un nuovo algoritmo, come ad esempio quello di *Shor*, potrà permettere a Ripple di "sopravvivere".
La funzione di hash utilizzata è *SHA-512Half*, ossia dall'output dell'hash SHA-512 vengono presi i primi 256 bit.

SHA-512: variante del protocollo *SHA-2* da cui eredita la struttura, restituendo in uscita un output a 512 bit.
Le differenze da sottolineare sono dunque quelle riferite alla lunghezza dei blocchi M_i da processare, non più di lunghezza 512, bensì 1024.
Conseguentemente anche i valori iniziali delle parole H^0 sono differenti, così come anche le sequenze di costanti $k(j)$ tabulati ed utilizzati nell'aggiornamento del messaggio. Tutto il resto, a meno dei necessari aggiustamenti di bit, è uguale a quanto presentato dettagliatamente per *SHA-256*.

Un nodo deve mandare necessariamente lo stesso messaggio a tutti i nodi che attendono da lui riscontro. Il network si definisce **fork-safe** se non è possibile che due nodi onesti convalidino transazioni in contraddizione fra loro.
Le principali componenti del protocollo sono tre:

1. **Delibera:** i nodi propongono delle transazioni da aggiungere al database, in base alle segnalazioni avute dal proprio network fidato UNL.



2. **Validazione:** gli stati del sistema, account e blocchi vengono aggiornati da tutti in maniera irreversibile quando ogni nodo raggiunge il quorum necessario, proponendo la validazione di un certo ledger L, l'insieme delle informazioni di stato condivise dalla rete, a partire da un precedente $\tilde{L}$. Il codice identificativo del ledger *seq(L)* deve essere incrementale rispetto al precedente.

   if $P_j \in UNL_i$ *then*
   $vals[L] = vals[L] \cup j$
   if $|vals[L]| \geq q_i$ *and* $seq(L) > seq(\tilde{L})$ *then*
   $\tilde{L} = L$
   end if
   end if.

   con *vals* funzione che manda L nell'insieme dei nodi che lo validano.

3. **Ramo da preferire:** in alcune circostanze in cui il network non sta procedendo correttamente, è necessario allineare la convalida così da aggiornare il *Ledger*.
   Ciò che l'algoritmo suggerisce è che i nodi devono optare per il ramo che è approvato da più partecipanti, alla stessa maniera delle biforcazioni in Bitcoin.
   Siano:
   L= il più recente ledger condiviso dal network
   C = array dei "figli" di L ordinato in maniera decrescente per $supp_{branch}$, numero dei nodi corretti che hanno validato i discendenti di L.
   $\Delta = supp_{branch}C[0]$.
   $uncommitted(s)$ è il numero di nodi che hanno convalidato blocchi fino al ledger numero s se $s < seq(L)$, altrimenti fino al ledger L.

   Iterativamente:
   if $|children(L)| > 1$ *then*
   $\Delta = \Delta - supp_{branch}C[1] + \phi(C[0, C[1]])$
   end if
   if $\Delta > uncommitted(seq(L) + 1)$ *then*

$L = C[0]$

end if

si seleziona il ledger con il più alto supporto anche se gli $uncommitted(s)$ fossero tutti orientati verso un'altra catena.

$$\phi(A, B) = \begin{cases} 1 & se\, hash(A) > hash(B) \\ 0 & altrimenti \end{cases}$$

funzione che preserva l'ordine della catena.

Se non vengono soddisfatte le condizioni allora viene restituito L, altrimenti si ripete iterativamente la ricerca sui discendenti del nuovo ledger trovato fino a quando non ci si ferma.

2.5 Stellar

Come per le precedenti criptovalute, una piena comprensione del protocollo e di cosa differenzia Stellar dalle altre è possibile solo dopo un'attenta analisi di quali idee e principi abbiano contribuito alla sua nascita.

Nel 2014 *Jed McCaleb*, uno dei due fondatori di *Ripple Labs*, lascia la precedente compagnia per fondare l'organizzazione no-profit *Stellar Development Foundation* con un obiettivo chiaro in mente: **rendere accessibile i servizi finanziari a tutti e a basso costo.**

Rispetto al "padre Ripple" dunque, si cerca di entrare nella vita quotidiana di tutte le persone, soprattutto nelle parti del mondo attualmente "unbanked", sostenendone lo sviluppo economico e finanziario.

Nei suoi primi sei mesi di vita, da Agosto del 2014, Stellar è stata un fork di Ripple, ereditandone di fatto tutte le caratteristiche tecniche già descritte. Successivamente i suoi utilizzatori hanno effettuato un update del codice introducendo novità che lo hanno allontanato dal protocollo del consenso di Ripple.

Una prima grande differenza fra i due sta nel fatto che Stellar, diversamente da Ripple che permetteva solo ad individui selezionati o organizzazioni di partecipare

al network, autorizza tutti ad essere membri del processo di consenso.
Non è possibile tuttavia non riconoscere la grande quantità di punti in comune. Viene descritto in dettaglio il suo protocollo di consenso basato, come in Ripple, sul *Byzantine Agreement*.

2.5.1 Stellar Consensus Protocol

E' necessario introdurre alcune definizioni e concetti ereditati dalla teoria *Federal Byzantine Agreement*.

Ogni nodo della rete v dichiara dei set di nodi chiamati **quorum slices** in modo che:

(a) se tutti i nodi del quorum slices concordano su un aggiornamento, allora tale è corretto;

(b) almeno un nodo della slice sia capace di apportare informazioni sugli stati del sistema.

Per ogni messaggio da inviare, ogni nodo specifica i suoi quorum slices. Si definisce **quorum** un insieme non vuoto di nodi S che comprende almeno un quorum slice di ogni membro onesto.

Definizione 2.5.1. *Due nodi non difettosi v_1, v_2 sono **intrecciati** quando ogni quorum slice di v_1 interseca ogni quorum slice di v_2 in almeno un nodo onesto.*

Definizione 2.5.2. *Un insieme di nodi I è detto **intatto** se I è tale che $\forall\, v_i, v_j \in I$ questi sono intrecciati, anche se ogni nodo fuori I fosse non-onesto.*

Definizione 2.5.3. *Sia v un nodo, un insieme **v-blocking** è tale se interseca ogni quorum slice di v.*

Quando i nodi propongono uno statement e questo viene accettato dal quorum, le modifiche andranno a propagarsi "in cascata" ai set di nodi intatti.

Teorema 2.5.1 (Cascade theorem)**.** *Se I è un insieme intatto, Q quorum per ogni nodo di I, e $S \supset Q$, allora o $S \supseteq I$ oppure c'è un nodo $v \in I$ tale che $v \notin S$ e $I \cap S$ è $v - blocking$.*

Il modello di votazione è noto come *Federated voting*: ogni nodo v può votare per uno stato a che non sia in contraddizione con i precedenti stati approvati e può accettare a se v è membro di un quorum in cui ogni nodo vota/accetta a oppure se un $v - blocking$ set accetta a.
Il Teorema assicura che due nodi intrecciati non possono confermare transazioni contraddittorie, arrivando così a convergenza su uno stato, sebbene si parta da votazioni diverse.

La rete implementata da Stellar per gestire scambi e pagamenti è costituita da quattro tipi di registri:

- **Accounts**, identificati da una chiave pubblica. La corrispondente chiave privata serve per firmare le transazioni. Inoltre contiene un numero sequenziale, alcuni flag e il bilancio in XLM (la criptovaluta di Stellar).
- **Trustlines** tracciano per ogni account e per ogni asset il bilancio, limiti ed ulteriori informazioni utili. Ad esempio alcuni istituti finanziari possono richiedere di risalire all'identità tramite un documento. Le trustlines possono settare un campo opzionale per quel specifico asset così da fornirne l'identità per quel bene e non per altri.
- **Offers** sono la disponibilità di un determinato account a scambiare un particolare asset ad un prezzo fissato. Domanda e offerta si incontrano così da poter effettuare lo scambio.
- **Account data** sono costituiti dalla tripletta account-chiave-valore.

Per evitare che si attacchi la rete creandone un numero spropositato, ad ogni account è richiesta una riserva minima di XLM. La funzione hash utilizzata è ancora una volta SHA-256.
Il modello è di tipo transazionale-atomico: gli account richiedono di effettuare certe operazioni pagando una fee[8] e vengono validate secondo i criteri accordati. Se

[8]Le fees sono pari a $10^{-5} XLM$ per transazione; salgono con un meccanismo di asta in caso di particolari congestioni.

qualsiasi problema impedisce il completamento, l'intera transazione viene annullata. Non vi è la figura del miner e quanto raccolto dalle fees viene poi distribuito proporzionalmente ai partecipanti.

Aggiornare o meno i registri condivisi con il contenuto di una nuova transazione richiesta è l'output del meccanismo di **consenso SCP**, costituito da due sotto-protocolli: *nomination* e *ballot*.
Nella nomination i nodi votano nominando uno (o più) statement x, valore di aggiornamento per gli stati e le transazioni. Quando viene confermato non sarà più possibile votare per nuovi valori. Ogni nodo poi potrà confermare o modificare x in base alle informazioni che riceve dagli altri nodi del quorum slice. Il processo di nomination è dunque dinamico e vedrà la conferma di un NOMINATE statement x. Se è vero che matematicamente si può raggiungere convergenza, è altrettanto vero che nella pratica spesso i tempi impediscono che ciò avvenga.

Successivamente si avrà il balloting, un protocollo di votazione che assicura ai nodi di propagare un valore di aggiornamento non contraddittorio rispetto alle precedenti decisioni e che rimangano coerenti per un determinato periodo di tempo.
In ogni votazione n viene proposto il federated voting su statement del tipo

$$\text{PREPARE} < n, x > = \text{gli statement con solamente il valore } x \text{ sono stati o saranno trattati in una votazione} \leq n.$$

Quanto un nodo conferma il PREPARE, allora si avvia il

$$\text{COMMIT} < n, x > = \text{gli stati con valore } x \text{ vengono discussi nella votazione } n.$$

I nodi hanno un certo periodo di tempo per confermare gli aggiornamenti, oltre il quale abbandonano la votazione.
Tuttavia spesso la sincronizzazione dei nodi può venir meno e per fronteggiare tale problema il protocollo prevede che venga avviato il timer solo quando il quorum sta votando per il ballot corrente. In questo modo vengono rallentati i nodi partiti in anticipo. Il teorema a cascata permette poi di rendere sincroni anche i nodi arrivati successivamente e con differente statement.

Lumens

La valuta nata insieme al progetto della Stellar Development Foundation è nota come **Lumens**, con simbolo **XLM**, e nel 2014 ne sono stati creati 100 miliardi. Per i primi cinque anni l'offerta di lumens è cresciuta dell' 1% all'anno, tasso che effettivamente ne ha rappresentato l'inflazione.
Nell'Ottobre del 2019 però la rete ha votato per delle modifiche al protocollo, riducendo la somma totale a 50 miliardi.
Attualmente, come riportato nel sito ufficiale [41], i lumens sul mercato sono circa 20 miliardi, mentre i rimanenti 30 sono ancora posseduti dalla fondazione.
Ancora una volta questo mette in discussione la piena decentralizzazione del protocollo.
Si era già citato come ogni account debba avere una minima quantità di valore, pari ad 1 lumen, così come per ogni transazione si deve pagare una tassa di almeno 0.00001 lumen. Sono quantità molto piccole e dunque si comprende la filosofia di una "finanza per tutti", ma grandi abbastanza da scoraggiare ipotetici attacchi alla rete.

Il principio economico alla base della disponibilità di valuta di Stellar è opposta rispetto a Ripple, in cui la quantità di valuta decresce nel tempo bruciando le transaction fee. Al contrario, Stellar segue una *politica inflazionista* in cui l'offerta cresce nel tempo e ciò esercita una pressione al ribasso sul prezzo di un lumen.
Il confronto con blockchain stile Bitcoin in cui vige una politica inflazionistica ma limitata nel tempo è meno diretto. Infatti, sebbene noto che per ogni blocco aggiunto alla catena il miner viene ricompensato con nuovi bitcoins che teoricamente dovrebbero portare ad una riduzione del valore, è altrettanto vero che gran parte della moneta è già in circolazione e, nella previsione che la quantità totale è quasi raggiunta, il valore di un bitcoin tende ad aumentare seguendo nella pratica un andamento deflazionistico.

2.6 Algorand

Un nuovo campo di ricerca, come lo è quello delle criptovalute e blockchain, pone sempre numerosi interrogativi. "Sarà una moda passeggera? Dove sono nascosti i problemi? Quali garanzie ci sono che il mio investimento non vada perso? Quanto posso fidarmi dei fondatori e degli sviluppatori?". A queste ed altre domande non è possibile dare risposte indiscutibili, ancora di più quando allontanarsi da un'autorità centrale rappresenta uno dei primari obiettivi e quando in gioco è il proprio denaro. E non a caso lo scetticismo del mondo economico, finanziario, politico ed istituzionale è ancora oggi preponderante e potremmo dire predominante.
Sono dubbi che anche i singoli investitori, persino i più coraggiosi e innamorati del progetto, non possono non avere.

Quando però si viene a conoscenza che questo mondo diventa oggetto di studi ed interesse non solo di giovanissimi programmatori in tutto il mondo, pieni di entusiasmo ma pur sempre privi di esperienza, bensì anche di grandissime autorità dell'informatica, uomini e donne con un background di decenni di studi intensi e risultati eccezionali, allora qualche certezza in più torna.
Quando poi tali personalità sono connazionali che hanno segnato la storia dello sviluppo della crittografia, eccellenze nel mondo riconosciute da premi importantissimi, un guizzo di orgoglio, stima e fiducia pervade ogni appassionato.
E' il caso di **Silvio Micali**, palermitano di origine e americano d'adozione, laureato in matematica a Roma e con un dottorato in informatica all'Università della California, uno delle menti italiane più brillanti (purtroppo) all'estero. I suoi riconoscimenti negli anni sono stati tantissimi, fino al *Premio Turing*[9] nel 2012 per i suoi studi sulla *teoria della complessità* nell'ambito della crittografia, la sua passione da sempre, arricchita dai suoi innumerevoli contributi dagli anni '80 in poi.

Come dichiarato in alcune interviste per *Forbes* e *Fortune*, non appena Micali lesse il paper di Satoshi subito ne colse la genialità e le prospettive brillanti. Alcuni

[9]Il Premio Turing è il riconoscimento più elevato per l'Informatica, paragonato spesso al Premio Nobel per altre discipline o alla medaglia Fields per la Matematica.

aspetti però gli apparsero subito da perfezionare e non a caso lui stesso si impegnò totalmente per formulare una soluzione a tali problemi.
Di lì a poco fondò insieme a dei colleghi dell'MIT **Algorand**, la sua piattaforma di scambio. Importanti imprese hanno investito nell'idea e alla domanda posta sul perché non abbia ricorso anche lui ad una ICO, la sua risposta è stata *"Credo che le ICO siano illegali, io voglio coinvolgere investitori accreditati"*.

Nel mondo Crypto vi è una discussione molto accesa nota come *trilemma*: non è possibile costruire una Blockchain in cui siano contemporaneamente valide le proprietà di **decentralizzazione**, **scalabilità** e **sicurezza**. Dal momento che nessuno sarà mai disposto a rinunciare alla sicurezza, la diatriba riguarda quanto un sistema sia scalabile o realmente decentralizzato.
Micali non è mai stato convinto della veridicità di tale affermazione e il suo lavoro mira verso la costruzione di una blockchain che scardini tale trilemma.

2.6.1 Pure Proof-of-Stake

Le novità che portano Micali ad affermare di aver risolto i problemi delle blockchain riguardano essenzialmente il meccanismo di consenso formulato.
I classici difetti del *Proof-of-Work* riguardano la scalabilità e la decentralizzazione che, a suo dire, non si può considerare raggiunta dal momento che, se si pensa ad esempio a Bitcoin, il mercato è governato da circa tre grandi mining pool[10]. Anche i fork, sebbene non malevoli, sono visti come un'ambiguità troppo frequente e che rallenta eccessivamente il protocollo.
Altri approcci come quelli basati sul *Byzantine Agreement*, come scritto nel paper [45], non sono adatti in quanto un potente avversario potrebbe corrompere gli utenti coinvolti nel set per la convalida di un nuovo blocco.

[10]Non tutti sono d'accordo con l'opinione di Micali secondo cui vi sia una mancanza di decentralizzazione. Al contrario è diffusa anche l'opinione che un'eventuale attacco sarebbe troppo costoso e controproducente per i miner stessi dal momento che i nodi onesti potrebbero forkare agevolmente su una nuova blockchain non appena colto il pericolo.

Il protocollo più vicino al lavoro di Micali è quello del **Proof-of-Stake**:

> Una quantità di moneta viene messa a garanzia; più questo *stake* è grande, più probabilmente quel nodo verrà scelto per "forgiare" un nuovo blocco. Aggiustamenti di selezione randomica vengono aggiunti ai protocolli per evitare che solo pochi nodi partecipino sempre alla validazione.

Le difficoltà legate a questo meccanismo del consenso sono evidenti: altissimo rischio di decentralizzazione, necessità di processi randomici adeguati, gestione di eventuali transazioni approvate con scopo fraudolento. Questi ed altri problemi hanno di fatto impedito alla Proof-of-Stake di diffondersi[11].
Algorand pone lì le sue basi per sfociare in quella che i fondatori stessi definiscono *Pure Proof-of-Stake*.

Il modello proposto prevede alcune assunzioni sulla rete:

- gli utenti del protocollo devono essere onesti per grande parte, ed in particolare si assume l'**Honest Majority** $> \frac{2}{3}$. Questo aspetto viene spesso criticato in quanto è una richiesta che, se non rispettata, potrebbe fare fallire la rete. Si ricordi ad esempio che tale percentuale è del 51% in blockchain tipo Bitcoin.

- **Honest Majority of Money** $HMM_k > \frac{1}{2}$, ossia in ogni round (unità logica di organizzazione di Algorand) gli utenti onesti possiedono più della metà di tutta la valuta del sistema al round $r - k$ precedente, $\forall r, k \in \mathbb{Z}$.

- **Power** distribuita su tutti gli utenti.

- **Message Propagation** Per ogni $\rho > 95\%$ e per ogni $\mu \in \mathbb{Z}^+$, esiste $\lambda_{\rho,\mu}$ tale che ogni messaggio m di μ byte inviato prima del tempo $t - \lambda_{\rho,\mu}$ avrà raggiunto nel tempo t almeno una frazione di ρ nodi onesti.

[11] Da anni Ethereum manifesta la volontà del passaggio alla Proof-of-Stake, attualmente ancora non avvenuto.

Procedura di selezione

Il primo passo del protocollo di consenso Algorand consiste nello scegliere un certo numero di utenti che saranno chiamati alla partecipazione attiva per un determinato *role*.
Era necessario che ciò dovesse avvenire in maniera randomica, altrimenti un avversario potrebbe cercare di corrompere i nodi che sa già voteranno.
Ogni utente è come se giocasse alla lotteria chiedendosi se è lui il "fortunato" a poter partecipare ad un round. Questa selezione come già detto, risente del proprio *peso* w nel network, misurato in termini di valuta posseduta.
Sia W la quantità totale di valuta in Algorand del sistema, τ la soglia per selezionare un certo numero di utenti per un determinato ruolo.
La probabilità di essere selezionato sarà $p = \frac{\tau}{W}$ per ogni unità di valuta.
Ogni utente calcolerà:

$$VFR_{sk}(seed||role) \rightarrow < hash, \pi >$$

con VFR_{sk} Verifiable Random Function che restituisce un output funzione della chiave segreta *sk*, il seme ed un ruolo specificato. Tale costruzione risale ad un lavoro dello stesso Micali insieme a Micheal Rabin e Salil Vadhan, nel 1999; l'obiettivo era quello di realizzare un generatore pseudocasuale che fosse anche verificabile, ovvero tale per cui il proprietario della chiave segreta potesse anche provare che è stato lui a valutare a funzione. Nulla in più deve essere mostrato e non deve essere compromessa l'impredicibilità dell'output per un nuovo valore in input.

La probabilità $P(k)$ che k unità della propria valuta w siano stati selezionati segue una distribuzione binomiale $B(w, p)$:

$$P(k) = \binom{w}{k} p^k (1-p)^{w-k}$$

con $\sum_{k=0}^{w} P(k) = 1$.
Ogni utente partecipa con le proprie valute; per sapere se e quanti sub-user sono stati selezionati (ovvero se e con quanti token si può partecipare al protocollo), viene diviso l'intervallo $[0, 1)$ in intervalli della forma $I^j = [\ \sum_{k=0}^{j} P(k), \sum_{k=0}^{j+1} P(k)\ )$ con $j \in \{0, 1, \cdots, w\}$.

Se $2^{\frac{hash}{hashlen}} \in [\ \sum_{k=0}^{j} P(k), \sum_{k=0}^{j+1} P(k)\ )$, allora l'utente parteciperà con j sub-users[12]. Tutti gli altri partecipanti del network potranno provarlo calcolando:

$$VerifySort_{pk}(hash, \pi, seed||role)$$

Il valore di ritorno è il numero di sub-user j dell'utente con chiave pubblica pk, 0 se l'utente non è stato selezionato.
Come già evidenziato in precedenza, questo metodo permette di selezionare gli user in base al loro peso e scelti in maniera casuale. Inoltre un avversario non sa in anticipo se un utente verrà selezionato e quante volte è scelto, non avendo accesso alla sua chiave privata sk. Solamente quando gli utenti selezionati cominciano a diffondere la prova insieme al proprio parere sul blocco da aggiungere un attaccante può provare ad attaccarli. Ma a quel punto, come lo stesso Micali spiega nelle conferenze e sui paper, "non è più possibile richiamare il messaggio, allo stesso modo di come un potente governo non possa celare un contenuto di WikiLeaks divenuto virale".

La scelta del seme *seed* deve essere gestita in modo da evitare eventuali attacchi. Per ogni round r deve essere selezionato in modo randomico e pubblico a partire dal seme del round precedente $r-1$. Ogni utente u selezionato per la convalida del blocco, propone un seed calcolando:

$$VRF_{sk_u}(seed_{r-1}||r) \rightarrow < seed_r, \pi >$$

Questa informazione verrà inclusa nel blocco così che tutti verranno a conoscenza del nuovo valore da utilizzare al round r.

Proposte e aggiunta di un blocco

Dopo aver accuratamente settato la soglia τ e selezionato un certo numero di partecipanti, ognuno di questi presenterà, insieme alla prova della selezione, un blocco di transazioni da aggiungere alla catena.
Quale fra le tante proposte selezionare però, deve essere deciso senza ambiguità e

[12] Hashleg è la lunghezza in bit dell'hash.

nel tempo più veloce possibile da tutto il network. Per farlo, viene ancora una volta utilizzata la *sortition hash*: per ogni sub-user vincente di un certo user i, la **priorità** di un blocco viene calcolata facendo l'hash dell'output (hash) del VFR concatenato con l'indice j del sub-user. L'user che propone un blocco con il valore di priorità più altro è il **leader** e, dopo opportuni controlli di verifica, la sua proposta sarà aggiunta alla catena.
Per evitare di appesantire il network, le informazioni vengono divise in due messaggi: un primo contiene la prova della selezione e del blocco proposto; il secondo messaggio contiene l'intero blocco. In questo modo l'informazione si propaga più velocemente selezionando il leader e solo successivamente attingendo alla seconda comunicazione.

Un aspetto da sottolineare ancora è il **tempo di attesa** che ogni utente deve rispettare prima di validare un blocco. Si comprende come settare tale valore troppo basso possa portare alla convalida, spesso, di blocchi vuoti. D'altra parte, aspettare molto tempo può implicare problemi al protocollo a discapito della scalabilità.
La convenzione è di attendere un tempo pari a $\lambda_{STEPVAR} + \lambda_{PRIORITY}$ in cui il primo addendo occorre per far sì che venga completato il round $r - 1$, il secondo è necessario per identificare la più alta priorità nel round r.
Simulazioni sperimentali hanno permesso di osservare che un tempo adeguato per evitare problemi ed essere efficienti è di circa 5 secondi per ognuno dei due parametri[13].

Agreement

A questo punto inizia la seconda fase del protocollo che permette di raggiungere un accordo. In particolare vi sono due possibili esiti: o si approva il blocco proposto oppure si andrà avanti aggiungendo un blocco vuoto alla catena.
Per prima cosa un'ulteriore selezione, nella modalità descritta in precedenza, permette di formare una commissione votante.
Essenzialmente ciò che ogni nodo selezionato deve fare è contare quanti messaggi

[13]Informazioni dettagliate sulla valutazione dei parametri si possono trovare nel paper [46], §10.

riceve; sia

$$\#_i^s(v) = n$$

il numero di volte che i riceve il valore v nel round s. Nel caso specifico 0 e 1 sono codifiche per le due scelte possibili (blocco proposto o blocco vuoto).
Sia t il numero massimo di partecipanti non onesti; $lsb(x)$ è la funzione che restituisce il bit meno significativo di un input binario x.
Vengono effettuati loop costituiti da tre step in cui i giocatori si scambiano valori booleani. Un contatore γ registra quante volte un loop completo è stato eseguito.

PROTOCOLLO AGREEMENT

STEP 1: *Ogni nodo i manda il messaggio b_i.*

1. *Se* $\#_i^1(0) \geq 2t+1$ *allora* $b_i = 0$, *invia* 0^* *e* $out_i = 0 \longrightarrow STOP$
2. *Se* $\#_i^1(1) \geq 2t+1$ *allora* $b_i = 1$
3. *Altrimenti* $b_i = 0$.

STEP 2: *Ogni nodo i manda il messaggio b_i.*

1. *Se* $\#_i^2(1) \geq 2t+1$ *allora* $b_i = 1$, *invia* 1^* *e* $out_i = 1 \longrightarrow STOP$
2. *Se* $\#_i^2(0) \geq 2t+1$ *allora* $b_i = 0$
3. *Altrimenti* $b_i = 1$

STEP 3: *Ogni nodo i manda b_i e la firma $SIG(r, \gamma)$.*

1. *Se* $\#_i^3(0) \geq 2t+1$ *allora* $b_i = 0$
2. *Se* $\#_i^3(1) \geq 2t+1$ *allora* $b_i = 1$
3. *Altrimenti, dato* $S_i = \{j \in N$ *che hanno mandato un messaggio nello STEP 3* $\}$, *allora i setta* $b_i = lsb(\min_{j \in S_i} H(SIG_i(r, \gamma)))$, *viene aumentato di 1 e si ritorna allo STEP 1.*

Il protocollo si può generalizzare in più step, fino ad un certo MAXSTEP settato e un TIMEOUT di riferimento.

