LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Impresa e Management

Cattedra di Economia dei Mercati e degli Intermediari Finanziari

Analisi delle criptovalute alternative al Bitcoin

Relatore:

Chiar.mo Prof.

Claudio Boido

Candidato:

Emanuele Rampioni

Matricola: 200181

Anno accademico 2017/2018

Indice

Introduzione

Lo scopo del presente elaborato è quello di analizzare le criptovalute alternative al Bitcoin.
Quest'ultimo, anche se rappresenta la moneta digitale più importante, dalla quale non si può prescindere in un'analisi del settore delle criptovalute, non è l'unico meritevole di attenzione, in quanto esistono altre possibilità di investimento rappresentate dagli altcoin.
Nel primo e nel secondo capitolo l'obiettivo sarà quello di esaminare sia le caratteristiche tecniche e finanziarie delle monete virtuali, approfondendo l'esame delle più "disruptive", sia la tendenza abbastanza automatica ma errata di ritenere sinonimi i termini criptovalute e Bitcoin. Infatti è un errore considerare le criptomonte in maniera standardizzata, come se tutte avessero un funzionamento che poco differisce rispetto al Bitcoin. Basta per esempio fare un raffronto tra quest'ultimo e l'ether, la seconda criptovaluta a livello di capitalizzazione di mercato, per capire che tra le due monete digitali non ci sono tanti punti in comune. Il Bitcoin infatti è una moneta virtuale che può essere utilizzata sia come mezzo di scambio sia come riserva di valore, se l'investitore crede in un futuro rialzo del suo prezzo. Lo stesso Satoshi Nakamoto, presunto creatore di Bitcoin, definiva la sua invenzione un "sistema di pagamento".[1] Differentemente Ethereum è una "piattaforma decentralizzata" che serve per tanti scopi: la moneta, l'ether, permette alla piattaforma di funzionare, ma il suo obiettivo principale è la creazione di contratti intelligenti (smart contracts), dApps, ICO o token e non l'utilizzo dell'ether come mezzo di scambio.
Nel terzo capitolo si indagherà l'eventuale pericolo di bolle speculative collegate al Bitcoin. A tal scopo nella prima parte del capitolo si analizzeranno due modelli matematici adatti a identificare le caratteristiche di una bolla, nella seconda parte si studieranno le variazioni di prezzo del Bitcoin dalla sua creazione fino ad oggi per esaminare le tre macro-bolle finanziarie della criptovaluta più famosa al mondo.

[1] (Nakamoto, 2008)

Capitolo 1 – Le criptovalute: Bitcoin e altcoin

1.1 Caratteristiche generali delle criptovalute

Le caratteristiche della maggior parte delle monete digitali sono:

1.1.1 Assenza di un'autorità centrale che ne regola il funzionamento

Mentre per le tradizionali monete fiat è presente un organismo sovranazionale che gestisce la politica monetaria (decide quanta moneta deve essere stampata, ne regola i flussi ecc..), nel mondo delle criptovalute non esiste questa autorità centrale ma un sistema peer-to-peer (P2P), cioè un protocollo in cui la gestione delle transazioni e l'emissione dei token viene fatta direttamente dalla rete. Tendenzialmente il sistema è open source, quindi nessuno possiede o controlla la moneta. Le implicazioni di un sistema P2P sono quelle di avere una rete informatica non gerarchizzata in cui tutti i nodi sono paritari: questo porta ad una condizione di uguaglianza tra tutti coloro che operano nella rete. Ovviamente i limiti alle possibilità dei nodi vengono stabiliti dal protocollo; chi viola il protocollo viene escluso automaticamente dalla rete. La tecnologia peer-to-peer alla base delle criptovalute altro non è che un metodo di matrice informatica per condividere file in rete (file sharing); un esempio di applicazione, conosciuta da tutti, che utilizza una tecnologia P2P è Bittorrent.[2]

1.1.2 Riduzione o annullamento dei costi di transazione

Avviene grazie all'assenza di intermediari che, attraverso le commissioni, possono influenzare il valore di una transazione tra due controparti (si pensi ad esempio al costo di un bonifico bancario). E' vero che per trasferire qualche criptovaluta (ad esempio bitcoin) c'è comunque una fee da pagare, però questa è inferiore rispetto a quella applicata dagli intermediari finanziari. Infatti il costo di un bonifico online da parte di un correntista di Unicredit ad un altro che ha il proprio conto in una banca dell'area SEPA è di 2,25 euro e la somma impiega minimo due giorni lavorativi per essere accreditata sul conto del ricevente. Una transazione in bitcoin invece ha un costo di 0,11 euro e viene confermata in 10 minuti circa.

Nel caso di bonifico bancario erogato verso un conto corrente di una banca fuori dall'area SEPA, il costo dipende dall'istituto, dalla nazione di destinazione e dalla somma da trasferire ma è superiore a 10 euro e può arrivare anche a molte decine di euro (dati del 24/08/18).

La domanda a questo punto sorge spontanea. Chi verifica le transazioni? Chi cioè è in grado di certificare che la transazione è andata effettivamente a buon fine?

Per i Bitcoin (ma anche per molte altre criptovalute il procedimento è simile) abbiamo i cosiddetti "miners". Questo termine deriva dal fatto che come i minatori una volta estraevano carbone, oro, argento dalle miniere muniti di torcia e piccone, i miners lavorano davanti ad un computer, con una connessione Wi-Fi, estraendo

[2] (Nakamoto, 2008)

transazioni tra controparti. Essi, fornendo la potenza di calcolo dei loro computer, verificano e confermano gli scambi tra un acquirente e un venditore. La conseguenza è che attraverso il lavoro di verifica e conferma, aggiungono nuovi blocchi alla blockchain, ovvero una catena di blocchi pubblica (visibile ad esempio dal sito blockchain.info) in cui sono registrati tutti gli scambi di criptovalute.

Quale è però il profitto del minatore? Ogni volta che un blocco viene aggiunto alla blockchain, al miner che si è occupato della conferma del blocco, viene assegnata una ricompensa sotto forma di criptovaluta, più delle commissioni volontarie promosse dai mittenti. Prendendo come esempio il Bitcoin si specifica che ogni blocco della blockchain viene confermato in un tempo medio di 10 minuti: secondo Satoshi Nakamoto, un tempo inferiore avrebbe causato una difficoltà oggettiva nel capire quale fosse l'ultimo blocco della catena, mentre il requisito fondamentale della blockchain è la continuità dei blocchi e quindi dei trasferimenti; un tempo superiore invece avrebbe portato ad una eccessiva lentezza nella conferma delle transazioni. In termini monetari la ricompensa per i minatori che confermavano un blocco della blockchain era inizialmente di 50 bitcoin, poi è stata dimezzata a 25 alla fine del 2012 ed è scesa a metà 2016 a 12,5; un ulteriore calo è previsto a metà 2020 per poi arrivare ad una progressiva riduzione in maniera proporzionale insieme alla fine dell'emissione dei bitcoin (i bitcoin in circolazione non potranno essere più di 21 milioni). Come già scritto, oltre alla ricompensa in bitcoin, per i miners c'è anche la ricompensa delle fees, che possono essere inserite liberamente da chi vuole effettuare la transazione in Bitcoin. Ovviamente i miners verificano prima gli scambi che presentano le fees più alte.

Ad oggi se voglio che il mio acquisto/cessione di bitcoin venga certificato nel prossimo blocco (quindi nei prossimi 10 minuti) devo pagare 0.13 dollari di fee; se voglio che venga minato nei prossimi 3 blocchi (30 minuti) devo pagare 0,12 dollari; se invece voglio che venga verificato nei prossimi 6 blocchi devo pagare 0,07 dollari (dati del 24/08/18).

Non c'è una regola matematica fissa per cui un miner potrà convalidare più blocchi rispetto ad un altro, ma è solo un discorso di natura probabilistica: colui che avrà più hardware per aumentare la potenza di calcolo, avrà maggiori probabilità di aggiudicarsi la ricompensa.

Proprio per ovviare al rischio di alcuni miners minori di non riuscire mai a confermare un blocco, consumando inutilmente energia, si stanno sviluppando le cosiddette mining pools. Una mining pool è costituita da un insieme di miners che mettono insieme la loro potenza di calcolo (hashing power) per cercare di verificare i blocchi; nel momento in cui un miner certifica un blocco e ottiene la ricompensa, la deve dividere con gli altri appartenenti alla mining pool, ovviamente in proporzione alla potenza di calcolo di ciascuno di essi. In questo modo si riduce la volatilità connessa all'attività di mining. Per fare in modo di non incorrere in truffe interne (non dichiaro di aver minato un blocco) e per calcolare l'hashing power di tutti i componenti della mining pool, tutti i tentativi di calcolo devono essere quotidianamente mandati al mining pool operator.[3]

[3] (Bonneau, 2015)

Si precisa che più dell'80% delle mining pools si trova in Cina a causa del costo più basso che l'energia elettrica ha in questo paese rispetto agli altri. Le regioni industriali cinesi proliferano di impianti idroelettrici la cui produzione è talmente elevata che nel passato si sono verificati problemi di surplus di produzione, tanto che l'elettricità era in alcuni casi sovvenzionata dallo stato. Quando è nato il mining, la maggior parte dei minatori si è trasferita in Cina, creando un problema di centralizzazione di questa attività.

A livello informatico, si puntualizza che i miners per chiudere il blocco devono trovare un codice alfanumerico scritto con linguaggio hash, che è una funzione matematica non invertibile: dall'input si riesce ad arrivare all'output, ma dall'output non si riesce a risalire all'input. La stringa di hash della rete Bitcoin è composta da 32 bit: cambiando anche una sola lettera dell'input, si modifica totalmente l'output (si può verificare con un qualsiasi generatore di hash code online). Per cui deve essere scaricato un cryptographic hash software ovvero un software in grado di cifrare il linguaggio hash: l'unico modo per decriptare questa stringa è quello che in informatica viene definito il "metodo forza-bruta" ovvero la ricerca di un algoritmo di risoluzione di un problema che consiste nel verificare tutte le soluzioni teoricamente possibili fino ad arrivare a quella corretta. La stringa in linguaggio hash, per essere calcolata, utilizza un valore chiamato nonce, che è un numero casuale o pseudo-casuale che ha un utilizzo unico. Questo pertanto consente di fare in modo che il codice del blocco possa essere utilizzato una volta sola, anche perché una blockchain che presenta codici di chiusura identici è ovviamente impossibile da utilizzare. Il grande beneficio del nonce è quello di rendere impossibile replay attack, ovvero attacchi di rete che consentono di impossessarsi dei dati di autenticazione di un sistema e utilizzarli per entrare illecitamente in un software o in un'applicazione.

Un replay attack tipico si verifica quando un soggetto terzo si inserisce in una comunicazione tra due controparti e riesce ad impossessarsi dei codici criptati di una delle due: in questo caso sarà in grado di interagire con l'altra parte senza che essa ne sia consapevole. Ultimamente questi problemi vengono combattuti con password o codici usa e getta, come ad esempio i token di autenticazione elettronici dell'online banking. Nel caso di Bitcoin queste tecnologie non sono necessarie grazie all'utilizzo "for the nonce" ovvero per l'occasione. La stringa hash della rete Bitcoin inizia con un numero di zeri che differisce sulla base dell'hashing power della rete: il miners non fanno altro che, in maniera del tutto automatica, cambiare il valore del nonce continuamente fino ad arrivare al codice hash che presenta il numero di zeri richiesto dalla rete e permette di confermare il blocco.

Fin qui sembra che il processo di mining sia portatore solamente di benefici. In realtà un individuo con un normale computer non può dedicarsi al mining e le ragioni sono essenzialmente tre (non considerando i costi di installazione di memorie aggiuntive, per aumentare la potenza di calcolo, che per una piccola postazione in una camera di medie dimensioni si aggirano intorno ai 6000 euro e che dovranno poi essere cambiate nel giro di 2-3 anni per una normale perdita di prestazioni):

a) Nel momento in cui si presta la potenza di calcolo, il computer è inutilizzabile in quanto operazioni di questo tipo rallentano il PC in maniera pressoché totale.

b) Il costo dell'energia elettrica: normalmente i miners operano in stati in cui il costo dell'energia elettrica è basso perché il consumo per l'attività di estrazione è veramente altissimo. L'Italia per esempio è uno dei peggiori paesi europei dove svolgere questa attività, a causa dell'elevato costo dell'energia. I paesi migliori in Europa si trovano ad est, come ad esempio Russia, Ucraina, Bulgaria ecc.
c) Il rischio connesso al surriscaldamento della postazione, spesso sottovalutato da chi decide di aprire una postazione: queste macchine infatti, considerando anche che devono rimanere accese 24 ore su 24, sprigionano una quantità di calore veramente elevata che può portare a rischi di cortocircuito; è necessario pertanto un buon impianto di raffreddamento affinché non si verifichino danni irreparabili.

Oltre a questi problemi, di natura strettamente tecnica, ma assolutamente prevedibili, esiste quello che viene definito il Selfish mining, che può essere visto come un attacco all'integrità della rete Bitcoin. Un Selfish mining si verifica quando un miner trova la soluzione di un blocco; anziché pubblicarla nel momento in cui l'ha trovata, decide di aspettare e inizia a lavorare sul blocco successivo. Quando anche altri miners stanno per arrivare alla soluzione, il miner disonesto pubblica la soluzione con una catena di blocchi più lunga; questo attacco aumenta il rendimento del miner disonesto e amplifica la difficoltà dell'hash code dei blocchi anche se non dovrebbe essere aumentata.

1.1.3 Anonimato parziale nelle transazioni

La blockchain rende pubbliche tutte le transazioni: è sufficiente andare sul sito blockchain.info per potere analizzare tutti gli scambi che vengono fatti e capirne le dimensioni, le quantità scambiate, il nonce, la ricompensa per i miners (che è 12,5 nel caso dei bitcoin più le fees) e altre informazioni. Tuttavia non è dato sapere chi siano i soggetti coinvolti nella transazione.

Si faccia un passo indietro: si deve considerare che per poter mantenere e scambiare criptovalute è necessario possedere un Wallet, ovvero un portafoglio che anziché essere fisico è virtuale. Le piattaforme che permettono di scaricare un wallet forniscono due chiavi: una chiave pubblica che deve essere inviata alla persona che ci deve spedire dei bitcoin e una chiave privata che serve quando siamo noi a dover inviare bitcoin. Questi costituiscono la firma digitale dei Bitcoin e rappresentano un esempio di crittografia asimmetrica, in cui si usano due chiavi diverse per spedire e ricevere moneta. In particolare Bitcoin utilizza un codice di autenticazione denominato ECDSA per calcolare le due chiavi; data la chiave privata che viene generata sulla base di un numero pseudo-casuale compreso tra 1 e 1,158*10^77, si calcola la chiave pubblica con la formula K=k*G dove K=chiave pubblica, k=chiave privata e G=punto generatore. La chiave pubblica è un punto sulla curva ellittica che per il Bitcoin ha funzione y^2=x^3+7.

Equazione 1.1 Curva ellittica Bitcoin Fonte: Bitcoin: A Peer-to-Peer Electronic Cash System.

ECDSA vuol dire infatti Elliptic Curve Digital Signature Alghoritm. E' evidente che poiché la funzione è irreversibile, non è possibile risalire alla chiave privata conoscendo la sola chiave pubblica.[4]

A questo punto è facile comprendere perché si dice che le criptovalute garantiscano l'anonimato delle transazioni: infatti attraverso la blockchain si possono verificare i "passaggi di mano" tra le criptovalute, ma non si conoscono le persone fisiche a cui corrispondono i vari wallet. Inoltre non esiste un limite al numero di wallet che possono essere mantenuti da ciascun soggetto. Ognuno pertanto può avere nel suo computer 10,100,1000 wallet diversi, motivo per cui risalire ai soggetti proprietari è molto difficile. Per questa ragione molti pensano che Bitcoin possa incentivare gli scambi illegali: chiariamo subito che non è così.

Quando compiamo qualsiasi attività su Internet siamo facilmente rintracciabili ed è facile risalire dalla chiave pubblica di ciascun wallet all'indirizzo IP del computer. Leggermente più difficile è collegare l'indirizzo IP alla persona fisica, ma anche in questo caso è abbastanza certo che l'FBI e altre autorità siano già riuscite in questo obiettivo; basta pensare che quando si istalla una piattaforma di Exchange si deve essere registrato con dati personali per cui il 99% delle persone è rintracciabile nel momento in cui viene fatto un illecito. Anche nell'1% dei casi in cui vengono utilizzati software in grado di nascondere informazioni personali o l'indirizzo IP (si pensi a TOR), ci sono comunque avanzati sistemi informatici in grado di capire l'identità del soggetto. Oltre a ciò c'è un altro problema: nel momento in cui converto il bitcoin in euro o qualsiasi altra moneta fiat sono facilmente tracciabile. Per cui il bitcoin è la moneta peggiore da usare per fare transazioni illecite in quanto comunque è tutto registrato.

Un esempio? Silk Road. Silk Road era un sito di commercio elettronico in cui si poteva accedere solamente attraverso il software TOR in modo da garantire l'anonimato. Ovviamente le merci che venivano vendute su questo sito, che infatti era definito "l'Amazon delle droghe", erano prodotti di contrabbando, armi, droga, farmaci proibiti ecc.

L' FBI riuscì a tracciare oltre 3500 bitcoin arrivando ai server coinvolti nelle operazioni illegali di Silk Road conducendoli al computer di Ross Ulbricht, fondatore del sito, che è stato condannato con il carcere a vita.

Tuttavia, come meglio vedremo dopo, esistono alcune monete digitali che cercano di mantenere l'anonimato dei soggetti coinvolti nelle transazioni, nascondendo la maggior parte delle informazioni sugli scambi e anche la stessa blockchain.

[4] (Saberhagen, 2013)

1.2 Caratteristiche innovative delle criptovalute

Le criptovalute hanno certamente portato una ventata di innovazione e in un futuro ormai prossimo si potranno vedere se e quali ripercussioni avranno sul sistema monetario tradizionale.

Quali sono le novità che hanno permesso a qualcosa che esiste solamente in forma virtuale, di affermarsi sul mercato e avere una capitalizzazione (alla data del 17 luglio 2018) di oltre 271 miliardi di dollari?

Di seguito verranno esaminate quattro importanti innovazioni racchiuse nelle monete digitali che sono esplicative di un processo che è solo la fase iniziale di una possibile rivoluzione nel sistema dei pagamenti.

1.2.1 Assenza di un'autorità centrale

Come visto in precedenza, a differenza delle classiche monete fiat in cui esiste un'autorità centrale che stabilisce la politica monetaria, la maggior parte delle criptovalute sono gestite dal mercato, infatti il loro prezzo viene definito dall'incontro tra domanda e offerta.

1.2.2 Assenza di inflazione

Questa è una caratteristica fondamentale per la maggior parte delle criptovalute. Infatti, prendendo come riferimento il Bitcoin (solamente per questioni di semplicità ma il discorso vale per la maggior parte degli altcoin), sappiamo che il numero totale di bitcoin che può essere emesso tende asintoticamente al limite di 21 milioni. In particolare, ogni quattro anni viene dimezzata l'emissione di bitcoin fino a quando non si raggiungerà il limite massimo: nel 2013 ne è stata emessa la metà, nel 2017 i tre quarti e in questo modo in meno di 32 anni verranno emesse tutte le monete possibili.

L'idea di Satoshi Nakamoto è quindi abbastanza evidente: il Bitcoin nasce come moneta che non solo non può essere soggetta ad inflazione perché ha un limite massimo di emissione, ma è addirittura una moneta deflattiva, perché andando avanti nel tempo, l'offerta tenderà a diminuire e conseguentemente il prezzo tenderà a salire.

Ovviamente questa era un'idea di Nakamoto: si può affermare che, seppur con andamenti altalenanti, fino a dicembre 2017 è stato così; anzi probabilmente il valore delle criptovalute è salito in maniera troppo rapida creando poi una bolla speculativa che è scoppiata nei mesi successivi.

Quale potrebbe essere una falla nel ragionamento riguardo inflazione/deflazione di Satoshi Nakamoto? Probabilmente un problema potrebbe essere un significativo calo della domanda. Questo calo potrebbe avvenire per innumerevoli motivi, alcuni dei quali si sono effettivamente verificati in questi anni:

-Una posizione avversa da parte dei governi nazionali e delle autorità internazionali. In alcuni paesi del mondo, le criptomonete sono proibite perché considerate pericolosi strumenti speculativi e forme di erosione del risparmio privato. Laddove si diffondesse un vincolo a livello giuridico nei confronti delle monete virtuali non ci potrebbe essere un'espansione del settore; questa prospettiva, seppur possibile, è abbastanza difficile,

considerata anche la recente apertura della BCE nei confronti delle monete virtuali, rappresentata dalla Direttiva UE 2018/843 che verrà analizzata nel prossimo paragrafo.
-Paura degli investitori. Si potrebbe verificare una caduta o addirittura il fallimento di alcune criptovalute (ricordiamoci che le monete virtuali in circolazione ormai sono più di 1900); questo potrebbe causare un effetto domino sulle altre per il sentiment negativo ingenerato negli investitori.
-Elevata volatilità. Le criptomonete essendo uno strumento che non ha ancora una legislazione chiara e non è ben conosciuto dal mercato rappresenta un investimento ad alta volatilità. La maggior parte degli investitori è diffidente sul loro acquisto e questo ovviamente rallenta un po' la loro circolazione. Inoltre, famosi investitori e premi Nobel per l'economia hanno assunto posizioni fortemente contrarie nei confronti delle monete virtuali; per esempio Joseph Stiglitz, vincitore del premio Nobel per l'economia nel 2001, ha dichiarato che il Bitcoin non ha alcuna funzione lecita né utile, anzi permette di aggirare le leggi.

Un esempio che potrebbe essere per certi versi rivoluzionario relativamente all'inflazione ed alle criptovalute è rappresentato dalla recente crisi in Venezuela.
Dal 2013 il paese sudamericano è oggetto di una particolare crisi economica, istituzionale e sociale nata allorché lo storico leader Hugo Chavez muore e il suo posto viene preso da Nicolas Maduro. Il nuovo presidente, da un punto di vista sociale, attua una politica volta all'oppressione della libertà di parola, pensiero e opinione, da un punto di vista politico, cancella totalmente i poteri del Parlamento, utilizzando spesso per governare una "legge abilitante" che gli dà il potere di emanare leggi senza l'approvazione del Parlamento e, da un punto di vista economico, concentra la sua politica sull'estrazione del petrolio che viene realizzato con tecniche antiquate, salvo poi pagarne le conseguenze quando il prezzo inizia a scendere vertiginosamente nel 2013. Per fare in modo che lo stato non vada in default decide di stampare moneta con il solo risultato di ottenere un'inflazione del 14000% che rende carta straccia la moneta nazionale venezuelana (Bolivar).
A rendere ancora più difficile la situazione venezuelana intervengono gli Usa che, per tutelare il risparmio dei cittadini americani, impongono delle sanzioni contro il Venezuela: imposizione agli investitori americani di non comprare nuove obbligazioni venezuelane, divieto di commerciare obbligazioni esistenti, congelamento degli asset di Maduro negli Usa e divieto di intrattenere relazioni commerciali.
Ma come si inserisce la crisi venezuelana nel sistema criptovalute?
Molti Venezuelani hanno deciso di investire in bitcoin non come valuta per le transazioni ma come riserva di valore: il bitcoin infatti viene chiamato anche per questo motivo "oro digitale" ovvero un bene deflattivo, decentralizzato, sicuro, trasportabile, nel quale poter investire quando le tradizionali valute vanno male.
Maduro ha ritenuto invece possibile uscire dalla crisi e rivalutare la moneta nazionale attraverso il lancio di una criptovaluta chiamata Petro, che è diventata la prima criptovaluta nazionale, ovvero la prima moneta virtuale supportata da uno stato. Lanciato in pre-vendita nel febbraio del 2018, il Petro presenta alcune caratteristiche precise: è pre-minato, cioè impedisce la creazione di altri token dopo l'emissione da parte del

governo; è la prima criptovaluta con un sottostante, ovvero i 5 miliardi di barili delle riserve di petrolio del paese e ha un valore corrispondente al prezzo di un barile di petrolio venezuelano scambiato sul mercato.
Queste erano le premesse con cui il Petro sarebbe dovuto nascere. In realtà la nuova moneta non è mai partita. Insomma un totale flop.

1.2.3 Proof of Work (PoW) e Proof of Stake (PoS)

Il sistema Proof of Work (PoW) indica l'algoritmo originale che deve essere trovato dai miners per poter controllare le transazioni e aggiungere blocchi alla blockchain. E' a causa di questo protocollo che i minatori devono competere tra di loro per poter trovare il codice hash; in particolar modo la maggior parte delle criptovalute (ad esempio Bitcoin, Litecoin ecc..) utilizzano il sistema Hashcash che è una delle funzioni del PoW.
Hashcash fu creato da Adam Back che lo ideò inizialmente per combattere lo spamming: per riuscirci ideò un sistema che imponeva al mittente che voleva mandare 3 mail verso lo stesso destinatario di risolvere un puzzle crittografico per la prima, un algoritmo per la seconda e un problema matematico per la terza. Queste funzioni erano progettate in modo da essere molto difficili da svolgere per il mittente, ma molto facili per il destinatario: quindi alla base dell'Hashcash ci deve essere un'asimmetria rispetto al livello di difficoltà tra le controparti.
Adam Back infatti pensò il sistema Hashcash come una funzione di costo che imponeva ai soggetti malintenzionati, ovvero coloro che mandavano spam, di utilizzare la potenza di elaborazione dei loro dispositivi come proof of work: detto in altre parole faceva lavorare in maniera eccessiva le loro CPU. Significative sono le parole di Back riguardo alla sua invenzione: "Per te come utente normale, con un computer entry-level per desktop o laptop, il sovraccarico della CPU per posta è trascurabile perché non invii più messaggi; nel peggiore dei casi la posta viene ritardata di alcuni secondi prima di essere inviata su hardware vecchio e lento. Tuttavia, per gli spammer, questo è uno show-stopper".
La tecnologia appena vista fu ideata proprio per combattere attacchi di tipo Denial of Service (DoS) (Adam Back chiamò proprio l'articolo che spiegava il protocollo Hashcash:" Hashcash: una contromisura contro attacchi Denial of Service").[5]
Un attacco Denial of Service è un attacco che mira a rendere inutilizzabile per un lasso di tempo indeterminato risorse e funzioni di un Pc. Negando un servizio infatti, posso mandare in crash un sistema; per spiegarlo con un esempio possiamo vedere un attacco DoS quando un malintenzionato (normalmente solo un cracker riesce a fare queste cose) invia al server in cui è ospitato il sito Internet numerose richieste: se il sito ne può gestire solo 20000 e il cracker ne manda 20500 il server va in crash. Esiste anche una versione più complessa del DoS, chiamata Distributed Denial of Service (DDoS), ancora più difficile da contrastare perché l'incursione proviene da più computer. Hashcash sfruttando il sistema PoW cerca di contrastare questi attacchi.

[5] (Back, 2002)

A questo punto si analizza come il sistema Hashcash entra nella blockchain delle criptovalute. Come esempio viene scelto Bitcoin, ma per molte altre criptomonete è la stessa cosa.

Satoshi Nakamoto capì le enormi potenzialità del sistema Hashcash ed intravide la possibilità di utilizzarlo nella blockchain. Infatti nel white paper di Bitcoin, Nakamoto asserì "Per implementare un server timestamp (un server che indica data e orario delle operazioni) distribuito su base peer-to-peer, dovremo utilizzare un sistema di proof-of-work simile all'Hashcash di Adam Back".[6]

Tuttavia il sistema usato dall'Hashcash di Back era un sistema SHA-1. Questo hash era composto da un digest (stringa di numeri e lettere) a 160 bit. Non si ha alcuna verifica empirica o dato certo che possa affermare che Bitcoin con un sistema SHA-1 non avrebbe funzionato; in termini di grandezza andava bene, probabilmente è stata una scelta di sicurezza. Bitcoin invece utilizza un sistema SHA-2 che porta alcune modifiche in termini di affidablità e amplifica il digest delle stringhe a 256 bit: infatti il sistema di proof of work di Bitcoin è un SHA-256.

Infine mentre l'Hashcash è progettato per aumentare o diminuire a metà la difficoltà dell'algoritmo, SHA-256 è progettato per rispondere dinamicamente ai livelli di crescita delle capacità di mining. Praticamente Nakamoto aveva previsto che ci sarebbe stato un miglioramento degli ASIC (Applicated Specific Integrated Circuit) nel tempo (in pratica aveva capito che le macchine per minare bitcoin si sarebbero evolute con il passare degli anni, cosa che sta effettivamente succedendo) insieme ad un aumento dei miners. Contemporaneamente però voleva mantenere invariato il tasso di creazione dei blocchi (che come abbiamo visto sopra è di uno ogni 10 minuti circa); per raggiungere questo obiettivo ha fatto in modo che anche la difficoltà nel decifrare gli hash aumenti o diminuisca in base alle capacità di calcolo della rete. Infatti se per un qualsiasi motivo l'hashing power della rete venisse a mancare e i miners impiegassero più di 10 minuti circa per risolvere un blocco, la difficoltà dei blocchi dovrebbe essere diminuita. Come Bitcoin risolve questo problema?

Per Bitcoin viene fatta una revisione dell'hashing power ogni 2016 blocchi confermati in blockchain, che corrispondono a circa 2 settimane. Se i miners impiegano più di 2 settimane per confermare 2016 blocchi, la difficoltà di risoluzione degli hash codes dovrà essere diminuita, nel caso contrario dovrà essere aumentata. Per aumentare il livello di difficoltà, Bitcoin aumenta il numero di zeri all'inizio della funzione hash; viceversa se Bitcoin vuole diminuire la difficoltà, riduce il numero di zeri all'inizio della stessa.

Si analizzi ora il sistema Proof of Stake (PoS). Il concetto alla base del PoS è che l'attività di estrazione di una criptovaluta può essere fatta solo da chi effettivamente possiede dei token di quella specifica criptovaluta; infatti gli ideatori del sistema PoS ritenevano che maggiore è la partecipazione (stake), quindi il possesso di token, da parte di un determinato soggetto, maggiore è la possibilità che esso non stia violando il sistema ritendendolo quindi maggiormente meritevole di svolgere un'attività di validazione dei blocchi. Nelle monete virtuali che usano i sistemi PoS, la ricompensa per aver aggiunto un blocco non consiste, come nel PoW, in

[6] (Nakamoto, 2008)

un premio in criptomonete (ricordiamo per il Bitcoin ora sono 12,5 BTC a blocco), perché le stesse sono già state tutte pre-minate: la ricompensa è rappresentata dalle commissioni e dall'idea che il soggetto, essendo in possesso di tanti token, avrà interesse che l'utilizzo della moneta continui e si espanda in modo da fare aumentare la domanda.

Ogni qualvolta viene aggiunto un blocco alla blockchain deve essere scelto il creatore del blocco successivo. Come visto, avere più moneta, porta a maggiori possibilità di essere scelti per coniare il blocco successivo; esistono tuttavia alcune varianti:

1) Selezione casuale ad esempio usato da Nxt e Blackcoin, in cui si adopera una funzione random per stabilire il soggetto che conierà il blocco successivo.

2) Selezione basata sull'anzianità, ad esempio usata da Peercoin, in cui si mescola la selezione casuale con il concetto di "anzianità", ovvero un risultato che si ricava dal prodotto tra il numero di monete in portafoglio per il numero di giorni in cui le stesse sono state mantenute.

3) Selezione basata sulla velocità, ad esempio usata da Reddcoin, in cui si cerca di privilegiare la velocità di movimentazione della moneta piuttosto che il suo accumulo.

4) Selezione basata sul voto, ad esempio usata da Bitshares, in cui invece di utilizzare solamente il concetto PoS, i validatori dei blocchi possono essere indicati tramite votazione.

Quali sono gli svantaggi di questi due sistemi?

Normalmente viene utilizzato un sistema PoW che però sta creando problemi dal punto di vista ambientale: l'attività di mining utilizza una quantità spropositata di energia elettrica, producendo un inquinamento sostanziale.

Si esaminino alcuni dati: una transazione Bitcoin richiedeva la stessa quantità di energia elettrica necessaria per alimentare 1.57 famiglie americane al giorno (dati del 2015). In base ai dati dello studio di Digiconomist, in un anno vengono spesi per minare Bitcoin 30,14 terawattora (TWh) di elettricità. Il consumo energetico annuale medio dell'Irlanda è di 25 appena. In una recente ricerca, gli esperti hanno affermato che le transazioni di bitcoin potrebbero consumare più elettricità della Danimarca entro il 2020. Altro problema che non trova soluzione è l'inutilità dei milioni di calcoli che vengono fatti dalle macchine per arrivare alla soluzione corretta dell'hash del blocco; tutti i tentativi sbagliati non possono essere riutilizzati e sono inutili consumi di CPU.

Questi sono i maggiori problemi di un sistema PoW e sono anche i motivi che stanno spingendo Ethereum a passare da un sistema PoW ad uno PoS. Ovviamente anche PoS non è perfetto: non presenta i problemi di consumo di energia elettrica perché il compito di aggiungere un blocco spetta solamente ad un individuo scelto in anticipo, ma ha altri problemi.

Il primo è che si possano creare gravissime disuguaglianze nel lungo periodo, specialmente laddove un soggetto sia in grado di possedere grandi quantità di criptovaluta, riuscendo ad incentrare su di se l'attività di staking.

Il secondo è che il soggetto che si occupa dello staking possa decidere di approvare transazioni maligne (ricordiamo che colui che è detentore di moneta virtuale e colui che convalida i blocchi nel PoS sono la stessa persona).
Il terzo è che usando un sistema PoW, i cattivi partecipanti vengono esclusi grazie a disincentivi tecnologici ed economici. In effetti, programmare un attacco su una rete PoW è molto costoso e occorrerebbe più denaro di quello che si potrebbe riuscire a rubare. Invece l'algoritmo del PoS deve essere il più sicuro possibile, perché, senza sanzioni particolari, una rete basata sul sistema proof of stake, potrebbe essere più economica da attaccare.
Il quarto è il cosiddetto "nothing at stake" (nessuna posta in gioco). Significa che, nel caso di una ramificazione della blockchain (o qualsiasi altro tipo di disaccordo nel consenso), una persona possa "votare" per entrambe le varianti, perché ha degli interessi in ciascuna delle stesse. Non costa molto lavorare su diverse blockchain (non come nel sistema proof-of-work dove invece è molto costoso), e ciò permette di provare ad ingannare “gratis” (ad esempio spendendo la stessa cifra due volte in un'istanza di riorganizzazione della blockchain).

1.2.4 La Blockchain

E’ una tecnologia che consente la creazione e l’utilizzo di un grande database distribuito per la gestione di transazioni condivisibili tra più nodi di una rete, dove con il termine nodi si definiscono i partecipanti alla blockchain.
La blockchain è costituita da una catena di blocchi che contengono ciascuno più transazioni. La soluzione per tutte le transazioni è affidata ai miners che devono vedere, analizzare e approvare tutti gli scambi creando una rete che condivide su ciascun nodo l’archivio di tutta la blockchain e dunque tutti i blocchi con tutte le transazioni.
Quale è il vero problema che viene risolto dalla blockchain? Il problema della fiducia.
Imprese, ma soprattutto banche e Pubbliche Amministrazioni, hanno utilizzato i ledgers, archivi che contengono tutte le informazioni, per gestire la contabilità, l’archiviazione dei dati e le transazioni contabili. In particolare le PA hanno basato sui ledgers le registrazioni e i passaggi di proprietà per terreni, edifici e asset immobiliari.
Ad ogni cambiamento, ad esempio nella proprietà di un immobile, si procedeva con una modifica del ledger attraverso una autorità centrale deputata alla gestione del Central Ledger. Con questa organizzazione, agendo sul Central Ledger, gli uffici delle Pubbliche Amministrazioni o gli Istituti di credito potevano in qualsiasi momento conoscere e identificare il proprietario di un immobile o di determinate risorse. Questo controllo permetteva alle banche stesse o agli uffici pubblici di verificare che eventuali passaggi legati a nuove transazioni su determinati beni fossero effettivamente possibili e soprattutto legittimi. Quindi, con il Central Ledger, era possibile verificare se il soggetto X intenzionato a vendere l’immobile Y fosse effettivamente in possesso dello stesso o non lo avesse già ceduto a un soggetto Z. La banca a sua volta poteva controllare che

il soggetto H in procinto di acquistare l'immobile Y dal soggetto X fosse effettivamente in possesso della cifra necessaria e non l'avesse già utilizzata per altre acquisizioni.
La base del Central Ledger è tutta racchiusa nella fiducia che tutti devono avere nel gestore del Central Ledger. Banche e Pubbliche Amministrazioni devono avere quell'autorevolezza in grado di infondere la fiducia necessaria perché le persone possano comprare e vendere anche senza essersi mai incontrate prima e in assenza di stima reciproca; ciò perché c'è un soggetto terzo che garantisce per tutti.
Il grande cambiamento arriva con la blockchain. La blockchain è un database decentralizzato che archivia asset e transazioni su una rete di tipo peer-to-peer. È un registro pubblico per la gestione di dati correlati alle transazioni presenti nei blocchi e gestite tramite crittografia dai partecipanti alla rete che verificano, approvano e successivamente registrano tutti i blocchi con tutti i dati di ciascuna transazione.
La blockchain permette di garantire la stessa funzionalità nella gestione dei ledgers ma senza dover fare riferimento a una struttura centralizzata, senza cioè che sia necessario che una autorità centrale verifichi, controlli e autorizzi la legittimità di una transazione, di uno scambio, di un passaggio.
La domanda che ci si pone è: come si può verificare la legittimità di una transazione se non c'è un'autorità centrale che ha la possibilità di effettuare i controlli necessari? La risposta della blockchain è nella decentralizzazione del Libro Mastro, del ledger.
Se prima il Libro Mastro era univoco, uno solo e stava in capo all'autorità centrale, adesso il Libro Mastro è di tutti, ovvero tutti gli utenti ne hanno una copia e tutti possono controllarlo, visionarlo e, a fronte di regole che vanno a comporre la Governance della blockchain, modificarlo. Perciò il primo, vero, grande passaggio tra la gestione dei ledgers tradizionali e la blockchain è data dal fatto che i Libri Mastro sono molteplici e che sono accessibili a tutti.
Il secondo grande passaggio riguarda il fatto che tutti possono attuare una transazione.
Ogni nuovo scambio che deve essere registrato viene unito ad altri nuovi scambi e va a formare un "blocco", che viene aggiunto come anello di una lunga "catena" di transazioni cronologiche. Ogni volta che si genera un blocco si allunga la catena. Questa catena va a comporre il grande Libro Mastro blockchain, che è posseduto da tutti i partecipanti.
Perché un nuovo blocco di transazioni sia aggiunto alla blockchain è necessario che sia controllato, validato e crittografato. Per effettuare ciò è necessario che, ogni volta che viene composto un blocco, venga risolto un complesso problema matematico che richiede un cospicuo impegno in termini di potenza e di capacità elaborativa. Questa operazione è il mining (visto in precedenza).
Il lavoro del miner è assolutamente fondamentale nell'economia della gestione delle blockchain. Chiunque può diventare un miner e può competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di ogni nuovo blocco. Nel caso in cui il processo di verifica dovesse rilevare un errore, una anomalia, una discrepanza, il blocco viene rifiutato e tutti possono vedere che la transazione non è stata autorizzata. Diversamente, se tutte le transazioni sono validate, il blocco viene creato ed entrerà a far parte

della blockchain a tutti gli effetti come un record (una registrazione) pubblico, permanente e immutabile; nessun partecipante alla blockchain potrà cambiarlo o rimuoverlo.[7] [8]

All'interno di uno stesso blocco sono contenute tante transazioni, ciascuna dotata di un hash code differente. Tuttavia, quando si osserva la blockchain, si può notare che ogni singolo blocco possiede un hash code singolo: questo dipende dalla tecnologia del Merkle Tree.

Un Merkle Tree riepiloga tutte le transazioni in un blocco producendo un'impronta digitale dell'intero insieme di transazioni, consentendo in tal modo all'utente di verificare se uno scambio è incluso o meno in un blocco. I Merkle Trees vengono calcolati ripetutamente da coppie di nodi di hash finché non ne rimane solo uno (questo hash si chiama Root Hash o Merkle Root) e sono costruiti dal basso verso l'alto, dagli hash delle singole transazioni (conosciute come ID Transaction) fino ad arrivare al Merkle Root. I Merkle Trees sono binari e quindi richiedono un numero pari di nodi. Se il numero di transazioni è dispari, l'ultimo hash verrà duplicato una volta per creare un numero pari. La Merkle Root riepiloga tutti i dati delle transazioni correlate e viene memorizzata nell'intestazione del blocco. Essa mantiene l'integrità dei dati: se un singolo dettaglio in una qualsiasi delle transazioni o l'ordine delle transazioni cambia, lo stesso vale per il Merkle Root. L'utilizzo di un Merkle Tree consente di verificare in modo semplice e rapido se una transazione specifica è inclusa nell'insieme oppure no.

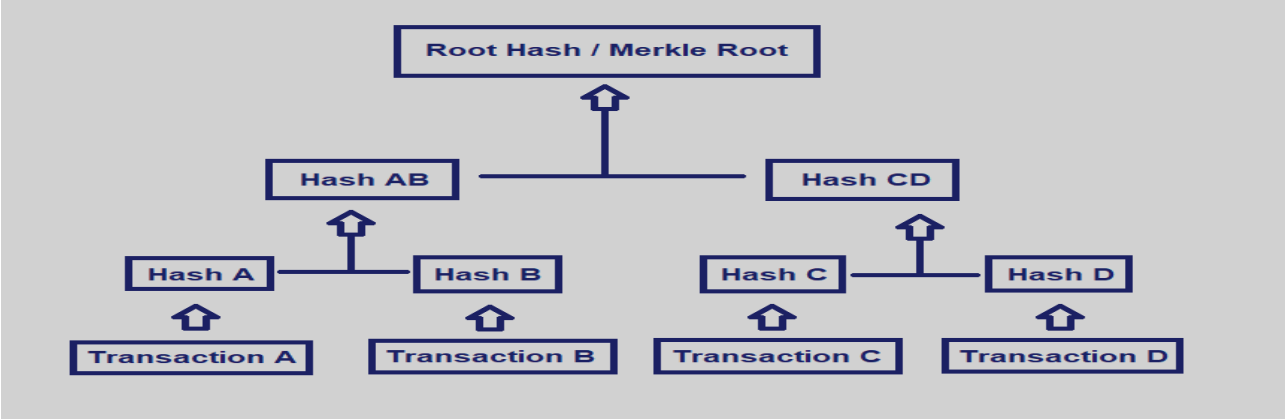

Figura 1.1 The merkle tree of transactions A,B,C & D Fonte: Shaan Ray, Merkle Trees

Una delle caratteristiche più importanti della blockchain è la sicurezza. La Marca Temporale (Timestamp) impedisce che l'operazione, una volta eseguita, venga alterata o annullata.

La Marca Temporale consente di associare una data e un'ora certe e legalmente valide a un documento informatico. In altre parole il Timestamp consente di definire una validazione temporale che può essere opponibile a terzi.

Un altro aspetto che garantisce la sicurezza della blockchain è il Distributed Ledger. Un esempio: Paypal è una società che offre servizi di pagamento digitale e trasferimenti di denaro tramite Internet, operando come

[7] (Bellini, 2018)
[8] (Swan, 2015)

istituto di credito. La società Paypal conta più di 160 milioni di utenti attivi in 203 paesi diversi e il suo grande vantaggio è quello di non divulgare alla controparte i dati della carta. Inoltre offre agli utenti e alle aziende un programma di protezione acquisti e vendite: nel caso in cui l'acquirente non riceva l'oggetto o lo riceva notevolmente non conforme alla descrizione, PayPal rimborsa l'intero importo, incluse le spese di spedizione. Nonostante ciò le transazioni che vengono fatte con Paypal vengono gestite e mantenute in un database centralizzato interno alla società che di conseguenza comporta un rischio di sicurezza: se il sistema va in down nessuno potrebbe più fare transazioni con Paypal.
Un altro problema di Paypal è legato alla possibile inflazione della moneta. Ipotizzando uno scenario inflattivo a causa di una eccessiva emissione di liquidità da parte delle Banche Centrali, il circuito Paypal subirebbe consistenti perdite.
Attraverso la blockchain e le criptovalute questi problemi sono risolti: infatti la blockchain proprio per il fatto di essere un registro distribuito non può essere attaccato in quanto è impossibile colpire contemporaneamente tutti i nodi della rete, mentre per il problema dell'inflazione abbiamo già visto sopra come alcune criptovalute (vedi il Bitcoin) risolvano il problema.
Ricapitolando la blockchain ha quattro caratteristiche fondamentali:

- È sicura, in quanto è un database distribuito, condiviso, decentralizzato e criptato con precise regole di sicurezza
- È immutabile, per cui è garantito che le informazioni contenute al suo interno non vengano modificate
- È trasparente, perché tutti i partecipanti possono vedere le informazioni in qualsiasi momento
- È basata sul consenso, dato che può essere modificata solo con l'approvazione di tutti i partecipanti

Esistono due tipi di blockchain:

- Permissionless o blockchain pubbliche

  La caratteristica delle blockchain pubbliche consiste nel fatto che sono aperte, non hanno una proprietà o un attore di riferimento e sono concepite per non essere controllate. Le Permissionless blockchain hanno l'obiettivo di permettere a ciascuno, senza permesso appunto, di contribuire all'aggiornamento dei dati sul ledger; non esiste nessun soggetto pre-selezionato che fa da validatore perché chiunque nel sistema può essere un miner e dispone, in qualità di partecipante, di tutte le copie immutabili di ogni operazione.

  Questo modello di blockchain pubblica impedisce ogni forma di censura: nessuno può impedire che una transazione possa avvenire e che possa essere aggiunta al ledger una volta che ha conquistato il consenso necessario tra tutti i nodi (partecipanti) alla blockchain.
- Permissioned o blockchain private

  Al contrario le Permissioned possono essere controllate e dunque possono avere una proprietà. Nel momento in cui un nuovo dato viene aggiunto alla blockchain, il sistema di approvazione non è

vincolato alla maggioranza dei partecipanti ma ad un numero limitato di attori che sono definibili come trusted. Questo tipo di blockchain può essere essere utilizzata da istituzioni, grandi imprese che devono gestire filiere con una serie di attori, imprese che devono gestire fornitori e subfornitori, banche, società di servizi, operatori nell'ambito del retail. Le Permissioned prevedono l'esistenza di uno o più soggetti pre-selezionati che svolgono la funzione di validatore nel network. Se il validatore è un solo agente viene definita come Distributed Ledger Technology (DLT) privata, mentre se il validatore è più di uno viene definita come DLT consortium. [9]

Bisogna fare attenzione che una blockchain privata per un'azienda non sia un'overskill. La blockchain nasce come strumento per disintermediare la fiducia e nel caso di permissioned blockchain il ruolo di validatore delle transazioni è comunque interno all'azienda. In questo caso ci sono poche differenze tra mettere i dati in blockchain oppure lasciarli in un "normale" database privato dotato di buona sicurezza. Spesso infatti una società che usa una blockchain come raccolta di dati aziendali si fa molta pubblicità per l'utilizzo della stessa e gode di vantaggi a causa dell'"offuscamento legislativo" che c'è intorno alla materia, collegato al fatto che il legislatore non ha ancora inserito delle leggi che la regolamentino perfettamente. Tuttavia, all'atto pratico, i vantaggi dell'adozione della blockchain non sono molti e il suo utilizzo risulta essere alcune volte solo una strategia di marketing. [10]

In una blockchain si può verificare un fork. Un fork è una biforcazione della blockchain che fa in modo che la catena di blocchi si divida in due parti: la catena originale, detta anche Legacy, continua per la sua strada mentre ne nasce un'altra differente che ha origine dalla prima. La catena secondaria presenterà un protocollo differente e, a volte, incompatibile rispetto all'originale, portando alla formazione di una nuova moneta virtuale.

I fork vengono utilizzati dal network per migliorare la performance della blockchain: si dividono in due tipi:

- Soft Fork si realizza e si attua dando vita a una versione aggiornata del protocollo blockchain compatibile con le versioni precedenti. Il Soft Fork mette in atto un cambiamento reversibile che consente la partecipazione alla rete blockchain anche a tutti quei nodi che per varie ragioni decidono di non effettuare l'aggiornamento.
- Hard Fork prevede un cambiamento irreversibile e impone ai partecipanti alla blockchain di effettuare obbligatoriamente l'aggiornamento. Con gli Hard Fork vengono create nuove criptomonete come sono state ad esempio in passato Bitcoin Cash o prima ancora Zcash e Litecoin.

  Gli Hard Fork possono essere di tipo Planned, ovvero pianificati e programmati, o di tipo Contentious, ovvero che non riescono a trovare il consenso della comunità: nel caso di Hard Fork Planned il cambiamento del protocollo è pianificato e il passaggio viene approvato dai partecipanti alla

[9] (Bellini, 2018)
[10] (BitFury, 2015)

community. L'Hard Fork Planned non conduce allo sdoppiamento della blockchain e le regole vengono aggiornate in forma di continuità.

Nel caso degli Hard Fork Contentious, il cambiamento proposto al protocollo non trova un accordo all'interno della community e con l'Hard Fork si arriva a una forma di scissione della blockchain. Gli Hard Fork Contentious portano alla creazione di una nuova moneta.