2.6.2 Dettagli tecnici

L'implementazione di questi protocolli richiede alcune informazioni tecniche.
Sempre in [46], viene esplicitato che la funzione hash utilizzata è **SHA-256**; la curva su cui costruire la firma digitale e VRF è **Curve 25519**; la VRF è quella descritta nel lavoro [47], §4.
La funzione SHA-256 è stata già descritta in dettaglio nel Capitolo 1, gli altri due aspetti necessitano invece una trattazione approfondita.

Curve25519

La curva ellittica utilizzata nel protocollo di firma digitale e nella funzione VFR in Algorand è *Curve15519*:

$$y^2 = x^3 + 48662\,x^2 + x$$

E' stata presentata per la prima volta nel 2005 da Bernstein. definita *state-of-the-art* delle curve ellittiche, e negli anni ha acquisito maggior rilevanza ed interesse internazionale. La sicurezza è stata a lungo testata e nel 2017 viene approvata dal NIST come curva ellittica utilizzabile dal governo americano.

Il campo su cui giace la curva è definito dal primo $q = 2^{255} - 19$, con punto base $(x, y) = (9, y)$.
Il numero dei punti della curva è, come atteso, molto grande e pari al primo: $p = 2^{252} + 27742317777372353535851937790883648 93$.
Le chiavi pubbliche e private sono molto brevi, solo 32 bytes, benché la sicurezza del logaritmo discreto su curva ellittica è molto elevata.

Rispetto alle curve ellittiche di Weierstrass, descritte di cui è stata portata la descrizione di Secp256k1 nel Capitolo 1, le curve di *Montgomerry* sono della forma

$$B\,y^2 = x^3 + A\,x^2 + x$$

e vantano calcoli molto veloci sui suoi punti.
In particolare le operazioni di somma e duplicazione, dati $P = (x_P, y_P)$ e $Q(x_Q, y_Q)$ punti sulla curva, sono le seguenti:

- somma P+Q=R :

$$x_R = \frac{B(y_Q - y_P)^2}{(x_Q - x_P)^2} - A - x_P - x_Q$$

$$y_R = \frac{(2x_P + x_Q + A)\,(y_Q - y_P)}{x_Q - x_p} - \frac{B(y_Q - y_P)^3}{(x_Q - x_P)^3} - y_P$$

- duplicazione P+P=R:

$$x_R = \frac{(x_P - 1)^2}{4x_P\,(x_P^2 + Ax_P + 1)}$$

$$y_R = \frac{(2x_P + x_P + A)\,(3x_P^2 + 2Ax_P + 1)}{2B\,y_P} - \frac{B(3\,x_P^2 + 2A\,x_P + 1)^3}{(2B\,y_P)^3} - y_P$$

Verifiable Random Function

Si è già citato il largo uso che Algorand fa di questa funzione. Il primo lavoro su queste Verifiable Random Functions venne pubblicato da Micali, Rabin e Vadhan nel 1999. Prima di allora, infatti, le funzioni pseudorandom esistevano ed erano note come *pseudorandom oracle* perchè, senza ricevere informazioni sia sul seme iniziale che sul valore x : $f(x) = z$, non era possibile distinguere z da una stringa random della stessa lunghezza. Dunque in nessun modo risulta verificabile il calcolo eseguito e il ricevente deve fidarsi che è stato effettuato a partire da un certo seme s.
Questo chiaramente pone molte limitazioni e sarebbe quasi del tutto inutile in questo contesto. Diversamente le VRF richiedono una chiave pubblica pk per ogni utente, tale per cui un unico valore v è possibile provare sia il valore di $f(x)$ (e dunque chiunque può verificare la correttezza del calcolo). Più formalmente:

Definizione 2.6.1. *Una funzione **VRF** richiede una coppia di chiavi (pk, sk), rispettivamente chiave pubblica e privata, tale che solo chi possiede la chiave privata sk può calcolare l'hash in un input α:*

$$\beta = F_{sk}(\alpha)$$

mentre tutti coloro che vedono la chiave pubblica pk devono essere in grado di verificarla.
*La proprietà di essere **pseudorandom** garantisce che β sia non distinguibile da*

un'altra stringa casuale. Solo chi possiede la chiave privata sk può farlo e tale prova va mostrata:

$$\pi = \Pi_{sk}(\alpha)$$

In letteratura sono state formulate diverse costruzioni di funzioni VFR, quella che Algorand adotta è quella costruita sulla *curva ellittica Curve25519.*
Sia p primo, ordine del gruppo ciclico Z_p e con un generatore g.
p, g, Z_p sono parametri pubblici. H la funzione hash che mappa stringhe di bit di lunghezza arbitraria nel gruppo ciclico Z_p.
La chiave segreta è un numero randomico $x \in \mathbb{Z}_p$; la chiave pubblica è la coordinata x del punto sulla curva $P = x\,G$, con G punto base $= (9, y_G)$ della curva.

Protocollo di VRF:

- *A partire dall'input α, trovare l'elemento del gruppo Z_p con una funzione hash adeguata $h(\alpha)$ e sia H il corrispettivo punto sulla curva*
- *Calcolare il punto della curva $\Gamma = x\,H$*
- *Scegliere un nounce $k \in \mathbb{Z}_p$*
- *Calcolare $c = h(G, H, xG, xH, kG, kH)$*
- *Sia $s = k - cx\,mod p$*
- *Mandare la coppia prova/hash:*

$$\pi = (\Gamma, c, s) \qquad\qquad \beta = H_2(\Gamma)$$

H_2 restituisce in output la coordinata x del punto sulla curva ellittica.
Ognuno dei punti della curva individuati viene espresso con una point compression rappresentando soltanto l'ascissa, di 256 bit, più un singolo bit che indica se la coordinata y è positiva o negativa.
Verifica del protocollo VRF:

- Calcolare $u = c\,(xG) + sG$, con xG chiave pubblica. Notare che $kG = u$.
- Dato α input, calcolare $h(\alpha)$ e H come prima;

- Calcolare $v = c\Gamma + sH$ considerando sempre solo la coordinata delle ascisse.
- Verificare che $c = h(g, H(\alpha), xG, \Gamma, c(xG) + sG, c\Gamma + sH)$
- Infine provare che $\beta = H_2(\Gamma)$.

2.6.3 Moneta e Applicazioni

E' ormai ben noto come una blockchain si leghi inevitabilmente ad una intrinseca criptovaluta. Algorand non fa eccezione e la valuta digitale coniata è **Algo**. L'obiettivo, ancora una volta, è quello di delineare una rete di incentivi e linee guida a sostegno della stabilità del protocollo. Ogni decisione su modalità e tempi in cui gli Algos entrano nel sistema è presa da tutta la comunità.
La quantità totale di valuta coniata nel primo blocco è di 10 miliardi. La distribuzione aggiornata a fine 2019 può essere osservata in figura **??** in base ai dati forniti da [49] e mostra che una buona percentuale non è stata ancora distribuita ma si trova nelle mani dell'azienda.

Distribuzione di Algo	
3.0 miliardi	Ricompensa ai leaders
2.5 miliardi	Valuta venduta
2.0 miliardi	Incentivi e supporto
2.0 miliardi	Algorand Inc.
0.5 miliardi	Algorand Foundation

Una decisione presa e dichiarata sul sito è quella di vendere non più di 150 milioni di Algos nel 2020. Ogni volta che viene completato un round, l'utente che ha aggiunto il blocco alla catena verrà ricompensato. Questo non avviene istantaneamente ma ogni 500 000 round (un periodo), circa ogni 26 giorni. Per i successivi periodi stabiliti (fino ad Ottobre 2020), il compenso da dividere sarà di 13 milioni di Algos ognuno.
In una serie di competizioni, concorsi ed eventi che permettono la crescita della comunità, viene messa in palio una certa quantità di valuta da vincere.

Periodicamente vengono pubblicati sul sito ufficiale dei Report a favore di una piena trasparenza sulla distribuzione della moneta. L'ultimo pubblicato copre il periodo dal 2 Novembre 2019 al 10 Febbraio 2020 durante il quale sono avvenuti i seguenti movimenti in Algo:

- 101 milioni sono stati distribuiti come ricompensa a tutti i possessori di valuta per la partecipazione alla blockchain.
- 17 milioni distribuiti alla comunità a supporto dello sviluppo della stessa.
- 7,4 milioni come ricompensa ai nodi leaders.
- 125 mila per pagamenti ai membri della Foundation e dei comitati direttivi.
- Altre spese sono pari a 312 mila Algos riconducibili a promozioni e partnership.

L'attenta gestione della criptovaluta sul mercato permette un controllo dell'inflazione e del rapporto domanda/offerta. L'obiettivo finale è quello di mantenere il valore di un Algo il più stabile possibile perché, come lo stesso Micali spiega in alcune conferenze, non si può pensare di utilizzare una moneta per le attività di tutti i giorni se questa cambia continuamente e di molto il suo valore. Ad eccezione della fase iniziale, il prezzo di una unità si è mantenuto entro certi valori, seppur oscillando sensibilmente[14]. Attualmente[15] il valore è di circa €0,2168.

Figura 2.10: Andamento dei prezzi di Algo, fonte [11]

[14]Il ritorno medio a cinque giorni $-4,2\%$.
[15]In data 11/06/2020, fonte [11].

Applicazioni

La community di Algorand, guidata sempre dal fondatore Silvio Micali, non ha come fine ultimo la diffusione di quella che abbiamo presentato come la moneta Algo. Come in tutte le blockchain assume indiscutibilmente un valore importante e assicura stabilità al protocollo e alla rete, nonché strumento per la decentralizzazione della finanza .
D'altra parte però le priorità degli appassionati Algorand mirano nella direzione di strumenti da tempo sotto l'egemonia Ethereum, ovvero gli Smart Contract. L'obiettivo è espandere sempre più i processi e le applicazioni decentralizzate che possono essere fornite tramite la piattaforma di Algorand, applicandoli a diversi contesti.
Molte grandi aziende si stanno interessando ad Algorand e tanti progetti stanno avviandosi sulla piattaforma. Fra questi se ne citano due, presentati anche in articoli divulgativi del *Sole24Ore*.

SIAE: *Società Italiana degli Autori ed Editori*, ha stipulato un accordo con Algorand il 6 Dicembre 2019. Dal 1882 l'azienda si occupa della protezione del Copyright di artisti, autori ed editori, garantendo il giusto compenso per i loro lavori quando utilizzati da terzi o diffusi.
Il Manager Gaetano Blandini ha ben chiaro che il futuro offre nuove tecnologie che garantiscono efficienza e trasparenza. Da qui l'interesse per un mondo innovativo che permetterà di gestire vecchie e nuove esigenze.

PlanetWatch: spin-off del CERN di Ginevra che ha richiesto la blockchain di Algorand per un obiettivo ambizioso e di estremo interesse globale. Si tratterà di realizzare un ledger distribuito ed incorruttibile, per l'appunto, con registrazioni sulla qualità dell'aria attraverso registrazioni effettuate da partecipanti in tutto il mondo.
Gli incentivi per chi vorrà contribuire alla blockchain di Algorand con sensori nelle proprie abitazioni o mezzi di trasporto sono degli utility token specifici dal nome PLANET. Un cambiamento epocale per dati importantissimi, da sempre registrati in maniera discontinua ed estremamente costosa.

Capitolo 3

Analisi comparativa

Lo scenario attuale del mercato delle criptomonete è tanto eterogeneo quanto dinamico. Sono tantissimi i tentativi riusciti, così come quelli presentati ma mai lanciati realmente. Come in ogni contesto la *fortuna* ha un ruolo determinante, bisogna essere *"nel posto giusto al momento giusto"*, riuscendo a convincere gente da tutto il mondo che la propria idea è valida.

Il modo in cui spesso i progetti prendono vita è la raccolta fondi su internet in *crowdfunding* che nel caso delle criptovalute spesso è una vendita di moneta ancora prima che sia realmente coniata, così da permettere di sviluppare il progetto nella sua interezza.

Può sembrare incredibile come si possa comprare qualcosa che ancora non esiste, investendo denaro reale in un bene inesistente e che potrebbe non vedere la luce mai. Perché non attendere che venga lanciata sul mercato, ad esempio?

La motivazione probabilmente risale ancora una volta alla madre di tutte le criptocurrencies, Bitcoin. Hanno avuto un guadagno enorme i primi che hanno creduto nel progetto, che hanno minato o acquistato bitcoin ad un prezzo relativamente basso ma senza alcun tipo di garanzia in quel momento.

Fino alle porte del 2017 il prezzo era quasi sempre stato sotto i 700 dollari per bitcoin, forse ancora alto per tanti, ma nulla se si pensa al valore che da lì a qualche mese avrebbe raggiunto: oltre 17 000 dollari per bitcoin.

E l'enorme impatto per i possessori si comprende ricordando che vi erano già oltre 15 milioni di token nelle tasche dei (pochi) fortunati.

Figura 3.1: Prezzo Bitcoin dal 3 Gennaio 2009 al 19 Marzo 2020, fonte [9].

L'entusiasmo comune dovette allora fare i conti con l'inevitabile crollo dei prezzi imminente e come sempre, affianco a enormi guadagni, si ebbero spaventose perdite[1].

L'insegnamento per gli appassionati del settore fu: "arriva prima degli altri". Da qui la corsa alla ricerca della nuova moneta-oro, il tentativo di finanziare tanti progetti, magari con piccole somme, sperando che uno di questi diventi il successore di Bitcoin. Con una domanda così alta da parte del mercato, si spiega anche l'alta offerta continua di nuovi progetti su cui puntare.

Se da un lato i guadagni più grandi richiedono un grande rischio e numerosi salti nel buio, tantissimi altri investitori sono interessati allo scambio di valute già in commercio. Quale moneta acquistare, quando e in che misura è sicuramente poco semplice da dire.
Young Platform gestisce le quattro monete descritte in dettaglio e le numerose differenze riscontrate fanno comprendere quanto variegato possa essere lo scenario complessivo di oltre 2000 valute.
Una maggiore conoscenza e delle analisi più dettagliate possono indirizzare verso scelte più consapevoli.

[1]Sono tante, troppe, le storie di famiglie che hanno perso i risparmi di una vita alla ricerca di enormi guadagni.

3.1 Bolle speculative

Bitcoin e le altre criptovalute sono state, sono o continueranno ad essere bolle speculative?
Queste domande risuonano spesso e le opinioni sono abbastanza discordanti. Per cercare di dare una risposta occorre prima definire cosa si intenda nel linguaggio economico per "bolla speculativa".

> Una bolla si manifesta quando il prezzo dell'asset sottostante subisce un incremento inconsueto non basato su ragioni di mercato solide.
> Essa diventa *speculativa* quando si presentano anche fenomeni di tale natura.

Esempi storici importanti sono diversi per tipologia di prodotto e per periodo temporale. Il primo caso noto è quello dei *tulipani* in Olanda nel 1600, delle *ferrovie inglesi* nel 1800. Più recenti sono la bolla *tecnologica* degli anni 90 del 1900 e quella *immobiliare* degli anni 2000.
Eppure la definizione stessa di questo fenomeno fa comprendere quanto sia difficile provare in generale che un titolo, un'attività o altro sia una bolla. Non vi sono parametri oggettivi o prestabiliti che regolino le "ragioni economiche", nessuna soglia di prezzo per discernere gli scenari. Se anche ci fossero, bisognerebbe necessariamente suddividere per quante più sotto-sezioni possibili i beni, altrimenti si paragonerebbero situazioni troppo differenti. Quando si può avere il riscontro che il prezzo raggiunto è nettamente superiore al valore del bene, allora è facile riconoscere una bolla, ma non è sempre così.
Queste difficoltà diventano ancora più evidenti in un mercato nuovo e privo di storia quale quello delle criptovalute. Si può provare comunque a fare luce su ciò che è avvenuto negli anni.

Un'analisi interessante è stata quella del giovane Justas Pikelis, fondatore dell'importante token *Monetha*, eletto dalla rivista Forbes nel 2018 fra gli under 30 più influenti e autorevole voce nel panorama internazionale sulla cripto-economia.

Durante un intervento per il noto show *TEDxSquareMile*, Justas Pikelis vuole sottolineare che la sua non è stata solo fortuna. Non è diventato milionario raccogliendo 37 milioni di dollari in 18 minuti solo perché baciato dal fato. No, il giovane economista aveva ben chiare le idee e all'inizio del 2017 sapeva già che si stava trovando difronte ad una bolla, la *Tech Bubble*, e comprese che era il momento giusto per agire. Lavorò intensamente su quel progetto e ad Agosto dello stesso anno raccolse quell'enorme cifra.
La sua analisi dai toni pittoreschi è certamente efficace e prende come esempio l'andamento di Bitcoin.

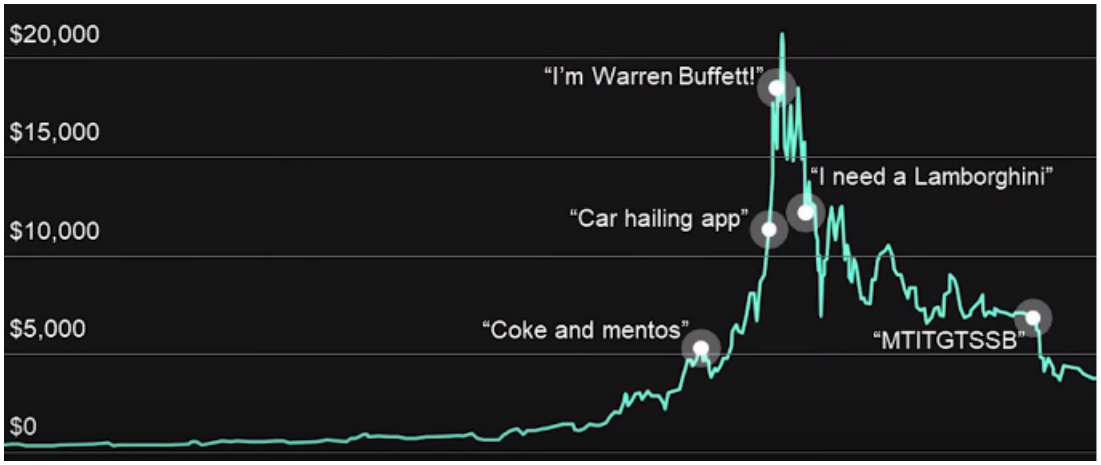


Figura 3.2: Slide dalla presentazione di Pikelis su TEDxSquareMile, 31 Maggio 2019.

Pikelis riconosce nell'andamento di Bitcoin le cinque fasi tipiche di una bolla speculativa:

1. **Displacement**, quando il prezzo e l'interesse generale iniziano a salire quasi improvvisamente, come la reazione istantanea tra la *Coca cola* e le caramelle *Mentos* insieme.

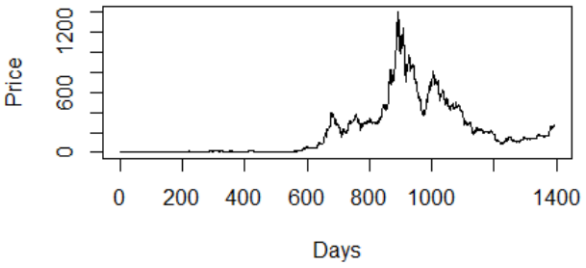
2. **Boom**: tantissima gente comune vuole partecipare a ciò che crede possa essere l'investimento della vita, facendo in modo che il prezzo continui a salire. Justas Pikelis paragona questa fase all'entusiasmo americano verso i servizi di carsharing.

3. **Euphoris**, il momento di massimo entusiasmo dei mercati in cui tantissimi individui cercano di partecipare, accecati da questo continuo rialzo del valore, investendo troppo spesso più del dovuto. Si innesca la certezza di stare puntando tutto in un guadagno facile e ci si sente trader come *Warren Buffett*, uno fra i più grandi investitori di tutte le epoche.

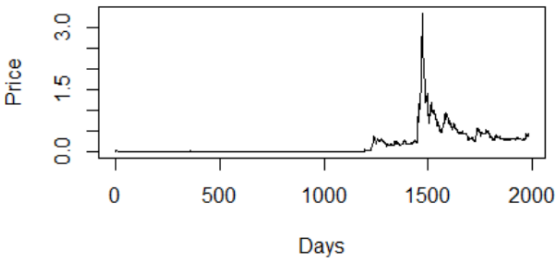
4. **Profit taking:** alcuni investitori iniziano a comprendere il pericolo e iniziano a vendere, realizzando altissimi guadagni che, come ironicamente dice Pikelis, permettono di chiamare questa fase "ho bisogno di una Lamborghini". Il prezzo inizia inevitabilmente a scendere.

5. **Panic:** l'opinione pubblica cambia radicalmente, il prezzo continua a scendere e chi è arrivato per ultimo, acquistando ad un prezzo elevato, perde tantissimo. Pikelis ribatezza tale periodo come "Maybe This Isn't The Greatest Thing Since Sliced Bread", un'espressione per dire che non si è di fronte ad un'innovazione così grande e positiva.

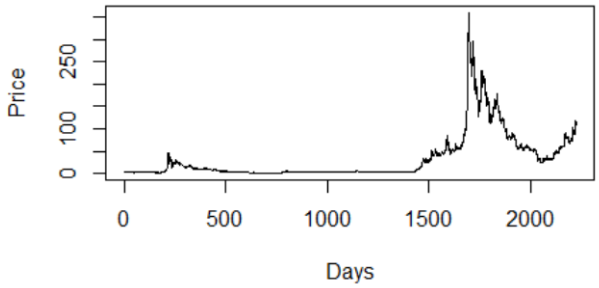
Quello in figura 3.2 è l'andamento di Bitcoin fino a Maggio 2019 ed è interessante osservare che argomentazioni analoghe possono essere fatte, sebbene con valori di mercato differenti, sulle variazioni del prezzo delle altre tre criptovalute trattate.



(a) Ethereum



(b) Ripple



(c) Litecoin

Ad un primo sguardo può sembrare che Ethereum abbia vissuto la fase di Euphoris in un momento diverso rispetto alle altre criptovalute. In realtà tale aspetto è dovuto semplicemente ad una diversa data di partenza della quotazione della valuta: Ethereum viene attivamente scambiata dal 2015, le altre dal 2013.

Guardare l'andamento dei prezzi su un arco temporale lungo porta sicuramente a trarre delle conclusioni in maniera più semplice. Difficile è comprendere tali dinamiche quando si sta vivendo una bolla speculativa.
Ancora di più nel caso della *Tech Bubble* il cui andamento è stato imprevedibile fin dalle origini: già nel 2015 si cercava di capire se vi fossero bolle speculative nel mercato Bitcoin [31]. L'intero grafico dal 2009 ad adesso non permette di cogliere variazioni di minor entità ma pur sempre significative perché in una scala da 0 a 20 000 dollari diventano non visibili. Se invece si guardano con attenzione i grafici di periodi più brevi si vede che andamenti tipici delle bolle speculative si sono susseguiti spesso.

(a) 2013

(b) 2016

(c) 2017-2018

(d) 2019

Figura 3.3: Andamento prezzi Bitcoin.

Fino al 2013 il prezzo era cresciuto costantemente raggiungendo circa 200 dollari per bitcoin. In pochi mesi il prezzo diventa sei volte più grande ed è possibile ritrovare le varie fasi tipiche delle bolle. Anche il quel caso il prezzo non rimase così elevato ma tornò ad assestarsi sui 400 dollari.
I mercati vissero un periodo di quiete fino a metà 2016 quando in un mese circa il valore dei bitcoin quasi raddoppiò per poi assestarsi sui 600 dollari. Anche questa variazione è significativa e chi in quel periodo investì molto ha dovuto gestire anche ingenti perdite.
Ciò che avvenne fra la fine del 2017 e il 2018 è già stato trattato e le variazioni sono così enormi che è l'unico andamento visibile globalmente.
Anche nell'ultimo periodo però i mercati hanno subito notevoli turbolenze, raddoppiando in un paio di mesi il valore per poi ritornare sui 7000 dollari.

In quest'ottica si può comprendere forse perché il fenomeno Bitcoin e Cryptocurrencies non sembra volersi arrestare: la storia ha segnato non un solo periodo, ma tanti, in cui i partecipanti si sono trovati in uno scenario che fino al giorno prima sembrava incredibile. Pensavano di aver perso tutto e invece puntualmente il mercato si rialza e diventa più forte. E' vero che ciò non è successo dopo la bolla del 2017, ma tanti entusiasti ancora ci sperano.

3.2 Analisi comparativa dati storici

Sono molti i siti che da anni si rivolgono al mercato delle criptovalute. Alcuni sono siti prettamente di *exchange*, altri si occupano di scrivere articoli che possano far conoscere questo mondo, fornendo informazioni e aggiornamenti[2]. Altri ancora inglobano le due funzioni con l'inclusione di altri servizi personalizzati, come nel caso di *Young Platform*.
Un'ulteriore fonte di informazione sono quelle pagine web da cui è possibile scaricare dati storici delle criptovalute; più dettagliati ed elaborati sono, più viene richiesto un

[2]E' il caso del portale italiano *Blockchain4Innovation* di Mauro Bellini, o dell'istituto *Binance Research*.

abbonamento elevato per accedervi, proiettando il loro utilizzo sul piano business. Fortunatamente alcuni siti forniscono ancora oggi gratuitamente la possibilità di accedere ad alcuni dati. La fonte scelta è stata per la maggior parte dei casi *Yahoo Finance*, così da avere possibilità di confronti anche con altri titoli e asset rilevanti sul mercato mondiale.