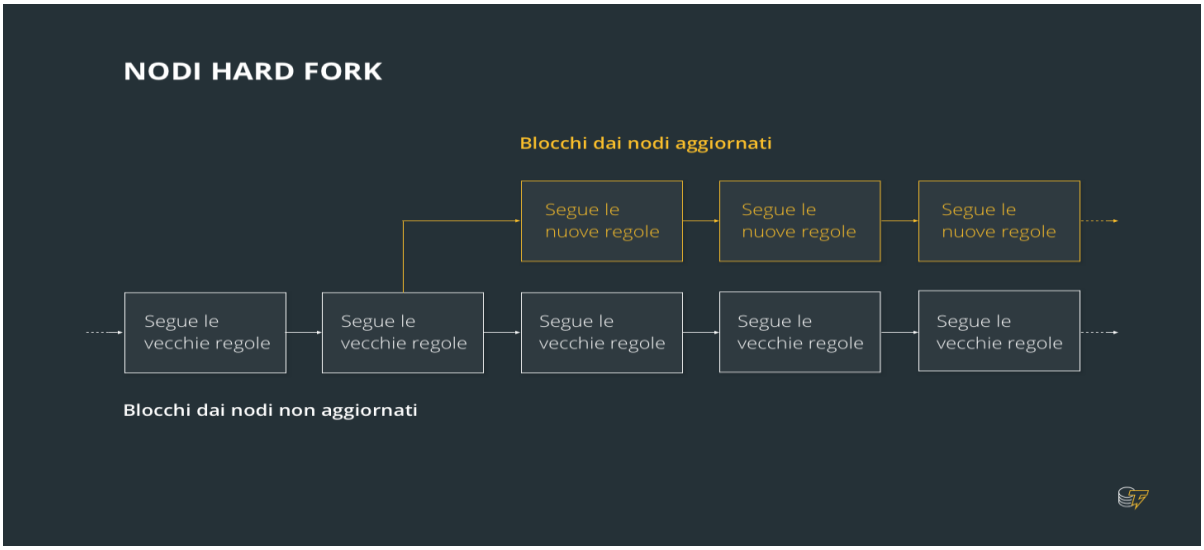

Figura 1.2 Hard Fork. Fonte: Cointelegraph.com, Cos'è una hard fork

Quali sono le ragioni che portano ad un Fork della blockchain?

Uno dei temi che spinge la comunità di una blockchain ad affrontare un Fork è quello della scalabilità.

Vediamo il più famoso Fork della blockchain di Bitcoin, che ha portato alla nascita di Bitcoin Cash, per capire i problemi di scalabilità di Bitcoin ampiamente dibattuti nell'ultimo anno e mezzo.

Il limite di 1 MB di ogni blocco di Bitcoin venne originariamente implementato per ridurre la possibilità di spamming o di attacchi DDoS. Poiché al tempo non venivano effettuate molte transazioni all'interno della rete, il limite non ebbe alcun effetto negativo.

A causa dell'aumento di scambi in Bitcoin, tale soglia ha causato un sovraccarico della rete ed un accumulo dei blocchi, incrementando esponenzialmente i tempi di transazione.

La situazione è peggiorata nel maggio del 2017, quando alcuni utilizzatori segnalarono di aver dovuto aspettare fino a quattro giorni per ricevere la conferma di avvenuto scambio. Gli utenti potevano accelerare il processo di conferma pagando spese di transazione più alte, ma tale approccio rese il Bitcoin inutilizzabile come metodo di pagamento, specialmente per acquisti di basso costo. Ad esempio acquistare un prodotto del valore di pochi euro avrebbe portato a commissioni spropositate che avrebbero reso impensabile l'elaborazione della transazione.

Da allora la comunità del Bitcoin è arrivata a due possibili soluzioni: Bitcoin Unlimited o Segregated Witness (SegWit).

Bitcoin Unlimited avrebbe eliminato totalmente il limite dei blocchi. Molti miners erano a favore di questa soluzione, in quanto la mancanza di un tetto massimo alla grandezza dei blocchi non solo avrebbe evitato accavallamenti, ma avrebbe portato anche ad un incremento delle tariffe.

Nonostante ciò molti sviluppatori furono contrari a questa proposta, poiché la sua implementazione avrebbe portato alla cessazione delle attività di molti piccoli miners e, di conseguenza, ad una maggiore centralizzazione della rete nelle mani di enormi compagnie di mining.

Una soluzione Segregated Witness avrebbe comportato invece l'archiviazione di alcuni dati al di fuori della blockchain vera e propria. Gli sviluppatori confermarono che in tal modo sarebbe stato possibile liberare moltissimo spazio: all'interno dei blocchi sarebbe entrato un numero maggiore di transazioni ed i tempi di conferma sarebbero stati fortemente ridotti. Tuttavia molte persone credettero che si sarebbe trattato di una soluzione provvisoria rispetto all'approccio Bitcoin Unlimited.

Di conseguenza, venne sviluppato un protocollo di compromesso chiamato SegWit2x. Il lancio di questo protocollo avrebbe portato all'archiviazione di alcune informazioni al di fuori della blockchain, e al tempo stesso ad un incremento della grandezza dei blocchi a 2 MB.

Il protocollo è stato adottato ufficialmente nell'agosto del 2017, quando il 95% dei miners votò positivamente alla sua implementazione. Purtroppo la rete non ha subito un incremento immediato dello spazio disponibile nei blocchi, portando molti utenti a credere che il problema non fosse realmente risolto, ma solo posticipato.

Inoltre, questa decisione sembrava indirizzata principalmente verso coloro che consideravano il Bitcoin come un'opportunità d'investimento e non il sistema di pagamento ipotizzato.

Dopodiché, durante la conferenza Future of Bitcoin tenutasi ad Arnhem, in Olanda, l'ex-ingegnere di Facebook Amaury Séchet annunciò la prima implementazione del protocollo Bitcoin Cash, chiamata Bitcoin ABC.

Séchet ed il suo team di sviluppatori decisero di abbandonare il protocollo SegWit2x e di incrementare il limite di grandezza dei blocchi a 8 MB. Però una modifica tanto drastica richiedeva una separazione dalla rete originale del Bitcoin: per questo motivo l'1 agosto del 2017 venne annunciata una Hard Fork e ci fu la nascita di Bicoin Cash che oggi (9 agosto 2018) è la quarta criptovaluta per capitalizzazione.[11]

[11] (Cos'è il Bitcoin Cash, 2018)

1.3 La regolamentazione europea delle criptovalute

L'Unione Europea ha finora mantenuto un atteggiamento piuttosto scettico nei confronti delle criptomonete, mettendo più volte in guardia gli investitori sui rischi delle stesse a causa della loro elevata volatilità. Ad esempio significative sono le dichiarazioni del 26 febbraio 2018 di Valdis Dombrovskis, Vice Presidente della Commissione Europea. Dombrovskis dichiarò che le criptovalute non essendo monete nel senso tradizionale del termine e non essendo garantito il loro valore, sono diventate oggetto di considerevoli speculazioni.[12]

Anche Mario Draghi, presidente della BCE, non aveva mostrato una grande predisposizione verso le criptovalute; in particolare quando gli era stato chiesto, a margine della conferenza della BCE di settembre 2017, cosa pensasse riguardo al progetto dell'Estonia di creare una propria moneta virtuale, l'Estcoin, Draghi disse: "La moneta dell'Eurozona è l'Euro. Nessuno Stato può lanciare una propria valuta."

Tuttavia, grazie all'entrata in vigore della Direttiva UE 2018/843 del Parlamento e del Consiglio Europeo, con la sua pubblicazione all'interno della Gazzetta Ufficiale dell'Unione Europea, l'UE riconosce ufficialmente le criptovalute. La Direttiva sentenzia "Valute virtuali: una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente".[13]

La Direttiva, che deve essere recepita dagli stati membri entro il 10 gennaio 2020, dà per la prima volta una definizione e un riconoscimento ufficiale alle criptomonete.

Malta da tempo opera nel settore delle monete virtuali e del FinTech, grazie soprattutto all'appoggio del suo Primo Ministro, Joseph Muscat, il quale dichiarò che le criptovalute saranno "l'inevitabile futuro del denaro" e che costituiranno la base di una nuova economia. Avvenimento centrale per un'isola di piccole dimensioni è il prossimo arrivo (per la prima volta in Europa) di Binance, la più grande piattaforma al mondo per volumi di scambi giornalieri per ciò che riguarda gli exchange di criptovalute. Zhao Changpeng, CEO di Binance, ha infatti dichiarato: "Malta è ultimamente molto incline ad atteggiamenti progressisti per quanto riguarda le criptovalute e il FinTech".

Per questa ragione, oltre che il basso livello di tassazione vigente sull'isola, si potrebbe pensare che la Direttiva UE 2018/843 trovi a Malta una situazione più agevolata rispetto a qualsiasi altro Stato dell'Unione Europea.

Successivamente si esamineranno Ethereum, Ripple, Iota e Monero.

[12] (Dombrovskis, 2018)
[13] (Direttiva2018/843, 2018)

1.4 Ethereum

E' una piattaforma decentralizzata del Web 3.0 che produce e gestisce i contratti intelligenti (smart contracts). La piattaforma fu creata da un ragazzo russo, Vitalik Buterin, che ha voluto creare delle applicazioni e dei contratti inseriti in blockchain che funzionino senza possibilità di downtime, censure, frodi o interferenze di terzi.

1.4.1 Smart contract

Gli smart contracts sono protocolli informatici che permettono di scambiare denaro, titoli azionari o qualsiasi altra cosa di valore in maniera trasparente, senza la necessità di rivolgersi ad un intermediario. A differenza di un contratto tradizionale in cui le parti possono ricorrere a misure correttive attraverso il sistema legale, un contratto intelligente è auto-applicato, a seconda che vengano soddisfatte determinate condizioni, monitorate tramite software. Proprio perché l'assenza di un intervento umano corrisponde anche all'assenza di un contributo interpretativo, lo smart contract deve essere basato su descrizioni estremamente precise per tutte le circostanze e tutte le condizioni. Per gli smart contracts è fondamentale definire in modo estremante preciso le fonti di dati alle quali il contratto deve attenersi.

Lo smart contract è di fatto "figlio" dell'esecuzione di un codice da parte di un computer. E' un programma che elabora in modo deterministico (con identici risultati a fronte di identiche condizioni) le informazioni che vengono raccolte. In altre parole, se gli input sono gli stessi i risultati saranno identici. Questo punto è estremamente rilevante perché se per un verso rappresenta una sicurezza in quanto garantisce alle parti una assoluta "certezza di giudizio oggettivo", escludendo qualsiasi forma di interpretazione, per l'altro sposta sul codice, sulla programmazione, sullo sviluppo il peso e la responsabilità o anche il potere di decidere.

Ai contraenti spetta il compito di definire condizioni, clausole, modalità, regole di controllo e di azione; tuttavia una volta che il contratto è diventato uno smart contract e i contraenti lo hanno accettato, gli effetti non dipendono più dalla loro volontà. Pertanto il tema della fiducia si sposta, esce dallo studio legale per entrare nel terreno dello sviluppatore.

Se lo smart contract funziona correttamente, dovrebbe fornire una serie di garanzie a tutte le parti coinvolte consistenti nell'assicurare che il codice con cui è stato scritto non possa essere modificato, che le fonti di dati che determinano le condizioni di applicazione siano attestate e affidabili e che le modalità di lettura siano a loro volta certificate.[14]

Non esiste un esempio unico di smart contract, ma questi possono essere classificati in due categorie:

-Smart Code Contract (contratti software privi di contenuto legale) il cui requisito chiave è che il codice debba essere eseguito correttamente e con precisione fino al completamento, entro un tempo ragionevole. Se la piattaforma di esecuzione ha il controllo completo di tutte le azioni che il codice del contratto intelligente desidera eseguire, allora queste dovrebbero essere compiute giustamente e con

[14] (Bellini, 2018)

risultati soddisfacenti. Eventuali impedimenti potrebbero essere problemi tecnici all'interno della piattaforma o problemi di esecuzione che si verificano al di fuori della stessa come ad esempio una mancata consegna fisica delle merci.

-Smart Legal Contract (contratti intelligenti di tipo legale) in cui le cose possono essere notevolmente più complesse. In genere un contratto legale dovrebbe avere un numero elevato di diritti e obblighi stabiliti in base ad accordi interni tra le parti e che possono essere garantiti. Questi sono spesso scritti in modo complesso, sono diversi in base al contesto in cui stanno operando, utilizzano un linguaggio giuridico e possono riguardare non solamente azioni individuali, ma anche comportamenti che dipendono dal tempo e dallo spazio della loro esecuzione. Potrebbero inoltre esserci obblighi imperativi su una o più parti in modo tale che una mancanza di azione possa essere considerata un comportamento errato.[15]

Gli smart contracts generalmente servono a quattro scopi:

1) Mantenere un archivio dati che rappresenti qualcosa di utile per altri contratti o per il mondo esterno; un esempio è un contratto che crea una valuta oppure che registra l'appartenenza a una particolare organizzazione.

2) Essere una sorta di account di proprietà esterna con una politica di accesso più complicata; questo è chiamato "forwarding contract" e in genere comporta il semplice invio di messaggi in arrivo ad una destinazione scelta solo al soddisfacimento di determinate condizioni; ad esempio si può avere un forwarding contract che aspetta fino a quando due delle tre chiavi private hanno confermato un particolare messaggio prima di inviarlo (ad esempio multisig). I forwarding contracts più complessi hanno condizioni diverse in base alla natura del messaggio inviato; il caso d'uso più semplice per questa funzionalità è un limite di prelievo che è sovrascrivibile tramite una procedura di accesso più complicata.

3) Gestire un contratto o una relazione in corso tra più utenti come un contratto finanziario, un impegno con qualche particolare gruppo di mediatori o un qualche tipo di assicurazione. Un esempio di questo è un contratto che paga automaticamente una somma a chiunque invii una soluzione valida ad un problema matematico o dimostri di fornire una risorsa computazionale.

4)Offrire funzioni ad altri contratti, come una libreria di software.[16]

Il linguaggio di programmazione utilizzato dagli smart contracts si chiama Solidity: per la sua realizzazione ha subito l'influenza di C++, JavaScript e Python ed è indirizzato per l'Ethereum Virtual Machine (EVM). Solidity prevale su altri linguaggi di programmazione (Viper, Serpent, LLL, Mutan) che erano stati creati anch'essi per la scrittura di smart contracts nell'EVM ma che poi, per loro problemi interni, non si sono riusciti ad affermare. I programmatori hanno deciso di utilizzare nuovi linguaggi di programmazione e non quelli già consolidati perché sarebbe stato necessario un adattamento di quelli esistenti che sarebbe risultato molto lungo e complesso.

[15] (Clack, 2016)
[16] (Buterin, 2014)

L'IDE (Integrated Development Environment) ufficiale di Solidity è Remix, che può essere scaricato dal github [17]. Remix è un insieme di tools per interagire con la blockchain di Ethereum che consente di eseguire il debug delle transazioni.

Dopo che è stato fatto uno smart contract con Solidity, lo stesso deve essere eseguito grazie all'Ethereum Virtual Machine (EVM): l'EVM è il centro di calcolo "Turing complete" che permette l'esecuzione di contratti intelligenti al di sopra della piattaforma Ethereum. È quindi una macchina virtuale, ossia un software in grado di emulare in tutto e per tutto una macchina fisica, attraverso un processo di virtualizzazione in cui vengono assegnate le risorse fisiche (CPU, RAM, disco fisso…) alle applicazioni che vengono eseguite al di sopra della macchina virtuale (tra cui il sistema operativo della stessa). Da un punto di vista pratico, l'EVM può essere pensato come un grande computer decentralizzato contenente milioni di codici, chiamati "account", che hanno la capacità di mantenere un database interno, eseguire codici e parlare tra loro.

Esistono due tipi di account aventi ciascuno un indirizzo di 20 byte:

- Externally Owned Account (EOA): controllato da una coppia di chiavi pubblica-privata (siamo nel mondo della crittografia asimmetrica) e quindi riferito ad una persona/entità.
- Contract Account (CA), controllato dal codice presente proprio nel contratto.

  Ogni account è composto da 4 campi: il nonce, un numero che, nel caso di un EOA, rappresenta il numero di transazioni inviate dall'indirizzo dell'account mentre, per un CA, rappresenta il numero di contratti creati dall'account; il balance, ossia il numero di wei (che è la più piccola unità di misura dell'Ether, in particolare 1 Ether=1*10^18 wei) posseduti dall'account; il contract code dell'account, che nel caso di un EOA è solo l'hash della stringa vuota; lo storage (dispositivi hardware, software infrastrutture, supporti di manutenzione ecc...) dedicato alla memorizzazione dei contratti intelligenti.

Ogni nodo della rete ha la propria EVM ed esegue in particolare lo stesso set di istruzioni degli altri nodi. Gli smart contracts, sviluppati con linguaggi di alto livello quali Solidity e Serpent, prima di essere eseguiti, vengono compilati producendo il bytecode interpretabile poi dall'EVM. Questo consiste in una serie di bytes, dove ogni byte rappresenta un'operazione. In generale l'esecuzione del codice è un loop infinito che consiste nel ripetere continuamente le operazioni indirizzate dal computer fintanto che il contract code non si imbatte in istruzioni di tipo return, stop o ad un errore.[18] [19]

È importante ricordare che il prezzo da pagare per il calcolo computazionale della EVM si traduce nel concetto di gas, il carburante del sistema Ethereum pagabile tramite ether (o meglio wei). Ad ogni smart contract è infatti associato un gasPrice ed un limite di gas "consumabile" dal contratto, da cui i miners traggono la ricompensa per il lavoro svolto. Il gas nasce come obiettivo per scongiurare attacchi DoS/DDoS per cui è possibile ottenere gas scambiandolo con Ether, la valuta di Ethereum.

[17] (Remix, 2018)
[18] (Bhargavan, 2016)
[19] (Ethereum Development Tutorial, 2018)

In base alla funzione che si vuole svolgere sulla blockchain di Ethereum si avrà bisogno di un certo quantitativo di gas: ovviamente non è possibile sapere a priori quanto sia il costo di un'unità di gas che si debba mantenere, in quanto questo varia a seconda del mercato, ovvero di quanto gli altri utilizzatori della rete di Ethereum sono disposti a pagare. Tuttavia è possibile effettuare una ragionevole approssimazione consultando ad esempio il sito ethgasstation.info che consente di vedere gli andamenti minuto per minuto. Un trasferimento ETH standard richiede un limite di gas di 21.000 unità.

Tutto il denaro speso dal mittente per il gas viene inviato all'indirizzo "beneficiario", che di solito è quello del miner. Poiché i miners stanno spendendo le loro risorse per eseguire i calcoli e convalidare le transazioni, ricevono la fee come ricompensa. In genere più alto è il prezzo del gas che un mittente è disposto a pagare maggiore sarà il valore che il miner ricaverà dalla transazione. In questo modo i miners sono liberi di scegliere quali transazioni convalidare e quali ignorare. Per orientare i mittenti verso un prezzo del gas da loro ritenuto accettabile, i vari miners hanno la possibilità di pubblicizzare il prezzo minimo del gas al quale sono disposti ad effettuare transazioni. Il sistema del gas svolge lo stesso ruolo delle fees per i bitcoin: quando i miners vedono che il gasPrice è elevato allora decideranno di cedere la potenza di calcolo del loro computer per svolgere il contratto; in caso contrario, come per le fees sotto la media in Bitcoin, ci saranno meno incentivi per i miners per svolgere l'operazione, perché il costo in termini di elettricità e tempo è superiore rispetto a quello di aggiungere un blocco alla blockchain di Ethereum. Questo trade-off consente al sistema di auto-equilibrarsi.

Se il mittente non fornisse il gas necessario per eseguire una transazione, quest'ultima si esaurirebbe e non sarebbe considerata valida. In questo caso l'elaborazione della transazione si interromperebbe e qualsiasi cambiamento di stato che si fosse verificato verrebbe ripristinato in modo da tornare allo stato di Ethereum precedente. Inoltre verrebbe registrata una transazione non riuscita per mostrare che l'operazione è stata tentata ed è fallita. In aggiunta, poiché la macchina ha già speso risorse per eseguire i calcoli prima di esaurire il gas, nessun importo verrà rimborsato al mittente. Se invece il mittente ha abbastanza Ether-gas nel proprio saldo per coprire un importo, la transazione può essere eseguita. Costui sarà poi rimborsato per l'importo di gas non utilizzato al termine della transazione, scambiato al tasso di cambio originale.

1.4.2 Initial Coin Offering (ICO)

Vediamo ora le ICO (Initial Coin Offering) e le dApps e capiamo come esse si appoggiano sulla blockchain di Ethereum.

Una ICO è un nuovo metodo di crowdfunding non regolamentato che consente di scambiare un nuovo token con i servizi che l'azienda creatrice del token offre. L'Initial Coin Offering è uno strumento rivoluzionario nel mondo del venture capital perché permette di superare le rigide regole dei processi di valutazione tradizionalmente adottati da fondi e banche. In sintesi, per reperire dei finanziamenti si propone al pubblico (normalmente tramite un "whitepaper") un progetto che sarà realizzato tramite blockchain con creazione di

token da vendere, a fronte di un corrispettivo, ai soggetti finanziatori. Il ritorno finanziario degli investitori, o meglio di coloro che per primi credono nelle potenzialità della startup, è essenzialmente legato al valore che la nuova criptovaluta assumerà nel tempo. Il meccanismo è quindi molto simile a quello di una IPO (Initial public offering) tradizionale, ovvero la quotazione di una società in Borsa con però tre importanti differenze: la prima è che l'ICO avviene all'inizio della vita della startup e porta valore finanziario da subito; la seconda è che non richiede, non essendo regolamentata, i tempi e i costi finanziari e burocratici tipici di una IPO; la terza è che nella ICO, per raccogliere fondi, c'è la creazione di una nuova moneta virtuale.

Generalmente una ICO presenta un soft cap e un hard cap, che rappresentano rispettivamente l'obiettivo minimo e quello massimo della raccolta di fondi. Qualora il soft cap non venga raggiunto la ICO potrebbe procedere in diversi modi che vanno dalla restituzione dei soldi fino alla messa in commercio delle poche monete vendute.

Il meccanismo delle ICO è esposto alla possibilità che il soggetto emettitore abbia in realtà fini poco onorevoli. Una truffa che si è verificata in diverse occasioni è la cosiddetta "Pump & Dump", in cui il valore del token viene gonfiato artificialmente tramite dichiarazioni molto positive sul progetto, con l'obiettivo di vendere le monete a un prezzo più alto. Una volta che i token vengono venduti, il prezzo precipita e gli investitori perdono i loro soldi.

A causa di situazioni come questa, regolatori come la SEC o la UK Financial Conduct Authority hanno segnalato agli investitori che le ICO sono particolarmente rischiose e speculative, costituendo possibili truffe. La cronaca ci segnala ad esempio che nel settembre 2017 la People's Bank of China ha ufficialmente vietato le ICO, definendole uno strumento che mette a rischio la stabilità economica e finanziaria, proibendo sia l'utilizzo dei token come valuta di scambio sul mercato sia la possibilità delle banche di offrire servizi collegati alle ICO.

Non bisogna ovviamente criminalizzare il fenomeno. Non tutte le ICO sono truffe. La stessa Ethereum si è finanziata con questo meccanismo nel 2014, raccogliendo 3.700 bitcoin nelle prime 12 ore, equivalenti a circa 2,3 milioni di dollari. E' però molto importante avere la consapevolezza che si tratta di un investimento ad altissimo rischio perché i progetti finanziati sono tipicamente in una fase preliminare del loro sviluppo e quindi hanno esiti ancora incerti. [20]

Per la maggior parte dei nuovi token lanciati tramite ICO si utilizza lo standard di Ethereum ERC-20.

ERC-20, che è l'acronimo di Ethereum Request for Comments e '20' è il numero identificativo della proposta univoca, definisce una serie di regole che devono essere soddisfatte affinché un token possa essere accettato e chiamato 'ERC-20 Token'. Le regole standard si applicano a tutte le monete ERC-20 poiché queste norme sono necessarie per interagire tra loro sulla rete Ethereum. Questi token sono beni che utilizzano la blockchain e possono essere inviati e ricevuti, come Bitcoin, Litecoin, Ethereum o qualsiasi altra criptovaluta. La differenza tra queste monete virtuali e una valuta standard è che i token ERC-20 sono sulla rete Ethereum

[20] (Gaschi, 2017)

e sono ospitati dagli indirizzi di Ethereum. Il solo protocollo ERC-20 non sempre è sufficiente per gli scopi di una valuta virtuale, piattaforma decentralizzata o società che utilizza criptomonete per funzionare: è soltanto uno standard per creare token basati su Ethereum.
Lo standard del token ERC-20 presenta sei parametri obbligatori più tre opzionali per ogni smart contract; facoltativamente è possibile impostare il numero massimo di decimali che un token supporta.
Le sei funzioni obbligatorie sono legate al numero e al trasferimento dei token.
Le prime due vengono utilizzate per assegnare lo stato iniziale della distribuzione dei token: 1) La funzione "totalSupply" deve essere impostata. Una volta raggiunto il massimo, non possono essere creati ulteriori token dallo smart contract. 2)La funzione "balance0f" assegna un numero iniziale di token a qualsiasi indirizzo specificato, solitamente i proprietari della ICO. Sono inoltre necessari due metodi di trasferimento per una ripartizione aggiuntiva e l'invio di token tra gli utenti 3) La funzione "transfer" sposta i token dalla fornitura totale a qualsiasi utente che acquista moneta durante la fase della ICO. 4) La funzione "transferFrom" viene utilizzata per inviare token da una persona all'altra.
Sono richieste due ulteriori funzioni per verificare le funzioni 3 e 4.
5) La funzione "approve" verifica che uno smart contract possa distribuire token, in base alla fornitura restante.
6) La funzione "allowance", infine, si assicura che un indirizzo abbia un saldo sufficiente per inviare token ad un altro indirizzo. Queste sei semplici fasi hanno permesso ai fornitori di portafogli ed exchange di creare un unico codebase, che può interagire con qualsiasi smart contract ERC-20.
Poiché ERC-20 è stata la prima implementazione su Ethereum per la creazione di nuovi token, ultimamente stanno nascendo nuovi protocolli migliorati rispetto ai bug presenti in ERC-20, come ad esempio ERC-223 che ha come tema centrale la sicurezza nel trasferimento dei token oppure ERC-777 che offre un'ampia e migliorata gamma di servizi per la gestione delle transazioni.[21] [22] [23]
Alcune criptovalute che utilizzano il protocollo ERC-20 sono ad esempio (dati dell'11 agosto 2018) TRON, decima moneta per capitalizzazione, BNB, sedicesima, OMG, ventesima.

1.4.3 Decentralized Application (dApp)

dApp invece è un acronimo per indicare un'applicazione decentralizzata (Decentralized Application) ovvero un software creato attraverso gli smart contracts nella blockchain di Ethereum. Gli sviluppatori di dApps scrivono degli insiemi di smart contracts che determinano la funziona complessiva di ogni applicazione decentralizzata.
Le dApps, che funzionano con Solidity, sono applicazioni eseguite su una rete P2P di computer anziché su un singolo computer e sono un tipo di programma software progettato per esistere solo su Internet in modo da non essere controllato da una singola entità.

[21] (Nizza, 2018)
[22] (Mulders, 2018)
[23] (Wood, 2014)

Una dApp è un sito web "blockchain enabled", in cui lo smart contract è ciò che gli consente di connettersi alla blockchain. Il modo più semplice per capire questo è analizzare come funzionano i siti web tradizionali. L'applicazione web tradizionale utilizza HTML, CSS e Javascript per il rendering di una pagina. Dovrà inoltre raccogliere i dettagli da un database che utilizza un'API. Quando vai su Facebook, la pagina chiamerà un'API per prendere i tuoi dati personali e visualizzarli sulla pagina.

Siti Web tradizionali: Front-End (cosa puoi vedere-interfaccia utente) → API → Database

Le dApps sono simili a un'applicazione web convenzionale. Il front-end utilizza la stessa identica tecnologia per il rendering della pagina. L'unica differenza fondamentale è che invece di un'API che si connette a un Database, hai uno smart contract che si connette a una blockchain.

Sito Web dApp abilitato: Front-end → Contratto intelligente → Blockchain

A differenza delle tradizionali applicazioni centralizzate, in cui il codice back-end (parte che permette il funzionamento dell'interfaccia utente) è in esecuzione su server centralizzati, le dApps hanno il loro codice back-end in esecuzione su una rete P2P decentralizzata. Le applicazioni decentralizzate consistono in tutto il pacchetto, dal back-end al front-end. Il contratto intelligente è solo una parte della dApp. Uno smart contract, d'altra parte, consiste solo nel back-end e spesso solo in una piccola parte dell'intera dApp. Ciò significa che se si desidera creare un'applicazione decentralizzata su un sistema basato su di un contratto intelligente, è necessario combinare diversi contratti intelligenti e affidarsi a sistemi di terze parti per il front-end.

Esistono 3 tipi di dApps:

1. Applicazioni di gestione del denaro: gli utenti possono effettuare transazioni tra loro su una rete blockchain, utilizzando la propria valuta intrinseca.
2. Applicazioni che integrano denaro con eventi esterni reali del mondo: ad esempio, un'azienda di logistica può utilizzare un chip localizzatore RFID per determinare se una spedizione di merci ha raggiunto un porto e solo successivamente rilasciare il pagamento per la consegna. Questo potrebbe anche essere ottenuto con disponibilità liquide sulla blockchain, senza alcun intervento umano, se sia l'acquirente che il venditore stipulano uno smart contract.
3. Organizzazioni autonome decentralizzate (DAO): organizzazioni decentralizzate e senza leader sulla blockchain. Queste si basano su regole stabilite da un codice interno che definisce quali entità possono essere componenti della DAO, come i membri possano votare, quali attività o business possano essere coinvolti e come vengano scambiati token, fondi o valori. Una volta distribuiti, le dApps operano in modo autonomo in base alle loro regole. I loro membri possono essere geograficamente dispersi ovunque.[24]

Proprio da una organizzazione autonoma decentralizzata nel 2016 si realizzò un hard fork sulla blockchain di Ethereum che fece nascere Ethereum Classic, la 14a valuta per capitalizzazione di mercato (dati del 11 agosto

[24] (Ray, What is DAPP, 2018)

2018). Questa vicenda permette di comprendere meglio il significato di hard fork e fa capire i rischi a cui si può andare incontro nel momento in cui si fa uno smart contract o una dApp che hanno bug al loro interno. Smart contract e dApp sono irreversibili: una volta creati non si può più tornare indietro.

1.4.4 The DAO ed Ethereum Classic

The DAO (così si chiamava l'organizzazione) era una organizzazione autonoma decentralizzata ossia un'organizzazione creata sulla blockchain di Ethereum (tramite una serie di smart contracts correlati) caratterizzata dal fatto di non essere formalmente definita (ossia era un'organizzazione senza una sede, senza una personalità giuridica, senza veri e propri amministratori). I creatori di The DAO per costituire tale organizzazione hanno seguito i vari passaggi che anche oggi vengono usualmente effettuati per la realizzazione di una ICO: creazione di un sito Internet per fornire informazioni, redazione di un whitepaper in cui viene descritto il progetto, audit del codice sorgente degli smart contracts utilizzati, accordi con alcuni "exchange" per permettere lo scambio dei token una volta acquisiti, etc.

Obiettivo di The DAO era quello di raccogliere capitali (tramite lo scambio di DAO Tokens a fronte di ETH) da investire su progetti che venivano previamente selezionati da un comitato e successivamente votati dai possessori di DAO Token. Questi ultimi potevano esprimere il loro voto (proporzionale al quantitativo di DAO Token posseduti) per determinare quali progetti sarebbero poi stati finanziati con i capitali. The DAO ha avuto un periodo di creazione durante il quale a chiunque è stato permesso di inviare Ether a un indirizzo di portafoglio unico in cambio di token DAO su una scala 1-100. Il periodo di creazione è stato un successo inaspettato poiché è riuscito a raccogliere una cifra pari a circa $ 150 milioni, rendendolo il più grande crowdfunding di sempre. Ad un certo punto, quando l'Ether scambiava a $ 20, il valore totale di The DAO era più di $ 250 milioni.

Si può affermare che il marketing è stato migliore dell'esecuzione, perché durante il crowdsale, diverse persone hanno espresso preoccupazione sul fatto che il codice fosse vulnerabile agli attacchi.

Una volta terminato il crowdsale (ICO), si è discusso molto riguardo ad eventuali vulnerabilità prima di iniziare a vagliare proposte da finanziare. In particolare, Stephan Tual, uno dei creatori di The DAO, ha annunciato il 12 giugno 2016 che nel software era stato trovato un "bug di recursive call" ma che "nessun fondo DAO era a rischio".

Tuttavia, il 17 giugno 2016, un hacker ha trovato un bug nel codice che gli ha permesso di drenare fondi da The DAO. Nelle prime ore dell'attacco sono stati rubati 3,6 milioni di ETH, l'equivalente di 70 milioni di dollari all'epoca. Una volta che l'hacker ha rubato il denaro, ha ritirato l'attacco.[25]

In questa circostanza, l'hacker è stato in grado di "chiedere" al contratto intelligente (di The DAO) di restituire gli Ether più volte, prima che il contratto intelligente potesse aggiornare il suo bilancio.

[25] (Nicotra, 2017)

Il furto si è verificato a causa di due motivi: il primo è che quando sono stati creati i contratti intelligenti di The DAO, i codificatori non avevano tenuto conto della possibilità di una "recursive call" e il secondo è che il contratto intelligente prima inviava gli Ether e poi aggiornava il saldo interno dei token.

È importante capire che questo bug non proviene da Ethereum stesso, ma da questa applicazione che è stata costruita su Ethereum. Il codice scritto per il DAO aveva diversi difetti e il problema di una "recursive call" era uno di questi. Un altro modo di guardare questa situazione è di paragonare Ethereum ad un sito Internet e qualsiasi applicazione basata su Ethereum ad un qualsiasi sito Web: se un sito non funziona, ciò non significa che Internet non funzioni, ma dimostra semplicemente che un sito Web ha un problema.

L'hacker ha smesso di prosciugare The DAO per ragioni sconosciute, anche se avrebbe potuto continuare a farlo. La comunità e il team di Ethereum hanno rapidamente preso il controllo della situazione e presentato molteplici proposte per affrontare il problema, anche se l'attacco aveva ormai creato un enorme danno reputazionale ad Ethereum come piattaforma di hosting e al concetto stesso di DAO.[26]

In seguito, in una lettera aperta a The DAO e alla comunità Ethereum, l'attaccante avrebbe affermato che la sua "ricompensa" era legale e minacciava di agire in giudizio contro chiunque avesse tentato di invalidare il suo "lavoro". Diversi programmatori hanno sottolineato che la firma crittografica in questo messaggio non era valida. Ma la lettera era ben scritta e, da un certo punto di vista, ben ragionata: la premessa degli smart contracts è che nulla al di fuori del codice può "cambiare le regole" della transazione.[27]

A questo punto la Fondazione Ethereum si divise in due parti: da una parte c'era chi riteneva giusto chiudere The DAO senza punire l'hacker, in quanto il suo comportamento era perfettamente legittimo; infatti era The DAO che conteneva un bug interno e l'attaccante lo aveva solamente sfruttato. Cancellato The DAO, la blockchain di Ethereum avrebbe ripreso il normale funzionamento. Dall'altra parte c'era invece Vitalik Buterin e coloro che ritenevano che il comportamento dell'hacker fosse illegittimo e volevano anche restituire il denaro rubato agli investitori truffati di The DAO.

Alla fine la decisione intrapresa fu quella di un hard fork con un upgrade delle regole della piattaforma Ethereum che impedì (o così si dice) all'hacker di ritirare la somma rubata: per raggiungere questo obiettivo venne bloccato l'account dell'attaccante e annullate le sue transazioni dalla blockchain. Nel prendere questa decisione si può tuttavia affermare che Buterin violò due condizioni base delle criptovalute: la prima è che per risolvere un problema di un protocollo interno ad Ethereum è stata presa una decisione centralizzata (da Buterin stesso) in un sistema che dovrebbe essere totalmente decentralizzato. La seconda è che è venuto meno il concetto di smart contract irreversibile e immutabile.

La decisione di Buterin è stata talmente forte e contestata che alcuni programmatori di Ethereum non l'hanno accettata e hanno dato origine ad un hard fork. Da qui nasce infatti Ethereum Classic ovvero una piattaforma esattamente uguale ad Ethereum che però possiede una moneta differente (sigla ETC per Ethereum Classic,

[26] (Falkon, 2017)
[27] (Siegel, 2016)

ETH per Ethereum) e i cui blocchi sono minati su una blockchain differente. Ovviamente i blocchi prima dell'attacco a The DAO sono identici.

Per notare questo distaccamento da Ethereum, basta andare sul sito di Ethereum Classic in cui si legge: "Ethereum Classic è una piattaforma decentralizzata che gestisce contratti intelligenti: applicazioni che funzionano esattamente come programmato senza alcuna possibilità di momenti di pausa, censura, frode o interferenza da parte di terzi. Ethereum Classic è una continuazione della blockchain originale di Ethereum - la versione classica che conserva la storia non modificata; è esente da interferenze esterne e manomissioni soggettive delle transazioni"[28] [29]

[28] (Merkle, 2016)

[29] (Beck, 2017)

1.5 Ripple

E’ un sistema di trasferimento di fondi in tempo reale (Real-Time Gross Settlement), di scambio valute e di spedizioni di denaro, fornito dall'omonima società Ripple.

A differenza di Bitcoin ed Ethereum, Ripple è una società con sede a San Francisco in California.

Ripple è il nome con cui viene identificata sia la criptovaluta, che ha come simbolo XRP, sia il protocollo di pagamento attraverso il quale la valuta viene scambiata. E’ un sistema pensato per trasferire somme di denaro (ma più in generale, qualsiasi cosa di valore) in qualsiasi valuta gratuitamente e rapidamente. I Ripple (XRP) sono la valuta universale nel sistema Ripple che, a differenza di Bitcoin, è gestita da un organo centrale e cioè la società omonima. È questa società a immettere nel mercato i Ripple (XRP), che a differenza dei bitcoin non possono essere “minati”, cioè non possono essere guadagnati dagli utenti contribuendo con i propri computer ai calcoli necessari a rendere la valuta sicura e attiva. Un'altra differenza rispetto al Bitcoin è la presenza di alcuni registri di transazioni, chiamati Ledger, che permettono di monitorare gli scambi e completare le transazioni in pochissimi secondi.

Per comprendere Ripple bisogna capire che una somma di denaro ha un valore diverso a seconda della forma in cui si trova. Una somma in contanti ha un valore differente rispetto alla stessa somma contenuta in una carta prepagata perché quest’ultima può non essere riconosciuta da tutti.

Il diverso valore dipende da dove ripongono la fiducia le persone coinvolte in una transazione economica: Ripple cerca proprio di trovare il modo più semplice per trasferire, attraverso una catena di fiducia, i soldi da una persona a un’altra.

Solo che nel suo caso non sono le persone quanto le grandi società o banche, soprattutto in Corea del Sud e in Giappone. Anche UniCredit, UBS e Santander stanno provando il sistema, perché in teoria dovrebbe semplificare il lavoro di chi deve fare milioni di trasferimenti ogni giorno tra enti e persone in tutto il mondo e in ogni valuta. A differenza delle transazioni in Bitcoin, che richiedono diversi minuti per essere approvate, quelle su Ripple sono realizzate in circa 4 secondi. L’obiettivo dichiarato di Ripple è fare per i soldi quello che Internet ha fatto per le informazioni; viene spesso fatto l’esempio delle mail negli anni Ottanta: ogni provider aveva un suo sistema e scambiarsi messaggi tra clienti di provider diversi era complicato. Ripple vuole rendere lo scambio dei soldi facile come è oggi lo scambio delle mail.

Per trasferire liquidità a livello globale, Ripple ha implementato, usando la tecnologia blockchain, tre soluzioni

1.5.1 xCurrent

xCurrent, il protocollo maggiormente collaudato, è la soluzione software aziendale di Ripple che consente alle banche di regolare immediatamente i pagamenti transfrontalieri con il monitoraggio end-to-end. Usando xCurrent, le banche si scambiano messaggi in tempo reale per confermare i dettagli del pagamento prima di iniziare la transazione e per convalidare il passaggio di denaro effettuato. Include un regolamento sviluppato in collaborazione con il comitato di RippleNet che garantisce coerenza operativa e chiarezza giuridica per ogni transazione.

xCurrent è composto dalle seguenti componenti:

Messenger è un modulo di messaggistica basato su API (Application Programming Interface) che consente la comunicazione bidirezionale tra le banche connesse a RippleNet: RippleNet è una rete di istituti di credito che inviano e ricevono pagamenti tramite la tecnologia finanziaria distribuita di Ripple; inoltre RippleNet è una rete decentralizzata basata su un accordo tra Ripple e partecipanti alla rete: tutti utilizzano la stessa tecnologia e aderiscono ad un insieme coerente di regole e standard di pagamento.

ILP Ledger è un subledger di ogni transazione iscritta nel ledger della banca. Questo componente di xCurrent è utilizzato per tracciare i crediti, i debiti e la liquidità nelle transazioni tra due controparti. ILP Ledger consente ai soggetti che effettuano transazioni di depositare fondi "atomically", il che significa che l'intera transazione o si risolve istantaneamente o non si risolve indipendentemente da quante siano le parti coinvolte. ILP Ledger è progettato per realizzare transazioni bancarie con disponibilità 24 ore su 24, 7 giorni su 7.

FX Ticker è il componente di xCurrent che facilita lo scambio tra i ledgers consentendo ai soggetti coinvolti nella transazione di registrare i tassi di cambio. Inoltre, tiene traccia del conto, valuta e credenziali di autenticazione per ciascun ILP Ledger.

Validator è un componente che conferma crittograficamente il successo o il fallimento di un pagamento. Coordina il movimento dei fondi attraverso i ledgers delle transazioni tra le parti, in modo da rimuovere tutte le possibilità di rischio e minimizzare i ritardi nel regolamento degli scambi. Il Validator fornisce l'unica prova di verità, per le controparti che effettuano transazioni, relativa al successo o al fallimento di un pagamento.

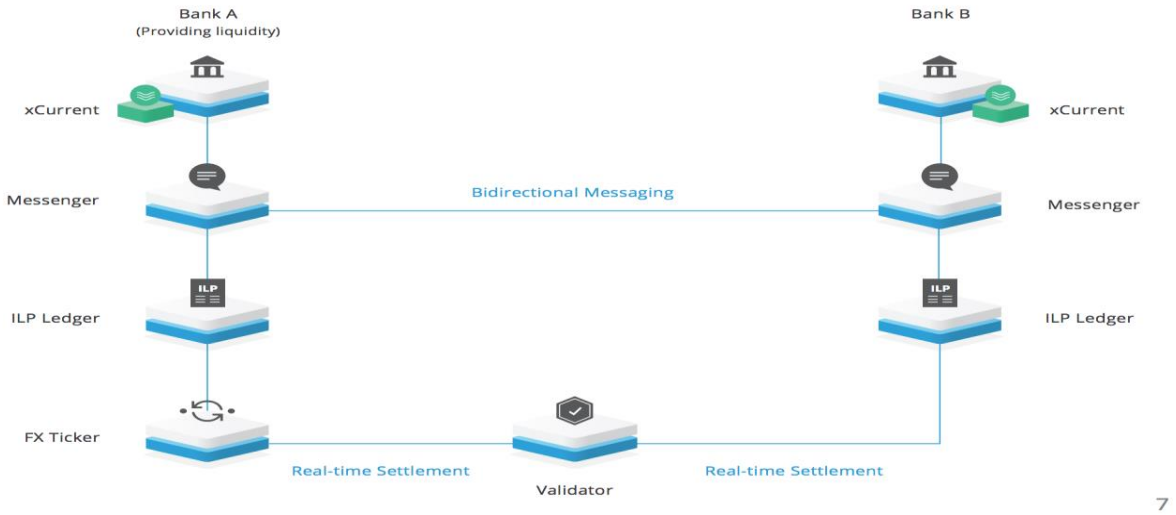

Figura 1.3 xCurrent. Fonte: Ripple.com

xCurrent dovrebbe sostituire il sistema di pagamenti SWIFT e molte banche, come ad esempio la BCE e la Fed, lo stanno sperimentando.

Il 13 agosto 2018 Il vicepresidente di American Express Colin O'Flaherty ha confermato che la società sta ufficialmente utilizzando xCurrent.

1.5.2 xRapid

xRapid è destinato ai fornitori di servizi di pagamento e ad altre istituzioni finanziarie che desiderano ridurre al minimo i costi di liquidità, migliorando al contempo la loro esperienza con i clienti.

xRapid utilizza la criptovaluta XRP per offrire liquidità on-demand, riducendo drasticamente i costi e consentendo al contempo pagamenti in tempo reale nei mercati emergenti. Costruito per uso aziendale, XRP offre alle banche ed ai fornitori di pagamento un'opzione di liquidità altamente efficiente, scalabile e affidabile per gli scambi internazionali. Infatti i pagamenti nei mercati emergenti devono essere fatti in valuta locale, il che significa che i costi di liquidità sono elevati. Il denaro verrebbe inviato nel sistema xRapid, convertito in XRP per spostarlo più velocemente, per poi essere riconvertito in qualsiasi altra valuta richiesta dalle controparti. Poiché XRP ha un tempo di transazione di quattro secondi, questa procedura sarebbe rapida e permetterebbe di ridurre il tempo di attesa del pagamento.

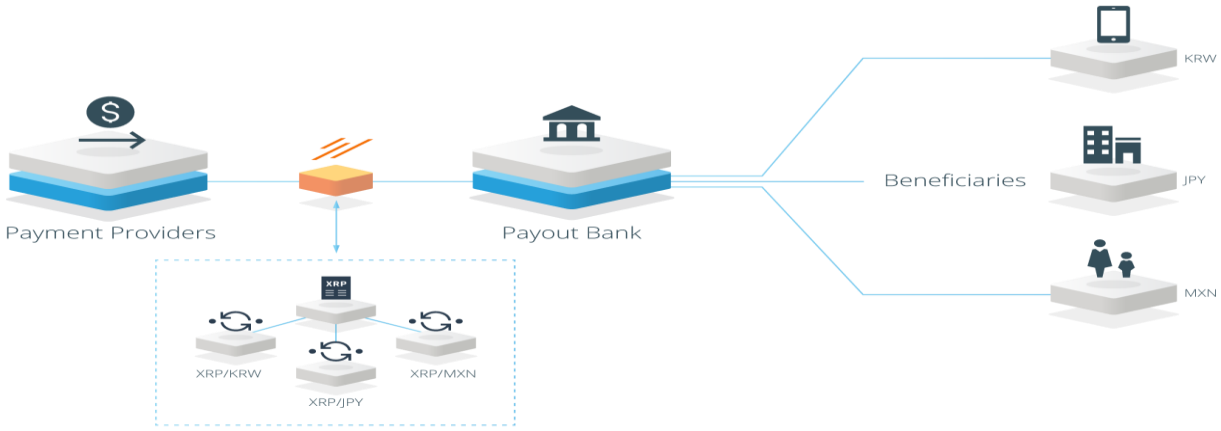

Figura 1.4 xRapid. Fonte: Ripple.com

1.5.3 xVia

xVia è destinato a società, istituti finanziari e banche che desiderano inviare pagamenti su vari network utilizzando un'interfaccia standard. La semplice API di xVia non richiede l'installazione di software e consente agli utenti di inviare pagamenti a livello globale, con trasparenza relativamente allo stato di pagamento e con informazioni dettagliate come per le fatture.

xVia consente alle istituzioni finanziarie ed alle imprese di inviare facilmente pagamenti da e verso i mercati emergenti sfruttando i vantaggi di RippleNet.

Fornendo una soluzione API standard, xVia consente alle aziende che desiderano inviare pagamenti di scalare rapidamente le loro attività, differenziare i loro servizi e soddisfare le esigenze specifiche dei loro clienti. Gli individui e le imprese possono inviare pagamenti in modo più veloce e meno costoso in qualsiasi parte del mondo.[30]

[30] (Process Payments, 2018)

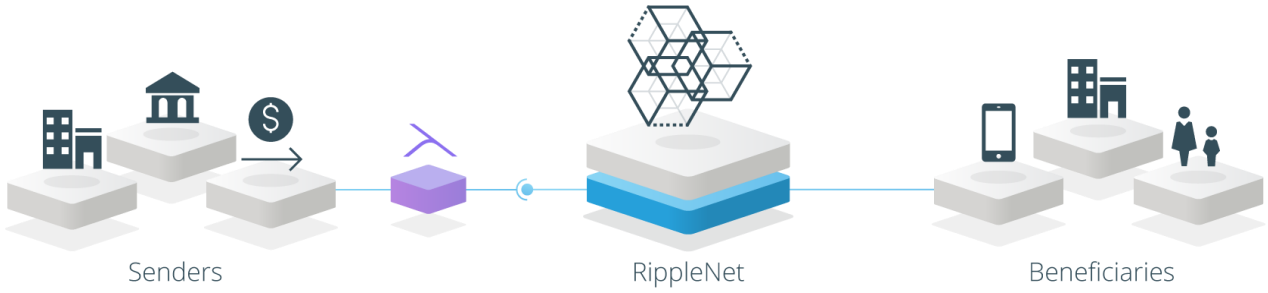

Figura 1.5 xVia. Fonte: Ripple.com

Dopo aver analizzato Ripple, vediamo alcune caratteristiche della valuta digitale che per non confondere con la società chiameremo XRP.

1.5.4 XRP Ledger

XRP Ledger è un ledger crittografico decentralizzato alimentato da una rete di server peer-to-peer. XRP Ledger è la "casa" di XRP, una moneta digitale progettata per collegare le numerose valute in uso in tutto il mondo. Ripple contribuisce allo sviluppo di XRP Ledger e promuove l'XRP come contributo chiave all'Internet of Value: un mondo in cui il denaro si muove nello stesso modo in cui si muovono le informazioni oggi.

Vediamo due caratteristiche di XRP: il mining e la protezione contro attacchi spam e DDoS.