3.2.1 Ritorno dell'investimento

Sebbene Nakamoto presentò il suo progetto con l'obiettivo di proporre un nuovo metodo di pagamento, è ben chiaro come ad oggi, e negli anni passati, la principale finalità è stata di investimento. Come tale, risulta interessante analizzarne alcune caratteristiche tipiche del classico mercato azionario.
La scelta è stata quella di trattare un periodo di circa cinque anni, dal 10 Agosto 2015, al 19 Marzo 2020, comune a tutte le valute. Gli anni precedenti a tale data non assicurano la presenta di tutti e quattro le monete; inoltre non vi erano stati andamenti particolarmente interessanti ma solo una lenta e costante crescita.

Un indicatore importante per scegliere se intraprendere o meno un investimento è sicuramente il **ritorno dell'investimento**. Si può definire come

$$r(t) = \frac{p(t) - p(t-1)}{p(t-1)}$$

con $p(t)$ prezzo dell'azione ad un determinato tempo t, supponendo che l'acquisto sia avvenuto al tempo $t-1$.
Qualitativamente esprime una misura della redditività di un'operazione finanziaria riportando un valore di guadagno per ogni t.
E' interessante osservare in figura 3.4, per il periodo considerato, l'andamento del ritorno dell'investimento giornaliero di Bitcoin.
Il valore medio 0.003541 dice poco osservando quanto alta sia la variabilità di $r(t)$ nel periodo considerato.
Ancora più evidente se paragonato con l'andamento del valore di ritorno su $S\&P500$, indice che raccoglie i cinquecento titoli americani più influenti sul mercato. L'incapacità di coglierne bene le osservazioni evidenzia come la banda di oscillazione è

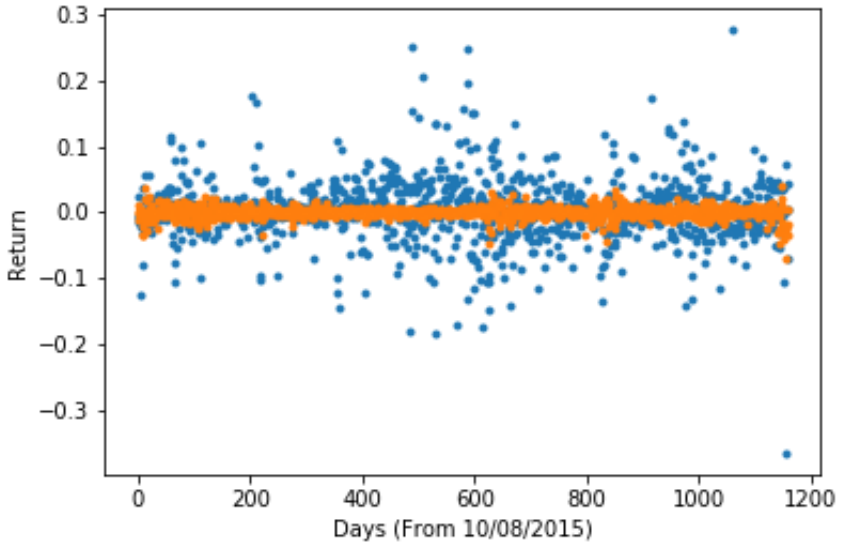


Figura 3.4: Ritorno dell'investimento su base giornaliera; in blu Bitcoin, in arancione S&P500.

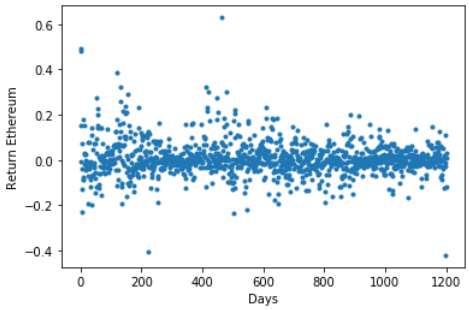
molto più ristretta.

Da un giorno all'altro, dunque, investire in Bitcoin comporta un ritorno sensibilmente differente.

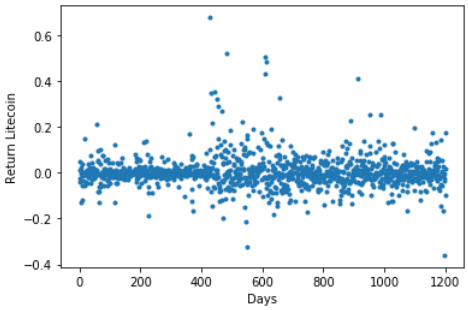
Per le altre tre criptovalute da poter scambiare in *Young Platform*, l'andamento del ritorno di investimento è del tutto simile nella dispersione, soprattutto ricordando che il ritorno per $S\&P500$ varia fra -0.006 e 0.004.

L'analisi presentata sottolinea una variabilità nel ritorno non indifferente già su un lag temporale di 1. Ci si domanda allora cosa accade se si calcolasse il ritorno dell'investimento su tempi più lunghi, ad esempio 30 giorni. Intuitivamente si attende una variazione maggiore in $r(t)$.

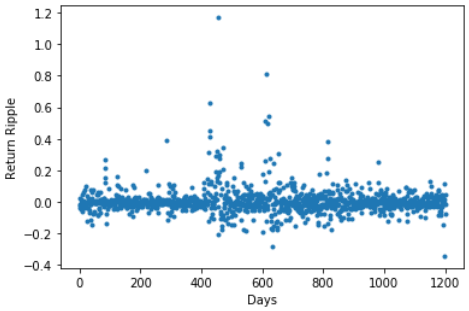
Dalla figura 3.6 è ancora più evidente quanto sia estremamente incontrollabile il mercato Bitcoin rispetto al restante mercato azionario: le aziende di $S\&P500$ sembrano aver avuto dei ritorni quasi costanti al confronto. In realtà anche loro su scala mensile hanno avuto oscillazioni di ritorno molto più corpose (da -0.2 a 0.2), ma non apprezzabile dalla scala in figura. Quello che appare incredibile è come sia cresciuto e diminuito in molti periodi il rendimento da un mese all'altro. Era già visibile da un primo grafico sull'andamento dei prezzi, ma qui è possibile capire perché tanta gente si sia arricchita e tantissima altra impoverita: da un momento all'altro



(a) Ethereum



(b) Litecoin



(c) Ripple

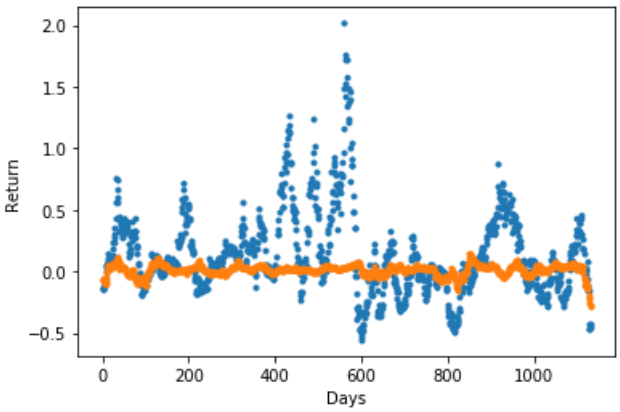


Figura 3.5: Ritorno dell'investimento su base mensile; in blu Bitcoin, in arancione S&P500.

l'investimento effettuato 30 giorni prima poteva valere il il doppio, così come perdere metà del suo valore.

3.2.2 Volatilità

Un modo per cercare di quantificare questa incertezza del prezzo nei mercati è il calcolo della volatilità.

In finanza, tale indice è uno strumento per gli investitori finalizzato alla comprensione generale dell'aspettativa di fluttuazione nel tempo del titolo acquistato.
I titoli con maggiore volatilità generalmente richiedono un periodo più lungo prima di comprenderne l'andamento.
Ci sono diversi modi per calcolare tale misura; uno fra questi è strettamente legato al *ritorno di investimento*, di seguito gli step per calcolarlo:

1. **Ritorno medio:** si sceglie il parametro M che indica il numero di osservazioni giornaliere di prezzo da considerare. Con tutti loro viene calcolata la media aritmetica dei ritorni di investimento su tali lag temporali.

$$\overline{r}(t) = \frac{1}{M} \sum_{k=0}^{M-1} r(t-k)$$

2. **Volatilità:** viene effettuata la media sugli M scostamenti del corrispondente ritorno dal ritorno medio al quadrato. Infine se ne calcola la radice quadrata.

$$\sigma(t) = \sqrt{\frac{1}{M} \sum_{k=0}^{M-1} \left(r(t-k) - \overline{r}(t)\right)^2}$$

Si considerano sempre i campioni di osservazioni precedentemente considerati, "Bitcoin VS $S\&P500$". La prima osservazione da fare è il confronto fra il ritorno medio di Bitcoin e dei 500 titoli americani. Ancora una volta la differenza nell'andamento è significativa.
Al variare di M, il lag temporale su cui calcolare il ritorno medio, l'andamento di entrambi i titoli è analogo: più cresce M, più le variazioni si smorzano. Tale risultato è atteso dal momento che si sta mediando un numero di osservazioni via via maggiore; l'effetto è simile al calcolo di una *media mobile*.
Ciò che ancora una volta va sottolineata è l'enorme differenza delle bande di oscillazione, in figura 3.8 ancora più evidente poiché è possibile vedere i valori $S\&P500$.
Il secondo step è il calcolo della volatilità. L'estrema variabilità conferma ancora una volta quanto rischioso sia il mercato delle criptovalute: è possibile avere grandissimi guadagni da un mese all'altro, così come ingenti perdite, tante volte mai recuperate del tutto.

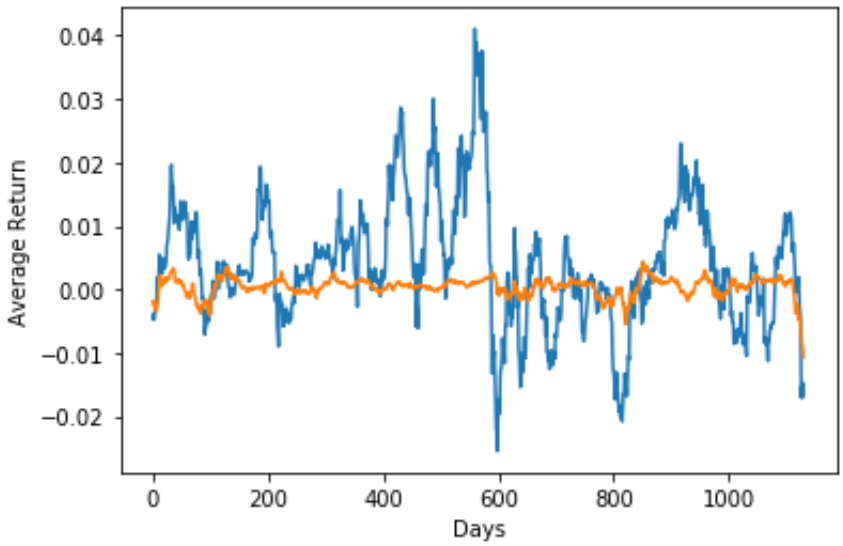
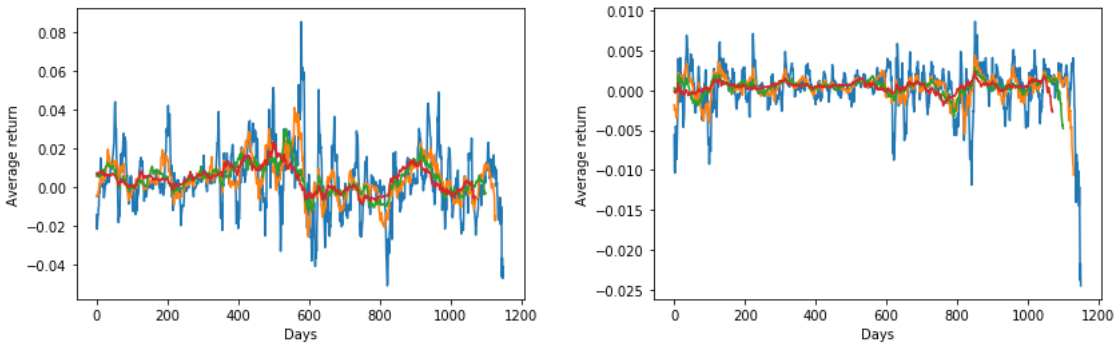


Figura 3.6: Ritorno medio dell'investimento $M = 30$; in blu Bitcoin, in arancione S&P500.

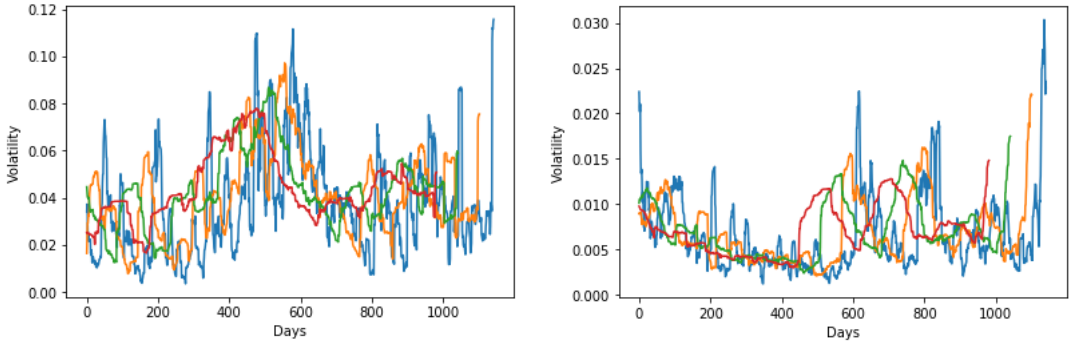


(a) Bitcoin (b) S&P500

Figura 3.7: Ritorno medio al variare di M: in blu $M = 10$, in arancione $M = 30$, in verde $M = 60$, in rosso $M = 90$.

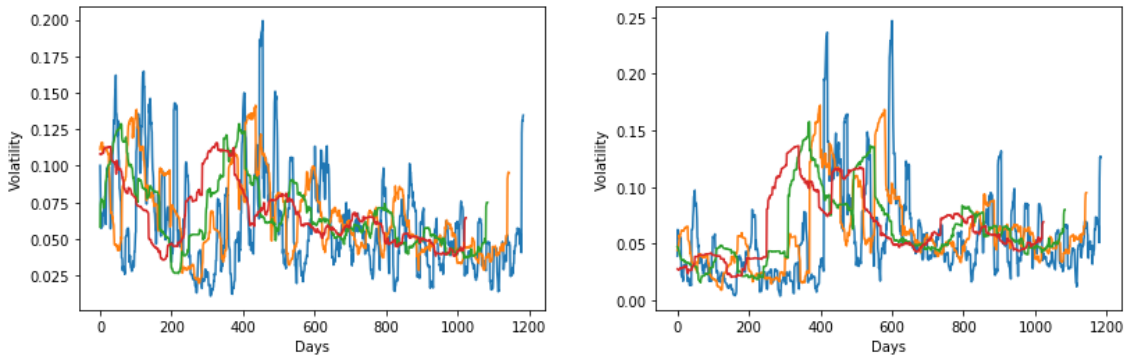
Comparando l'andamento della volatilità emerge un altro aspetto interessante: per diversi M vi è una traslata simmetria della volatilità in $S\&P500$ (con valori decrescenti al crescere di M), spesso assente in Bitcoin.

Ethereum, Litecoin e Ripple hanno un andamento piuttosto simile, come visibile in 4.6, sebbene con valori ancora più elevati di volatilità. Nonostante il prezzo, e conseguenzialmente la capitalizzazione di mercato, sia notevolmente più basso rispetto ai bitcoin, questo non deve far pensare che siano forme di investimento meno rischiose o più gestibili. Appare evidente che tutte condividono le stesse caratteristiche in

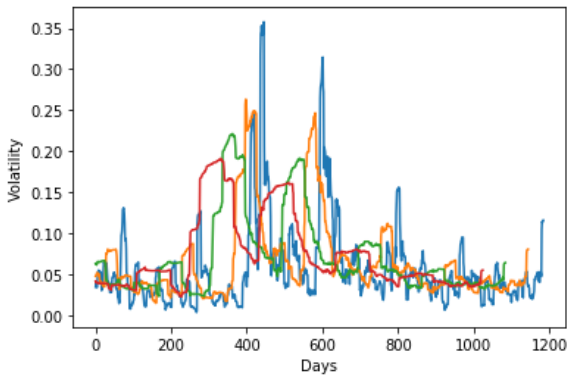


(a) Bitcoin (b) S&P500

Figura 3.8: Volatilità al variare di M: in blu $M = 10$, in arancione $M = 30$, in verde $M = 60$, in rosso $M = 90$.



(a) Ethereum (b) Litecoin



(c) Ripple

Figura 3.9: Grafico della volatilità per Ethereum, Litecoin, Ripple.

termini di ritorno e volatilità.

L'estrema variabilità delle criptovalute emerge in ogni sfaccettatura. Alle grandi

possibilità di rendimento elevato è associato un elevato fattore di rischio, così come sempre in finanza.

Chi si proietta in questo mondo deve però avere chiaro che **non si gestisce una forma di investimento simile alle altre presenti sul mercato**. Bitcoin, come gran parte delle altcoin, non è legato ad alcuna autorità e nessuno verrà in soccorso degli investitori in caso di grandi difficoltà.

Non a caso, un gran numero di istituiti finanziari ha chiarito la sua posizione rispetto alle *cripto-attività*. Anche la **Banca d'Italia** ha reso pubblica la regolamentazione e la visione italiana al riguardo [26]. Citando gli autori, *"... la Banca d'Italia mette in guardia i risparmiatori [...] e scoraggia gli intermediari dall'assumere rischi ..."*.

Le motivazioni sono la ben nota assenza di un'autorità centrale, mancanza di stabilità, fortissima dipendenza del prezzo dalla domanda, dinamica simile a quella di una bolla speculativa.

Nel paper viene fatta una chiara distinzione fra Bitcoin e tecnologia Blockchain, apprezzando quest'ultima e riconoscendo possibili applicazioni se opportunamente implementate al fine di garantire una forma di controllo centrale.

Gli approcci regolamentari adottati nel mondo sono molto eterogenei; si pensi al Giappone che ha autorizzato le valute virtuali come mezzo di pagamento, gli Stati Uniti richiedono una specifica licenza per le piattaforme di scambio, mentre l'Europa cerca di prevenire l'uso ai fini di riciclaggio e terrorismo.

3.3 Correlazioni

Per avere una comprensione più profonda e completa del mondo *cryptocurrencies*, è necessario conoscere a fondo quali sono le relazioni *inter-valuta*, fra le valute e con il mondo esterno.

Definizione 3.3.1. *Date due variabili* $A = \{x_1, \cdots, x_n\}$ *e* $B = \{y_1, \cdots, y_n\}$*, si definisce il* ***coefficiente di correlazione*** *come:*

$$\rho_{AB} = \frac{cov(A, B)}{\sigma_A \cdot \sigma_B}$$

con $cov(A, B)$ *covarianza di* A *e* B*;* σ_A*,* σ_B *deviazioni standard.*

E' noto anche come ***indice di correlazione di Pearson****.*

Il coefficiente di correlazione misura quanto due variabili si muovano congiuntamente fra loro. Due variabili si dicono:

- **positivamente correlate** $\rho_{AB} > 0$ se all'aumentare di una aumenta anche l'altra;
- **negativamente correlate** $\rho_{AB} < 0$ se tendono a variare in maniera opposta, ossia al crescere di una decresce l'altra.

Nel mercato finanziario, avere consapevolezza di tali relazioni è necessario per poter effettuare scelte mirate a costruire portafogli di titoli con massimo rendimento e minimo rischio possibile. Non a caso, uno dei "segreti" per investire con successo è scegliere titoli e strumenti che siano poco correlati e, quando si può, negativamente correlati. Ciò porta ad una *diversificazione del rischio* per cui se alcuni di essi dovessero andar male, gli effetti non si avrebbero sugli altri o addirittura, nel caso di correlazione negativa, altri titoli potrebbero esserne avvantaggiati.
Se è vero che nel mondo reale non è possibile trovare investimenti con $\rho_{ij} = -1$ per ogni coppia di titoli i, j, effetti positivi sulla riduzione del rischio si hanno già quando si selezionano strumenti poco correlati positivamente.

Relazioni interne

Prima di poter cogliere le correlazioni fra criptovalute e altri strumenti finanziari, è necessario conoscere meglio le relazioni interne alla valuta stessa. I dati forniti da [11] sono giornalieri e riguardano:

1. Prezzo di apertura;
2. Prezzo più alto;
3. Prezzo più basso;
4. Prezzo di chiusura;
5. Volume, ovvero il numero di transazioni effettuate ogni giorno;
6. Capitalizzazione di mercato: prodotto del prezzo unitario per il numero di

Sembra immediato ed ovvio dire che queste misurazioni sono effettivamente molto correlate fra loro: ci aspettiamo che un prezzo di apertura alto sia legato a prezzi più alti anche in chiusura. Allo stesso modo, un prezzo più alto è atteso quando la domanda è più alta e dunque vi è un maggior volume di transazioni giornaliere. La capitalizzazione di mercato segue dalle precedenti. Sebbene così ovvio, l'imprevedibilità e irrazionalità del mercato delle criptomonete giustifica un'attenzione e scrupolo particolare per accertarsene.

Con il software R è stato possibile estrarre la matrice di correlazione associata ad ognuna delle criptovalute trattate.

```
> cor(bitcoin)
               Open      High       Low     Close    Volume Market.Cap
Open       1.0000000 0.9989562 0.9982568 0.9977742 0.7228784  0.9969502
High       0.9989562 1.0000000 0.9978584 0.9990425 0.7229571  0.9976944
Low        0.9982568 0.9978584 1.0000000 0.9988197 0.7232817  0.9986421
Close      0.9977742 0.9990425 0.9988197 1.0000000 0.7225918  0.9990737
Volume     0.7228784 0.7229571 0.7232817 0.7225918 1.0000000  0.7440364
Market.Cap 0.9969502 0.9976944 0.9986421 0.9990737 0.7440364  1.0000000
```

(a) Bitcoin

```
> cor(ethereum)
               Open      High       Low     Close    Volume Market.Cap
Open       1.0000000 0.9986123 0.9966183 0.9965762 0.1974295  0.9957401
High       0.9986123 1.0000000 0.9966207 0.9984919 0.1982743  0.9971940
Low        0.9966183 0.9966207 1.0000000 0.9980552 0.1962378  0.9976454
Close      0.9965762 0.9984919 0.9980552 1.0000000 0.1974158  0.9989998
Volume     0.1974295 0.1982743 0.1962378 0.1974158 1.0000000  0.2304646
Market.Cap 0.9957401 0.9971940 0.9976454 0.9989998 0.2304646  1.0000000
```

(b) Ethereum

```
> cor(litecoin)
               Open      High       Low     Close    Volume Market.Cap
Open       1.0000000 0.9969058 0.9967191 0.9955798 0.4531856  0.9916593
High       0.9969058 1.0000000 0.9952235 0.9987522 0.4560107  0.9934499
Low        0.9967191 0.9952235 1.0000000 0.9969338 0.4586552  0.9943978
Close      0.9955798 0.9987522 0.9969338 1.0000000 0.4593893  0.9957365
Volume     0.4531856 0.4560107 0.4586552 0.4593893 1.0000000  0.5163822
Market.Cap 0.9916593 0.9934499 0.9943978 0.9957365 0.5163822  1.0000000
```

(c) Litecoin

```
> cor(ripple)
               Open      High       Low     Close    Volume Market.Cap
Open       1.0000000 0.9945715 0.9930678 0.9918568 0.6010918  0.9912536
High       0.9945715 1.0000000 0.9907376 0.9962864 0.6271781  0.9948123
Low        0.9930678 0.9907376 1.0000000 0.9952238 0.5940782  0.9954535
Close      0.9918568 0.9962864 0.9952238 1.0000000 0.6179811  0.9992705
Volume     0.6010918 0.6271781 0.5940782 0.6179811 1.0000000  0.6344021
Market.Cap 0.9912536 0.9948123 0.9954535 0.9992705 0.6344021  1.0000000
```

(d) Ripple

Come noto, non è solo importante cogliere il segno e la forza della correlazione,

bensì anche comprendere se questa sia statisticamente significativa o meno. Questa viene testata dalla funzione *cor.test()* su coppie di variabili:

$$ipotesi\,nulla:\ \rho_{i,j} = 0$$

$$ipotesi\,alternativa:\ \rho_{i,j} \neq 0$$

se il $p-value$ è inferiore ad una certa soglia, solitamente 0.05, viene rigettata l'ipotesi nulla.

Per tutte e quattro le criptovalute analizzate, la correlazione fra le grandezze *Open, High, Low, Close* è positiva e $\rho > 0.99$, quindi hanno correlazione quasi perfetta. Supportati da evidenza statistica, non si commettono errori se viene considerato uno di essi come valore di riferimento per il prezzo della moneta. I valori del *cor.test()* sono riportati in Appendice E.

In tutti i casi emerge *Volume*, la variabile che riporta il numero di transazioni giornaliere. La correlazione è ancora una volta positiva e significativa[3], esprimendo che l'aumento del prezzo della valuta non può che essere alto quando la domanda è alta e dunque il numero di transazioni effettuate per scambiare la moneta elevato.