La più grande differenza di XRP Ledger rispetto alla maggior parte delle criptovalute è che utilizza un algoritmo di consenso unico, che non richiede il tempo e l'energia del "mining", come Bitcoin, Ethereum e quasi tutti gli altri sistemi simili. Invece del "proof of work" o addirittura "proof of stake", l'algoritmo di consenso di XRP Ledger utilizza un sistema in cui ogni partecipante ha una serie di "trusted validators (validatori attendibili)" ed essi concordano in modo efficiente l'ordine con cui avvengono le transazioni.

All'inizio del 2018, la quantità di elettricità che la rete Bitcoin utilizzava per ogni transazione era superiore a quella che una famiglia negli Stati Uniti utilizzava in un giorno intero e la conferma della transazione richiedeva molto tempo. Una singola transazione XRP utilizza una quantità trascurabile di elettricità e richiede 4 o 5 secondi per essere confermata.

Invece come forma di protezione contro spam e attacchi DDoS bisogna partire dal considerare che a causa di guerre e disordini politici, l'iperinflazione è una delle principali cause di morte per le valute. Mentre il sistema decentralizzato di trusted validator fornisce a XRP una certa resistenza ai fattori politici, le regole dell'XRP Ledger forniscono una soluzione più semplice all'iperinflazione: la fornitura totale di XRP è finita. Senza un meccanismo per crearne di più, diventa molto meno probabile che l'XRP possa soffrire di iperinflazione: sono stati creati infatti 100 miliardi di XRP e non è possibile crearne di nuovi.

L'invio di transazioni nel XRP Ledger distrugge una piccola quantità di XRP. I mittenti scelgono quanto distruggerne, con determinati minimi in base al lavoro previsto per l'elaborazione della transazione e alla quantità di rete occupata.

Questa è una misura anti-spam per renderlo proibitivo da un punto di vista economico per un attacco DDoS all'XRP Ledger. Questo costo di transazione è progettato per aumentare insieme al carico sulla rete, rendendo molto costoso sovraccaricare deliberatamente o inavvertitamente il network. Ogni transazione deve specificare la quantità di XRP da distruggere per pagare il suo costo: l'attuale costo minimo richiesto dalla rete per una transazione standard è 0,00001 XRP. A volte aumenta a causa del carico più elevato rispetto al solito.

Non c'è pericolo di esaurire l'XRP in circolazione a causa delle distruzioni per le transazioni: al ritmo attuale ci vorrebbero infatti 70000 anni e comunque le condizioni del protocollo possono essere modificate.

Inoltre ogni account dell'XRP Ledger deve contenere una piccola quantità di XRP come riserva. Questa è una misura anti-spam per disincentivare chi occupa troppo spazio nel Ledger. I validatori XRP Ledger possono votare per modificare la quantità di XRP richiesta come riserva per compensare i cambiamenti nel valore reale di XRP (l'ultima volta che ciò è successo è stato a dicembre 2013, quando l'obbligo di riserva è diminuito da 50 XRP a 20 XRP). Se il requisito di riserva diminuisce, l'XRP precedentemente bloccato dalla riserva diventa nuovamente disponibile.

Ripple detiene una grande riserva di XRP in deposito. All'inizio di ogni mese, 1 miliardo di XRP viene rilasciato dal deposito in garanzia di Ripple per essere utilizzato (Ripple usa XRP per incentivare la crescita nell'ecosistema XRP Ledger e vende XRP agli investitori istituzionali). Alla fine di ogni mese, l'XRP rimanente, che la società non vende, viene conservato in deposito per un periodo di 4 anni e 8 mesi.[31]

[31] (Xrp Concepts, 2018)

1.6 Iota

E' un open source distributed ledger sviluppato per consentire la comunicazione e i pagamenti sicuri tra una rete di sistemi e prodotti progettati per connettersi e condividere le informazioni. Questo sistema prende il nome di Internet of Things (IoT). Il principio dell'IoT è di consentire agli oggetti di interagire da remoto attraverso le infrastrutture delle reti esistenti, offrendo l'opportunità di integrare il mondo fisico con quello elettronico. L'obiettivo è di migliorare l'efficienza e la precisione, fornendo allo stesso tempo i guadagni economici derivanti da una minore interazione umana. Alcuni esempi: in un piccolo paese ogni abitazione ha un impianto fotovoltaico collocato sul tetto. Gli impianti sono connessi a Internet attraverso la rete IOTA, grazie a un programma installato in ogni impianto fotovoltaico. Il software in automatico legge le produzioni di corrente ora per ora e, allo stesso tempo, conosce le esigenze di energia di ogni abitazione del paese. In automatico smista la corrente elettrica prodotta in surplus da un impianto fotovoltaico verso una abitazione che richiede più energia di quanta il suo impianto stia producendo.

IoT è un frigorifero che ordina il latte quando "si accorge" che è finito. IoT è una casa che accende i riscaldamenti appena ti sente arrivare. Questi sono esempi di IoT, ovvero di oggetti che, collegati alla rete, permettono di unire il mondo reale con quello virtuale.

Per poter operare, l'IoT ha bisogno di raccogliere e archiviare una grossa mole di dati real time (ad esempio dai sensori, dai semafori e da qualsiasi dispositivo IoT connesso), sia in azienda per migliorare sicurezza e produttività, sia in qualsiasi ambito e per qualsiasi tipo di oggetto connesso. Per questo c'è bisogno di sistemi integrati tra big data, database nosql e dati IoT.

L'Internet delle Cose è una delle nuove frontiere dell'uso della rete internet che si sta pian piano consolidando. Non più solo le persone o le "persone giuridiche", le imprese, sono riconoscibili sulla rete Internet, ma anche le cose possono esserlo: cose, oggetti, strumenti che acquisiscono intelligenza, ovvero capacità di rilevare informazioni e di comunicarle. L'Internet delle Cose è un vero e proprio Nuovo Internet proprio perché apre prospettive un tempo inimmaginabili, in cui gli oggetti assumono un ruolo attivo grazie al fatto di essere in rete e di inviare e ricevere dati sui network.

1.6.1 Il Tangle

Iota, per consentire il raggiungimento di una società basata sull'IoT, utilizza una tecnologia differente dalle altre criptovalute.

Al posto della blockchain c'è il Tangle che permette di risolvere il problema della scalabilità e dei costi associati ad ogni transazione che per esempio ha Bitcoin. Infatti una blockchain è una catena sequenziale di blocchi in cui ogni blocco fa riferimento al precedente. I blocchi contengono più transazioni e vengono aggiunti ad intervalli di tempo più o meno regolari. Nel Tangle ogni transazione (invece di un blocco di transazioni) fa riferimento a due precedenti, formando non una lista concatenata, ma una struttura web complessa, conosciuta in matematica come un Grafico Aciclico Diretto (DAG). Diretto perché tutti i nodi

puntano nella stessa direzione, aciclico perché non è possibile seguire il percorso da una qualsiasi transazione e tornare alla stessa transazione (in altre parole, nessun loop) e grafico perché i nodi e le transazioni formano un grafico di bordi e vertici. È importante sottolineare che questa struttura DAG consente di fare transazioni simultaneamente, in modo asincrono e continuo, in contrapposizione agli intervalli di tempo regolari e all'espansione lineare di una blockchain.

Ogni transazione fa riferimento a due precedenti e questa procedura può essere esemplificata in 4 parti.

Firma di input e/o costruzione di un messaggio: in IOTA ci sono due tipi di transazioni; transazioni in cui si trasferiscono token IOTA (e quindi è richiesta una firma digitale per dimostrare la proprietà degli stessi) e transazioni "a valore zero", che semplicemente trasmettono un messaggio o dei dati (e quindi una firma digitale non è strettamente necessaria).

Selezione e convalida dei suggerimenti: nel Tangle un tip è una transazione che non è stata ancora precedentemente convalidata da altre transazioni. La selezione dei tips è un processo mediante il quale due tips vengono selezionati a caso, utilizzando un algoritmo specifico ovvero il Markov Chain Monte Carlo Random Walk. Con catena di Markov si intende un modello stocastico che descrive una sequenza di eventi possibili in cui la probabilità di ciascun evento dipende solo dallo stato raggiunto nell'evento precedente. Un algoritmo Monte Carlo è un algoritmo randomizzato il cui output può essere errato con una certa probabilità (tipicamente piccola). Con Random Walk si indica un processo matematico stocastico che descrive un percorso che consiste in una successione di passaggi casuali su uno spazio matematico. Un esempio di Random Walk è il percorso tracciato da una molecola mentre viaggia in un liquido o in un gas, il prezzo di un'azione ecc..

Una volta selezionati due tips, questi devono essere convalidati, per verificare che le loro due rispettive transazioni non siano discordanti, ovvero che non vi siano fenomeni di double-spending o altre forme di imbroglio.

Proof of work: una volta che i tips sono stati selezionati e convalidati, è richiesta una piccola quantità di proof of work in cui devono essere spese alcune risorse di calcolo per trovare la risposta a un semplice puzzle crittografico.

Trasmissione: una volta completati questi 3 passaggi, le transazioni possono essere trasmesse ai nodi vicini nella rete peer-to-peer che trasmetteranno le informazioni ai loro vicini e così via, utilizzando un protocollo di trasmissione P2P standard.

Al compimento di queste 4 fasi e assumendo che la transazione sia valida, anche altre transazioni nella rete con molta probabilità verranno scelte casualmente per la convalida. Una volta che una parte significativa delle transazioni di nuova emissione (cioè i tips) farà indirettamente riferimento ad essa, la transazione potrà tranquillamente essere considerata confermata.

Un problema è rappresentato dal fatto che le nuove transazioni scelgono due tips a caso da convalidare e pertanto a volte alcune sono sfortunate e non vengono selezionate per la convalida. Questo è un comportamento negativo che si può verificare nel Tangle. Poiché l'algoritmo per la scelta dei suggerimenti favorisce i tips freschi (appena emessi), se la transazione non è stata confermata nei primi minuti, è molto

probabile che non verrà mai confermata senza l'esecuzione di una tra queste tre azioni: Rebroadcast, Reattach e Promote.

Il reabroadcasting invia di nuovo la stessa transazione a tutti i nodi vicini. È solo necessario ritrasmettere una transazione nei casi estremamente rari in cui i nodi vicini non hanno ricevuto la tua trasmissione iniziale (perché la tua connessione internet, per esempio, è stata disconnessa).

Il reattacching emette la stessa transazione originale nel Tangle, ma in una posizione diversa, trovando due nuovi tips da convalidare ed eseguendo nuovamente la proof of work.

Il promoting è un processo mediante il quale si effettuano transazioni "a valore zero" (ovvero senza trasferimento di IOTA) che direttamente (o indirettamente) fanno riferimento alla transazione. Al contrario del reattacching, non si sposta la transazione originale, ma piuttosto se ne emettono di nuove a valore zero collegate alla transazione iniziale, nel tentativo di aumentare le possibilità di essere convalidata dalla rete.

Il grande vantaggio del Tangle è la scalabilità: infatti mentre la blockchain di Bitcoin per convalidare un blocco di transazioni impiega mediamente 10 minuti, nel Tangle la convalida impiega un tempo brevissimo e questo meccanismo utilizza sempre meno tempo all'aumentare del numero degli operatori che adottano IOTA. La potenza di hashing inferiore richiesta per le transazioni sulla rete Tangle è anche un ulteriore incentivo ad utilizzare IOTA per i nuovi utenti. Ad esempio al momento il numero massimo di TPS (Transazioni per secondo) raggiunto durante uno stress test su IOTA è superiore a 800, un numero molto più alto rispetto alla grande maggioranza delle criptovalute disponibili sul mercato (Bitcoin al momento si limita a circa 7 TPS, Ethereum a 40). Tuttavia, grazie alla scalabilità infinita del Tangle, man mano che il network cresce anche il numero di TPS aumenterà di conseguenza, senza necessità di ulteriori interventi dedicati.

Poiché non ci sono minatori nel Tangle e la responsabilità della convalida è una parte intrinseca obbligatoria per effettuare ogni transazione, non ci sono transaction fees. Ciò consente micro e persino nano pagamenti feeless che l'emergente machine-to-machine sharing economy richiederà.

Nello IOTA ogni partecipante alla rete che effettua una transazione partecipa attivamente al consenso. A differenza della blockchain, dove c'è una differenza di ruolo tra i minatori e gli utenti del sistema i cui interessi sono diametralmente opposti (i minatori spesso vogliono tempi di conferma delle transazioni più lenti e commissioni più alte, mentre gli utenti vogliono l'esatto opposto), nel Tangle gli incentivi di tutti i partecipanti sono perfettamente allineati.

Tutti gli IOTA sono stati distribuiti tramite una ICO e ne esistono in totale 2 779 530 283 277 761.

Un altro aspetto che differenzia il Tangle dalla blockchain è la quantum-resistant di IOTA rispetto ad esempio a Bitcoin. E' possibile immaginare che un computer quantistico sufficientemente potente potrebbe essere molto efficiente per gestire tentativi di calcolo degli hash codes. Il processo di ricerca di un nonce per generare un blocco Bitcoin è un buon esempio di tale problema. Ma il numero di nonce che è necessario verificare per trovare un hash adatto per l'emissione di una transazione nel Tangle non è irragionevolmente grande. L'algoritmo utilizzato nell'attuale implementazione IOTA è strutturato in modo tale che il tempo per trovare un nonce non sia molto più ampio di quello necessario per altre attività finalizzate all'emissione di una

transazione. Quindi, il guadagno di efficienza anche con un computer quantistico "ideale" non sarebbe un rischio per le ipotesi di sicurezza del Tangle mentre per Bitcoin potrebbe essere potenzialmente fatale.

1.6.2 Altre caratteristiche di Iota

IOTA utilizza firme basate su codici hash al posto della crittografia a curva ellittica (ECC) come fa Bitcoin. Non solo le firme basate su hash sono molto più veloci di ECC, ma semplificano notevolmente anche il protocollo generale (firma e verifica). La funzione di hash ternaria di IOTA è chiamata Curl ed è basata sulla "costruzione spugna" che in crittografia indica una classe di algoritmi con stati interni finiti che, preso un input di qualsiasi lunghezza, producono un output della lunghezza desiderata: questa funzione piccola ed efficiente consente di soddisfare al meglio le esigenze dell'IoT.

Ultima grande innovazione portata da IOTA rispetto all'IoT fa riferimento al valore di uno stesso bene o servizio offerto in due posti diversi. Spesso infatti alcuni prodotti identici che si trovano al supermercato o alcune public utilities hanno prezzi diversi in base alla zona nella quale vengono forniti. Attraverso IOTA si riesce a superare questa condizione di disuguaglianza: quando ad un'abitazione manca un tot di Wh di energia elettrica, questo viene pagati in IOTA annullando qualsiasi differenza geografica.[32] [33] [34]

[32] (Popov, 2018)
[33] (Popov, Equilibria in the Tangle, 2018)
[34] (Iota, 2018)

1.7 Monero

E’ un sistema monetario (la cui criptovaluta viene indicata nei mercati con la sigla XMR) sicuro, privato, che utilizza una crittografia differente rispetto a Bitcoin per garantire che tutte le sue transazioni rimangano al 100% non collegabili e non rintracciabili. In un mondo in cui tutti gli scambi finanziari possono essere tracciati, si può intuire perché Monero possa diventare così desiderabile nel mercato.

1.7.1 Ring Signature, Indirizzi Stealth e Ring CT

A differenza di Bitcoin, Monero è basato sul protocollo CryptoNote. Infatti Bitcoin è un sistema completamente trasparente, in cui le persone possono vedere esattamente quanti soldi vengono inviati da un utente ad un altro. Monero nasconde queste informazioni per proteggere la privacy dell'utente in tutte le sue transazioni.

Il protocollo CryptoNote è una tecnologia Open Source che nasce nel 2013 dopo anni di sviluppo da parte di un team di matematici e programmatori. L’obiettivo del team di sviluppo è quello di offrire al mondo uno strumento decentralizzato, completamente anonimo, sicuro, egualitario e dunque senza discriminazioni tra i miners che eseguono il Proof of Work.

Per raggiungere questo obiettivo Monero utilizza tre modelli informatici differenti:

- Ring signature (firma ad anello): gli attuali sistemi di verifica delle firme digitali prevedono l’utilizzo della chiave pubblica del mittente della transazione. Questa condizione è necessaria per verificare che l’autore sia in possesso anche della relativa chiave privata univoca.

Figura 1.6 Ordinary signature Fonte: CryptoNote.org

Il meccanismo di verifica della Ring Signature invece, prevede che tutte le transazioni siano firmate a nome di un gruppo di individui. In questo modo, durante il processo di verifica, risulta praticamente impossibile risalire al mittente, in quanto tutte le firme degli appartenenti al gruppo sono fra loro indistinguibili. Il destinatario della transazione sarà l’unico in grado di riscuotere il trasferimento, sfruttando la chiave privata ed il concetto matematico di immagine associata ad essa.

Figura 1.7 Ring signature Fonte: CryptoNote.org

Perciò, nel caso in cui si abbia a che fare con una firma ad anello in cui siano presenti le chiavi pubbliche di Alice, Bob e Carol, il meccanismo di verifica può solamente decretare che uno di loro era il firmatario del messaggio, ma non è in grado di indicare chi sia tra i 3.

Questo concetto può essere utilizzato per rendere le transazioni digitali non tracciabili. Verranno poi usate le chiavi pubbliche degli altri membri per la verifica, in quanto una e solamente una di esse andrà a confermare la transazione, ovvero quella del destinatario. Questo approccio fa in modo che il creatore della transazione sia idoneo ad inviare l'importo specificato nello scambio mantenendo l'identità indistinguibile rispetto agli altri utenti, le cui chiavi pubbliche sono state utilizzate nella fase di verifica della firma ad anello.[35] [36] [37]

- Indirizzi Stealth: sono una parte importante della privacy intrinseca di Monero.

  Una delle grandi differenze tra Bitcoin e Monero è che gli indirizzi Bitcoin sono generalmente riutilizzati per molteplici transazioni. Tutti gli scambi e i dati in entrata e in uscita rimangono pubblicamente visibili attraverso l'indirizzo pubblico.

  Sebbene l'utilizzatore non abbia rivelato la propria identità, le transazioni possono essere ricondotte al singolo indirizzo: infatti attraverso l'analisi di modelli comuni e il collegamento tra le quantità di bitcoin che entrano ed escono dall'indirizzo del Wallet, è facile determinare l'identità della persona che possiede l'indirizzo.

  Differentemente la blockchain Monero non mostra l'indirizzo di destinazione di colui che riceve i token Monero, ma mostra il suo hash crittografico.

  Monero infatti utilizza 2 chiavi private e due chiavi pubbliche. Le 2 chiavi private sono una chiave di accesso privata e una chiave di spesa privata e le 2 chiavi pubbliche sono la chiave di visualizzazione pubblica e la chiave pubblica di invio.

[35] (Rivest, 2006)
[36] (Saberhagen, 2013)
[37] (Ring signature: Untraceable payments, 2018)

Figura 1.8 Chiavi Monero Fonte: Imgur.com

La chiave di spesa privata funziona come in Bitcoin: serve per firmare le transazioni. La view key privata è necessaria per cercare nella blockchain i pagamenti in entrata. Solo se hai accesso a questa chiave, puoi sapere se l'output di una transazione è associato al tuo indirizzo Monero.

Vediamo come funziona una transazione tra Alice e Bob:

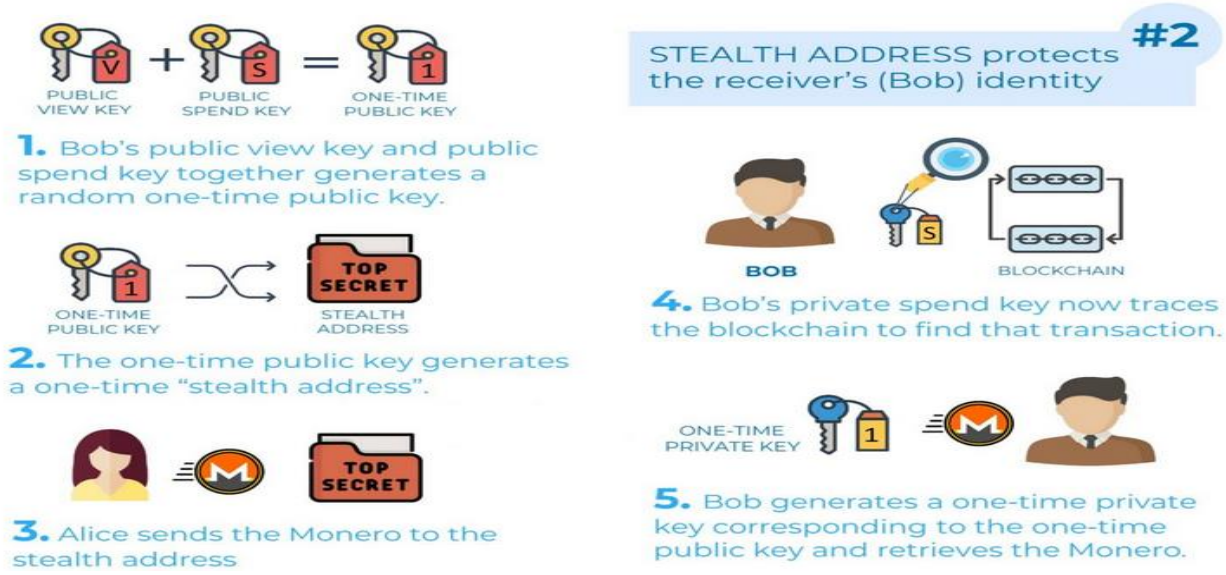

Figura 1.9 Transazioni con Monero Fonte: Imgur.com

La prima cosa è il calcolo della chiave pubblica monouso. Il calcolo di questa chiave pubblica una tantum genera un indirizzo pubblico chiamato "indirizzo stealth" nella catena di blocchi in cui Alice invia la sua somma di Monero destinata a Bob.

La chiave di spesa privata permette a Bob di scansionare la blockchain per trovare la sua transazione. Una volta trovata, Bob può calcolare una chiave privata che corrisponde alla chiave pubblica monouso e ottenere la sua somma di Monero. Quindi Alice ha pagato Bob in Monero senza che nessuno lo sapesse.[38]

- RingCT, abbreviazione di Ring Confidential Transactions, indica come gli importi delle transazioni sono nascosti in Monero.

[38] (Rosic, 2018)

Ring CT è stata implementata nel blocco n. 1220516 a gennaio 2017. Dopo settembre 2017, questa funzione è diventata obbligatoria per tutte le transazioni sulla rete.

RingCT introduce una versione migliorata della Ring Signature chiamata “A Multi-layered Linkable Spontaneous Anonymous Group Signature" che consente di mantenere nascosti gli importi delle transazioni.[39]

Ricapitolando la privacy di Monero funziona così:

- La firma ad anelli cripta l’indirizzo di invio
- RingCT nasconde l’importo della transazione
- Gli indirizzi stealth nascondono l’indirizzo di ricezione della transazione

Questi 3 fattori lavorano in armonia per creare un sistema in cui la privacy totale è garantita.

Questo non era ancora abbastanza per gli sviluppatori di Monero: avevano bisogno di un ulteriore livello di sicurezza, che è stato raggiunto grazie a Kovri.

1.7.2 Kovri

Kovri è un'implementazione C ++ della rete I2P. La rete I2P è un protocollo di routing open source che consente alle applicazioni di inviarsi messaggi in privato senza alcuna interferenza esterna. I2P permette di realizzare una rete anonima in cui scambiarsi dati e informazioni, oltre che navigare protetti da diversi livelli di crittografia. Viene, inoltre, offerto un livello di comunicazione anonimo peer-to-peer per accedere a qualsiasi servizio Internet e alle più famose applicazioni.

Per rendere anonimi i messaggi inviati, ogni client application (applicazione autonoma che funziona nel computer di ogni utilizzatore della piattaforma I2P) ha il suo "router" I2P che consente di creare alcuni "tunnel" in entrata e in uscita ovvero una sequenza di nodi che trasmettono i messaggi in una direzione (rispettivamente da e verso il client). Quando un client desidera inviare un messaggio ad un altro client, trasmette quel messaggio in uno dei suoi tunnel in uscita indirizzato a uno dei tunnel in entrata della controparte, raggiungendo infine la destinazione. Ogni partecipante alla rete sceglie la lunghezza di questi tunnel e, così facendo, effettua un compromesso tra anonimato, latenza (tempo che ci mette il messaggio per arrivare) e velocità effettiva, in base alle proprie esigenze.

La prima volta che un client vuole contattare un altro client, fa una query sul "database di rete" completamente distribuito e questo viene fatto per trovare efficientemente i tunnel in entrata dell'altro client; tuttavia i messaggi successivi tra i due soggetti coinvolti includono dei dati scambiati la prima volta, quindi non sono richieste ulteriori ricerche nel database di rete.[40] [41]

Kovri è una tecnologia gratuita, decentralizzata e anonima sviluppata da Monero. Kovri nasconde il tuo traffico Internet in modo tale che il monitoraggio passivo della rete non rivelerà che stai utilizzando Monero. Affinché

[39] (Monero, 2018)
[40] (The Invisible Internet Project (I2P), 2018)
[41] (Shahbar, 2017)

questo funzioni, tutto il traffico Monero verrà crittografato e instradato attraverso i nodi I2P, i quali sapranno che i tuoi messaggi stanno passando, ma non avranno idea di dove esattamente stiano andando e quali siano i loro contenuti.

Kovri pertanto crea un'overlay-network (una rete di computer sovrapposta ad un'altra rete, in questo caso la rete Internet) privata protetta sul Web, che offre agli utenti la possibilità di nascondere in modo efficace la loro posizione geografica e l'indirizzo IP di Internet.

Ma allora perché non usare direttamente I2P invece di Kovri? I2P è sviluppato in Java, mentre lo sviluppo di un router in C ++ aiuta il codice sorgente a essere più veloce e leggero. Inoltre l'implementazione I2P di Java contiene molte funzionalità extra che per Monero non sono necessarie.[42]

1.7.3 Altre caratteristiche di Monero

Altre caratteristiche di Monero sono le seguenti: la blockchain aggiunge un blocco mediamente ogni due minuti e non ci sono limiti di dimensione per ciascun blocco come ad esempio per Bitcoin (ogni blocco massimo un 1 MB).

Per Monero la dimensione del blocco può aumentare o diminuire nel tempo in base alla domanda. È limitata a un certo tasso di crescita per impedire che aumenti eccessivamente, cosa che sarebbe negativa per la rete. Per questi motivi, Monero gode anche di un'alta scalabilità.

Anche la blockchain di Monero utilizza il Proof of Work per convalidare i blocchi; però, a differenza di Bitcoin, il PoW è molto più semplice da risolvere tanto che può essere fatto utilizzando le normali CPU dei computer. Monero infatti utilizza l'algoritmo CryptoNight Proof of Work (PoW), progettato per l'utilizzo in CPU e GPU ordinarie. Questo consente il mining da parte del processore del computer dell'utente, lontano dalla centralizzazione di fatto di mining pools di dimensioni elevate come in Bitcoin, perseguendo la visione originale di Satoshi Nakamoto di una vera valuta P2P.

Un'altra caratteristica di Monero è la fungibilità. Le unità di Monero non possono essere inserite nella blacklist dai venditori o dagli exchange a causa della loro associazione in transazioni illecite precedenti. Fungibilità significa che due unità di una valuta possono essere liberamente sostituite e la valuta sostituita è uguale ad ogni altra unità della stessa dimensione. L'oro è probabilmente l'esempio più adeguato di vera fungibilità, dove ogni oncia di oro dello stesso grado vale lo stesso di ogni altra oncia.

Monero è fungibile a causa della sua natura che non permette in alcun modo di collegare le transazioni o di tracciare la cronologia di un particolare Monero. La fungibilità è un vantaggio che esso ha rispetto a Bitcoin ed a quasi tutte le altre criptovalute, a causa della privacy che caratterizza la blockchain Monero rispetto alla natura permanentemente tracciabile della blockchain Bitcoin.

[42] (Kovri, 2018)

Il Bitcoin può essere rintracciato da chiunque: pertanto, se una moneta è stata utilizzata per scopi illegali in passato, questa macchia sarà contenuta nella blockchain in perpetuo. Questa mancanza di fungibilità comporta che alcune aziende evitano di accettare bitcoin che sono stati precedentemente utilizzati per scopi illegali.[43]

[43] (Monero, 2018)

Capitolo 2 – Analisi finanziaria delle criptovalute

In questo capitolo verranno esaminati gli aspetti legati ai mercati finanziari.

In particolare viene suddiviso in quattro differenti analisi:

1. Analisi del rendimento di alcune criptovalute confrontato con quello di indici di mercato, commodities e currencies
2. Analisi delle tre maggiori criptovalute per capitalizzazione di mercato rispetto al mercato azionario, obbligazionario e immobiliare
3. Analisi della correlazione tra criptovalute e tra criptovalute e alcuni indici di mercato
4. Analisi delle criptovalute come strumento di hedging o diversificazione nel portafoglio di un investitore

2.1 Confronto tra il rendimento delle criptovalute e indici di mercato, commodities e currencies

Inizialmente si esamina l'andamento di cinque criptovalute (Bitcoin, Ethereum, Ripple, Litecoin e Monero) confrontato con quello dello S&P 500.

Figura 2.1 Grafico su scala logaritmica dei tassi di crescita Fonte: Cryptocurrencies, Mainstream Asset Classes and Risk Factors – A Study of Connectedness

La Figura 2.1 *Grafico su scala logaritmica dei tassi di crescita* rappresenta i tassi di crescita calcolati su scala logaritmica delle cinque monete digitali menzionate sopra, rispetto all'indice S&P 500. Nonostante l'indice S&P 500 sia cresciuto di oltre il 30% durante il periodo compreso tra agosto 2015 e aprile 2018, la crescita dei prezzi delle criptovalute è stata nettamente superiore. Il picco di crescita è stato raggiunto dalla moneta

che tutela maggiormente la privacy - Monero (XMR) - alla fine del 2017. Infatti, nel periodo tra il luglio 2015 e il dicembre 2017 tutte le cinque criptomonete hanno mostrato rendimenti compresi tra il 400% e il 600%. Sebbene gli ultimi quattro mesi del periodo campione abbiano registrato un calo significativo dei prezzi delle monete digitali, la crescita nel periodo considerato è dieci volte superiore rispetto all'indice S&P 500.

La Figura 2.2 *Analisi rendimenti giornalieri dal 7 Agosto 2015 al 13 Aprile 2018* fornisce statistiche riassuntive dei rendimenti giornalieri di tredici variabili.

	Mean	Std.	Min	Median	Max	JB Stat.	Mean/Std.
BTC	0.50	4.76	-24.59	0.43	22.76	526.42	0.10
ETH	0.76	9.80	-91.63	0.13	49.76	5482.23	0.08
LTC	0.51	7.04	-31.25	0.00	55.16	6422.02	0.07
XMR	0.82	10.71	-51.08	0.00	75.05	2526.89	0.08
XRP	0.65	10.10	-56.33	-0.28	74.08	3250.14	0.06
SP500	0.04	0.85	-4.18	0.05	3.84	537.89	0.05
10YR	-0.01	0.36	-1.89	0.01	1.46	59.28	-0.02
WTI	0.06	2.43	-8.08	0.10	11.29	149.85	0.03
GOLD	0.03	0.86	-3.38	0.02	4.59	259.10	0.04
USD	-0.01	0.42	-2.40	0.00	2.49	355.51	-0.03
SPGSCI	0.04	1.26	-4.49	0.06	5.26	46.22	0.03
TED	0.13	6.71	-34.17	0.00	27.87	206.14	0.02
GPR	0.27	70.17	-268.40	-0.26	313.81	54.39	0.00

Figura 2.2 Analisi rendimenti giornalieri dal 7 Agosto 2015 al 13 Aprile 2018 Fonte: Cryptocurrencies, Mainstream Asset Classes and Risk Factors – A Study of Connectedness

Le prime cinque sono le monete virtuali, la sesta (SP500) è lo S&P 500, la settima (10YR) è un indice che racchiude i titoli di stato decennali americani, l'ottava (WTI) è il petrolio, la nona (GOLD) è l'oro, la decima (USD) è il dollaro, l'undicesima (SPGSCI) è un indice delle commodities, la dodicesima è lo spread TED (TED) ovvero la differenza tra il tasso LIBOR e il debito pubblico degli Stati Uniti privo di rischio a breve termine e la tredicesima (GRP) è il l'indice di rischio geopolitico.

Come visto, Monero (XMR) ha il rendimento medio giornaliero più alto (0,82%), seguito da Ethereum (ETH) allo 0,76%.

Il miglior rendimento corretto per il rischio è raggiunto da Bitcoin (BTC), seguito da Ethereum (ETH) e Monero (XMR), mentre le rimanenti criptovalute arrivano al quarto (Litecoin LTC) e quinto (Ripple XRP) posto.

Tra gli asset, il petrolio (WTI) ha il rendimento medio più elevato (0,06%), seguito dallo S&P 500 e dall'indice delle materie prime SPGCSI con rendimenti giornalieri medi dello 0,04%.

Le risorse digitali presentano rendimenti minimi e massimi estremamente variabili, come raffigurato dalle colonne Min e Max.

Tutti i tredici indici studiati falliscono il test di Jarque-Bera, ovvero un test per la verifica dell'ipotesi di normalità, basato su asimmetria e curtosi di una distribuzione.

Ultimo aspetto rilevante è l'indice di rischio geopolitico (GPR), il quale presenta la massima deviazione standard e i cambiamenti minimi e massimi giornalieri maggiormente variabili: ciò riflette la natura sporadica e imprevedibile degli incidenti geopolitici.[44]

2.2 Confronto tra Bitcoin, Ethereum e Ripple e il mercato azionario, obbligazionario e immobiliare

A questo punto l'analisi viene limitata alle tre maggiori criptovalute per capitalizzazione di mercato (Bitcoin, Ethereum e Ripple) e si procede a confrontarle con il mercato azionario, obbligazionario e immobiliare.

Per Bitcoin, si utilizzano i dati dall'01/01/2011 al 31/05/2018 perché negli anni precedenti non c'erano molti scambi né molta liquidità. I dati per Ripple vanno dall'8/04/2013 al 31/05/2018 e per Ethereum vanno dall'8/07/2015 al 31/05/2018.

Panel A							
Daily	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Bitcoin	0.52%	5.55%	4.88	0.09	0.80	15.21	53.69
Stock	0.05%	0.94%	2.44	0.06	-0.51	7.95	54.91
Stock*	0.04%	1.06%	6.10	0.03	-0.13	19.72	55.07
Weekly	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Bitcoin	3.79%	16.64%	4.49	0.23	1.76	10.25	58.72
Stock	0.26%	1.93%	2.59	0.13	-0.38	5.17	59.95
Stock*	0.21%	2.45%	6.02	0.06	-0.27	10.14	58.40
Monthly	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Bitcoin	21.60%	69.46%	2.95	0.31	4.32	25.38	60.00
Stock	1.08%	3.24%	3.12	0.33	-0.10	3.78	68.89
Stock*	0.91%	4.27%	5.36	0.12	-0.51	5.02	62.16
Bond	0.95%	3.00%	2.18	0.32	-0.10	2.73	64.58
Housing	0.40%	0.72%	5.15	0.55	-0.01	3.17	73.56
Note: Stock* shows results for the whole sample between 1953/07 and 2018/04.							

Figura 2.3 Comparazione rendimento Bitcoin con il mercato azionario, obbligazionario e immobiliare. Fonte: Risks and Returns of Cryptocurrency

Per Bitcoin sia il rendimento sia la volatilità sono molto alti.

Su base giornaliera, il rendimento medio è dello 0,52% e la deviazione standard è del 5,55%; su base settimanale, il rendimento medio è del 3,79% e la deviazione standard è del 16,64%; su base mensile, il rendimento medio è del 21,60% e la deviazione standard è del 69,46%. Sia i rendimenti che le deviazioni standard sono di un ordine di grandezza superiore rispetto a quelli delle classi di asset tradizionali.

[44] (Milunovich, 2018)

Lo Sharpe ratio dei rendimenti Bitcoin è 0,09 su base giornaliera, 0,23 su base settimanale e 0,31 su base mensile. Su base mensile, lo Sharpe ratio è simile a quello delle azioni per il periodo di tempo comparabile, mentre è superiore allo Sharpe ratio per le azioni studiate dal 1953 al 2018. Su base giornaliera e settimanale, gli Sharpe ratio sono circa il 50% e il 75% più alti di quelli delle azioni a parità di periodi temporali analizzati.

Panel A: Return Summary							
			Ripple Returns				
	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Daily	0.59%	9.11%	2.74	0.06	6.11	99.05	46.09
Weekly	6.26%	47.39%	2.11	0.13	7.62	76.26	46.27
Monthly	36.20%	143.31%	1.94	0.25	3.82	18.69	40.68
			Same Period Bitcoin Returns				
	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Daily	0.34%	4.47%	3.17	0.08	0.54	13.08	54.58
Weekly	2.42%	12.68%	3.04	0.19	0.88	5.72	56.86
Monthly	14.93%	64.87%	1.77	0.23	5.88	41.58	55.93

Figura 2.4 Rendimenti Ripple Fonte: Risks and Returns of Cryptocurrency

Per quanto riguarda Ripple, lo Sharpe ratio è 0,06 su base giornaliera, 0,13 su base settimanale e 0,25 su base mensile. Il rendimento di Ripple ha una media e una deviazione standard notevolmente più alta rispetto al rendimento di Bitcoin nel periodo considerato. Tuttavia, lo Sharpe ratio di Ripple è simile a quello di Bitcoin.

Panel A: Returns Summary Statistics							
			Ethereum Returns				
	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Daily	0.81%	7.71%	3.41	0.11	0.24	15.71	49.33
Weekly	6.88%	24.51%	3.43	0.28	1.71	7.24	54.00
Monthly	30.26%	67.56%	2.65	0.53	1.24	3.95	54.29
			Same Period Bitcoin Return				
	Mean	SD	T-Statistics	Sharpe	Skewness	Kurtosis	% Return >0
Daily	0.38%	4.07%	3.04	0.09	0.19	7.54	56.88
Weekly	2.84%	11.80%	2.94	0.24	0.26	4.05	62.00
Monthly	12.05%	25.10%	2.84	0.48	0.51	2.88	65.71

Figura 2.5 Rendimenti Ethereum Fonte: Risks and Returns of Cryptocurrency

Per Ethereum, lo Sharpe ratio è 0,11 su base giornaliera, 0,28 su base settimanale e 0,53 su base mensile. Anche il rendimento di Ethereum ha una media e una deviazione standard più alta rispetto a Bitcoin durante lo stesso periodo, ma lo Sharpe ratio del rendimento di Ethereum è simile a quello di Bitcoin.

Il rendimento di Bitcoin ha l'indice di asimmetria positivo, differentemente da quello dei rendimenti azionari, obbligazionari e immobiliari. L'asimmetria aumenta da 0,80 su base giornaliera a 1,76 su base settimanale e a 4,3 su base mensile.

La curtosi è 15.21 su base giornaliera, 10.25 su base settimanale e 25.38 su base mensile. Bitcoin ha alte probabilità di rendimento giornaliero positivo e negativo particolarmente elevato. Ad esempio, la probabilità di un rendimento giornaliero del -20% è quasi dello 0,5%; la probabilità di un rendimento giornaliero del +20% è quasi dell'1%. I rendimenti di Ripple ed Ethereum hanno caratteristiche simili, ovvero hanno un indice di asimmetria positiva su tutte le frequenze, un'alta curtosi e alte probabilità di rendimenti giornalieri negativi e positivi eccezionali.

La Figura 2.6 *Rendimenti Bitcoin, Ethereum e Ripple nei vari giorni della settimana* mostra la media, la deviazione standard e gli Sharpe ratio dei rendimenti nei vari giorni della settimana.

Bitcoin	Mean	SD	T-Statistics	Sharpe	Ripple	Mean	SD	T-Statistics	Sharpe
Monday	0.67%	5.48%	2.43	0.12	Monday	0.05%	7.70%	0.11	0.01
Tuesday	1.01%	6.09%	3.25	0.17	Tuesday	0.75%	9.04%	1.32	0.08
Wednesday	0.46%	5.62%	1.62	0.08	Wednesday	0.45%	6.86%	1.03	0.06
Thursday	0.66%	5.95%	2.18	0.11	Thursday	1.45%	10.90%	2.13	0.13
Friday	0.32%	5.71%	1.09	0.06	Friday	0.97%	7.71%	2.01	0.13
Saturday	0.33%	5.32%	1.24	0.06	Saturday	-0.14%	7.32%	-0.29	-0.02
Sunday	0.18%	4.52%	0.80	0.04	Sunday	0.61%	12.72%	0.76	0.05
Ethereum	Mean	SD	T-Statistics	Sharpe	Stock	Mean	SD	T-Statistics	Sharpe
Monday	0.38%	7.39%	0.62	0.05	Monday	-0.03%	1.00%	-0.47	-0.03
Tuesday	1.53%	8.86%	2.11	0.17	Tuesday	0.12%	0.90%	2.55	0.13
Wednesday	0.86%	6.83%	1.53	0.13	Wednesday	0.04%	0.93%	0.94	0.05
Thursday	1.72%	8.72%	2.41	0.20	Thursday	0.06%	0.97%	1.23	0.06
Friday	0.21%	6.75%	0.39	0.03	Friday	0.06%	0.88%	1.31	0.07
Saturday	0.26%	8.83%	0.36	0.03					
Sunday	0.74%	6.15%	1.47	0.12					

Figura 2.6 Rendimenti Bitcoin, Ethereum e Ripple nei vari giorni della settimana Fonte: Risks and Returns of Cryptocurrency

A differenza delle azioni, non esiste un Monday effect. Tuttavia, i rendimenti sono più bassi il sabato: Bitcoin: 0,33% con lo Sharpe ratio dello 0,06% rispetto allo 0,52% della media giornaliera con lo Sharpe ratio dello 0,09%. Ripple: -0,14% con lo Sharpe ratio del -0,02% rispetto allo 0,59% di media giornaliera con lo Sharpe ratio dello 0,06%. Ethereum: 0,26% di rendimento con lo Sharpe ratio dello 0,03% rispetto allo 0,81% come media giornaliera e uno Sharpe ratio dello 0,03%.

Inoltre, mentre i rendimenti di Bitcoin sono leggermente inferiori anche di domenica, i rendimenti di sabato sono costantemente inferiori per tutte e tre le criptovalute.[45]

[45] (Liu, 2018)

2.3 La correlazione e le criptovalute

Un aspetto particolarmente interessante riguarda la correlazione tra le criptomonete. La maggior parte di esse sono correlate positivamente e le correlazioni aumentano quando il periodo di analisi diventa più ampio. In aggiunta le correlazioni tra grandi criptovalute per capitalizzazione di mercato sono maggiori rispetto alle correlazioni tra le monete con capitalizzazione di mercato minore. Quindi si può affermare che la maggior parte delle criptovalute si muove insieme e questo avviene particolarmente per quelle a maggiore capitalizzazione.

Per scoprire come si sviluppano nel tempo le correlazioni tra le criptovalute, eseguiamo una "rolling analysis" come mostrato nella Figura 2.7 *Correlazione tra le criptovalute*

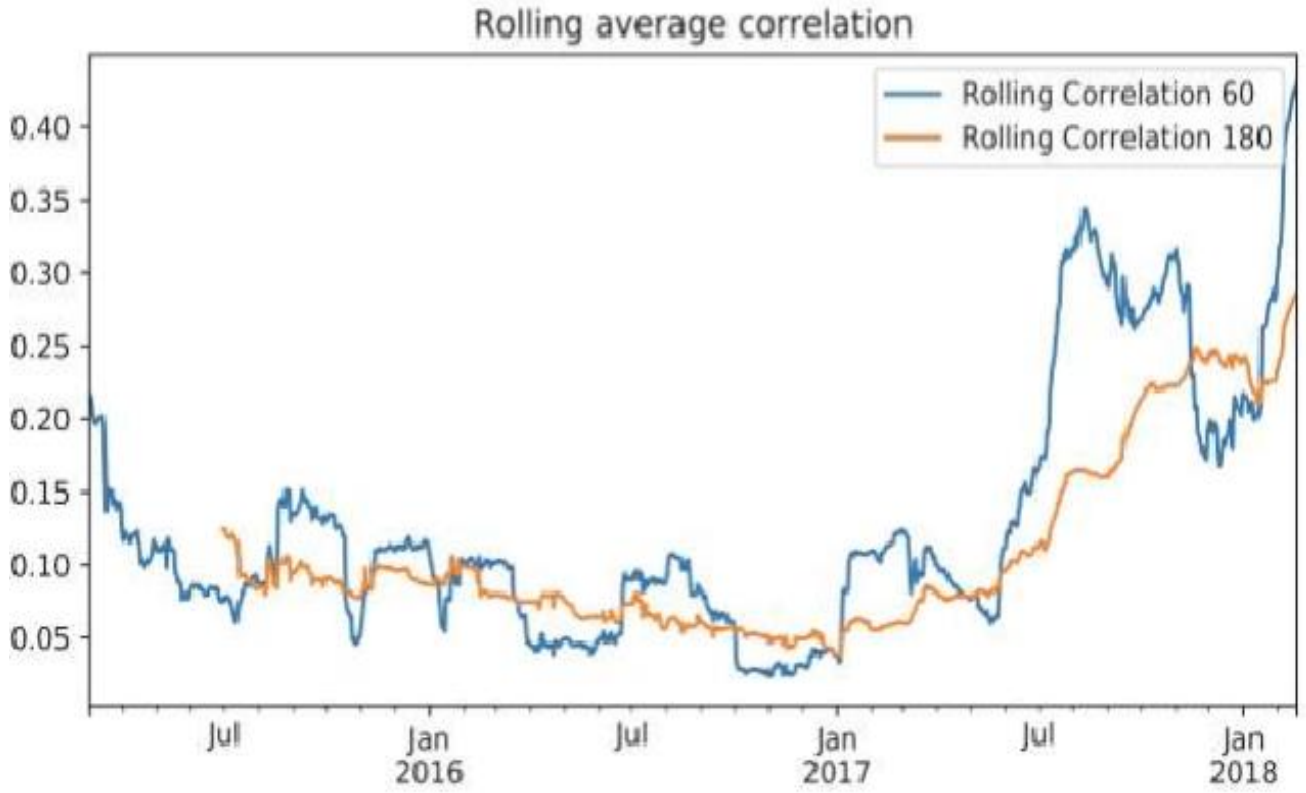

Figura 2.7 Correlazione tra le criptovalute Fonte: Crypto-Currency Investing Examined

Ogni giorno si calcolino le correlazioni basate sui rendimenti giornalieri degli ultimi 60 e 180 giorni, e si utilizzi la media aritmetica come correlazione media per quel giorno. Il grafico rappresenta il livello di correlazione del mercato delle monete virtuali negli ultimi 60 e 180 giorni. Una scoperta interessante è il picco di correlazione del mercato nella seconda metà del 2017, che è stato accompagnato dall'aumento di valore delle criptovalute.

Si analizzi la correlazione di Bitcoin rispetto alle altre 99 maggior monete virtuali per capitalizzazione di mercato: le statistiche della sua correlazione sono raffigurate nella Figura 2.8 *Correlazione tra Bitcoin e le altre 99 maggiori valute per capitalizzazione di mercato in un intervallo di tempo che va da gennaio 2015 a febbraio 2018.*

	Mean	Standard deviation	Minimum	Median	Maximum
Daily	0.2211	0.1158	-0.0140	0.2225	0.5035
Weekly	0.1897	0.1382	-0.1135	0.1962	0.4976

Figura 2.8 Correlazione tra Bitcoin e le altre 99 maggiori valute per capitalizzazione di mercato in un intervallo di tempo che va da gennaio 2015 a febbraio 2018 Fonte: Crypto-Currency Investing Examined

In media, Bitcoin ha una correlazione dei rendimenti di prezzo (giornaliera e settimanale) di circa 0,20 con le altre criptovalute.

La Figura 2.9 *Criptovalute più e meno correlate rispetto a Bitcoin* invece elenca quali sono le criptovalute più correlate e quelle meno correlate con Bitcoin, considerando il periodo di analisi che va da gennaio 2015 a febbraio 2018.

	Daily returns		Weekly returns	
	Symbol	Correlation	Symbol	Correlation
Most correlated	PPC	0.5035	SBD	0.4976
	LTC	0.5006	LTC	0.4706
	DOGE	0.4740	GOLOS	0.4463
	NMC	0.4678	EMC2	0.4315
	WAVES	0.4401	NMC	0.4281
Least correlated	PASC	-0.0140	ZOI	-0.1135
	PURA	0.0029	GAME	-0.0991
	NYC	0.0244	PIVX	-0.0915
	MOON	0.0248	EMC	-0.0829
	EXP	0.0306	CRW	-0.0681

Figura 2.9 Criptovalute più e meno correlate rispetto a Bitcoin Fonte: Crypto-Currency Investing Examined

E' possibile notare come, oltre alle criptovalute a maggiore capitalizzazione di mercato, le criptomonete che sono fortemente correlate con Bitcoin sono quelle che presentano una tecnologia simile; viceversa, quelle che hanno minore correlazione, utilizzano protocolli differenti.

Alcuni esempi: Litecoin (LTC), presente come valuta particolarmente correlata con Bitcoin sia su base giornaliera che su base settimanale, ha caratteristiche affini rispetto al Bitcoin da cui si differenzia

principalmente per la velocità di aggiunta di ogni blocco alla blockchain (per Litecoin è di 2,5 minuti), per la differente funzione del Proof of Work e per il numero di criptomonete, quattro volte maggiore rispetto a Bitcoin.

Namecoin (NMC), anche essa presente in ambedue le classificazioni della Figura 18, è la prima valuta digitale ad avere imitato il codice Bitcoin e le sue principali caratteristiche, tra cui il numero totale di monete: 21 milioni.

Dogecoin (DOGE) ha proprietà simili rispetto a Bitcoin e Litecoin, a parte la velocità di mining di ogni blocco che si assesta sul minuto di media.