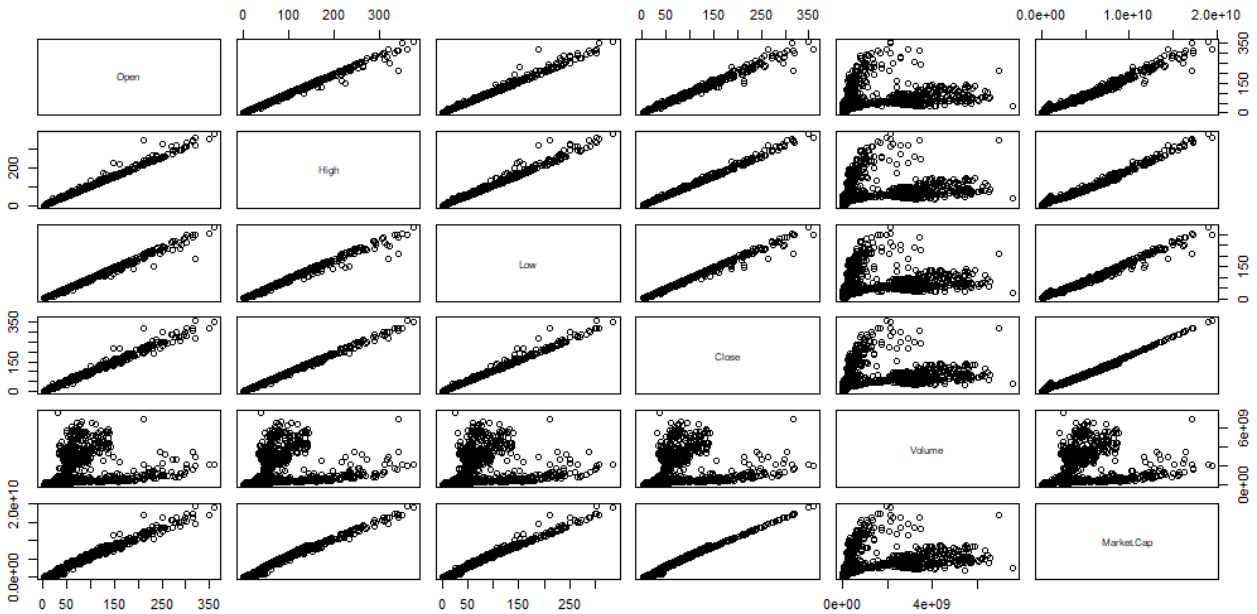


Figura 3.10: Grafico correlazioni Litecoin.

[3]Risultati sulla significatività in Appendice E.

Questo è sicuramente sensato, pensando al comportamento dei mercati, ma la minor forza del legame evidenzia che sì, ci aspettiamo più transazioni, ma tenendo presente che tanti investitori preferiranno mantenere valuta fiduciosi che il prezzo aumenterà ancora nel tempo. Come visibile in figura nell'esempio Litecoin, inizialmente al crescere del prezzo si è registra un grande aumento nel numero di transazioni, motivato anche dal fatto che la valuta si diffonde e diventa più utilizzata. Più cresce il prezzo più l'aumento del numero di transazioni è minore.
Mantenere l'investimento per un periodo elevato di tempo è una caratteristica peculiare delle criptocurrencies, come vedremo in seguito.

Relazioni fra valute

Prendendo come riferimento per il prezzo della valuta i valori di *Open*, si cercano eventuali relazioni fra le quattro analizzate. Il periodo in cui osservarle deve essere comune, quindi si è selezionato l'arco temporale fra Agosto 2015 e Marzo 2020.
Oltre ad un approccio grafico che permette già delle osservazioni interessanti, è importante riportare i valori di correlazione e accertarsi che siano statisticamente significativi.

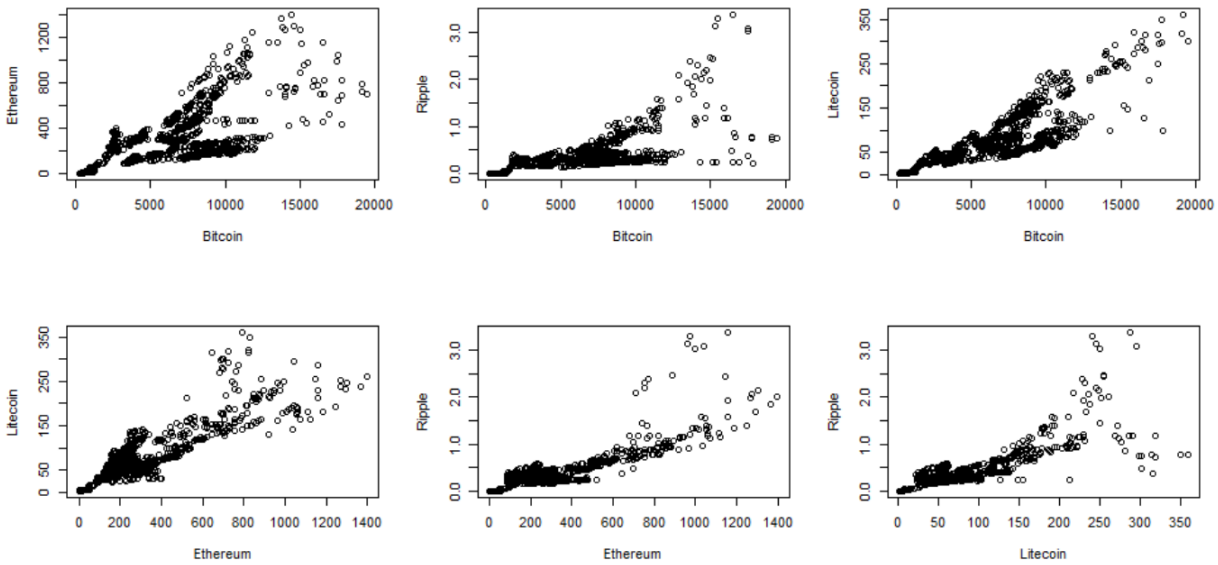


Figura 3.11: Correlazioni fra le valute da Luglio 2015 a Marzo 2020.

Da una prima analisi emergono dei coefficienti di correlazione sicuramente molto elevati che evidenziano uno strettissimo legame fra i prezzi delle criptovalute, sebbene con differenze non trascurabili. Investire in due valute diverse sembrerebbe comportare una diversificazione del rischio pressoché nulla.

Valute	**Correlazione**
Bitcoin-Ethereum	$\rho = 0.7563827$
Bitcoin-Ripple	$\rho = 0.7201083$
Bitcoin-Litecoin	$\rho = 0.8693512$
Ethereum-Litecoin	$\rho = 0.9092478$
Ethereum-Ripple	$\rho = 0.8747912$
Litecoin-Ripple	$\rho = 0.8556285$

Graficamente però si osserva anche un altro aspetto: vi è un primo periodo di fortissima correlazione, prossima ad 1, ed un secondo periodo in cui le osservazioni sono visibilmente meno legate e dall'andamento irregolare. Nel dettaglio questo cambiamento si registra in concomitanza con l'altissimo valore del prezzo di Bitcoin a **Novembre del 2017** e che ha avuto conseguenze dirette anche sulle altre criptovalute. Da quel momento il mercato ha subito dei cambiamenti sostanziali.
Sarebbe allora lecito chiedersi quanto valga la correlazione esclusivamente nell'ultimo periodo? Come se avvenisse il lancio di una nuova moneta, ad esempio a *Gennaio 2018*. La risposta probabilmente è no, la storia delle valute potrebbe essere tutta fondamentale per comprenderne l'andamento e le oscillazioni tipiche delle bolle speculative[4] devono essere sempre tenute in mente.
Però è pur vero che per investimenti di breve termine in cui le dinamiche sono limitate, potrebbe essere utile conoscere i valori di correlazione dell'ultimo periodo.

Valute	**Correlazione**
Bitcoin-Ethereum	$\rho = 0.5551728$
Bitcoin-Ripple	$\rho = 0.6843975$
Bitcoin-Litecoin	$\rho = 0.5108913$
Ethereum-Litecoin	$\rho = 0.9000568$
Ethereum-Ripple	$\rho = 0.8375890$
Litecoin-Ripple	$\rho = 0.8164152$

[4]Riferimento al paragrafo *Bolle Speculative.*

Lo scenario è molto variegato. Per alcune di loro il legame è notevolmente inferiore (Bitcoin-altre tre valute); altre invece hanno una correlazione ridotta ma pur sempre elevata. Come già detto questo approccio potrebbe essere discutibile e guardare solo una parte della storia di un titolo fornisce meno informazioni sullo stesso. E' altrettanto vero però che la storia delle criptovalute non è tale da poter utilizzare i classici strumenti della finanza con estrema confidenza e fiducia. Ad oggi questo mercato è imprevedibile, volatile come nessun altro e di conseguenza raccogliere più informazioni possibili può apportare un po' di consapevolezza in più.

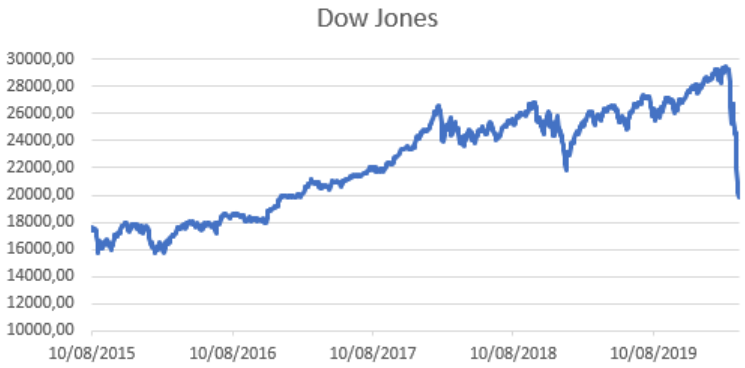
Guardando congiuntamente entrambi gli scenari, la migliore strategia per diversificare il proprio portafoglio potrebbe essere o quella di puntare su una singola valuta e poi diversificare con qualcosa di totalmente differente, oppure associare Bitcoin con una delle altre tre.

Relazioni con altri mercati

Un investitore potrebbe essere interessato a costruire portafogli diversificati in modo da ridurre il rischio anche attraverso strumenti finanziari differenti fra loro.
Il mondo delle criptovalute è allettante per i possibili grandi guadagni, ma tutt'oggi rimangono molto attivi anche i mercati azionari di tutto il mondo. Cercare di comprendere i legami fra questi settori apparentemente simili è di fondamentale importanza per un utente attento. Tre confronti interessanti sono stati esaminati:

- **Euro Stoxx 50:** ingloba 50 dei titoli più influenti dell'Euro-zona; Francia e Germania sono le nazioni più rappresentate.

- **Dow Jones:** dal 1895 e quasi ininterrottamente, viene fornito un indice della borsa di New York che misura l'andamento di 30 titoli azionari molto influenti su quel mercato.

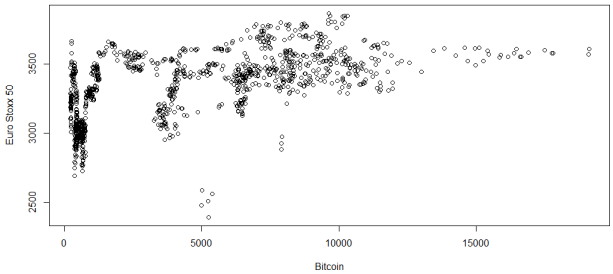


- **Oro:** ancora oggi vi è un'alta richiesta di questo bene considerato "rifugio" rispetto alle tante turbolenze dei mercati azionari. La misurazione è in Oncia.

Prendendo inizialmente come criptovaluta Bitcoin, si indaga su quale tipo di interazione intercorra con gli strumenti precedentemente citati.

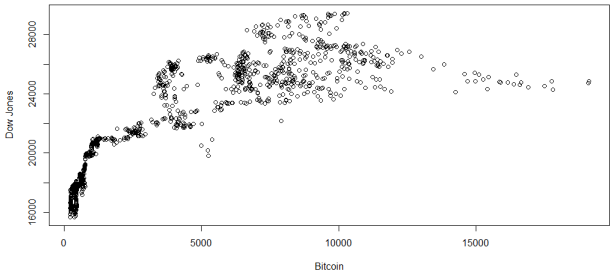
L'andamento in figura 4.12 è piuttosto variegato. Il legame più forte è sicuramente con i titoli americani: quando cresce il prezzo di Bitcoin cresce anche Dow Jones sebbene con un andamento logaritmico rispetto alla criptovaluta. La forte dipendenza con il mercato statunitense non stupisce e sottolinea come gran parte degli investitori Bitcoin abbia probabilmente lì sede.

Differente è il confronto con i titoli europei; nei primi mesi, quando i valori di bitcoin erano molto bassi, l'andamento dei titoli è stato abbastanza irregolare, diminuendo dapprima e poi risalendo. Successivamente il loro valore è quasi del tutto rimasto costante al crescere del prezzo di Bitcoin.



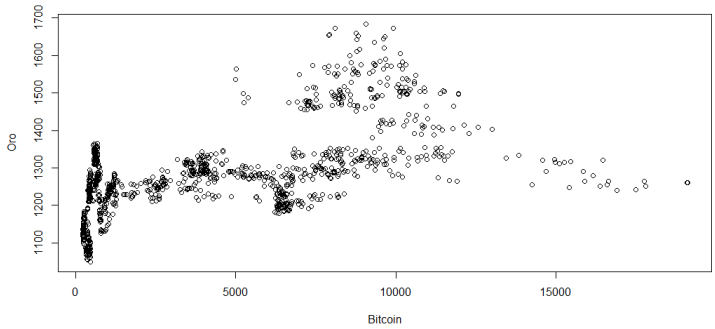
(a) Euro Stoxx 50

$\rho = 0.5971089$



(b) Dow Jones

$\rho = 0.8382639$



(c) Oro

$\rho = 0.5900697$

Figura 3.12: Correlazioni con Bitcoin.

L'andamento dell'oro è quello meno comprensibile rimanendo stabile per gran parte del tempo e con un aumento che non corrisponde al massimo prezzo raggiunto da Bitcoin. Va comunque ricordato che le variazioni di prezzo degli altri strumenti finanziari sono quasi nulle se confrontate con quelle di Bitcoin.

Vediamo inoltre se ci sono differenze significative considerando le altre criptovalute. I grafici vengono riportati in Appendice E, in tabella i valori di correlazione riscontrati. Emerge che le correlazioni di queste criptovalute sono più basse rispetto a Bitcoin. Diversificare il portafoglio con questi strumenti potrebbe portare all'effetto desiderato.

Valute	**Correlazione**
Litecoin-Euro Stoxx 50	$\rho = 0.4825242$
Litecoin-Dow Jones	$\rho = 0.6192099$
Litecoin-Oro	$\rho = 0.3227448$
Ripple-Euro Stoxx 50	$\rho = 0.5456887$
Ripple-Dow Jones	$\rho = 0.3815972$
Ripple-Oro	$\rho = 0.2180803$
Ethereum-Euro Stoxx 50	$\rho = 0.4877631$
Ethereum-Dow Jones	$\rho = 0.5317932$
Ethereum-Oro	$\rho = 0.2308761$

3.4 Valutazione delle criptovalute

I mercati finanziari non sono governati da leggi ed equazioni ben precise. Non solo mosso da approcci razionali, l'andamento del prezzo dei titoli è imprevedibile in quanto espressione dell'incontro fra domanda e offerta di investitori che agiscono secondo principi differenti. Qualcuno è più propenso al rischio, c'è chi si fida dei portafogli efficienti costituiti da algoritmi di ottimizzazione capaci, teoricamente, di trovare la combinazione di titoli con un certo rischio e massimo rendimento possibile. Ma nessuno può assicurare che l'indomani il mercato segua lo stesso andamento e allora tanti altri si lanciano in titoli in cui credono, sperando che le loro previsioni siano giuste.
Non a caso l'*economia* viene associata alla *sociologia, psicologia*: studi economici non possono prescindere da approfondimenti di tipo sociale e comportamentale.
Questo deve essere sempre tenuto in mente e non farlo porta all'eccesso di "matematizzazione dell'economia" che tanti esperti criticano; a loro dire uno dei grandi problemi che ha portato alla crisi finanziaria del 2008.

Al contempo però, non si smette mai di cercare misure ed analisi oggettive che possano aiutare ad investire in maniera quanto più razionale possibile. La ricerca continua anche nell'ambito cryptocurrency che, in più, si differenzia dai mercati tradizionali per tanti aspetti.
L'articolo di Yulin Liu [27] indaga proprio a tal proposito spiegando perché le classiche misure non siano direttamente importabili al mondo delle monete virtuali ma necessitano di trasformazioni.

3.4.1 Price-to-earnings

Fra i più noti indici in finanza, per comprenderlo occorre prima definire l'*earning per share* o utili per azione

$$EPS = \frac{Utili\ annuali}{Numero\ di\ azioni}$$

che misura quanto l'azienda stia producendo utili rapportato al numero di azioni in circolazione. Più alto è il valore, maggiormente appetibile è la società per i mercati.

Senza dubbi questa può essere vista come una misura oggettiva.
Meno lo è il P/E che esprime quanto gli investitori siano disposti a pagare un'azione in relazione agli utili per azione:

$$P/E = \frac{Prezzo\ dell'azione}{EPS} = \frac{Prezzo\ dell'azione}{\frac{Utili\ annuali}{Numero\ di\ azioni}} = \frac{Market\ Cap}{Utili\ annuali}$$

Un valore elevato di questo indice esprime fiducia dei mercati alla base dei dati storici passati oppure anche in vista di una futura crescita. Di contro un valore basso mostra poche aspettative. Come sempre è opportuno confrontare P/E di settori simili e con valori paragonabili, altrimenti l'analisi risulterebbe falsata.

E' però evidente un problema a monte che rende impossibile l'utilizzo di questo indice per il mercato *cryptocurrency*: Bitcoin, così come le altre monete, non ha un vero e proprio guadagno, non ha degli utili che incrementano il valore della stessa. Gli incentivi che vengono attribuiti dalle transaction fees e dal mining non sono una valida alternativa perché diretti ai miners e non ai possessori della moneta.
Qualsiasi tentativo di utilizzo dell'indice a tale ambito sarebbe dunque privo di senso[5].

3.4.2 Network-Value-to-Transactions

Questa metrica è stata pensata e sviluppata appositamente per il mercato delle criptovalute. L'idea di base è che il *valore del network* sia proporzionale al numero dei suoi utilizzatori o meglio, il numero di *bitcoin address*, coloro i quali scambiano valuta.

$$NVT = \frac{network\ value}{transaction\ volume\ in\ USD} = \frac{token\ price \cdot token\ supply}{token\ price \cdot transacted\ token}$$
$$= \frac{token\ supply}{transacted\ token} = \frac{1}{token\ velocity}$$

L'obiettivo dell'analista *Willy Woo*, il primo ad aver proposto ed utilizzato tale

[5]L'articolo [27] riporta l'esempio di una valuta che utilizza parte dei suoi profitti per incrementare il valore della moneta; in questo caso l'approccio P/E è applicabile.

indice, è quello di indicare a posteriori la formazione di una bolla speculativa. Quando il valore dell'NVT ratio è alto vuol dire che il network value, che corrisponde al *Market Cap*, è elevato se comparato al volume delle transazioni. Il mercato dunque sta in qualche modo sovrastimando il valore della valuta, avendo fiducia in una successiva crescita. Ciò è successo nei primi anni ed è noto come **speculative period.**

L'indice permette di distinguere se un rapido incremento del prezzo abbia causato una bolla oppure se abbia portato ad un consolidamento del prezzo stesso. Se il valore dell'NVT oscilla in un range standard, allora a grandi volumi di Market Cap si sono affiancate tante transazioni di valuta. Se invece l'NVT diventa dapprima molto grande e rapidamente crolla, allora il valore del network non si è sostenuto dalla necessaria attività di scambio e dunque inevitabilmente l'indice è destinato a scendere. In quest'ultimo caso si è registrata una bolla speculativa.

L'unità di tempo è giornaliera e il seguente grafico è stato costruito con i dati relativi a Bitcoin.

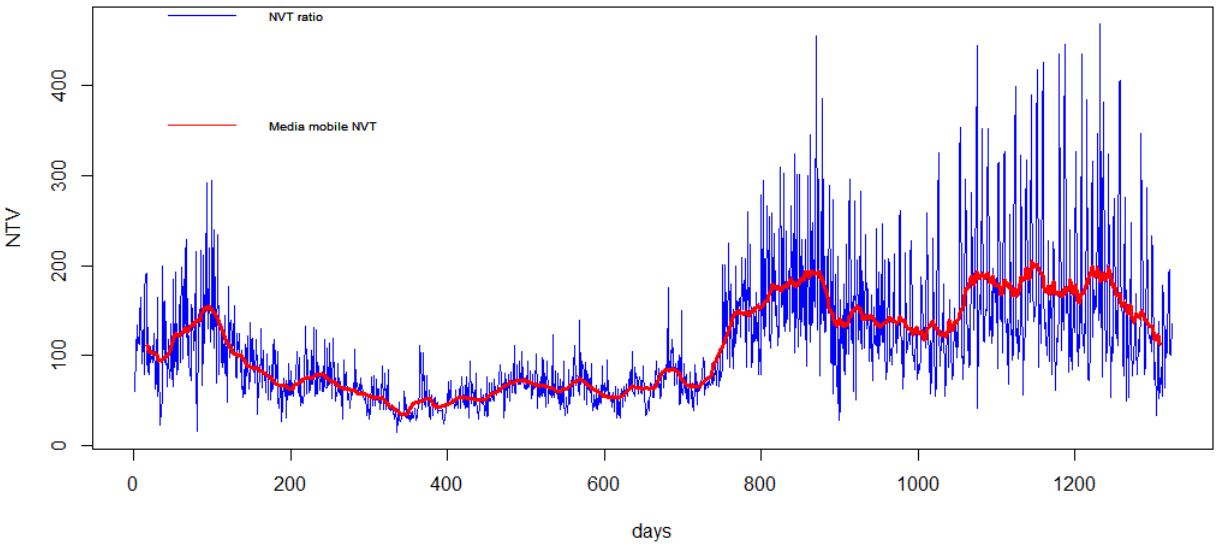


Figura 3.13: NVT da Gennaio 2014 a Marzo 2020, dati da [9].

In figura 3.13 oltre ai dati grezzi in blu, è stata plottata la media mobile su 30 osservazioni che permette di mitigare le oscillazioni e sottolineare meglio l'andamento.

A posteriori dunque è possibile affermare che nel 2014 si ebbe una bolla speculativa in quanto l'aumento dell'NVT è stato solo temporaneo (Osservazioni in figura 3.13 da 1 a 200).
Non lo stesso esito si può trarre dal periodo di fine 2017 (Ossevazioni in figura 3.13 da 650 a 750 circa) in cui evidentemente grandi valori di mercato sono stati affiancati da un gran numero di scambi, tanto che non si è registrato nulla di anomalo . Ciò non è condiviso da tutti gli economisti ma è pur sempre un punto di vista che sottolinea come il prezzo nel tempo si sia consolidato, benché non sull'occasionale punta di 17 000 dollari.
L'ultimo periodo, da metà del 2018 a Marzo 2020, ha registrato dei valori di NVT mediamente più elevati ma non con variazioni percentuali rilevanti. L'impressione generale è di solidità di un mercato che si sta attestando su un rapporto *Network value* su *Transaction Volume* più alto.

Le difficoltà di applicare questo modello ad altre criptovalute è duplice: da una parte attingere ai dati relativi alla stima del volume di transazioni in dollari, presenti in rete per Bitcoin ma non per le altre. Inoltre il confronto potrebbe non essere adeguato trattandosi di valute dalle caratteristiche anche molto differenti; si pensi ad Ethereum che fonda la sua storia su obiettivi e caratteristiche del tutto peculiari. Allo stesso modo che per il P/E, risulterebbe falsato un paragone diretto.

Questo modello proposto ingloba bene la funzione delle valute come **mezzo di scambio**, ma non come deposito di valore. Il successivo indicatore è quello che cerca di colmare questa mancanza.

3.4.3 Price-to-Utility

Il seguente indice viene presentato dall'autore nell'articolo [27] come capace di incorporare le due funzioni principali di una criptomoneta: mezzo di scambio e deposito di valore.
Il primo passo è definire cosa si intende con "utilità". Per farlo occorrono **staking ratio** e **dilution rate**, due strumenti importanti.

Staking ratio

Un fattore rilevante sul panorama criptovalute è quello dei *"staked tokens"* ossia valuta virtuale che una volta acquistata non viene più scambiata per una certa quantità di tempo. Diverse ricerche hanno sottolineato come questo aspetto sia molto rilevante tanto da affrontarlo in trattazioni approfondite[6].

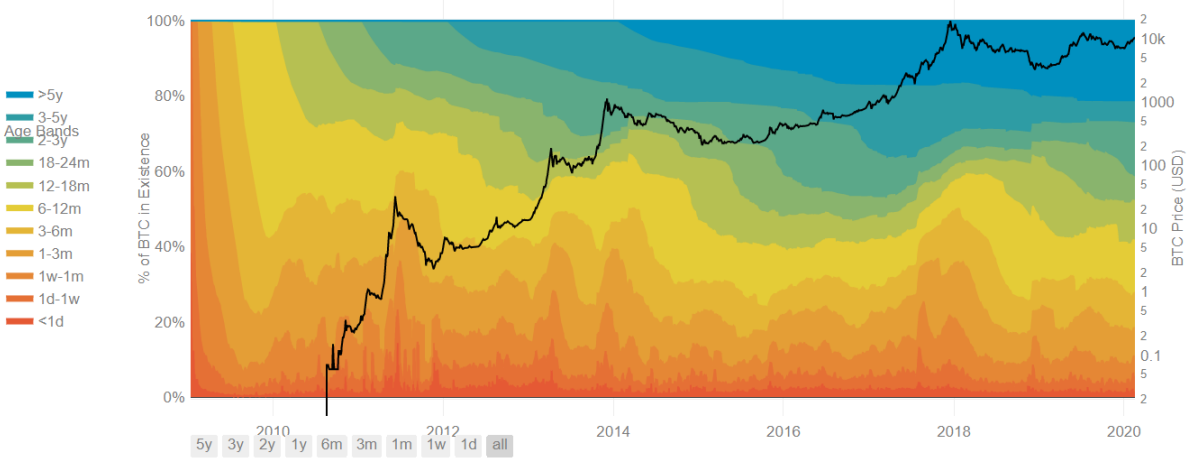


Figura 3.14: *Bitcoin Age Distribution*, fonte [28].

In figura 3.14 sono raffigurate bande di diverso colore che esprimono la frazione di bitcoin scambiati l'ultima volta tanto tempo precedente quanto espresso nella legenda. In nero vi è l'andamento del prezzo in scala logaritmica, ricordando che nei primi tempi non vi era un modo oggettivo per stabilirne un prezzo in dollari. Manipolando adeguatamente i dati in figura forniti da [29], è possibile estrarre informazioni più esplicative della percentuale di *staked tokens* Bitcoin negli anni rispetto al totale di valuta in circolazione.