Differentemente le criptovalute che presentano minore correlazione hanno tecnologie diverse rispetto a Bitcoin: PascalCoin (PASC) è una criptovaluta fortemente innovativa che permette di realizzare circa 72000 transazioni al secondo e contratti intelligenti sotto forma di protocolli Layer-2 (si usa per il collegamento dei dati), grazie ad una nuova struttura dati crittografica nota come SafeBox.

Zoin (ZOI) è una criptovaluta basata sul protocollo Zerocoin che fornisce il completo anonimato sui fondi. Utilizza l'algoritmo "lyra2zoin" ed è gestita da un sistema di voto in cui le decisioni non sono prese da un piccolo gruppo di sviluppatori, ma dalla sua comunità.

PIVX (PIVX) è la prima moneta che utilizza Proof of Stake con il protocollo zerocoin (chiamato zPIV) e zerocoin staking (denominato zPOS); un algoritmo Proof of Stake completamente nuovo che offre privacy senza precedenti, velocità delle transazioni e bassi costi di transazione.

PIVX impiega una rete decentralizzata di secondo livello che fornisce servizi aggiuntivi come la governance del voto della comunità, il sistema di tesoreria autofinanziato e le transazioni istantanee.

Si esamini anche l'autocorrelazione di Bitcoin mostrata dalla Figura 2.10 *Autocorrelazione Bitcoin*.

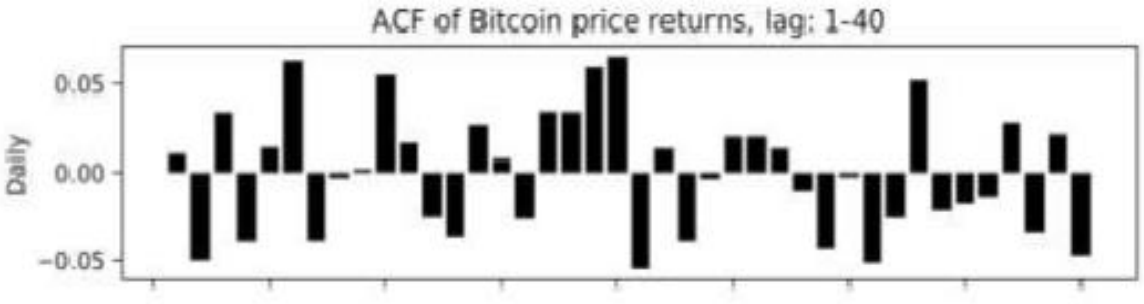

Figura 2.10 Autocorrelazione Bitcoin Fonte: Crypto-Currency Investing Examined

Le autocorrelazioni per i ritorni giornalieri di Bitcoin sono comprese tra -0,05 e 0,05; questo risultato dimostra una bassa autocorrelazione.

Dopo aver analizzato la correlazione tra le criptovalute, si analizzi la correlazione tra le stesse ed alcuni indici di mercato, in modo da condurre un'analisi sull'utilizzo delle monete virtuali nel portafoglio degli investitori come strumento di diversificazione.

Si analizzi la relazione cross-market tra le prime 100 criptovalute (VW) e le risorse tradizionali. In particolare si consideri: ● Indice S&P 500 (SP500) ● Indice MSCI World (MSCI): è un indice azionario ponderato free-float che racchiude gli scambi di titoli nei mercati sviluppati. ● Indice MSCI Emerging Markets (Indice Emg): è un indice azionario ponderato free-float che racchiude titoli azionari a media e alta capitalizzazione nei mercati emergenti. ● Indice Dollaro USA (USD): una misura del valore del dollaro statunitense rispetto al valore di un paniere di valute scelte tra i maggiori partner commerciali degli Stati Uniti. ● Prezzo a pronti dell'oro in dollari (GOLD) ● Indice Bloomberg Commodity (Commo): è un indice che riflette il movimento dei prezzi futuri sulle materie prime. ● Indice VIX (VIX): misura della volatilità implicita nelle opzioni dell'indice S&P 500.

	BTC	VW	SP500	MSCI	Emg	USD	Gold	Commo	VIX
BTC	1.0000	0.9416	0.0441	0.0232	-0.0212	0.0134	0.0419	0.0351	-0.0921
VW	0.9416	1.0000	0.0538	0.0316	-0.0204	-0.0049	0.0526	0.0359	-0.0975
SP500	0.0441	0.0538	1.0000	0.9093	0.4480	0.0831	-0.1674	0.2967	-0.7880
MSCI	0.0232	0.0316	0.9093	1.0000	0.6587	-0.0413	-0.1262	0.3836	-0.7283
Emg	-0.0212	-0.0204	0.4480	0.6587	1.0000	-0.0426	-0.0053	0.3641	-0.3848
USD	0.0134	-0.0049	0.0831	-0.0413	-0.0426	1.0000	-0.4070	-0.2427	-0.0828
Gold	0.0419	0.0526	-0.1674	-0.1262	-0.0053	-0.4070	1.0000	0.2441	0.1365
Commo	0.0351	0.0359	0.2967	0.3836	0.3641	-0.2427	0.2441	1.0000	-0.2224
VIX	-0.0921	-0.0975	-0.7880	-0.7283	-0.3848	-0.0828	0.1365	-0.2224	1.0000

Figura 2.11 Correlazione tra criptovalute e asset tradizionali Fonte: Crypto-Currency Investing Examined

La Figura 2.11 *Correlazione tra criptovalute e asset tradizionali* presenta le correlazioni tra Bitcoin, altre criptovalute e risorse tradizionali, calcolate in termini di rendimenti giornalieri. Bitcoin è a malapena correlato con qualsiasi risorsa tradizionale (correlazioni assolute <0,1). Mostra una correlazione leggermente positiva con S&P 500, MSCI, USD, Oro e Commo, mentre dimostra una correlazione negativa con Emg e VIX.
La bassa correlazione fa emergere la possibilità di utilizzare il Bitcoin e gli altcoin come efficiente strumento di diversificazione di portafoglio, aspetto che verrà ulteriormente approfondito nella successiva analisi.[46]

[46] (Liew, 2018)

2.4 Bitcoin, Litecoin e Ripple come strumento di copertura o diversificazione nel portafoglio di un investitore

Lo studio verrà condotto su tre criptovalute (Bitcoin, Litecoin e Ripple) per verificare la possibilità di utilizzare le stesse come strumento di copertura o diversificazione all'interno di un portafoglio. I risultati, analizzati nell'arco temporale che va dal 5/8/2013 al 8/1/2018, sono esposti nella Figura 2.12 *Utilizzo delle criptovalute come strumento di copertura per un portafoglio*

Table III: Estimation results of hedging capability of cryptocurrencies using a DCC model

This table shows the results of the regression analysis of the equation: $DCC_t = h_0 + h_{1i}D(r_{other\ asset,t(q10)}) + h_{2i}D(r_{other\ asset,t(q5)}) + h_{3i}D(r_{other\ asset,t(q1)}) + v_t$. h_0 is a coefficient that indicates whether cryptocurrencies is a hedge (statistically negative or zero) or a diversifier (statistically slightly positive). h_{1i}, h_{2i}, h_{3i} are coefficients to check whether cryptocurrencies can be used as safe haven during 10%, 5%, and 1% lower quantile of the return of asset i respectively. If the value is statistically negative or zero, it means the cryptocurrency under study is a safe haven for the particular asset i, otherwise it is not.

COEFFICIENTS	Stocks (S&P500)			Bond (Merrill Lynch World Sovereign Bond Index)			Gold (London Bullion Market $US/Troy Ounce)			h_0 Constant
	h_{11} (10% quantile)	h_{21} (5% quantile)	h_{31} (1% quantile)	h_{12} (10% quantile)	h_{22} (5% quantile)	h_{32} (1% quantile)	h_{13} (10% quantile)	h_{23} (5% quantile)	h_{33} (1% quantile)	
Panel A: Bitcoin (BTC)										
Stocks	0.003	0.001	-0.048*							-0.013***
	(0.010)	(0.015)	(0.025)							(0.002)
Bond				-0.002	0.014	0.009				-0.002
				(0.010)	(0.014)	(0.023)				(0.002)
Gold							0.017*	-0.020	0.024	-0.004*
							(0.010)	(0.014)	(0.023)	(0.002)
Panel B: Litecoin (LTC)										
Stocks	0.011	-0.012	-0.03							-0.001
	(0.012)	(0.017)	(0.029)							(0.003)
Bond				0.009	0.004	-0.02				-0.009***
				(0.009)	(0.014)	(0.023)				(0.002)
Gold							0.007	-0.018	0.046*	-0.041***
							(0.010)	(0.015)	(0.024)	(0.002)
Panel C: Ripple (XRP)										
Stocks	-0.015	0.061***	-0.024							0.006*
	(0.015)	(0.021)	(0.035)							(0.003)
Bond				0.007	0.011	0.004				0.028***
				(0.01)	(0.015)	(0.024)				(0.002)
Gold							-0.001	0.011	0.009	0.009***
							(0.01)	(0.015)	(0.025)	(0.002)

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Figura 2.12 Utilizzo delle criptovalute come strumento di copertura per un portafoglio Fonte: Cryptocurrency: A new investment opportunity? An investigation of the hedging capability of cryptocurrencies and their influence on stock, bond and gold portfolios

Si utilizzi il modello DCC (Dynamic Conditional Correlation) in grado di catturare le correlazioni che variano nel tempo attraverso i rendimenti delle classi di asset con pochi errori di stima ed errori computazionali.
La formula DCC è la seguente:

$$DCC_t = h_0 + h_{1i}D(r_{other\ asset,t(q10)}) + h_{2i}D(r_{other\ asset,t(q5)}) + h_{3i}D(r_{other\ asset,t(q1)}) + v_t$$

Equazione 2.1 Dynamic Conditional Correlation Fonte: Cryptocurrency: A new investment opportunity? An investigation of the hedging capability of cryptocurrencies and their influence on stock, bond and gold portfolios

$DCCt$ è la correlazione condizionale bivariata tra ciascuna criptovaluta e gli altri asset oggetto di studio; $rother\ asset$ è il rendimento giornaliero di ciascuno degli altri asset; D è la variabile introdotta per catturare shock estremi se il rendimento delle altre attività è inferiore al q% percentile e, in questo caso, si utilizza il 10%, il 5% e l'1%; $h0$ è il coefficiente che indica se la criptovaluta rappresenta una possibile copertura ($h0$ è negativa

o 0), o è solo un semplice strumento di diversificazione ($h0$ è leggermente positivo); $h1i$, $h2i$ e $h3i$ sono i coefficienti per verificare se le criptovalute sono un rifugio sicuro durante elevati shock del rendimento dell'attività i (dove i = azioni, obbligazioni o oro). Se il valore è statisticamente negativo o pari a zero, significa che la criptovaluta studiata è un rifugio sicuro per il bene in questione, altrimenti non lo è.

Nel pannello A della Figura 2.12 *Utilizzo delle criptovalute come strumento di copertura per un portafoglio*, Bitcoin è statisticamente correlato negativamente con gli stocks con un coefficiente di -0.013, mentre la correlazione tra Bitcoin ed obbligazioni è pari a zero poiché non possiamo respingere l'ipotesi nulla che il coefficiente $h0$ sia zero. La Figura 2.12 *Utilizzo delle criptovalute come strumento di copertura per un portafoglio* mostra anche che Bitcoin può essere utilizzato come strumento di copertura per l'oro con un coefficiente di -0.004.

Questi risultati dimostrano che Bitcoin può essere utilizzato come copertura per azioni, obbligazioni e oro; tuttavia, il Bitcoin è visto come una copertura più forte per gli stocks rispetto ad obbligazioni e oro, dato che il coefficiente -0.013 significa che con 1 punto di diminuzione del prezzo delle azioni, il valore del Bitcoin aumenterà di 0,013. Pertanto, Bitcoin può essere usato come hedging invece che come strumento di diversificazione per lo S&P 500.

Bitcoin inoltre può essere scelto come rifugio sicuro per i rendimenti azionari al quantile dell'1%: il coefficiente di -0.048 implica che quando i rendimenti azionari sono in cattive condizioni, il decremento di un'unità nel prezzo delle azioni può determinare un incremento di 0,048 unità nel prezzo di Bitcoin.

Nel pannello B, Litecoin dimostra proprietà di copertura per azioni, obbligazioni e oro. Rispetto a tutte le classi di asset qui studiate, Litecoin dimostra una proprietà di hedging maggiore per l'oro: il valore statisticamente significante di -0.041 indica che con una diminuzione unitaria del prezzo dell'oro, il valore di Litecoin aumenterà di 0,041. Non esiste una relazione lineare tra azioni e Litecoin, quindi il movimento dei prezzi delle azioni non influirà sul prezzo di Litecoin. In nessuno degli scenari possibili per tutte le classi di attività, Litecoin può essere utilizzato come investimento sicuro.

Per quanto riguarda il pannello C, è interessante osservare che Ripple è statisticamente correlato positivamente con le obbligazioni e l'oro nell'intervallo di confidenza dell'1% e con gli stocks nell'intervallo del 10%. La coppia Bond-Ripple ha la più alta correlazione positiva, con un valore pari a 0,028. Questo indica che il prezzo delle obbligazioni si muove nella stessa direzione di Ripple: se il prezzo dell'obbligazione aumenta di 1 punto, anche il prezzo di Ripple aumenterà di 0,028 punti. La leggera correlazione positiva di Ripple con azioni, obbligazioni e oro indica che Ripple può essere utilizzato solo come strumento di diversificazione. I risultati mostrano anche che Ripple non può essere utilizzato come rifugio sicuro per nessuna delle attività durante i periodi negativi. Inoltre, quando i rendimenti delle azioni sono al quantile del 5%, Ripple è statisticamente correlato positivamente con lo S&P 500. Il coefficiente di 0,061 indica che durante i periodi di stress, il prezzo di Ripple aumenta di 0,061 insieme ad una crescita unitaria del prezzo delle azioni.

I diversi risultati tra Ripple e Bitcoin/Litecoin potrebbero essere spiegati dalle differenti caratteristiche delle criptomonete stesse. Poiché Litecoin è stato implementato per affrontare i punti deboli di Bitcoin, come ad

esempio la poca scalabilità, esso condivide la stessa tecnologia sottostante e quindi possiede caratteristiche simili. Al contrario, l'idea alla base di Ripple è quella di funzionare come una rete di pagamento per le banche, mantenendo così caratteristiche molto diverse rispetto a Bitcoin o Litecoin. A differenza di quest'ultimi, sotto il setup di Ripple, non ci sono minatori poiché tutte le monete XRP sono state create al momento del lancio della società. Di queste monete emesse, una parte significativa è mantenuta dalla società e dai soci fondatori. Ciò è in forte contrasto con il sistema decentralizzato di Bitcoin e Litecoin per il quale la proprietà dei token è distribuita in tutto il mondo. Poiché Ripple si basa sulla capacità di funzionare come una rete di pagamento avanzata per le banche, offrendo transazioni più veloci ad un costo inferiore rispetto al sistema bancario convenzionale, risulta essere interessante per le grandi istituzioni finanziarie. Il collegamento di Ripple a queste istituzioni potrebbe spiegare perché la correlazione tra questo protocollo e le classi di asset è leggermente positiva.

In base a questi risultati è evidente che le criptovalute possono essere utilizzate come mezzo di copertura, in particolare Bitcoin e Litecoin. Tuttavia, non è ancora sicuro che queste criptomonete possano effettivamente ridurre il rischio o migliorare i rendimenti di un portafoglio. Pertanto, si cerchi di scoprire se un investitore possa migliorare la produttività dei suoi investimenti aggiungendo monete virtuali.

Variable	Obs	Mean	Std. Dev.	Min	Max
Stock - Bitcoin	1155	-0.0028	0.0135	-0.0575	0.0482
Bond - Bitcoin	1155	0.0002	0.0052	-0.0134	0.0152
Gold - Bitcoin	1155	-0.0006	0.0151	-0.0507	0.0456
Stock -Litecoin	1155	-0.0007	0.0086	-0.0363	0.0320
Bond - Litecoin	1155	-0.0004	0.0034	-0.0115	0.0097
Gold - Litecoin	1155	-0.0057	0.0115	-0.0478	0.0368
Stock - Ripple	1155	0.0025	0.0093	-0.0289	0.0502
Bond - Ripple	1155	0.0017	0.0038	-0.0103	0.0145
Gold - Ripple	1155	0.0020	0.0113	-0.0327	0.0459

Figura 2.13 Rapporto di copertura dei portafogli bivariati Fonte: Cryptocurrency: A new investment opportunity? An investigation of the hedging capability of cryptocurrencies and their influence on stock, bond and gold portfolios

La Figura 2.13 *Rapporto di copertura dei portafogli bivariati* mostra il risultato dei rapporti di hedging dinamici stimati in ciascuno dei portafogli bivariati. Si può vedere come le coppie Stock-Bitcoin, Gold-Bitcoin e tutte le coppie Litecoin hanno un rendimento medio negativo come rapporto di copertura. Questo segno negativo indica che le criptovalute e le attività si muovono in direzioni opposte (correlazione negativa), il che conferma i risultati visti in precedenza. Ciò comporta che un gestore di portafoglio assuma una posizione lunga in criptovalute per coprire la posizione lunga in azioni, obbligazioni e oro. Tutti gli altri portafogli bivariati hanno medie positive come rapporti di copertura dinamici. Tuttavia, i valori sono piuttosto piccoli, con un massimo di solo 0,0025, ottenuto da Stock-Ripple. Il valore 0,0025 significa che per un'unità di stock in cui si ha una posizione lunga, bisogna andare corti con 0,0025 unità di Ripple per avere copertura nel portafoglio.

Per concludere sia Bitcoin che Litecoin mostrano un possibile loro utilizzo come strumento di hedging mentre Ripple può essere usato come investimento per diversificare il portafoglio. Il Bitcoin è significativamente correlato negativamente con lo S&P 500 e correlato in modo non significativo con gli altri asset, in modo da essere uno strumento di hedging per azioni, obbligazioni e oro. Litecoin rivela una significativa correlazione negativa con le obbligazioni e l'oro e una correlazione insignificante con le azioni, quindi è utile come copertura per questi asset. Ripple non può essere usato come copertura e si suppone che ciò sia dovuto a differenze nella tecnologia e nelle caratteristiche di base. Contrariamente a Bitcoin e Litecoin, Ripple rivela una leggera correlazione positiva con altre classi di attività; ciò lo rende un utile investimento per la diversificazione di un portafoglio. Pur mostrando la loro utilità come hedging o diversificazione, i negativi rapporti di efficacia della copertura dimostrano che le monete virtuali aggiungeranno sempre varianza alla "minimum variance" di portafoglio, aumentando quindi il rischio dello stesso. Questo non sorprende conoscendo gli alti livelli di volatilità caratteristici delle criptovalute. Tuttavia, gli alti livelli di volatilità sono spesso accompagnati da alti rendimenti quindi l'utilizzo delle monete digitali aumenterà il rischio-rendimento del portafoglio.[47]

[47] (Seng, 2018)

Capitolo 3 – Le criptovalute e le bolle speculative

In questo capitolo l'attenzione si concentra sull'andamento del prezzo del Bitcoin e sulle bolle speculative che si sono verificate dalla sua creazione fino ad oggi. Come visto in precedenza, la correlazione tra Bitcoin e gli altcoin è altissima, per cui una significativa variazione di prezzo di Bitcoin si riflette quasi totalmente sull'intero settore delle criptovalute. Questo permette di capire che le macro-bolle di Bitcoin, in realtà sono state macro-bolle per tutte le monete virtuali.

Nella prima parte del capitolo verranno spiegati i metodi statistici utilizzati per individuare le bolle finanziarie, nella seconda verranno descritte le bolle di Bitcoin dal 2009 fino ad oggi.

Identificare una bolla speculativa non è semplice. Tradizionalmente viene definita come un aumento anomalo del prezzo di un asset, a cui fa seguito un crollo dello stesso nella fase di scoppio della bolla. Questa descrizione intuitiva è tuttavia troppo limitata, difficile da concettualizzare e piena di incognite poiché richiede la definizione implicita di "aumento anomalo del prezzo" e "crollo". Per misurare le crescite anormali dei prezzi, occorre definire un metodo di riferimento rispetto al quale misurare le variazioni, con la possibilità che, quando si impiega tale modello di riferimento, una bolla possa essere valutata erroneamente a causa della fallacità del metodo impiegato. Per questa analisi viene utilizzata una metodologia che combina due criteri adatti a identificare sistematicamente e automaticamente l'inizio e la fine delle bolle, le dimensioni e la durata della caduta di prezzo.

3.1 L'Epsilon Drawdown Method

Il primo metodo, chiamato Epsilon Drawdown Method, consente di riconoscere i picchi delle bolle speculative: il punto centrale è quello di riuscire a identificare nella bolla il rincaro dei prezzi, definito come "drawup", ovvero una successione di rendimenti positivi che possono essere interrotti da rendimenti negativi non più ampi rispetto ad un livello di tolleranza pre-specificato ε. Lo scoppio della bolla corrisponde al successivo "drawdown", ovvero una successione di rendimenti negativi che possono essere interrotti da rendimenti positivi non più grandi in ampiezza rispetto al livello di tolleranza pre-specificato ε. Con questo metodo, i periodi di drawup e drawdown si alternano e l'andamento del prezzo può essere sistematicamente scomposto in una sequenza di fasi di aumento e riduzione consecutivi. Il parametro di tolleranza ε è definito come il prodotto della volatilità realizzata σ, stimato su una finestra temporale di durata w, e un moltiplicatore costante e prestabilito ε_0. Quanto maggiore è il parametro di tolleranza, tanto maggiori sono i movimenti di prezzo diretti in senso opposto che sono tollerati in un dato drawup o drawdown. Un drawup termina quando si osserva un rendimento negativo la cui ampiezza supera ε (viceversa per il drawdown). Per ottenere risultati affidabili, ε_0 assumerà valori da 0,1 a 5 con incrementi di 0,1 e w da 10 a 60 giorni in intervalli di 5 giorni, ottenendo $50 \times 11 = 550$ valori (ε_0, w). Per ogni coppia, utilizziamo questo metodo per le serie temporali del prezzo Bitcoin espresso in dollari USA (btc/usd) da gennaio 2012 a gennaio 2018 e otteniamo una sequenza unica di drawup e drawdown. Nella sequenza vengono calcolati i punti di massimo (t_p), definiti come le date

alla fine di tutti i periodi di drawup contenuti nella sequenza. La scansione su 550 coppie (ε0, w) ci dà 550 diversi punti di massimo (t_p). In seguito, per ciascuna data giornaliera t nel periodo di tempo osservato, contiamo il numero di volte in cui t è stata identificata come un punto di massimo sull'intero insieme di 550 coppie (ε_0, w). Dividendo infatti il numero risultante per 550 otteniamo f_t ovvero le coppie (ε_0, w) che hanno un punto di massimo nel drawup in data t. I grandi picchi, che si verificano alla fine di lunghe bolle speculative, sono quei periodi tali per cui $f_t > 0{,}95$. I picchi di dimensione intermedia, che si verificano alla fine delle bolle corte, sono quei periodi tali per cui $f_t > 0.65$.

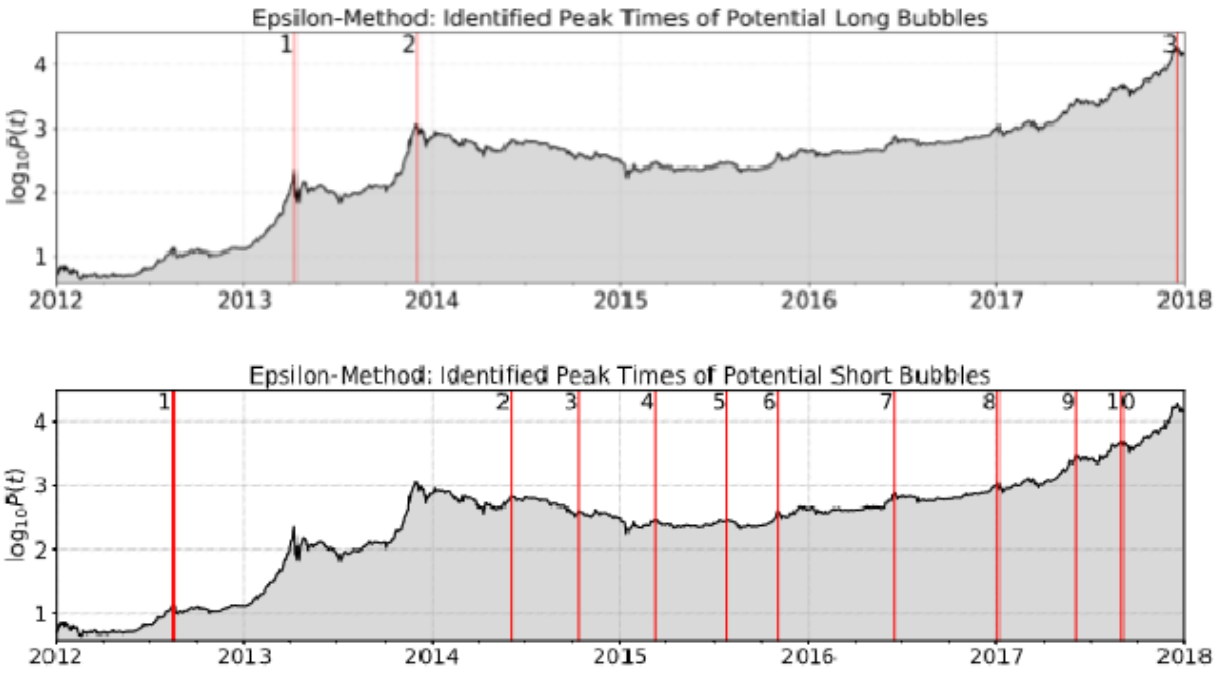

Figura 3.1 Punti di massimo nel prezzo di Bitcoin calcolati con l'Epislon Drawdown Method Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

La Figura 3.1 *Punti di massimo nel prezzo di Bitcoin calcolati con l'Epislon Drawdown Method* evidenzia i periodi di picco delle bolle su scala logaritmica rispetto al prezzo di btc/usd da gennaio 2012 a febbraio 2018. Il riquadro superiore mostra tre linee verticali che identificano i tre picchi sotto la condizione $f_t > 0{,}95$. Questi tre punti di massimo coincidono con le tre bolle di Bitcoin, sviluppatesi nel periodo da gennaio 2012 a febbraio 2018. Il riquadro inferiore mostra dieci linee verticali che identificano i 10 picchi, oltre alle tre precedenti, selezionati sotto la condizione $f_t > 0{,}65$. Questi dieci punti di massimo rappresentano le bolle più brevi.