Ciò che emerge in figura 3.15 è che negli anni gli utenti tendono a conservare maggiormente i token acquistati, sebbene con una certa variabilità tipica di Bitcoin. Il trend dunque sottolinea il massiccio utilizzo di token come **deposito di valore** e in maniera crescente: la fiducia degli utenti sull'evoluzione a lungo termine è elevata.

[6]Sono esempi portali autorevoli come *Digital Asset Data*, *Unchained Capital*, *Coindesk*.

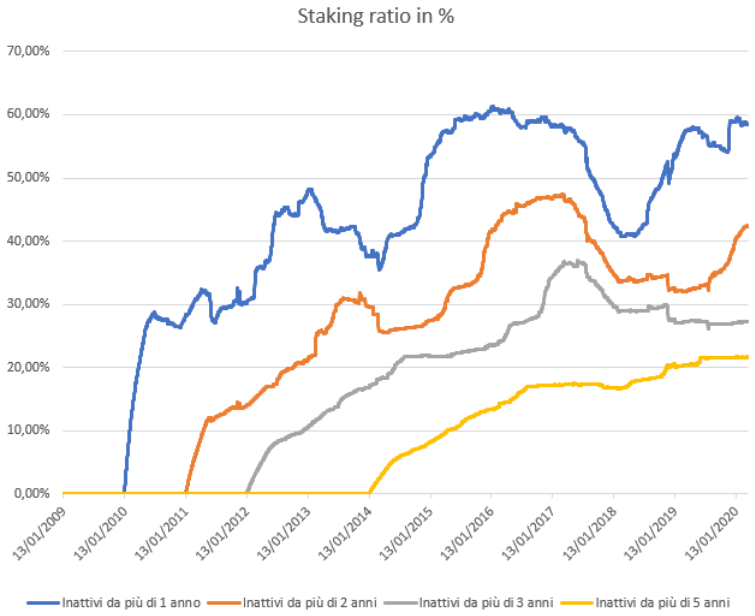
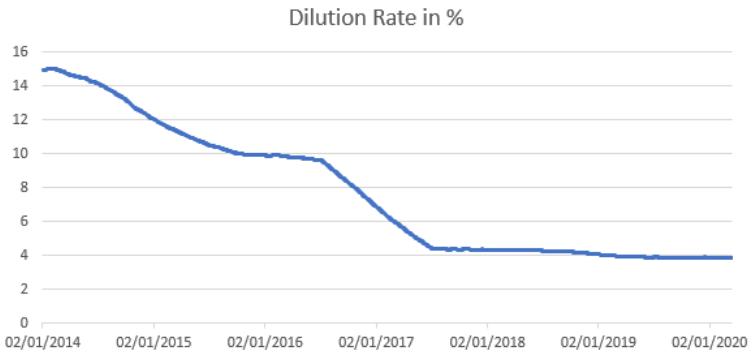


Figura 3.15: Staking ratio per diversi periodi di tempo.

Dilution rate

Il *dilution rate* misura il tasso di crescita annuo della valuta offerta. Come noto Bitcoin conia nuova moneta solo attraverso l'aggiunta di un blocco alla catena e con una velocità regolata periodicamente così da seguire un andamento ben preciso. Nel tempo però ci sono state delle variazioni del mercato, dettate soprattutto da più o meno richiesta di validazioni soprattutto nei primi anni di attività. Negli ultimi invece, da quando la diffusione è stata costante e molto elevata, il tasso è molto più regolare e segnato per lo più dai dimezzamenti nel compenso previsti ogni quattro anni.

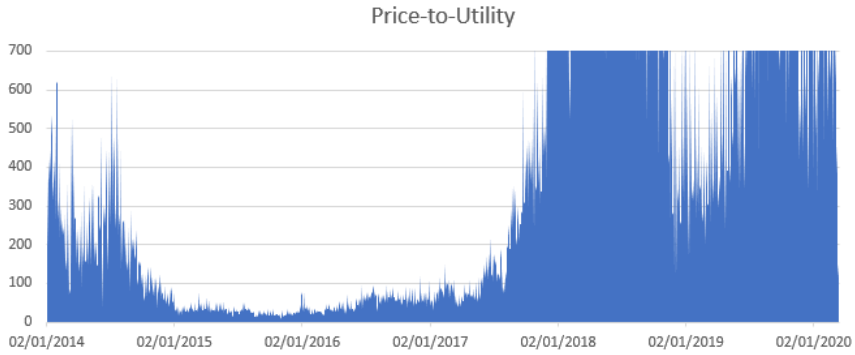


Attualmente il valore è attorno al 3.8% e ci si attende una diminuzione in seguito al dimezzamento nella ricompensa per i miners prevista intorno a Maggio 2020.

A questo punto è possibile definire

$$token\ utility = \frac{token\ velocity \cdot staking\ ratio}{dilution\ rate}$$

con *velocity token* l'inverso dell' NVT. La combinazione di questi tre elementi influenza l'utilità della valuta: quando la velocità e la quantità di moneta mantenuta sono alte, insieme ad un basso valore di dilution rate portano ad un'alta utilità.
Tutti gli elementi sono stati introdotti al fine di poter calcolare il price-to-utility **P/U** .



Quello che emerge è che in periodi "normali", ossia di apparente stabilità, i valori di P/U oscillano fra 50 e 300; diventa minore della soglia inferiore nei periodi in cui il prezzo della valuta continua a scendere. Qui risulta conveniente acquistare perché ci si aspetta che il prezzo cresca. Di contro il valore è maggiore di 300 quando si è in un periodo speculativo in cui il prezzo sale molto per scendere a breve inevitabilmente. Se ci si trova in questo range è molto più rischioso acquistare perché il rischio di perdere gran parte del valore è alto.
Da quando il prezzo è balzato su valori più elevati, il rapporto tende ad essere maggiore, con variazioni molto elevate. Questo perché l'utility invece non è cambiata altrettanto: il diluition rate e velocity sono quasi costanti, staking ratio in leggera crescita. Se tale indice risulta abbastanza esplicativo fino al 2017, probabilmente non lo è altrettanto negli ultimi anni in cui uno scenario molto differente da quello precedente si sta delineando. Nuovi strumenti e metodi vengono continuamente ricercati.

3.5 Confronto sicurezza delle criptovalute

Una condizione imprescindibile per qualsiasi criptovaluta che voglia affacciarsi sul mercato è la sicurezza del suo protocollo. Non può avere vita lunga se i partecipanti che si rivolgono ad essa sono incerti su come vengano conservati i propri possedimenti, se non vengono riconosciute le transazioni come corrette sebbene lo siano, oppure se si perde conoscenza del passato. Questi ed altri problemi devono essere necessariamente risolti, o meglio, gli utenti devono essere convinti che non possono mai presentarsi.

Questo è stato ben chiaro fin da subito a Satoshi Nakamoto che in [4] dedica il paragrafo *Calculations* alla spiegazione matematica di perché un partecipante possa porre la piena fiducia al sistema Bitcoin.

3.5.1 Sicurezza Proof-of-Work

Sono molte le criptovalute che hanno ereditato questo metodo di validazione da Bitcoin, adattandolo alle proprie esigenze. Come già osservato in precedenza, la struttura del protocollo è una lunga catena di transazioni condivisa dagli utenti in cui è possibile risalire a tutti i passaggi di valuta fra i partecipanti.

Quello che un hacker potrebbe voler fare è cercare di costruire una catena alternativa a quella onesta, inserendo pagamenti non corretti. Non gli sarebbe possibile accreditarsi impropriamente del denaro perché la catena non accetterebbe tali blocchi, ma potrebbe accreditarsi valuta già spesa[7].

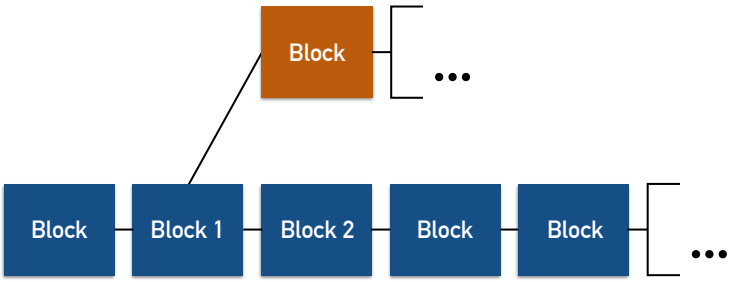


Figura 3.16: In blu la catena onesta, in arancione una catena alternativa.

[7] E' il citato problema del *double-spending*, per cui si era già espresso che la soluzione di Satoshi è la *Proof-of-Work* con conseguenti incentivi per comportarsi onestamente.

Matematicamente, questo tentativo da parte di un attaccante si può pensare come *Binomial Random Walk*, una catena di Markov a tempo discreto in cui:
p probabilità che la catena onesta si incrementa di un blocco
$q = 1 - p$ probabilità che la catena disonesta si incrementa di un blocco.

Immaginando che l'hacker abbia ricevuto, o ne fosse già in possesso, un tot di bitcoin in corrispondenza del blocco "1". Vengono spesi, mandati ad esempio ad un altro account. Nel miglior caso possibile questa transazione gli viene validata in quella subito successiva, "2". A quel punto l'attaccante vorrebbe rispendere la somma ricevuta, quindi cerca di costruire una catena alternativa. Nel frattempo però il network sta proseguendo nel mining, aggiungendo altri blocchi alla catena onesta. Non solo dunque deve gareggiare per battere la catena onesta, ma deve anche recuperare l'inevitabile svantaggio che si è creato. Questo si modellizza con la *Gambler's Ruin*, un giocatore che con infinita disponibilità economica vuole recuperare il suo svantaggio.
La probabilità che questo recuperi partendo da z blocchi indietro è

$$q_z = \begin{cases} 1 & se\ p \leq q \\ \left(\frac{q}{p}\right)^z & se\ p > q \end{cases}$$

Dunque condizione necessaria per la sopravvivenza del sistema è che il network sia gestito in maggioranza da nodi onesti che lavorano per validare le transazioni correttamente:

$$p > q$$

E' per questa ragione che viene spesso citato "*l'attacco al* 51%" come un pericolo da evitare. Se per esempio un *mining pool* avesse tale capacità di calcolo, potrebbe avere il controllo delle transazioni. Questo non è desiderabile per nessuno perché crollerebbe la fiducia e dunque il prezzo della valuta. Per questo motivo i miner si autoregolano spostandosi fra i vari gruppi.

La probabilità che un attaccante riesca a recuperare lo svantaggio diventa più piccola al crescere dei blocchi da recuperare z e al diminuire di q.

Ci si chiede quali siano le condizioni per cui un blocco e le transazioni al suo interno possano essere considerate valide senza possibilità di cambiamenti. Questo ovviamente dipenderà dal parametro q, non controllabile dal network perché non si può sapere chi sta minando in maniera onesta e chi no.

Il parametro su cui si può avere controllo è z, blocchi successivi da un certo punto in poi, chiedendoci quanti devono essere affinché sia matematicamente infeasible un recupero da parte dell'hacker.

In queste ipotesi il numero di blocchi che l'attaccante riesce ad aggiungere segue una *distribuzione di Poisson* con valore atteso $\lambda = z\,\frac{q}{p}$.

La probabilità che l'attaccante possa dunque avere la meglio sul sistema si ottiene moltiplicando la densità della distribuzione di Poisson nell'aver fatto un numero di blocchi k per la probabilità che riesca a recuperare lo svantaggio rimasto da quel punto raggiunto. Vengono sommati tutti i k possibili valori di tale scenario e uguagliato ad 1 meno la probabilità dell'evento contrario.

$$P = \sum_{k=0}^{\infty} \frac{\lambda^k\, e^{-\lambda}}{k!} \cdot \begin{cases} \frac{q}{p}^{z-k} & se\ k \leq z \\ 1 & se\ k > z \end{cases} = 1 - \sum_{k=0}^{z} \frac{\lambda^k\, e^{-\lambda}}{k!} \cdot \left(1 - \frac{q}{p}^{z-k}\right)$$

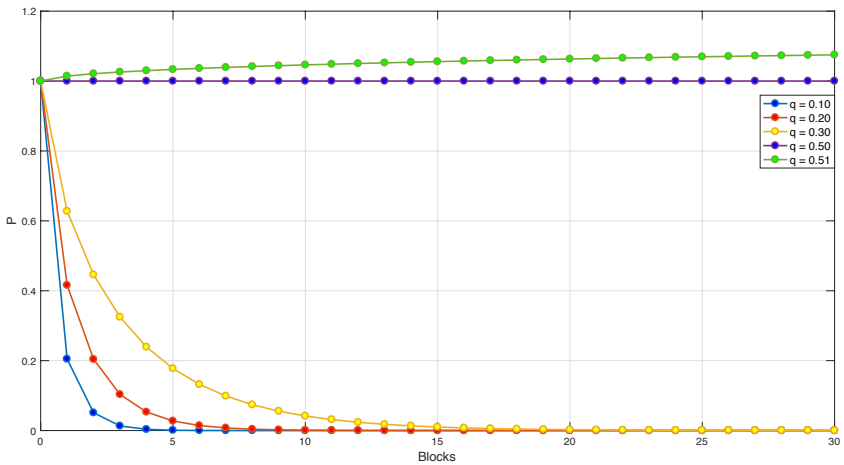


Figura 3.17: Probabilità P che un'attaccante riesca a recuperare lo svantaggio avendo la meglio sulla catena onesta al variare di z e per diversi valori di q.

Graficamente si osserva ciò che ci si aspetta: al crescere di q occorrono più z per avere lo stesso livello di sicurezza in quanto la probabilità P che l'attaccante riesca a recuperare aumenta.

Di contro, se q è fisso la probabilità che un attaccante riesca ad avere la meglio decresce rapidamente al crescere del distacco.
Se $q = \frac{1}{2}$ con probabilità 1 lo svantaggio verrà colmato e, anche se privo di senso dal punto di vista probabilistico, si osserva che con $q > 0.5$ il sistema è fortemente attaccabile.

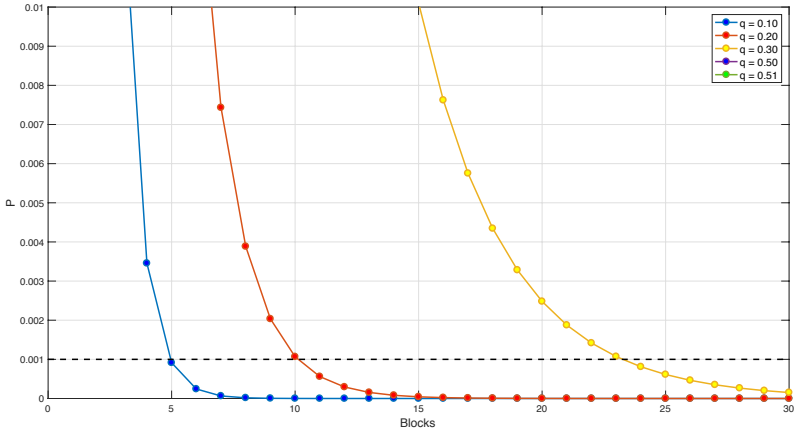


Figura 3.18: Zoom per trovare il numero di blocchi di vantaggio z che rendono sicuro il network.

Una soglia interessante e citata anche da Nakamoto potrebbe essere $P = 0.1\%$: ci si chiede cioè da che valore di z la probabilità P sia talmente bassa da considerare il sistema sicuro, al variare della potenza di calcolo avversaria q.
I tre casi in figura mostrano i valori

$$q = 0.1 \rightarrow z = 5; \qquad q = 0.2 \rightarrow z = 11; \qquad q = 0.3 \rightarrow z = 24;$$

Si può assumere che difficilmente degli attaccanti possano rimanere sul network molto tempo prima di essere identificati ed allontanati; dunque un $q > 0.1$ è improbabile. Ne segue che dopo circa 5 blocchi aggiunti il rischio è praticamente azzerato. [8]

[8] Considerazioni dello stesso tipo possono essere fatte nell'ottica di catene di blocchi orfani: nessun miner continuerebbe a lavorare su un'altra catena se quella vi è una avanti di cinque blocchi. Le transazioni al loro interno possono essere considerate approvate.

3.5.2 Sicurezza XRP LCP

Il sistema di consenso di Ripple è profondamente diverso da quello precedentemente trattato e dunque è necessario comprendere quanto e quando anche questo sia solido. La prima assunzione che viene fatta è che un nodo scorretto non possa mandare informazioni differenti a nodi distinti; si ipotizza cioè sincronia nei messaggi, aspetto non pienamente reale nel network.
Con la notazione utilizzata nel paragrafo 2.4.1, si dimostra la seguente proposizione [24]

Proposizione 3.5.1. *Due nodi P_i, P_j non possono validare ledger in conflitto se e soltanto se*

$$|UNL_i \cap UNL_j| > n_i - q_i + n_j - q_j$$

Dimostrazione. ($\Leftarrow$)
Sia P_i nodo che valida il ledger L e $|UNL_i \cap UNL_j| > n_i - q_i + n_j - q_j$.
Sia S l'insieme di nodi di UNL_i che hanno validato L; notoriamente $|S| \geq q_i$.
Alcuni in S appartengono anche ad UNL_j. Per dimostrare la tesi è sufficiente provare che

$$|S \cap UNL_j| > n_j - q_j$$

in quanto il numero dei nodi che hanno convalidato L che stanno anche in UNL_j ha sicuramente coperto il quorum necessario per P_j cosicché non possono essere approvati due ledger diversi.

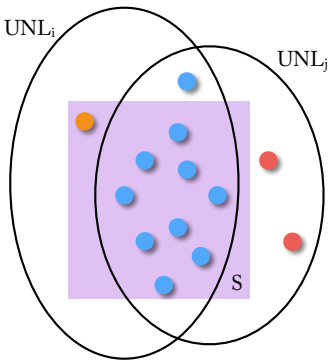


Figura 3.19: Esempio di verifica della condizione sufficiente per la sicurezza del protocollo.

Sfruttando le proprietà insiemistiche e l'ipotesi, si ha:

$$\begin{aligned}
|S \cap UNL_j| &= |S| - |S \setminus UNL_j| \\
&\geq |S| - |UNL_i \setminus UNL_j| \\
&= |S| - (|UNL_i| - |UNL_l \cap UNL_j|) \\
&> |S| - (n_i - (n_i - q_i + n_j - q_j)) \\
&\geq q_i - (n_i - (n_i - q_i + n_j - q_j)) \\
&= n_j - q_j
\end{aligned}$$

($\Rightarrow$)

- Se $|UNL_i \cap UNL_j| \leq n_j - q_j$ (e in maniera simmetrica $n_i - q_i$), potrebbe accadere che tutti questi nodi possono validare un ledger L, mentre i nodi in $UNL_j \setminus UNL_i$ un altro ledger $L^{'}$. In questo caso caso sarebbe possibile validare stati differenti.

- Se $|UNL_i \cap UNL_j| > n_j - q_j \ \wedge \ |UNL_i \cap UNL_j| \leq n_i - q_i + n_j - q_j$, allora

$$\begin{aligned}
|UNL_i \setminus UNL_j| &= |UNL_i| - |UNL_i \cap UNL_j| \\
&\geq n_i - (n_i - q_i + n_j - q_j) \\
&= q_i + q_j - n_j
\end{aligned}$$

  Potrebbe dunque accadere che i nodi in $UNL_i \setminus UNL_j$ validino L e che $n_j - q_j$ nodi in $UNL_i \cap UNL_j$ validino L. Sicuramente il quorum per P_i sarebbe raggiunto perché

$$|UNL_i \setminus UNL_j| + n_j - q_j \geq (q_i + q_j - n_j) + n_j - q_j = q_i$$

  Tutti i nodi in UNL_j non nell'intersezione delle liste potrebbero validare un certo L', così come anche i nodi nell'intersezione ad eccezione dei $n_j - q_j$ nodi citati in precedenza. In questo caso P_j validerebbe L'.

Queste due condizioni hanno portato ad un assurdo, dunque l'unica possibilità è che

$$|UNL_i \cap UNL_j| > n_i - q_i + n_j - q_j$$

□

Sotto tale ipotesi di sovrapposizione, la decisione presa sarà la stessa per entrambi i nodi. E' questa una condizione indispensabile per la sicurezza del sistema.

Nella pratica però, bisogna fronteggiare anche i problemi che nascono dal fatto che non ci sia perfetta sincronia e i nodi disonesti potrebbero mandare messaggi diversi a nodi differenti.
In tale scenario occorre introdurre ulteriori notazioni:
$O_{i,j} = |UNL_i \cap UNL_j|$
t_i, t_j numero al più di nodi scorretti in UNL_i, UNL_j
$t_{i,j} = min\{t_i, t_j, O_{i,j}\}$ numero massimo di nodi scorretti in $UNL_i \cap UNL_j$.
Si può provare con argomentazioni analoghe [9] alle precedenti che la condizione di sicurezza del sistema diventa la seguente:

Proposizione 3.5.2. *XRP Ledger Consensus Protocol garantisce sicurezza se per ogni coppia di nodi P_i, P_j:*

$$O_{i,j} > \frac{n_j}{2} + (n_i - q_i) + t_{i,j}$$

Questa condizione sufficiente, assumendo che il quorum richiesto sia dell'80% e la percentuale di nodi disonesti al più 20%, si traduce con il fatto che l'intersezione fra le UNL deve essere maggiore del 90%. Infatti, considerando il caso estremo in cui i nodi *faults* di entrambe le UNL siano tutti presenti nell'intersezione delle UNL,

$$O_{i,j} > 0.5\, n_j + 0.2\, n_i + 0.2\, min\,\{n_i, n_j\}$$

Per coprire nei vari scenari possibili sia il 70% di n_j che il 40% di n_i, la soglia che viene scelta è una sovrapposizione del 90%.

L'obiettivo, al fine di preservare la sicurezza del sistema, deve essere quello di assicurare che non sia possibile andare in uno stato in cui i nodi onesti si trovino ostacolati dal poter validare un nuovo ledger. Rendere questo processo snello, veloce e sicuro è l'obiettivo degli sviluppatori di Ripple, i quali si impegnano per trovare soluzioni efficaci[10].

[9] Una trattazione estesa e dettagliata si trova nell'articolo [21].
[10] *Cobalt* [32], nuovo algoritmo di consenso per ridurre i tempi di convalida delle transazioni.

3.6 Privacy

Un ulteriore aspetto fondante nell'attuale approccio all'uso del denaro è la necessità di privacy[11], ossia la proprietà che solo le persone interessate siano a conoscenza delle informazioni dello scambio. Sia pensando alla valuta cartacea che ai metodi di pagamento digitali, gli utenti partecipanti pretendono che la transazione rimanga privata quanto più possibile. Comprensibilmente questo aspetto ha sempre presentato dei limiti notevoli: nei pagamenti in presenza è quasi impossibile preservare la privacy assoluta, più semplice negli acquisti online. Solo le parti interessate condividono la singola informazione, senza alcuna conoscenza di altri scambi.
In un'ottica più ampia però, bisogna ricordare che questa presunta *privacy* è pur sempre parziale in quanto un'autorità centrale ha costante accesso ai dati dei suoi utenti, saldo compreso. Dunque fino ad adesso la popolazione è stata disposta a rinunciare a parte della propria privacy, in cambio di uno storage "sicuro" e dei servizi annessi.

Si è già osservato quanto il mondo delle criptovalute abbia stravolto ogni scenario e la gestione della privacy non fa eccezione: la Blockchain nasce come un database distribuito, dunque condiviso da tutti gli utenti partecipanti. Ognuno può e deve ricostruire tutti i movimenti di un account prima di validare una transazione richiesta assicurandosi che possieda la valuta necessaria. Si comprende subito quanto sia differente questo approccio e potenzialmente rischioso se non si mettono in pratica accurate misure.
Il primo aspetto noto è che **non è più necessario associare il vero nome al proprio account**, in quanto non vi è più una o più autorità che deve controllarne l'autenticità. E' sufficiente possedere una coppia di chiavi, una pubblica e una privata, così da provare la propria identità tutte le volte che è necessario tramite i protocolli di firma digitale tipici di ogni criptovaluta e descritti in precedenza. Questo sicuramente è un radicale cambiamento rispetto all'attuale assetto finanziario.
Non bisogna però fare l'errore di credere che questa misura basti per assicurare pri-

[11] Si ricordi che la privacy è diversa dall'*anonimato*, in cui non si conosce nemmeno con chi si sta comunicando.

vacy ai suoi utilizzatori; al contrario il protocollo di una criptovaluta deve essere costruito in modo da prevedere e rendere computazionalmente infeasible ottenere informazioni dai dati condivisi sulla Blockchain.
I tre punti da preservare da possibili attacchi interni ed esterni alla rete sono:

1. **l'identità** degli individui che compiono un'operazione;
2. **l'operazione** che viene effettuata e i dati che essa contiene;
3. **lo stato della blockchain** costituito dell'insieme di tutte le informazioni.

3.6.1 Pericoli

I rischi per la privacy degli utenti che partecipano ad una blockchain permissionless possono essere di differente natura. I primi controlli da fare riguardano il mezzo personale utilizzato per unirsi alla rete, dunque è necessario che nessuno possa effettuarne l'accesso in remoto: un buon AntiVirus, rifiutare Cookies, localizzazione tramite GPS o condivisione dell'indirizzo IP e criptare l'Hard Disk risultano assunzioni necessarie. Se queste misure non venissero applicate potremmo avere da subito problemi legati alla privacy della nostra identità e delle nostre operazioni.
Anche l'infrastruttura Internet utilizzata deve rispettare i più noti protocolli di sicurezza e non avere bachi che permettano ad un attaccante di osservare le nostre azioni.
La cronologia Browser può essere attaccata e far perdere privacy, così come la memoria delle transazioni salvate sul Client utilizzato per acquisto e vendita di valute. Azioni ad hoc possono aggirare questi ed altri problemi noti ma ci sono alcuni aspetti strutturali della blockchain che anche i più accorti sistemi non riescono ad affrontare pienamente.

Oltre all'utilizzo di uno pseudonimo, una seconda azione utilizzata dagli utenti di tutte le maggiori blockchain, già citato nel Capitolo 1 nella descrizione del protocollo Bitcoin, è quella di **utilizzare account diversi** per transazioni diverse. Anche questa pratica è certamente indispensabile; si pensi al caso in cui Alice manda dei bitcoins a Bob perché lo ripaga di un servizio commerciale. Se Alice usasse sempre

un unico indirizzo per tutte le sue transazioni, Bob potrebbe ripercorrere la blockchain condivisa e ricostruire subito tutte le transazioni in cui Alice ha partecipato con la sua chiave pubblica già utilizzata con Bob in precedenza. E' stato chiaro fin da subito che tale scenario non deve presentarsi.
Nonostante l'accortezza di cambiare spesso indirizzo, vi sono attacchi molto potenti che mirano a identificare gli utenti e noti come **transaction clustering**. Fra questi si identificano due euristiche molto note:

- *Co-spend cluster*, basati sull'assunzione che tutti gli input di una certa transazione sono in realtà riconducibili ad un unico individuo.
  Come già spiegato infatti, ogni transazione deve indicare gli input degli indirizzi dai quali provengono i bitcoins (ma discorso analogo per tutte le altre criptovalute che utilizzano una blockchain) e tutti gli output, ossia gli indirizzi di arrivo. Questa pratica permette alla rete di poter validare agevolmente una transazione proposta ripercorrendo a ritroso la catena assicurandosi che quell'indirizzo sia stato output di quella quantità da inviare.
  Ciò che assumono queste euristiche è la ragionevole ipotesi che una transazione con più input è tale perché ad un utente occorre una somma di bitcoins in più suoi indirizzi per spedirli. Sulla base di questo, e ancora una volta ripercorrendo tutta la catena, si clusterizzano gli indirizzi associandoli a singoli utenti. Questo non permette di conoscerne esplicitamente l'identità, ma è pur sempre una perdita di privacy.
  Inoltre, se anche fosse pubblica o nota a qualcuno l'identità di un singolo indirizzo nel cluster, anche tutti gli altri sarebbero ricondotti alla stessa persona così da essere totalmente riconoscibili.
  Anche dati esterni potrebbero essere utilizzati per riconoscere gli indirizzi, come ad esempio le informazioni degli exchange online in cui è necessario registrarsi con documenti ufficiali.

- *Shadow address guessing* sfrutta un'altra caratteristica delle blockchain: tutto ciò che si ha in un indirizzo di input deve essere speso allocando opportunamente in indirizzi in uscita, meno la dovuta percentuale delle fees. Dunque se in output ci sono due indirizzi, ci si attende che uno fra i due sia del mittente

per spedirsi indietro il resto. Fra i due viene scelto, se esiste, quell'indirizzo che non è mai comparso prima nella blockchain perché si ipotizza che è stato creato proprio con la finalità di raccogliere il resto. In questo modo un altro indirizzo viene associato al cluster dei mittenti.

3.6.2 Possibili soluzioni

Le minacce sono così tante e di natura differente che risulta impossibile fornire un unico protocollo da seguire che possa risolvere ogni problema.
Rimangono imprescindibili tutte le accortezze a minacce esterne alla nostra rete e ai nostri dispositivi, così come l'impegno a non essere localizzabili.
Aggirare le difficoltà legate alla struttura delle blockchain è più difficile e spesso anche con i seguenti metodi proposti qualche aspetto rimane comunque incompleto. E' fondamentale tenerlo sempre presente nel caso si voglia procedere all'implementazione.

Zero knowledge Proof

Uno fra gli approcci proposti per aggirare i problemi di privacy intrinsechi della blockchain precedentemente esposti è quello della **zero knowledge proof**. Per comprenderlo occorre introdurne le principali caratteristiche.

Definizione 3.6.1. *Un protocollo si definisce* ***zero knowledge proof*** *quando il* ***prover P*** *riesce a dimostrare di essere in possesso di una informazione al* ***verifier V****, senza dover rilevare la stessa.*

L'utilità di questi protocolli è evidente in quanto permette di autenticare gli utenti senza dover condividere, e dunque senza porre in un potenziale rischio, nessuna chiave, password o parte del messaggio.
In letteratura esistono differenti protocolli di tale natura, fra cui *Fiat e Shamir* oppure quello di *Schnorr*.
Come già osservato, questi protocolli prevedono due figure, quella del Provatore e quella del Verificatore; quest'ultimo fa molte domande accertandosi così che il Provatore abbia realmente l'informazione segreta. Questa dinamicità li rende noti come

protocolli interattivi.

Nella tecnologia blockchain si richiede però che la prova a conoscenza nulla avvenga in modo **non interattivo**, ovvero il Prover risponde a delle domande randomiche automatizzate così da generare una singola prova che tutti gli altri partecipanti al network possono verificare.
L'obiettivo principale è mostrare di avere la chiavi di un certo account (e dunque possedere la valuta all'interno) senza rivelare le chiavi stesse.
Ciò che attualmente ostacola l'applicazione di tale protocollo è un costo computazionale alto che, sommatosi a quello della Proof of Work, renderebbe ancora più lento il protocollo. Inoltre il file di prova da mostrare deve essere accettato da tutti, nonostante scelto da un sottoinsieme di nodi, aspetto contrario al principio di completa decentralizzazione.

Un'applicazione di ZKP è la già trattata **firma digitale**: chi manda un messaggio firmandosi prova di avere la chiave privata senza inviarla direttamente ma effettuando dei calcoli che solo il reale possessore della chiave poteva compiere. Dunque anche in questo caso il Prover dimostra di conoscere un segreto ai Verifier. Ciò che è importante affinché sia zero-knowledge è che la firma apportata non riveli nessuna informazione sulla chiave segreta[12].
Tecniche particolari di utilizzo delle firme digitali permettono di accrescere la privacy dei partecipanti:

- **firme ad anello** con tutte le chiavi pubbliche di un certo sottoinsieme (rigorosamente causale!) di utenti più la chiave privata personale. In questo modo si nasconde maggiormente l'origine della transazione, in quanto non si conosce da chi è stata inviata.

  Il problema di tale protocollo, implementato per la prima volta in *Monero*,

[12]Nel Capitolo 1 è stato presentato il Protocollo di firma digitale ECDSA usato in Bitcoin e la difficoltà del logaritmo discreto su curve ellittiche assicura che inviando la coppia (r, s) non sia possibile risalire a nulla della chiave privata.

era di dover scegliere fra transazioni con lo stesso importo; questo ne limitava notevolmente la possibilità di scelta. Dunque nel caso in cui l'importo fosse non usuale e presente poche volte nella blockchain, le firme ad anello prendevano pochi input e la sicurezza del protocollo inevitabilmente si riduceva perché più semplice risalire al vero mittente.

- **Aggregate signature** dove più persone firmano lo stesso messaggio, non con firme multiple, bensì producendo un'unica firma per ogni transazione.
  Questo potrebbe aumentare notevolmente la privacy della blockchain, non sapendo più quanti abbiano firmato una transazione, ma il problema è che non possono essere implementate con gli attuali metodi di firma utilizzati[13].

Ulteriori protocolli di ZKP sono stati implementati in criptovalute come **Zcash** e sono noti come **zk-SNARK**: *zero-knowledge Succint Non-interactive ARgument of Knowledge*. Ognuna di queste parole sintetizza un aspetto importante:
- Succint, in quanto la lunghezza della proof deve essere piccola e i tempi di verifica brevi;
- Non-interactive, nella modalità spiegata in precedenza;
- ARgument poiché deve essere computazionalmente impossibile convincere i verificatori di una prova falsa;
- Knowledge da dimostrare senza rivelare nulla dell'informazione segreta.

Transazioni Confidenziali

Un ulteriore ambito di ricerca attualmente perseguito per aumentare la privacy di questi protocolli è quello delle *Confidential Transaction* che provano a risolvere la questione in un modo diverso, ossia nascondendo non tanto il mittente, quanto il *valore* della transazione, che per l'appunto viene criptato.
Il problema evidente di questo approccio è evitare che un attaccante possa far approvare transazioni il cui valore non è in accordo con la valuta realmente posseduta, ricordando che nelle blockchain stile Bitcoin, ogni utente deve validare la transazione

[13]Uno dei motivi per cui Bitcoin, Ethereum ed altre criptovalute stanno pensado di utilizzare nuovi protocolli di firma digitale è anche quello di rendere implementabili le aggregate signature.

richiesta osservando tutti i passaggi di valuta precedenti e affermando che l'importo da inviare sia realmente nell'account del mittente.
Una fra le soluzioni proposte è quella di sfruttare la **crittografia omomorfica**, che permette di eseguire operazioni su informazioni criptate senza bisogno di decriptarle. Nello specifico occorre sfruttare la proprietà:

$$Enc(val_1 - val_2) = Enc(val_1) \; - \; Enc(val_2)$$

Anche in questo caso l'utilizzo di tale approccio è ostacolato dagli attuali metodi di firma e i nuovi proposti mirano ad oltrepassare questo problema.

Mixer

Catalogati come "servizi esterni", i mixer hanno l'obiettivo di mischiare input e output di diverse transazioni in un'unica, così che non siano più noti i collegamenti fra gli indirizzi.
L'output viene rinviato ad altri account, collegati sempre agli originari destinatari, ma proveniente da un mittente unico.
Un esempio di mixer è il **CoinJoin**: sviluppato da Greg Maxwell, uno fra i principali programmatori di Bitcoin. Ciò che viene fatto è unire in input diverse transazioni (devono avere lo stesso importo) inviandoli al mixer; questo poi manderà una nuova transazione sul network così che ognuno degli input riceverà su un nuovo indirizzo lo stesso importo in modo randomico.
In questo modo, se tanti ne facessero uso, l'euristica *co-spend cluster* verrebbe progressivamente abbandonata.

I problemi di tali protocolli sono legati all'eventuale poca sicurezza di unire le proprie transazioni ad altre potenzialmente non legali, oltre alla fiducia in un'autorità centrale che dovrebbe regolare i mixer.

Capitolo 4

Stablecoin

"What is needed is an electronic payment system..."

Così aveva scritto Satoshi Nakamoto nel suo Paper [4] riferendosi al sistema Bitcoin. La sua idea era quella di stravolgere il mondo della finanza, annullando il ruolo delle banche, dei governi, sostituendo le monete presenti con una nuova valuta digitale decentralizzata.
Quanto la sua innovazione abbia stravolto i mercati finanziari è stato indagato approfonditamente nei capitoli precedenti. E' emerso però anche un altro aspetto intrinseco delle criptocurrencies: l'**elevata volatilità** sembra aver delegato Bitcoin e le altre Altcoin ad un interessantissimo asset di investimento, allontanandolo dalla funzione di mezzo di pagamento designata da Nakamoto.
Il prezzo di un bitcoin in dollari oscilla in maniera estremamente rapida ed imprevedibile ogni giorno; questo rende molto difficile usare le criptovalute come mezzo di scambio. Si pensi ad un commerciante che voglia accettare i bitcoin per essere ripagato di un servizio; quando viene effettuato il pagamento si trova il corrispettivo di valuta pari al bene dato o al lavoro eseguito, ma il giorno dopo quella quantità di bitcoin potrebbe valere la metà, così come il doppio, [1] rispetto al giorno precedente. Come può stabilire il giusto prezzo di vendita, come può gestire i suoi bilanci senza rischi? Così non si può pensare di sostituire le valute tradizionali.

[1] Rapportando il valore di bitcoin in dollari o in euro.

Ma il mercato scorre, così come le idee, e per nuovi problemi vengono presentate nuove soluzioni.

Già nel 2012 venne pubblicato il White Paper di *Realcoin*, una valuta che, sfruttando il protocollo blockchain di Bitcoin, avrebbe replicato l'andamento di un certo asset. Negli anni il progetto proseguì cambiando nome nel noto *Tether* e legandosi a valute differenti quali il dollaro, l'euro e lo yen. Era il 2015 quando iniziò a diffondersi sui principali *exchange* online.
Gli anni dal 2017 in poi hanno visto una rapida ascesa nel lancio di **stablecoin**: aziende private, sviluppatori, ma anche grandi banche e persino Stati stanno pensando o hanno già lanciato progetti in tale direzione.

Da alcuni dati riportati in [35], si può notare che la quota di Market Cap di alcune fra le più influenti è cresciuta in maniera rilevante da metà del 2017 in poi.
Due fra le più influenti valute stabili, quali *Binance Coin* e *Tether* che insieme coprono più dell'80% del Market Cap stablecoin in data 26 Aprile 2020, hanno negli anni incrementato la loro percentuale di dominanza sul mercato delle criptomonete passando da percentuali vicine allo zero, fino a circa il $2-3\%$ ognuna di loro. Uno scenario analogo si presenta considerando complessivamente tutte le numerose stablecoin che sono state lanciate.

Il motivo del crescente interesse è evidente e ricalca quanto detto anche in precedenza: la propensione verso il mondo delle criptovalute è ormai visibile a tutti e, per non venir spazzati via dal sistema finanziario, anche istituti di stampo "storico" devono trovare il modo di legarsi al "nuovo". Bitcoin e le altre Altcoin sono state sempre bocciate con forza e l'alta volatilità, come detto, le allontana attualmente dal ruolo di mezzo di scambio alternativo. Se queste però, sempre basandosi sul principio della decentralizzazione tipico della blockchain, riescono ad essere maggiormente stabili, allora ecco perchè diventano le candidate ideali.
Quanto tali criptovalute riescano a rimanere realmente **decentralizzate** è sicuramente oggetto di discussione.

Lo scenario è ancora una volta il più variegato possibile e la loro presenza sul mercato è forte. Bisogna ricordare che queste vengono comunque annoverate fra le criptomonete e la loro quota di mercato è perciò inclusa in quel numero enorme del Market Cap complessivo 218.899.944.776[2].

Ancora una volta *Young Platform* è reattiva su questa nuova frontiera e le stablecoin scambiabili dal portale sono **USD Coin** e **PAX Gold**. Di queste due viene effettuata una trattazione approfondita.

4.1 USD Coin

A Maggio del 2018 la società *Circle*, una startup di *Goldman sachs*,[3] lancia il progetto ***USD Coin***. Per la prima volta una grande istituzione finanziaria ha investito nel settore delle criptovalute promuovendo un token basato su una architettura open-source che permetta di partecipare attivamente come sviluppatori, ma che al contempo sia stabile rispetto al dollaro.
Dapprima scambiato nell'exchange *Poloniex*[4], in pochi mesi è stato accolto dalla maggior parte dei portali online.

Figura 4.1: Prezzo USD Coin da Ottobre 2018 ad Aprile 2020, fonte [11].

[2]Valore riportato da *CoinMarketCap*in data 26 Aprile 2020.
[3]*Goldman sachs* è una banca d'affari americana, una fra le più grandi del mondo.
[4]Circle ha acquistato recentemente il sito Poloniex.

USD Coin è uno fra i tantissimi **Ethereum Request Comment: Token ERC-20** presenti sul mercato, ossia valute digitali basati sul network di Ethereum e che seguono degli standard ben precisi e noti agli sviluppatori.
In particolare questi smart contract presentano sei parametri obbligatori più tre consigliati. I tre parametri opzionali riguardano il nome, il simbolo e la frazione del token che è possibile scambiare, espresso tramite il numero di cifre decimali ammissibili. Le sei funzioni obbligatorie sono:

- **totalSupply**, che specifica la quantità massima di token in circolazione e che impedisce di crearne in più;
- **balanceOf** inizializza la corretta quantità di token sugli indirizzi dei proprietari iniziali;
- **transfer** per spostare i token fra gli utenti che investono nel periodo dell'Initial Coin Offering;
- **transferFrom** per lo scambio continuo di token fra tutti gli utenti;
- **approve**, che si assicura della possibilità di distribuire ancora token;
- **allowance** verifica che un indirizzo possieda abbastanza quantità di valuta per effettuare la transazione ad un altro indirizzo.

Come specificato sul sito di USD Coin [33], la tecnologia CENTRE è quella usata per permettere la stabilità rispetto al dollaro e comunicare con gli smart contract di Ethereum; verrà trattata approfonditamente nel successivo paragrafo.

4.1.1 Centre

La vision di CENTRE è quella di permettere la diffusione di un "open internet" in cui gli utenti possano partecipare alla network distribuita seguendo un protocollo comune. Le innovazioni crittografiche, e in primis la tecnologia blockchain, permettono lo scambio di valore immediato, sicuro e con bassi costi di transizione in tutto il mondo. In futuro l'economia sarà, viene scritto nel paper [34], *open, shared, inclusive, distributed.* Questi principi risultano comuni alle criptovalute, ma in più

CENTRE si pone l'obiettivo di implementare un protocollo per ridurre la volatilità e raggiungere una maggiore scalabilità nelle transazioni.
L'obiettivo finale è quello di poter effettuare pagamenti senza alcun ostacolo in caso di valute digitali, e non, differenti. CENTRE è stata fondata come un'organizzazione indipendente, sebbene sia originariamente legata a *Circle*, la cui governance è delegata al network gestito da meccanismi di voto e consenso distribuito.

Il protocollo prevede i seguenti step:

1. Un utente decide di creare un account e deposita una certa quantità di dollari americani dalla sua banca all'applicazione web di USD Coin ricevendo il corrispettivo in token. Questi possono essere o coniati oppure trasferiti da un fondo disponibile.

2. L'utente può usare i token per la propria attività di trading; CENTRE preserva la sicurezza degli utenti con delle "liste nere" di account negativi impedendo scambi con essi.

3. Se l'utente desidera riscattare i token per ritirare i dollari, è sufficiente che depositi i token su un apposito indirizzo e gli sarà accreditato il corrispettivo in fiat.

Oltre a scambi sul mercato finanziario, accettare CENTRE come intermediario può permettere il pagamento immediato anche di servizi di uso quotidiano: è sufficiente che sia l'acquirente che il venditore utilizzino applicazioni che approvino tale protocollo così da poter inter-operare. Qui la grande rivoluzione nel poter finalmente utilizzare un asset digitale come mezzo di scambio.
Anche l'invio di denaro tramite criptovalute diventa semplice e veloce: è sufficiente che i wallet di entrambi supportino CENTRE così che l'exchange del mittente di bitcoin proponga un tasso di cambio con i dollari. Se questo viene approvato allora la transazione viene eseguita e salvata nella blockchain Bitcoin ed Ethereum.

Chi intende partecipare al network deve possedere un nodo che gli conferisce diverse abilità: emettere valuta digitale, decidere quale asset accettare come scambio,

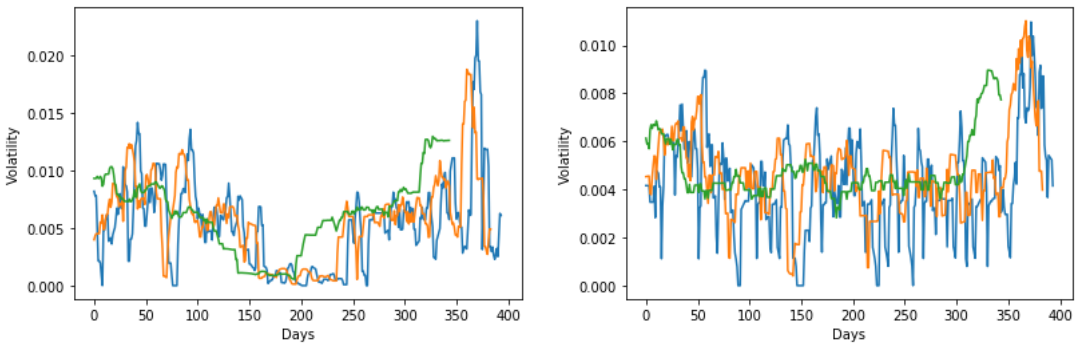
scegliere il proprio tasso di cambio, scambiare i metadata di una transazione prima di approvarla, assicurarsi della correttezza degli aggiornamenti degli stati.

Il modo in cui CENTRE assicura la stabilità del prezzo di un token è dunque attraverso un approccio **fiat-collateralized:** le riserve di una moneta reale, nel caso specifico il dollaro, provvedono ad ancorare il valore dei token emessi al valore del fiat depositato. Questo chiaramente allontana un po' dal principio di decentralizzazione completa perché è necessario che uno o più enti, tipicamente di stampo finanziario, assicurino ingenti depositi di asset tradizionale. CENTRE cerca di "distribuire" tale compito a diversi emittenti, sempre assicurandosi che rispettino i principi di solvibilità.

I contratti che regolano il sistema sono *open-source*, soggetti a revisione da parte di sviluppatori da tutto il mondo.

4.1.2 Volatilità

Come spiegato precedentemente, il problema principale da superare di Bitcoin e delle *Altcoin* è l'elevata volatilità. Nel Capitolo 3 si era calcolata per Bitcoin e le altre criptovalute osservando che non solo era molto elevata, ma nettamente superiore confrontata con i principali titoli azionari americani [5].



(a) USD Coin (b) Euro

Figura 4.2: Volatilità al variare di M: in blu $M = 5$, in arancione $M = 10$, in verde $M = 30$. Valori da Ottobre 2018 ad Aprile 2020.

[5] Bitcoin registra una volatilità a 10 giorni che sfiora spesso il 10%, Ethereum, Litecoin e Ripple raggiungono anche valori più elevati.

Ad eccezione dell'ultimo periodo che ha visto una turbolenza elevata dei mercati finanziari e anche del valore dell'Euro rispetto al dollaro, la volatilità della stablecoin USD Coin oscilla in un range molto ristretto e generalmente comparabile con le oscillazioni della moneta dell'eurozona. Risulta ragionevole adesso pensare di utilizzare questa valuta per acquisti quotidiani, così come viene utilizzato l'Euro, soggetto pur sempre ad un tasso di cambio variabile, il cui rischio può essere affrontato da imprese, istituti finanziari, ma anche privati cittadini. Il cambio di paradigma economico e sociale è senz'altro evidente.

L'attuale rilevanza di questa valuta è sottolineata anche dalla recente scelta di **Maker DAO**, una stablecoin molto influente il cui meccanismo di stabilità è assicurato dal deposito di beni collaterali crypto e trattata in seguito. Fino a metà Marzo 2020 gli asset accettati erano *ether* e *BAT*[6]; la proposta di aprire anche agli USC Coin è stata accettata ed è divenuta attiva a partire dal 18 Marzo 2020.

4.2 PAX Gold

Nel 2012 è stata fondata una fra le tante aziende in ambito cripto-asset: *Paxos*. L'obiettivo, ancora una volta, è rivoluzionare l'assetto finanziario rendendo possibile scambiare beni e denaro in tutto il mondo in maniera rapida, sicura e con bassi costi di transazione. Negli anni ha creato una rete di fiducia nell'ambito dei servizi finanziari venendo riconosciuta da importanti investitori istituzionali e privati. Nel 2018 viene lanciato il token *Paxos Standard*, stablecoin ancorata al dollaro; a Settembre 2019 viene invece lanciato [36] il nuovo progetto **PAX Gold**.

L'importanza storica dell'oro nei millenni è ampiamente nota, si pensi alle diverse testimonianze in documenti sacri e non sull'utilizzo di questo bene come mezzo di scambio. In tutto il mondo il metallo è stato considerato come "prezioso", probabilmente per le sue proprietà chimiche altamente stabili[7] e per il suo aspetto glorioso,

[6]BAT: Basic Attention Token utility token pensato per inserzioni e pubblicità digitale.

[7]Nel white paper [36] vengono citate le caratteristiche che hanno contribuito a rendere l'oro così importante: scarsità, stabilità chimica, malleabilità, bellezza.

lucente. Di fatto l'oro è sempre stato il principale metallo monetario. Dal diciottesimo secolo l'economia europea coniò monete con una certa quantità di oro che ne determinava il valore. Inevitabilmente però si manifestarono nel tempo problemi di natura pratica, come trasportare in sicurezza grandi quantità di denaro o riuscire a regolamentarne l'offerta adeguata.
Si cominciò a diffondere un sistema di moneta cartacea a fronte della quale veniva posto in riserva il corrispettivo in oro. La politica monetaria ha subito nei secoli cambiamenti sostanziali e molto delicati che, al fine di essere pienamente compresi, necessiterebbero una trattazione approfondita. Ciò che qui ci si limita ad osservare è l'importanza strategica di un bene che non passa inosservato nemmeno nel mondo criptocurrency.

Da un paio di anni sembra si stia lentamente tornando al "Gold Standard", in quanto un gran numero di banche centrali[8] ha deciso di acquistare ingenti tonnellate di lingotti d'oro. Un "bene rifugio" visto da tanti come un modo per emettere nuovo denaro contante senza rischio e da alcuni esperti trattato come un sostituto alle obbligazioni. Al di là dei tecnicismi e delle interpretazioni economiche, l'interesse oggi verso l'oro è elevatissimo e il progetto PAX Gold lo rende accessibile a tutti: è possibile acquistare oro di qualità elevata per una quantità arbitraria.
La qualità dell'oro è certificata dalla *London Bullion Market Association* e *London Good Delivery*. Nella capitale britannica sono conservati in caveau di massima sicurezza i lingotti di circa 400 once ognuno, puri almeno al 99.5%, ognuno con un numero seriale ed il relativo peso.
Il token scambiabile si comporta nel seguente modo:

$$1\ PAXG = 1 \text{ lingotto d'oro}$$

ma è possibile specificare fino a 18 cifre decimali della quantità richiesta. E' sempre possibile convertire PAX Gold in oro o in dollari o viceversa. Poiché è possibile acquistare una frazione ordinaria di lingotti, al fine di garantire la minor dispersione

[8]Soprattutto si tratta di banche europee, ma sono molto interessate anche la Cina, India, Russia e Turchia.

possibile, Paxos cerca di riallocare in una stessa barra le diverse frazioni per ogni indirizzo degli acquirenti.

La tecnologia blockchain utilizzata è ancora una volta quella Ethereum con protocolli del tipo **ERC-20** precedentemente introdotti, rivendicando così la natura decentralizzata ed automatizzata degli smart-contract.

Un ulteriore punto di forza del progetto PAX Gold sono le **basse tasse**: non vi sono pagamenti sul deposito dei lingotti d'oro ma solo quelle legate alla transazioni, lo 0.02% del valore, oltre alle tasse richieste da Ethereum, che come noto sono molto basse.

Figura 4.3: Prezzo Pax Gold da Settembre 2019 ad Aprile 2020, fonte [11].

Il ruolo di "bene rifugio" è ben visibile dal grafico in figura 4.3 in quanto le oscillazioni nel tempo del prezzo di 1 PAX sono lievi e rivelano un andamento tendenzialmente crescente.

Una prima misura interessante è il **ritorno di investimento** (con lag temporale 1) di PAX Gold messo a confronto con i corrispondenti valori di ritorno per l'Oro.

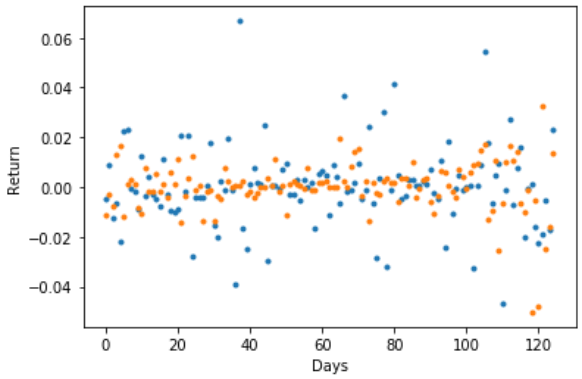


Figura 4.4: In blu PAX Gold; in arancione l'Oro.

Graficamente ci si può accorgere che le variazioni del ritorno giornaliero non sono elevate tanto quanto lo erano nello scenario delle *altcoin*, oscillando su valori molto più bassi e ben paragonabili con un bene storicamente stabile come l'oro.
Il confronto appare rilevante non solo per la loro natura chiaramente legata, ma anche per la forte correlazione statisticamente significativa fra i valori dei due asset: $\rho = 0.8775386$. In figura 4.5 si ha contezza visiva di come al crescere di uno tende a crescere anche l'altro.

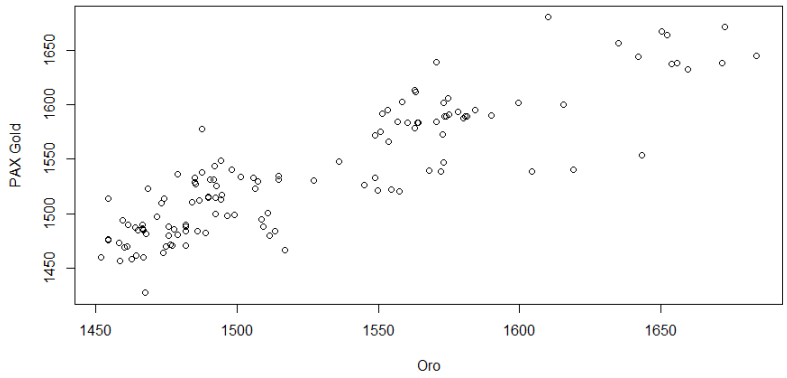


Figura 4.5: PAX/Oro da Settembre 2019 ad Aprile 2020.

4.2.1 Volatilità

Un'altra utile misura per rendere oggettiva l'idea sulle stablecoin è il calcolo della volatilità, ancora una volta con le stesse modalità presentate nel capitolo precedente.

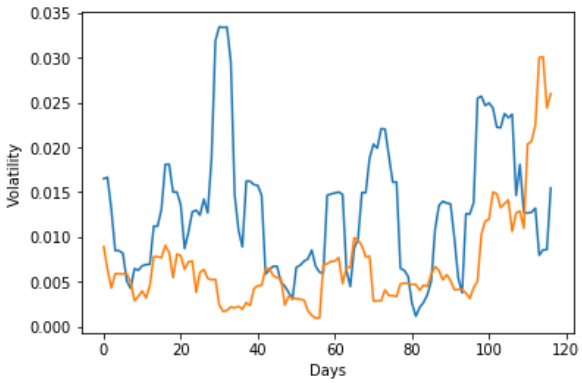


Figura 4.6: Volatilità con M=5. In blu PAX Gold; in arancione l'Oro.

La scarsa quantità di dati dovuta al recente lancio sui mercati induce a settare il parametro M, indicante il numero di osservazioni giornaliere di prezzo da utilizzare,

pari a 5. In figura 4.6 si ha ancora una volta il confronto con l'oro.
Emerge chiaramente che la stablecoin PAX Gold ha una volatilità maggiore rispetto a quella del suo bene sottostante, e questo ci appare ragionevole se si pensa ai numerosi vantaggi che questa comporta (frazionamento dell'asset, sicurezza nello store, immediatezza negli acquisti, decentralizzazione). Il "prezzo da pagare" rispetto ad investire direttamente nel mercato dell'oro è dunque un'incertezza maggiore, circa dello 1.5%, rispetto allo 0.5% circa. Una differenza sì presente, ma nulla confrontata ad esempio alla differenza fra le volatilità delle *altcoin* rispetto ai titoli azionari americani[9].
Infine è possibile osservare che anche il mercato dell'oro ha subito variazioni considerevoli nell'ultimo periodo considerato essendo aumentata in maniera visibile la volatilità. Si può osservare che queste oscillazioni sono state invece ben assorbite dal mercato PAX Gold in quanto non si sono registrati variazioni considerevoli nella sua volatilità e presentando valori stabili rispetto ai giorni precedenti. Questo aspetto ci conferma ancora una volta la grande forza stabilizzante di questo criptoasset.

4.3 MakerDAO

Le due stablecoin precedentemente analizzate sono radicalmente diverse fra loro se si pensa al bene collateralizzato o alle modalità di storage dell'asset. Quello che invece le accomuna profondamente è la tecnologia utilizzata, ovvero la blockchain Ethereum ed i contratti ERC-20, così come il principio per cui le aziende che hanno dato l'avvio a tali idee possiedono riserve fisiche di dollari o di oro che permettono di mantenere stabile il valore di un USD Coin o di un PAX. Le due analizzate sono fra le più note attualmente, ma tantissime altre stablecoin sono presenti sul mercato con caratteristiche analoghe.
Quello che visibilmente manca a questi protocolli è una vera e propria forma di *decentralizzazione:* se è vero che le transazioni avvengono velocemente, in maniera condivisa e con bassi costi di transazione grazie alla blockchain di Ethereum, è al-

[9]Il suddetto confronto è stato analizzato nel Capitolo 3, paragrafo *Analisi comparativa dati storici*.

trettanto vero che gli utenti affidano i loro asset collaterali ad un'azienda, una nuova autorità centrale. Questo non solo potrebbe presentare dei rischi, ma va contro la filosofia cardine delle criptomonete e di un mondo libero da un "potere finanziario centralizzato".
Inoltre tali soluzioni non permetteranno mai il passaggio ad una nuova economia visto che dollaro, euro, oro fungono da base anche in questo nuovo paradigma.

In tale clima di forte opposizione si colloca **MakerDAO**, un progetto di Ethereum sviluppato a partire dal 2015 e che ha subito nel tempo diverse innovazioni. Il primo White Paper [38] viene pubblicato nel 2017 introducendo il *Dai Stablecoin System*; nel Novembre del 2019 il protocollo Maker si evolve presentando le caratteristiche attualmente in vigore nel **Multi-Collateral Dai** [39].
La valuta corrispondente è il **Dai** e il legame mantenuto con il dollaro è 1:1.
Nella prima fase di Maker l'unico asset accettato per avere Dai in cambio era l'ether; nel multi-Collateral si è aperti a *BAT, SAI*[10]. Recentemente sono stati aggiunti anche *USD Coin* e *WBTC, wrapped Bitcoin*, token ERC-20 che punta ad uno scambio più veloce di liquidità Bitcoin sulla blockchain di Ethereum.
Ciò che lo rende molto interessante è non tanto la tecnologia utilizzata per effettuare gli scambi, ancora una volta Ethereum con lo standard ERC-20, ma il meccanismo di gestione della stabilità costruito ad hoc per gestire tutte le potenzialità e le difficoltà legate al mondo delle criptomonete. La descrizione del protocollo è articolata ed è opportuno presentarla per step.

4.3.1 Partecipanti interni ed esterni

Al fine di preservare la stabilità del valore della valuta, alcune figure esterne alla blockchain hanno un particolare ruolo.

- **Utenti:** chiunque voglia partecipare al Network per l'acquisto, vendita o deposito di Dai. Non vi sono restrizioni se non quella di seguire il protocollo della blockchain Ethereum e degli smart contract ERC-20.

[10] I Dai della fase mono-collateral.

- **MKR Voters:** oltre alla valuta Dai, un token molto importante è il **MKR**. Ne sono stati creati un milione e distribuiti fra gli sviluppatori della piattaforma e altri utenti che hanno avuto un ruolo determinante.
  Possedere un MKR è come essere "un'azionista" perché corrisponde ad "un voto" in decisioni come la scelta di nuovi asset collaterali, la modifica di parametri del sistema, aggiornamenti. Ad oggi il 25% è ancora nelle mani della fondazione MakerDAO e questo rende non pienamente decentralizzato il sistema.

- **Keepers:** utenti solitamente automatizzati, hanno il ruolo di mantenere la stabilità del valore della valuta, dunque vendono Dai quando il prezzo è più alto rispetto al valore target e acquistano quando è più basso.
  Non ci sono restrizioni e tutti potrebbero partecipare come keepers, ma la grande quantità di dati della blockchain Ethereum, insieme ad una difficoltà reale nel software da implementare, delega questo ruolo a pochi partecipanti.
  Potranno anche partecipare alle aste di liquidazione, come trattato in seguito.

- **Price Oracles:** forniscono informazioni sui prezzi di mercato dei collateral. In totale sono tredici, autonomi e spesso automatizzati. Come protocollo di sicurezza, per proteggere il sistema da eventuali attacchi da parte degli stessi oracoli, le comunicazioni vengono trasmesse con un ritardo di un'ora, così che ulteriori controlli possano essere effettuati. Nel caso di dubbia correttezza, il voto di qualcuno di essi viene sospeso.

- **Emergency Oracles:** accuratamente selezionati per poter svolgere la funzione di controllo dell'operato degli altri oracoli e di ulteriori rischi per gli utenti, autorizzati a prendere anche decisioni estreme per salvaguardare gli asset.

- **Team DAO:** esterni alla Maker Foundation, forniscono servizi di supporto alla comunicazione, governance e studi sul rischio finanziario legato agli asset collaterali.

4.3.2 Vault

Come già introdotto, MakerDAO è un progetto di Ethereum e come tale ne eredita tutti gli aspetti tecnici. Nello specifico ogni utente, per avere una certa quantità di Dai, deve creare una sorta di portafoglio digitale noto come *vault*, attraverso l'apposito smart contract. La piattaforma direttamente collegata a MakerDAO per far ciò è **Oasis Borrow**. Recentemente però tanti altri siti di exchange hanno permesso l'acquisto e la vendita di Dai.

I Dai vengono generati per l'utente che li richiede a fronte di un adeguato valore di collateral vincolato nello smart contract provocando un debito.

Dal momento che i collateral accettati dal protocollo sono cripto-asset e considerata la loro elevata volatilità, è necessario che il valore sia sempre più alto rispetto a quello del debito. Questo è l'aspetto chiave che permette la stabilità della valuta nonostante si basi su asset tutt'altro che stabili.

Quanto il valore dei collateral deve essere maggiore non è lasciato al caso o alla libertà personale, ma viene settato un **rapporto di liquidazione**, attualmente [11] pari al 150% per ether, BAT e WBTC, 125% per USD Coin. Ci si aspetta dunque che, per ogni Dai posseduto, bisogna provvedere con asset pari a quasi 1.5 dollari.

E' fondamentale rispettare il rapporto di liquidazione perché, se così non fosse, il sistema vede troppo rischioso quel vault e può procedere con protocolli di stabilizzazione.

Dal momento che il valore degli ether, così come quello degli WBTC, è estremamente variabile e potrebbe dimezzare (così come raddoppiare!) in poche ore, è necessario non stare mai troppo vicini al rapporto delineato: una variazione improvvisa potrebbe mandare il vault in liquidazione. Di questo rischio sono ben consapevoli gli utenti che, di fatto, stanno vincolando beni per un valore nettamente più alto. Basta osservare sul sito [40] che il **collateral Ratio** si aggira intorno al 365%.

Quando si vorrà riscattare il collateral è sufficiente ripagare il debito; va inoltre pagata in Dai una **commissione di stabilità** in base al tipo di asset vincolato nel vault. Attualmente questa commissione è settata a zero per tutti eccetto che

[11] Alla data 09/05/2020.

per WBTC, pari all' 1%. Questa tassa verrà inserita in un altro smart contract, il **Maker Buffer** e permetterà di far fronte ad eventuali criticità.
Questo parametro riesce a regolare l'offerta di Dai: quando il prezzo di mercato è troppo basso probabilmente vi è troppa offerta. Aumentando la commissione di stabilità, minore sarà l'incentivo ad aprire vaults perché più Dai devono essere restituiti. In questo modo il prezzo di mercato tende ad aumentare. Viceversa abbassando la commissione di stabilità, l'effetto finale è un aumento dell'offerta con l'obiettivo di incentivare l'acquisto di Dai.

Un'interessante possibilità che viene data agli utenti è quella di poter fissare Dai in dei contratti DSR **Dai Savings Rate** ricevendo gli interessi corrispondenti al tasso stabilito. Non vi sono limitazioni sulle quantità né restrizioni su quando e come poter accedere nuovamente alla risorsa vincolata. I premi per il saving rate sono attinti dal fondo *Maker Buffer*. Ancora una volta questa misura è stata pensata per stabilizzare il valore di mercato di un Dai avvicinandolo al prezzo target di 1 dollaro. Infatti quando vi sono delle fluttuazioni che causano instabilità, i MKR voters possono modificare le condizioni del DSR così da influenzare il mercato verso la direzione voluta: se l'obiettivo è far crescere la domanda, così da aumentarne il prezzo di mercato, l'azione proposta sarà quella di un saving rate più alto. Di contro, se il prezzo di mercato supera il valore target scelto, allora si ridurrà il saving rate così la domanda sarà inevitabilmente più bassa e di conseguenza il prezzo di un Dai scenderà.

4.3.3 Auctions

Come già introdotto nei precedenti paragrafi, mantenere il proprio collateral ratio superiore al rapporto di liquidazione è fondamentale al fine di preservare la stabilità del sistema e del Dai. Non è affatto banale se si pensa che gli asset vincolati sono altamente volatili e può accadere che perdano gran parte del proprio valore in poco tempo.
Quando questo accade e un vault raggiunge un valore inferiore a tale soglia, automaticamente viene avviata una ***Collateral Auction:*** il sistema prende possesso

degli asset e li inserisce in un'asta con l'obiettivo di riottenere i Dai corrispondenti, commissione di stabilità più una **penale di liquidazione** fissata attualmente al 13% con l'obiettivo di responsabilizzare gli utenti.

I Keepers partecipano all'asta offrendo di ripagare il debito con Dai in cambio del collateral sottostante. Come ci si attende, quest'asta sarà crescente e si possono presentare diversi scenari:

1. se un keeper offre Dai per un importo pari al debito, si avvia un' ***inverse Collateral Auction*** in cui per quella quantità di Dai pari al debito si richiedono asset collateral in maniera decrescente. In questo modo al termine dell'asta si potrà restituire la maggiore parte di collateral all'utente possibile.
   La quantità di Dai pari al debito confluisce nel Maker Buffer.

2. Se invece la *collateral auction* si arresta ad un valore offerto minore del debito, questo keeper prende tutto il collateral pagando quanto stabilito. La differenza di Dai viene coperta dal Maker Buffer se vi è sufficiente liquidità. Quando così non è, inizia una ***Debt Auction***: il debito mancante in Dai viene offerto dai keepers in cambio di nuovi token MKR generati. Occorre sottolineare che questo step è negativo per il sistema perché, creando nuovi MKR, alla stessa maniera di quando si emettono nuove azioni, il valore di ognuno di essi diminuisce. Anche in questo caso l'asta è al ribasso, così da minimizzare la ricapitalizzazione del sistema.

Ponendoci nel primo scenario, quello positivo in cui si riesce agevolmente a ripagare il debito, il sistema si avvia verso un'ultima asta ***Surplus Auction*** non appena il numero di Dai nel Buffer raggiunge un livello stabilito e noto.
In questa asta al rialzo, vengono offerti ai keepers Dai in cambio di token MKR; questi ultimi verranno bruciati così da ricapitalizzare positivamente il sistema.

La durata delle aste, delle offerte e l'incremento d'offerta vengono regolarizzati da *parametri di rischio* settati dai MKR voters attraverso sistemi di votazione appositamente indetti. Sono specifici per ogni tipo di asset collateralizzato e pensati per stabilizzare il più possibile il sistema, preservandolo da attacchi e perdita di valore.

Un meccanismo di sicurezza estremo è l'**Emergency Shutdown**, che prevede di resettare la piattaforma facendo uscire tutti gli utenti e ripartendo dal punto precedente. Occorre un numero elevato di MKR, 50 000, affinché il protocollo di shutdown venga attivato.
Fino ad oggi non è mai stato utilizzato come strumento di sicurezza dagli attacchi ma solo nel passaggio al *Multi-Collateral Dai*.

4.4 Decentralized Finance

Cosa si intenda per "finanza decentralizzata", o **DeFi**, non è ancora noto e chiaro a tutti, ma la stima attuale [12] mostra che la quantità di valore in dollari impiegata in tali attività è di circa un miliardo con una rapida e quasi del tutto costante crescita dal 2018 in poi. Tutto ciò fa comprendere come il fenomeno sia più che un concetto astratto e come stia attirando l'attenzione di tanti.
Come per gran parte degli argomenti trattati fino ad adesso, non è possibile dare una definizione formale, unica e rigorosa di De-Fi. Questo perché sono tematiche recenti ed in continua evoluzione.

E' comunque possibile cercare di far luce su questo "mondo nuovo" e inizialmente occorre precisare che ci si muove nell'ambito più generale e noto della *FinTech*, ovvero i frutti dell'innovazione apportata dalle nuove tecnologie dell'informazione e della comunicazione nei servizi finanziari. Si pensi ai metodi di pagamento diretti per il cliente, mobile bank, startup per prestiti fra singoli individui online, piattaforme per la consulenza finanziaria; sono solo alcuni dei settori di sviluppo della FinTech, anche in Italia.
In questo mondo già di per sé estremamente variegato, si colloca la **decentralized finance**, impossibile da definire in maniera univoca, il cui nome suggerisce il riferimento alle attività finanziarie offerte tramite protocolli decentralizzati.
Conseguenzialmente al lavoro di tesi fin qui esposto, risulta evidente che la decentralizzazione è un concetto basilare del mondo cripto. D'altronde si può anche

[12] Stima riportata dal sito *https://defipulse.com* in data 07/06/2020.

rivendicarne l'originalità, se si pensa che il primo progetto applicato di tale filosofia di pensiero è proprio Bitcoin. Ad eccezione del movimento cripto-anarchico degli anni novanta, nessuno aveva prima di allora pensato ad un mondo che rinunciasse a porre la propria fiducia in una o più autorità centrali.

Potremmo dunque far risalire la nascita del De-Fi proprio alla circolazione di bitcoin: per la prima volta diventa possibile acquistare valuta in una rete peer-to-peer. Eppure questa seppur immensa trasformazione non ha da subito iniziato a far parlare di finanza decentralizzata. Si è atteso un po' ancora, ed è stata la larga diffusione di Ethereum e degli smart contract, così come lo sviluppo delle stablecoin, a darvi la spinta definitiva. Questo non stupisce se si pensa che gli smart contract permettono quella flessibilità necessaria per proporre e attivare soluzioni diverse, dinamiche.

Attualmente le applicazioni decentralizzate, o *Dapps*, sono costruite esclusivamente sulla blockchain Ethereum e riguardano scommesse, prestiti, pagamenti, assicurazioni... Quello che oggi ostacola non è la tecnologia, pronta e matura ad accogliere una grande varietà di applicazioni, ma piuttosto la fiducia e il consenso pubblico.

4.4.1 Maker

Fra gli appassionati cripto, l'associazione Maker-DeFi è immediata.

MakerDAO domina per il 53% circa[13] il mercato DeFi. Il protocollo descritto nel paragrafo precedente permette di accedere ad una differente forma di prestito. Qui non ci sono garanzie da mostrare ad un'autorità, bensì *collateral* da vincolare in uno smart contract; non vi è un interesse mensile da pagare, ma una commissione di stabilità relativa al bene collateralizzato e un rapporto di liquidazione da mantenere entro certi valori. Non rispettarlo non implicherà una mora nel pagamento o un pignoramento, ma una liquidazione del collateral.

Anche nuove forme di investimenti diventano possibili: non più un tasso fisso/variabile, inflazionato o meno; con MakerDAO diventa possibile fissare dei Dai e ricevere un saving rate ad un tasso stabilito e comune a tutti, senza nessun tipo di vincolo su tempistiche o quantità.

[13]Valore riferito al 05/06/2020.

Stability fees e *Saving rates* sono i parametri globali che, come già spiegato nel precedente paragrafo, sono settati periodicamente tramite votazioni per mantenere la stabilità della valuta. Domanda ed offerta vengono così orientati dalle decisioni della rete.
Nel tempo sono state molte le modifiche; di seguito alcune delle votazioni per settare la commissione:

$7,5\%$	Marzo 2019
$11,5\%$	Aprile 2019
$19,5\%$	Maggio 2019
$14,5\% - 22,5\%$	Agosto 2019
$12,5\% - 20,5\%$	Settembre 2019
$8,5\% - 16,5\%$	Settembre 2019
$6,5\% - 14,5\%$	Ottobre 2019
$1,5\% - 9,5\%$	Ottobre 2019
$1\% - 9\%$	Novembre 2019
$0\% - 8\%$	Dicembre 2019
$2\% - 10\%$	Gennaio 2020
$4\% - 12\%$	Febbraio 2020
$0\% - 4\%$	Marzo 2020

Si nota come si sia sentita nel corso del 2019 l'esigenza di innalzare la commissione di stabilità, probabilmente per regolare un eccesso nella domanda, così come per far fronte ad una grande instabilità del collateral ether.
Nel Novembre del 2019 la rete ha approvato l'aggiornamento al Multi-Collateral Dai; fra i vari cambiamenti l'introduzione del tasso di risparmio. Di seguito alcune delle votazioni che lo hanno interessato:

$0\% - 8\%$	Dicembre 2019
$2\% - 10\%$	Gennaio 2020
$4\% - 12\%$	Febbraio 2020
$0\% - 4\%$	Marzo 2020

La tendenza dei primi mesi indica come il mercato stesse acquisendo fiducia progressivamente in tale strumento finanziario: il Saving rate all' 8% sul deposito di Dai ha rappresentato una buonissima fonte di investimento, se paragonato a qualsiasi altra disponibile sui mercati. Parallelamente le Stability fees si sono adeguate oscillando su valori nello stesso range. La correlazione fra i due tassi è molto forte e, come comprensibile per la salvaguardia del sistema, il saving rate assume dei valori leggermente più bassi.

Ciò che è avvenuto a Marzo 2020 è stata la conseguenza della grave turbolenza dei mercati a seguito della crisi da COVID-19: il valore dell'ether è crollato in poche ore di circa il 30%. Gran parte dei Vault MakerDAO hanno perciò subito una forte decollateralizzazione che ha portato gli utenti a cercare di rimediare aumentando gli asset anche tramite l'acquisto massiccio di Dai (non a caso il valore è salito ad 1,20 dollari). Non tutti però sono riusciti a mantenere il rapporto di liquidazione e per tanti vault è iniziato il meccanismo d'asta.

Fin qui nulla di particolarmente anomalo, se non il fatto che all'apertura delle aste la maggioranza dei Keepers, generalmente automatizzati, non ritenevano conveniente partecipare, visto il crollo del valore degli ether. Un Keeper invece colse la situazione e vinse le aste offrendo 0 Dai in cambio di collateral per un valore di circa 5,5 milioni.

L'intera cifra è dunque diventata debito che il sistema ha colmato con nuove aste generando MKR in cambio dei Dai mancanti, diminuendo il valore di ciascuno di essi.

Per cercare di ristabilire il rapporto 1:1 con il dollaro, le stability fees sono state abbassate, così che i possessori di un Vault fossero maggiormente spinti a non liquidare e attirare nuovi utenti. Contemporaneamente il saving rate è stato settato allo 0%, così da disincentivare il fermo di Dai, ridurre la domanda e abbassarne il prezzo. Sebbene le stability fees dei vari asset sono stati modificati negli ultimi mesi, ancora oggi il saving rate non è aumentato.

4.4.2 Compound

Al secondo posto delle attività più influenti in ambito DeFi si trova **Compound** con 114 milioni di dollari impiegati.

Nome	Blockchain	Valore in dollari	Influenza
Maker Dao	Ethereum	494,3 milioni	44,30%
Compound	Ethereum	221 milioni	19,70%
Synthetix	Ethereum	164,5 milioni	14,70%

Figura 4.7: Progetti più influenti in data 18/06/2020; fonte dati [43]. Quantità totale in dollari: $1,12$ miliardi.

Le idee innovative, la tempestività nel proporle, rigore e design accattivante sono alcuni dei fattori che segnano il successo di un progetto. E' il caso di Compound che a fine del 2018 si presenta con una risposta concreta all'idea di permettere degli scambi diretti di credito/debito fra privati.
Detto in questo modo potrebbe sembrare che ci sia ben poco di diverso rispetto ai depositi in banca e prestiti.
Nella pratica invece il settore è totalmente rivoluzionato:

- Trattazione di asset crittografici;
- Struttura decentralizzata su Ethereum con smart contract e ctoken che seguono il protocollo ERC-20, coniati quando vengono depositati degli asset crittografici e trasferiti come "ricevuta" (cETH, cDAI, cBAT...). Vanno invece depositati a garanzia quando si vogliono prendere in prestito degli asset;
- Non prestiti diretti fra le parti, ma un fondo comune in cui poter depositare o prelevare;
- Nessun vincolo di tempo: è possibile riscattare in qualsiasi momento le risorse vincolate oppure ripagare il prestito.

Gli asset che è possibile trattare sono elencati nel sito ufficiale [43] e per ognuno di loro sono indicati gli interessi di prestito/deposito. Vengono presentati come tassi

annuali, nonostante effettivamente l'aggiornamento sia molto frequente. Inizialmente il tasso di cambio di un ctoken parte dal valore corrente di mercato e aumenta nel tempo, così che quando poi verranno ritirati saranno convertiti in una quantità maggiore di asset. La formula che regola gli aggiustamenti nel tasso di cambio del ctoken con il vincolato asset sottostante è la seguente:

exchangeRate = (getCash() + totalBorrows() - totalReserves()) / totalSupply() [14]

dove *getCash()* riporta l'importo del saldo del contratto;
totalBorrows() l'importo totale prestato sul mercato del relativo asset;
totalReserves() parte degli interessi accantonati;
totalSupply() la quantità del ctoken in circolazione.
Dal momento che i debiti maturati portano alla crescita dei debiti complessivi del mercato, il tasso di cambio del ctoken aumenta.
Per calcolare l'interesse di chi prende in prestito un determinato asset invece bisogna calcolare:

$$U = totalBorrows()/(getCash() + totalBorrows())$$

Da cui:

$$borrowingRate = 2,5\% + U * 20\%$$

Trattando criptovalute anche estremamente volatili come ether, Compound ha implementato un meccanismo di **liquidazione** che viene attivato quando il rapporto fra l'asset collateralizzato e il prestito scende sotto un certo valore fissato. Quando ciò avviene i liquidatori prendono parte degli asset ripagandoli con ctoken e incentivati da uno sconto del 5%. E' premura di ogni account, dunque, mantenere il *collateral factor*[15] elevato.

Nuove regole, nuove tecnologie per classiche esigenze, nuovi rischi da considerare. Nessuna autorità centrale da garante, nessun intermediario da pagare per il servizio offerto. La rivoluzione è tanto grande quanto incontenibile.

[14] Formula riportata dalla documentazione del sito ufficiale [43].

[15] Sul portale del sito Compound il parametro che regola per ogni asset il corretto rapporto da mantenere è noto come *collateral factor*

Conclusioni

Il lavoro di tesi svolto ha pienamente confermato l'importanza che attualmente riveste il mercato delle criptovalute. L'influenza sull'economia globale è sempre maggiore, così come la sua crescita, con Bitcoin capo-pista indiscussa.
Durante i mesi di studio le caratteristiche sono state molto evidenti: ingente capitalizzazione di mercato, volatilità giornaliera e mensile estremamente alta, dinamicità dei mercati. Nuovi interessanti progetti si sono diffusi, altri hanno dovuto fare i conti con problemi imprevisti.
E' stato molto interessante, ad esempio, osservare "da vicino" la reazione del mondo *cryptocurrency* allo shock che il COVID-19 ha portato sul mondo finanziario. L'11 Marzo l'Organizzazione Mondiale della Sanità ha dichiarato lo stato di *pandemia*, le borse di tutti i mercati sono calate giù a picco, destabilizzando equilibri già assai precari. E in questo clima di grande sfiducia ed incertezza, complice la crisi del mercato dell'energia, cadono a picco anche Bitcoin e tutte le altre maggiori criptovalute. In poche ore circa il 30% (con punte del 50%) del valore è andato perso. *USD Coin* e *PAX Gold* hanno fatto presto a rialzarsi: dopo pochi giorni il valore è ritornato stabile. *Bitcoin* ed *Ethereum* hanno faticato di più, ma entrambe oggi sono tornate a valori anche più alti di prima. Conseguenze più forti sono quelle che ha subito il progetto *MakerDAO* e che ancora non sembra aver trovato la forza pre-crisi.

Un altro evento rilevante di questi mesi è stato l'*halving* Bitcoin, il dimezzamento della ricompensa per i miner vincenti, passando da 12.5 bitcoin a 6.25 bitcoin a blocco. C'era molta attesa fra gli appassionati: nei precedenti dimezzamenti l'effetto deflazionistico ha sempre portato un aumento del valore di un bitcoin. Le previsioni erano e sono fra le più disparate. Analisti accreditati scommettono che la crescita

sarà enorme, per altri è un *halving* non-halving. Ad oggi pochi effetti si sono visti, sebbene forse è ancora troppo presto[16].

Infine, proprio a seguito di una approfondita conoscenza dei protocolli Blockchain, è sempre più difficile non vedere quanto forte è il cambiamento di paradigma. Una rivoluzione tecnologica al pari di Internet, come molti dicono. E' solo meno evidente perché sembra che le stesse cose possano essere già fatte. Eppure l'innovazione è tanto straordinaria quanto viscerale: ogni aspetto della nostra vita può essere stravolto, ogni cosa potrebbe non essere più come la vediamo adesso.
Oltre all'evidente inutilità di istituzioni finanziarie da garanti, blockchain come Ethereum (e prossimamente Algorand) potrebbero rendere obsolete figure come quelle dei notai, delle assicurazioni e, pensando in grande, aziende intere. Forse utopia, forse voglia di fantasticare allo stesso modo di chi pensava alle auto-volanti, ma smart contract sempre più "smart" potrebbero permettere di far gestire, in maniera distribuita per l'appunto, ogni aspetto di un'impresa. Tutto sarebbe condiviso, trasparente, immutabile.

Un plauso va a chi crede in questo e ogni giorno si impegna per inseguire un cambiamento, rendendolo accessibile a tutti. E' vero che non ci sono vincoli per partecipare come nodi in Bitcoin, ma è difficile farlo operativamente, è impossibile negarlo.
Young Platform colma questo gap e avvicina chiunque voglia a questo mondo affascinante, offrendo contenuti formativi selezionati. In questi mesi sono state aggiunte nuove valute al portale e tanti nuovi progetti molto interessanti sono in cantiere. Presto diventeranno nuove entusiasmanti occasioni da cogliere al volo.

[16]Nel passato gli sbalzi nel prezzo dopo gli halving si sono visti in archi temporali pari circa a sei mesi.

Appendice

A. RIPEMD-160

Di seguito vengono riportate le definizioni di funzioni e costanti necessari per il protocollo di hash RIPEMD-160 presentato nel Capitolo 1.

Funzione non lineare f:

$$f(j,x,y,z) = \begin{cases} x \oplus y \oplus z & 0 \leq j \leq 15 \\ (x \wedge y) \vee (\neg x \wedge z) & 16 \leq j \leq 31 \\ (x \vee \neg y) \oplus z & 32 \leq j \leq 47 \\ (x \wedge z) \vee (y \wedge \neg z) & 48 \leq j \leq 63 \\ x \oplus (y \vee \neg z) & 64 \leq j \leq 79 \end{cases}$$

Costanti K, K' in esadecimale:

$$K(j) = \begin{cases} 00000000 & 0 \leq j \leq 15 \\ 5A827999 & 16 \leq j \leq 31 \\ 6ED9EBA1 & 32 \leq j \leq 47 \\ 8F1BBCDC & 48 \leq j \leq 63 \\ A953FD4E & 64 \leq j \leq 79 \end{cases} \quad K'(j) = \begin{cases} 50A28BE6 & 0 \leq j \leq 15 \\ 5C4DD124 & 16 \leq j \leq 31 \\ 6D703EF3 & 32 \leq j \leq 47 \\ 7A6D76E9 & 48 \leq j \leq 63 \\ 00000000 & 64 \leq j \leq 79 \end{cases}$$

Selezione parole $r(j)$:

$$r(j) = \begin{cases} j & 0 \leq j \leq 15 \\ 7,4,13,1,10,6,15,3,12,0,9,5,2,14,11,8 & 16 \leq j \leq 31 \\ 3,10,14,4,9,15,8,1,2,7,0,6,13,11,5,12 & 32 \leq j \leq 47 \\ 1,9,11,10,0,8,12,4,13,3,7,15,14,5,6,2 & 48 \leq j \leq 63 \\ 4,0,5,9,7,12,2,10,14,1,3,8,11,6,15,13 & 64 \leq j \leq 79 \end{cases}$$

Selezione parole $r'(j)$:

$$r'(j) = \begin{cases} 5,14,7,0,9,2,11,4,13,6,15,8,1,10,3,12 & 0 \leq j \leq 15 \\ 6,11,3,7,0,13,5,10,14,15,8,12,4,9,1,2 & 16 \leq j \leq 31 \\ 15,5,1,3,7,14,6,9,11,8,12,2,10,0,4,13 & 32 \leq j \leq 47 \\ 8,6,4,1,3,11,15,0,5,12,2,13,9,7,10,14 & 48 \leq j \leq 63 \\ 12,15,10,4,1,5,8,7,6,2,13,14,0,3,9,11 & 64 \leq j \leq 79 \end{cases}$$

Rotazioni sinistre s(j):

$$s(j) = \begin{cases} 11,14,15,12,5,8,7,9,11,13,14,15,6,7,9,8 & 0 \leq j \leq 15 \\ 7,6,8,13,11,9,7,15,7,12,15,9,11,7,13,12 & 16 \leq j \leq 31 \\ 11,13,6,7,14,9,13,15,14,8,13,6,5,12,7,5 & 32 \leq j \leq 47 \\ 11,12,14,15,14,15,9,8,9,14,5,6,8,6,5,12 & 48 \leq j \leq 63 \\ 9,15,5,11,6,8,13,12,5,12,13,14,11,8,5,6 & 64 \leq j \leq 79 \end{cases}$$

Rotazioni sinistre s'(j):

$$s(j) = \begin{cases} 8,9,9,11,13,15,15,5,7,7,8,11,14,14,12,6 & 0 \leq j \leq 15 \\ 9,13,15,7,12,8,9,11,7,7,12,7,6,15,13,11 & 16 \leq j \leq 31 \\ 9,7,15,11,8,6,6,14,12,13,5,14,13,13,7,5 & 32 \leq j \leq 47 \\ 15,5,8,11,14,14,6,14,6,9,12,9,12,5,15,8 & 48 \leq j \leq 63 \\ 8,5,12,9,12,5,14,6,8,13,6,5,15,13,11,11 & 64 \leq j \leq 79 \end{cases}$$

Valori da inizializzare in esadecimale:

$$h_0 = 67452301$$

$$h_1 = EFCDAB89$$

$$h_2 = 98BADCFE$$

$$h_3 = 10325476$$

$$h_4 = C3D2E1F0$$

B. Controllo transazioni in Bitcoin

Segue l'elenco di verifiche su ciascuna *transazione* che ogni nodo sulla rete Bitcoin deve effettuare per validarla:

- Correttezza sintattica e strutturale.
- La lista degli input e la lista degli output non devono essere vuoti.
- La dimensione deve essere minore del parametro MAX_BLOCK_SIZE e maggiore o uguale a 100 bytes.
- Nessun input può avere hash 0.
- Il numero di firme digitali deve essere minore del limite.
- L'output, per ogni input, non deve corrispondere in altre transazioni nel pool da approvare.
- Aggiungere alla lista di transazioni orfane del pool se ogni input non si riesce a ricollegare ad un output di preedenti transazioni.
- Per ogni input, se l'output a cui fanno riferimento è un coinbase, allora deve avere almeno $COINBASE_MATURITY(100)$ conferme.
- Per ogni input deve esistere l'output corrispondente e non può essere già speso.
- Controllare che la somma degli input sia maggiore di zero e minore della soglia di 21 milioni.

- La somma degli input deve essere maggiore della somma degli output.
- Accettare la transazione se la fee è maggiore di una certa soglia.

La rete dei partecipanti aggiorna spesso le condizioni da verificare in modo da scongiurare nuovi attacchi o per rendere più efficiente in protocollo. Ogni modifica viene però sempre ampiamente discussa prima di essere accettata.

C. Ethereum: block header

Anche in Ethereum un blocco contiene un certo numero di transazioni insieme e informazioni indispensabili per la rete. Queste vengono racchiuse nel block header H. Di seguito ne viene riportato un elenco secondo la notazione dello Yellow Paper:

- parentHash H_p: hash del block header precedente.
- ommersHash H_o: hash della parte iniziale del blocco.
- beneficiary H_c: address dell'indirizzo a cui andranno le fees.
- stateRoot H_r: l'hash della radice del merkle tree degli stati.
- transactionsRoot H_t: l'hash della radice del merkle tree delle transazioni.
- receiptRoot H_e: l'hash della radice del merkle tree delle ricevute delle traslazioni.
- logsBloom H_b: log delle informazioni relative alle transazioni da effettuare.
- difficulty H_d: valore scalare per settare la difficoltà nel minare il blocco.
- number H_i: valore scalare che identifica il numero degli antenati di quel blocco.
- gasLimit H_l: limite di gas per quel blocco.
- gasUsed H_g: valore totale di fas usato nelle transazioni del blocco.
- timestamp H_s: informazione sul tempo espresso in Unix. extraData H_x: un vettore di massimo 32 bytes contenenti dati aggiuntivi se ocorrono.

- mixHash H_m: hash di 256 bit che, insieme al nounce, prova che è stato effettuato un certo sforzo computazionale.
- nonce H_n: valore a 64-bit che è stato utilizzato, insieme al mixHash, per compiere un certo sforzo computazionale.

D. Keccak

La funzione f richiede di specificare alcune costanti. In ρ e π vi è $r[x, y]$, mentre le costanti $RC[i]$ sono nello step l in notazione *int64* di interi con segno a 64 bit.

RC[i]	valore				
i=0	0x0000000000000001	i=8	0x000000000000008A	i=16	0x8000000000008002
i=1	0x0000000000008082	i=9	0x0000000000000088	i=17	0x8000000000000080
i=2	0x800000000000808A	i=10	0x0000000080008009	i=18	0x000000000000800A
i=3	0x8000000080008000	i=11	0x000000008000000A	i=19	0x800000008000000A
i=4	0x000000000000808B	i=12	0x0000000080008088	i=20	0x8000000080008081
i=5	0x0000000080000001	i=13	0x800000000000008B	i=21	0x8000000000008080
i=6	0x8000000080008081	i=14	0x8000000000008089	i=22	0x0000000080000001
i=7	0x8000000000008009	i=15	0x8000000000008003	i=23	0x8000000080008008

	x=0	x=1	x=2	x=3	x=5
y=2	3	10	43	39	25
y=1	36	44	6	20	55
y=0	0	1	62	27	28
y=4	18	2	61	14	56
y=3	41	45	15	8	21

Figura 4.8: Costanti RC nello Step l, rotazioni $r[x, y]$ nello Step ρ e π ; fonte dati [14].

E. Relazioni interne: correlazioni

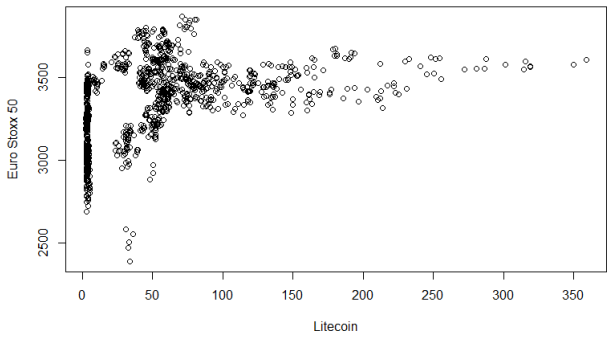
Nel Capitolo 3 sono state indagate le relazioni interne alle criptovalute calcolando la correlazione fra le grandezze misurate: *Open, High, Low, Close, Volume, Market-Cap*. Di seguito vengono invece riportati i valori di *cor.test()* per poter affermare che le misurazioni di correlazione siano statisticamente significative.

	Litecoin		**Ethereum**		**Ripple**	
	cor()	p-value	cor()	p-value	cor()	p-value
Open-High	0.9969058	< 2.2e-16	0.9986123	< 2.2e-16	0.9945715	< 2.2e-16
Open-Low	0.9967191	< 2.2e-16	0.9966183	< 2.2e-16	0.9930678	< 2.2e-16
Open-Close	0.9955798	< 2.2e-16	0.9965762	< 2.2e-16	0.9918568	< 2.2e-16
Open-Volume	0.4531856	< 2.2e-16	0.1974295	2.539e-16	0.6010918	< 2.2e-16
Open-Market.Cap	0.9916593	< 2.2e-16	0.9957401	< 2.2e-16	0.9912536	< 2.2e-16
High-Low	0.9952235	< 2.2e-16	0.9966207	< 2.2e-16	0.9907376	< 2.2e-16
High-Close	0.9987522	< 2.2e-16	0.9984919	< 2.2e-16	0.9962864	< 2.2e-16
High-Volume	0.4560107	< 2.2e-16	0.1982743	< 2.2e-16	0.6271781	< 2.2e-16
High-Market.Cap	0.9934499	< 2.2e-16	0.997194	< 2.2e-16	0.9948123	< 2.2e-16
Low-Close	0.9969338	< 2.2e-16	0.9980552	< 2.2e-16	0.9952238	< 2.2e-16
Low-Volume	0.4586552	< 2.2e-16	0.1962378	3.857e-16	0.5940782	< 2.2e-16
Low-Market.Cap	0.9943978	< 2.2e-16	0.9976454	< 2.2e-16	0.9954535	< 2.2e-16
Volume-Market.Cap	0.5163822	< 2.2e-16	0.2304646	< 2.2e-16	0.6344021	< 2.2e-16

Figura 4.9: Correlazione e p-value per Litecoin, Ethereum, Ripple.

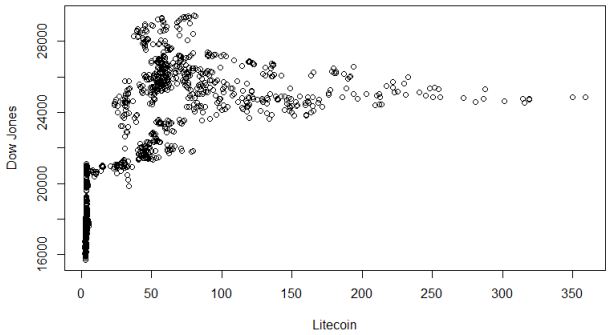
Relazioni esterne: Euro Stoxx 50, Dow Jones, Oro

Sempre nel Capitolo 3, si è indagato circa il rapporto fra le quattro criptovalute analizzate e strumenti classici del mercato finanziario. Di seguito si riportano i grafici della correlazione fra le tre valute rimanenti e dei tre asset indicati. Il confronto con Bitcoin era già stato allegato nel capitolo.



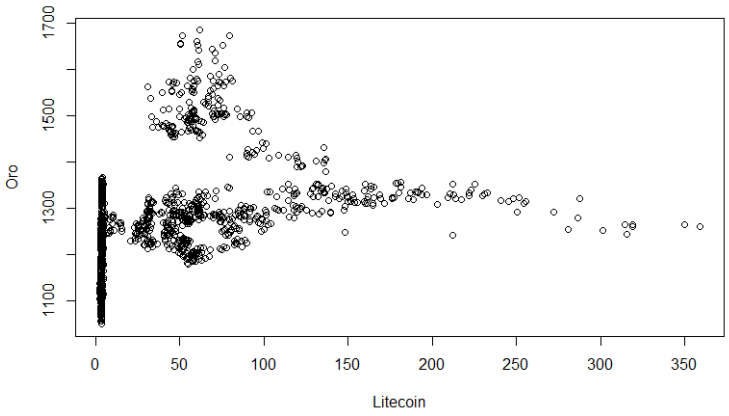
(a) Euro Stoxx 50

$\rho = 0.4825242$



(b) Dow Jones

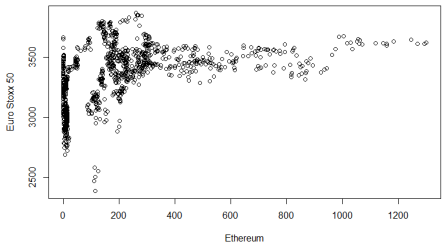
$\rho = 0.6192099$



(c) Oro

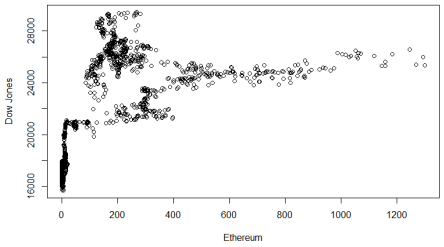
$\rho = 0.3227448$

Figura 4.10: Correlazioni con Litecoin.



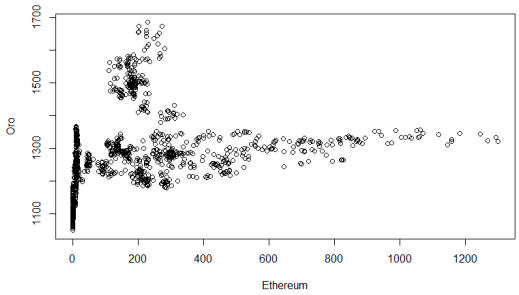
(a) Euro Stoxx 50

$\rho = 0.4825242$



(b) Dow Jones

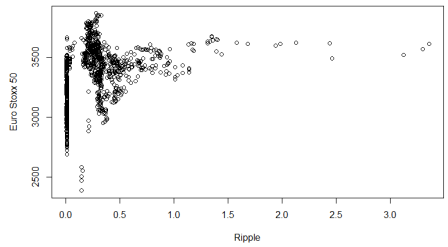
$\rho = 0.6192099$



(c) Oro

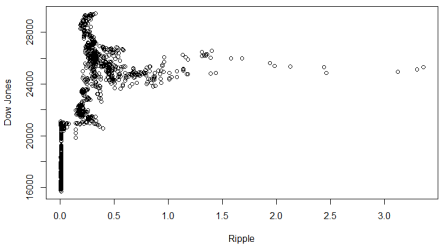
$\rho = 0.3227448$

Figura 4.11: Correlazioni con Ethereum.



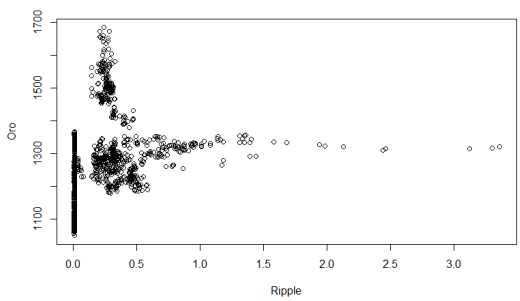
(a) Euro Stoxx 50

$\rho = 0.4825242$



(b) Dow Jones

$\rho = 0.6192099$



(c) Oro

$\rho = 0.3227448$

Figura 4.12: Correlazioni con Ripple.

Bibliografia

[1] Andreas M.Antonopoulos *Mastering Bitcoin-Unlocking Digital Cryptocurrencies*, 2014, O'Reilly Media.

[2] Hans Dobbertin, Antoon Bosselaers, Bart Preneel, *RIPEMD-160: A Strengthened Version of RIPEMD*, 18 Aprile 1996.

[3] Danilo Bazzanella, Dispense corso *Crittografia*, Politecnico di Torino, 2019.

[4] Satoshi Nakamoto *A peer-to-peer electronic cash system*, 2008.

[5] W. Dai, *b-money*, http://www.weidai.com/bmoney.txt, 1998

[6] https://www.activism.net/cypherpunk/crypto-anarchy.html

[7] http://www.gandalf.it/dati/dati1.htm

[8] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, *Bitcoin ad Cryptocurrency Technologies*, Princeton University Press, 2016.

[9] https://www.blockchain.com/

[10] Meni Rosenfeld, *Analysis of Bitcoin Pooled Mining Reward System*, 2011

[11] https://coinmarketcap.com

[12] Vitalik Buterin, *A Next-Generatio Smart Contract and Decentralized Applicazion Platform*, 2013.

[13] Gavin Wood, *Ethereum: a secure decentralized generalized transaction ledger*, 20/10/2019.

[14] https://keccak.team/index.html.

[15] Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche, Ronny Van Keer, *Keccak implemation overview*, 29 Maggio 2012.

[16] https://tutorialsdiary.com/merkle-patricia-tree-in-ethereum/

[17] https://litecoin.org/

[18] *S.*Asharaf, S.Adarsh, Decentralized Computing using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities

[19] https://cryptonomist.ch/

[20] https://it.finance.yahoo.com/

[21] Brad Chase, Ethan MacBrough, *Analysis of the XRP Ledger Consensus Protocol*, 21 Febbraio 2018.

[22] https://xrpl.org

[23] https://www.keylength.com/en/compare/

[24] Frederik Armknecht, Ghassan O. Karame, Avikarsha Mandal, Franck Youssef,Erik Zenne, *Ripple: Overview and Outlook*, Agosto 2015.

[25] https://www.coingecko.com/it/monete/xrp/historicaldata/

[26] Andrea Caponea, Carlo Gola, *Aspetti economici e regolamentari delle «Cripto-attività»,* Marzo 2019.

[27] Yulin Liu, *Cryptocurrency Valuation*, Giugno 2019 https://medium.com/coinmonks/cryptocurrency-valuation-d9979074404

[28] https://hodlwave.com/

[29] https://plotly.com/

[30] https://www.borsaitaliana.it/notizie/sotto-la-lente/bollaspeculativa.htm

[31] Eng-Tuck Cheah, John Fry, *Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin*, Febbraio 2015.

[32] Ethan MacBrough, *Cobalt: BFT Governance in Open Networks*, Febbraio 2018.

[33] https://www.centre.io/usdc

[34] Centre Whitepaper, Maggio 2018.

[35] https://coin360.com/charts

[36] Charles Cascarilla, *PAX GOLD white paper.*

[37] Andrea Gangemi, *STABLECOIN: The Maker protocol*, 20 Marzo 2020.

[38] *The Dai Stablecoin System*, Dicembre 2017.

[39] *The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*, Novembre 2019.

[40] https://daistats.com/

[41] https://www.stellar.org/

[42] https://defiprime.com/

[43] https://compound.finance/

[44] Robert Leshner, Geoffrey Hayes, *Compound: The Money Market Protocol-White Paper*, Febbraio 2019.

[45] Jing Chen, Silvio Micali, *ALGORAND- White Paper*, Maggio 2017.

[46] Y. Gilad, R.Hemo, S. Micali, G. Vlachos, N. Zeldovich, *Algorand: Scaling Byzantine Agreeements for Cryptocurrencies*, Ottobre 2017.

[47] Goldberg, Naor, Papadopoulos, Reyzin, *NSEC5 from Elliptic Curves*, Marzo 2016.

[48] Daniel J. Bernstein, *Curve25519: new Diffie-Dellman speed records*, Aprile 2006.

[49] https://algorand.foundation/