3.2 Log-Periodic Power Law Singularity (LPPLS)

Dopo aver utilizzato l'Epislon Drawdown Method per identificare i principali momenti di picco delle bolle, è necessario un modello che definisca in maniera automatica e obiettiva i tempi di inizio delle bolle corrispondenti. Per questo si usa il modello Log-Periodic Power Law Singularity (LPPLS), che rapporta un'accelerazione del prezzo più veloce di quella esponenziale, con una crescente volatilità. In contrasto con la

visione profondamente radicata in economia che le bolle finanziarie possano essere classificate come fenomeni imprevedibili, poiché si presume che i prezzi delle attività seguano percorsi casuali, il modello LPPLS evidenzia un'intuizione differente, ovvero che le bolle abbiano comportamenti prevedibili.
In un regime di bolle speculative, la traiettoria di prezzo di un dato bene si scinde dal suo valore intrinseco Per un dato valore fondamentale, il modello JLS assume che il logaritmo del prezzo p(t) è:

$$\frac{dp}{p} = \mu(t)dt + \sigma(t)dW - \kappa dj,$$

Equazione 3.1 JLS model Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

Nel JLS model μ(t) è il rendimento atteso, σ(t) è la volatilità, dW è l'incremento infinitesimale di un processo standard di Wiener (con media zero e varianza pari a dt) e dj rappresenta un salto discontinuo tale che j = 0 prima del crollo del prezzo e j = 1 dopo il crollo. Il parametro κ quantifica l'ampiezza di un possibile crollo di mercato. Nella struttura di rete che è alla base della LPPLS, vengono considerati due tipi di agenti: il primo è costituito da traders con aspettative razionali, mentre il secondo è costituito da "noise traders" ovvero investitori che prendono decisioni in merito all'acquisto e alla vendita di asset senza il supporto di consulenze professionali o analisi fondamentali avanzate. Il trading da parte dei noise traders tende ad essere impulsivo e irrazionale; in genere seguono le tendenze e reagiscono in modo esagerato a notizie buone e cattive. Il loro comportamento collettivo può destabilizzare i prezzi delle attività. Considerata questa distinzione, sotto l'ipotesi del modello JLS, il tasso di rischio di caduta del mercato provocato dai "noise traders" che si influenzano l'un l'altro, ha le seguenti dinamiche:

$$h(t) = \alpha(t_c - t)^{m-1}\left(1 + \beta\cos(\omega\ln(t_c - t) - \phi'\right)$$

Equazione 3.2 Tasso di crash del mercato Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

Nella Equazione 3.2 *Tasso di crash del mercato* α, β, ω e t_c sono parametri. Il comportamento imitativo da parte dei noise traders è determinato da $(\alpha(t_c\text{-}t)^{m\text{-}1})$, mentre t_c rappresenta il tempo critico nel quale è maggiormente probabile che scoppi la bolla. La condizione di non arbitraggio impone che il rendimento in eccesso μ(t) durante una fase di bolla sia proporzionale alla percentuale di rischio di crollo. Utilizzando gli integrali, si ottiene che la traiettoria del prezzo su base logaritmica durante una fase di bolla, a condizione che il crollo non si sia ancora verificato, è:

$$E[\ln p(t)] = A + B|t_c - t|^m + C|t_c - t|^m\cos(\omega\ln|t_c - t| - \phi)$$

Equazione 3.3 LPPLS Model Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

Nella Equazione 3.3 *LPPLS Model*, $A=\ln(p(t_c))$, $B=-k\alpha/m$ and $C = -k\alpha\beta/\sqrt{m2 + \omega2}$. L'esponente m quantifica il grado di crescita esponenziale del prezzo. La frequenza angolare periodica ω è correlata alle oscillazioni nel t_c. Infine, $\varphi \in (0, 2\pi)$ è una fase che incorpora una scala temporale caratteristica delle oscillazioni. I regimi di bolle sono in genere caratterizzati da 0 <m <1 e B <0. La prima condizione m <1 evidenzia l'esistenza di una singolarità, mentre m> 0 assicura che il prezzo rimanga finito (nel senso di positivo) nel momento critico t_c. La seconda condizione B <0 esprime che il prezzo cresca effettivamente in modo esponenziale verso t_c (per 0 <m <1).[48]

Attraverso la combinazione di questi due modelli che ci consentono di conoscere le date di inizio, del punto di massimo, della fine della discesa del prezzo di una bolla e della sua traiettoria di prezzo, vengono calcolate sia le dimensioni delle bolle in percentuale, definite come il rendimento cumulativo tra l'inizio e il punto di massimo, sia le dimensioni del crollo, calcolate come il rendimento cumulativo tra la durata del picco e la data di fine del crollo. I risultati ci portano a definire fino ad oggi l'esistenza di tre bolle "lunghe" e dieci bolle "corte", come rappresentato dalla Figura 3.2 *Caratteristiche delle bolle finanziarie*

Long Bubble Data						
Nr.	**Bubble Start t_1^***	**Bubble Peak t_{peak}**	**Crash End Date**	**Duration** [days]	**Bubble Size** [%]	**Crash Size** [%]
1	2012-05-28	2013-04-09	2013-04-16	316	4416	-70.27
2	2013-07-03	2013-12-04	2015-01-14	154	1367	-84.83
3	2016-01-15	2017-12-18	2017-12-25	703	5152	-26.55
Short Bubble Data						
Nr.	**Bubble Start t_1^***	**Bubble Peak t_{peak}**	**Crash End Date**	**Duration** [days]	**Bubble Size** [%]	**Crash Size** [%]
1	2012-05-07	2012-08-16	2012-08-20	101	165	-25.11
2	2014-04-15	2014-06-03	2014-06-25	49	28	-16.38
3	2014-06-30	2014-10-14	2014-10-23	106	-37	-11.45
4	2014-10-23	2015-03-11	2015-04-13	139	-16	-24.75
5	2015-04-13	2015-07-27	2015-08-24	105	31	-28.74
6	2015-08-26	2015-11-04	2015-11-11	70	80	-24.04
7	2016-01-15	2016-06-16	2016-08-02	153	112	-29.56
8	2016-08-03	2017-01-04	2017-01-11	154	97	-30.16
9	2017-03-24	2017-06-06	2017-06-07	74	210	-6.86
10	2017-06-07	2017-09-01	2017-09-14	86	83	-34.42

Figura 3.2 Caratteristiche delle bolle finanziarie Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018)

Si descrivano ora i fattori chiave, gli eventi e gli sviluppi che hanno causato le tre macro-bolle di Bitcoin.

3.3 Prima bolla speculativa: Maggio 2012-Aprile 2013

La crisi finanziaria del 2007-2008 ha permesso di capire come le economie di tutto il mondo fossero per molti aspetti fragili. Ha contribuito inoltre a rivelare l'insostenibile livello di indebitamento e la cattiva gestione finanziaria di alcune piccole, medie e grandi economie dell'Unione europea come Grecia, Irlanda, Portogallo, Spagna, Islanda, Italia e Cipro. In particolare, le crisi di Cipro e della Grecia si distinsero per intensità e

[48] (Sornette, 2016)

conseguenze: entrambi i paesi hanno raggiunto il loro peggiore stato economico nel 2012. Il declino economico è stato accompagnato da discussioni interne all'UE riguardo ai programmi di salvataggio per questi stati. La sfiducia nel governo e nelle istituzioni finanziarie ha innescato un'ondata di corse agli sportelli e di caccia ai paradisi monetari della popolazione locale. Il Bitcoin, proposto come riserva alternativa di valore, in quanto strumento non sottoposto al controllo dei governi e indipendente dalle politiche monetarie, sembrava l'investimento ideale. Non è una coincidenza che la comparsa della prima bolla lunga Bitcoin si sia verificata nel momento esatto in cui gli indici di Grecia e Cipro hanno raggiunto i loro minimi, come raffigurato nella Figura 3.3 *Confronto tra l'evoluzione del prezzo di Bitcoin e gli indici greci e ciprioti*

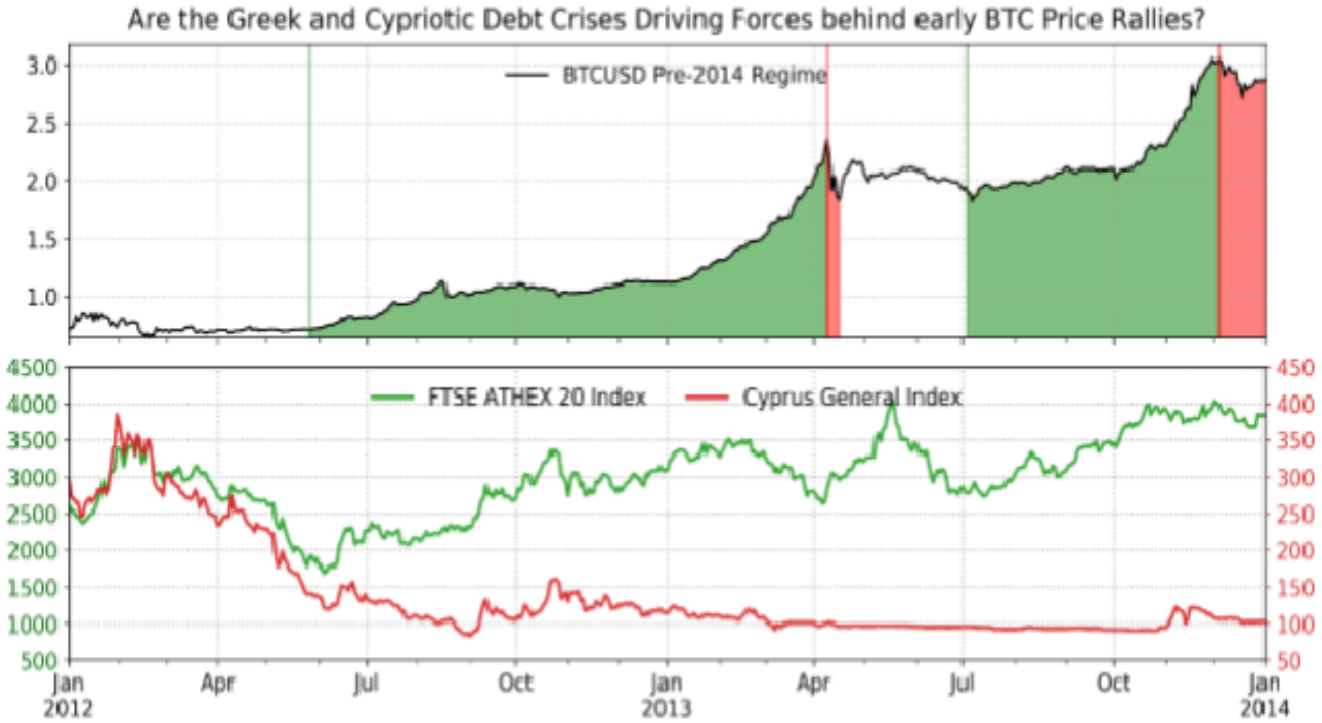

Figura 3.3 Confronto tra l'evoluzione del prezzo di Bitcoin e gli indici greci e ciprioti Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

Il 16 marzo 2013 è stato raggiunto un punto critico per l'economia cipriota, poiché è stata dichiarata una tassa di bail-in che in gran parte influiva sui titolari di conti correnti presso le banche cipriote. L'annuncio ha creato una massiccia ondata di corse agli sportelli da parte degli stessi per proteggere i propri risparmi. Questo ha coinciso con l'ultima crescita del prezzo di Bitcoin, prima del suo crollo nell'aprile 2013. Le vicende di Cipro sono state osservate con ansia in altri paesi della zona euro, ad esempio in Spagna, dove la gente temeva che simili interventi governativi potessero portare alla perdita dei propri risparmi. Bitcoin arrivò sulla scena, percepito come l'investimento alternativo perfetto, in quanto il suo valore non poteva essere influenzato da nessuna istituzione. La Figura 3.4 *Aumento del numero di transazioni nella blockchain* illustra il flusso di utilizzatori della criptovaluta sotto forma di crescenti transazioni in blockchain nel momento di formazione della bolla. Come risposta alla crescente domanda, il prezzo di un Bitcoin è salito di un incredibile 4400%, raggiungendo i 100 dollari.

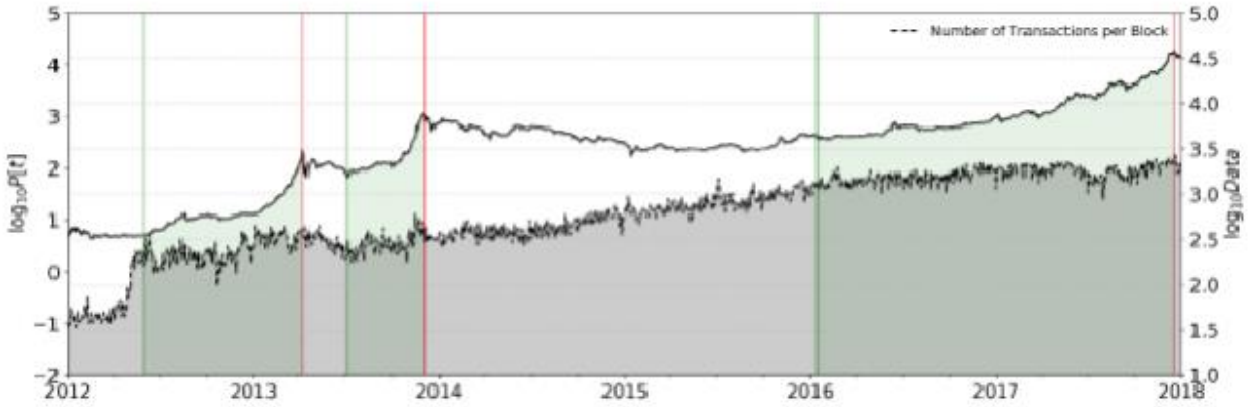

Figura 3.4 Aumento del numero di transazioni nella blockchain Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

La bolla ha raggiunto il punto massimo all'inizio di aprile 2013. Nello specifico, dopo aver raggiunto il picco il 9 aprile, è scoppiata, con circa il 70% della capitalizzazione di mercato di Bitcoin che è scomparso entro una settimana. La vera causa del crollo è stata una reazione negativa agli annunci di instabilità di MtGox, l'allora più grande Exchange in termini di volumi scambiati in Bitcoin. Ovviamente, l'evento che ha portato al crollo non è stato direttamente correlato alle situazioni politiche dell'Eurozona e alla crisi greca e cipriota. Come spesso accade nello scoppio di una bolla, si deve distinguere la causa prossima del crollo, che in generale non è correlata al motivo che ha portato alla formazione della bolla, dall'origine fondamentale della caduta, che in questo caso era rappresentata dal fatto che il mercato di Bitcoin era fragile, instabile e molto suscettibile alle notizie negative.

3.4 Seconda bolla speculativa: Luglio 2013-Dicembre 2013

La seconda bolla lunga è maturata alla fine del 2013 dopo un aumento del prezzo di circa tredici volte rispetto al prezzo post-incidente risultante dalla prima lunga bolla. Poiché la crisi del debito europeo era ancora in corso, anche questa volta, l'attrazione per il Bitcoin come investimento decentralizzato ed alternativo, ha contribuito al suo aumento di prezzo. Non bisogna tuttavia sottovalutare una serie di fattori aggiuntivi che hanno contribuito alla formazione di questa bolla: l'adozione del Bitcoin in Cina, la chiusura da parte dell'FBI del mercato della droga "Silk Road" e l'aumento dell'hashing power dei miners. La Figura 3.4 *Aumento del numero di transazioni nella blockchain* riporta anche la nascita e i volumi di negoziazione dei principali Exchange di Bitcoin a partire dal 2012. L'area grigio scuro rappresenta il volume totale su scala logaritmica di tutte le transazioni realizzate. L'area chiara mostra il volume degli Exchange ancora in attività nel 2018. I riquadri blu mostrano l'evoluzione degli scambi su scala logaritmica realizzati dalle singole piattaforme di scambio. Si può verificare che, durante la nascita della seconda bolla lunga, sono stati fondati i principali Exchange cinesi tra cui Huobi e OKCoin. L'emergere di essi ha notevolmente facilitato l'ingresso sul mercato di numerosi investitori, principalmente cinesi. In definitiva, l'ondata di nuovi investimenti ha spinto per la

prima volta i prezzi al di sopra del livello di 1000 dollari per bitcoin. La Figura 3.5 *Volumi scambiati dai maggiori Exchange* mostra che la quota del volume totale scambiato dalle borse cinesi è iniziata ad aumentare molto durante la seconda bolla lunga. Mentre la bolla si stava sviluppando rapidamente, il 2 ottobre 2013 il mercato della droga online chiamato Silk Road, il quale permetteva ai clienti di acquistare sostanze illegali in modo anonimo tramite pagamento in bitcoin, è stato chiuso dall'FBI e il suo presunto fondatore messo in carcere. Questo ha fatto capire alla comunità di Bitcoin che le autorità legali avevano gli occhi puntati su di essa ed intendevano vietare ogni attività illegale collegata a questa moneta. Sebbene Silk Road sia stato il primo, ma non l'unico, mercato della droga su Internet, la sua chiusura ha avuto ampie implicazioni: infatti ha permesso di capire come il Bitcoin fosse un investimento adeguato anche per gli investitori più prudenti che, fino a quel momento, erano scoraggiati a causa del suo utilizzo per fini illegali.

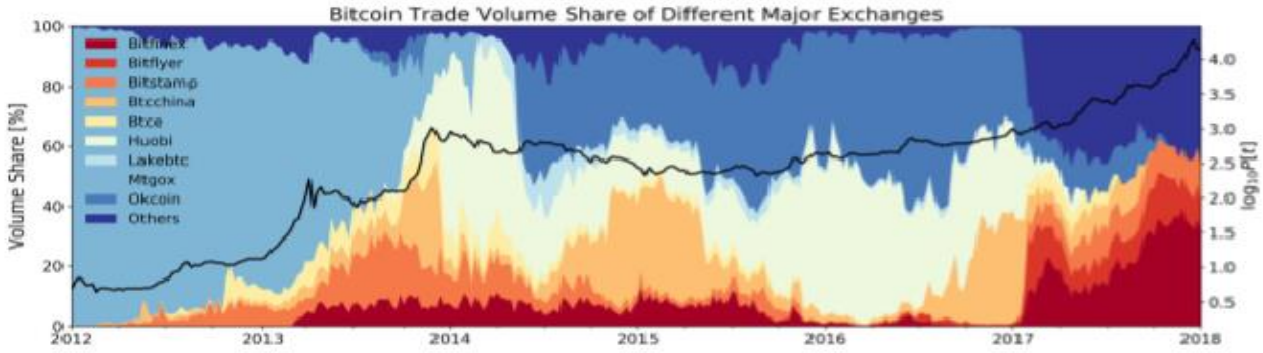

Figura 3.5 Volumi scambiati dai maggiori Exchange Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

La Figura 3.6 *Crescita della base utenti della rete Bitcoin e aumento della potenza mineraria* suggerisce il terzo fattore che contribuì alla crescita dei prezzi durante la bolla. Viene mostrato su scala logaritmica il tasso di hashing power dei minatori che minano i blocchi in blockchain, così come il numero di wallet creati che fornisce una misura riguardo alle dimensioni della rete di utenti. Si noti che la potenza di calcolo è cresciuta ad un ritmo molto più veloce rispetto al numero di portafogli dalla nascita della prima bolla lunga. Il più alto tasso di crescita è stato raggiunto durante la seconda metà del 2013, in coincidenza con la seconda bolla lunga. Quindi, un aumento dell'hashing power maggiore rispetto alla base di utenti segnala che in media i minatori hanno migliorato la propria potenza di calcolo durante il periodo considerato. Ciò è stato possibile grazie all'uso di hardware per il mining più efficienti: dato che il prezzo del bitcoin è cresciuto fino a raggiungere un livello abbastanza alto, i minatori sono stati incentivati a investire negli hardware per il mining. A causa del prezzo relativamente alto di un bitcoin rispetto all'efficacia computazionale necessaria per crearlo, si verificò che nuovi minatori entrassero nel business. Il crescente numero di minatori ha quindi attivato un "effetto catena". Può essere vista come una bolla che si rafforza da sola: maggiore è il prezzo, maggiore è l'incentivo ad investire nella potenza di calcolo dell'hardware; più miners ci sono, più nodi ci sono sulla blockchain, più aumenta il prezzo.

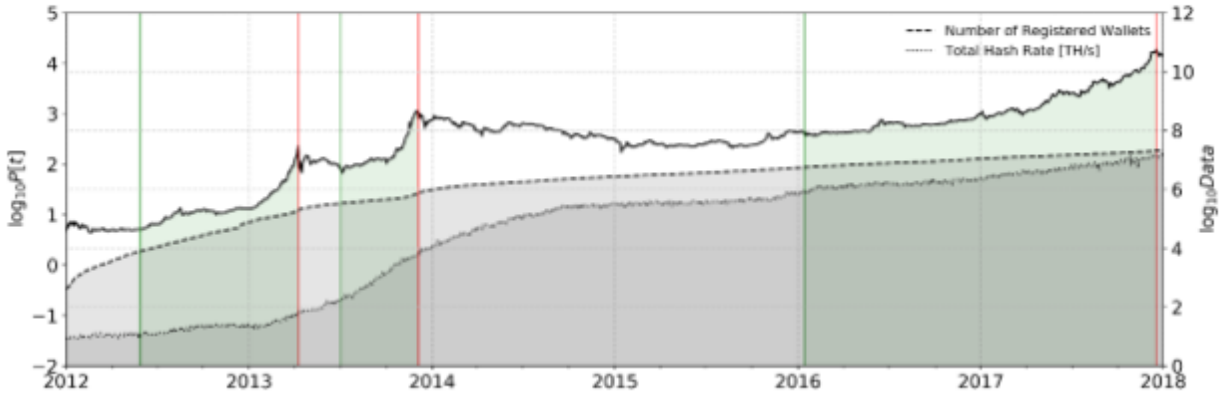

Figura 3.6 Crescita della base utenti della rete Bitcoin e aumento della potenza mineraria Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

Due sono i principali fattori che hanno scatenato il crollo del prezzo iniziato nel dicembre 2013. In primo luogo, il governo cinese vietò improvvisamente alle istituzioni finanziarie di utilizzare Bitcoin: l'annuncio destabilizzò la valuta e generò un tracollo disastroso. In secondo luogo, nel febbraio 2014, MtGox sospese gli scambi di Bitcoin, conseguentemente al furto di almeno 700.000 bitcoin: infatti il sistema di ritiro di token dal wallet di ciascun proprietario presentava un grave bug che permetteva di richiedere una seconda volta una somma già ritirata. La fine di MtGox fu percepita come una battuta d'arresto importante per il mondo Bitcoin. I detentori di wallet sull'Exchange persero denaro che fu recuperato solo parzialmente a causa della difficoltà nel tracciarlo. Ancora una volta, questo portò ad una perdita enorme di affidabilità di Bitcoin, già messa in discussione più volte in passato.

3.5 Terza bolla speculativa: Gennaio 2016-Dicembre 2017

La crescente domanda di bitcoin da parte dei mercati cinesi a seguito della nascita di mining pools e di Exchange, può essere visto come un importante fattore che ha scatenato la terza lunga bolla, il cui inizio può essere identificato nel 2016. Ma quale era l'origine della bolla? La svalutazione dello Yuan cinese è stato un fattore importante per lo sviluppo di un crescente interesse verso le criptovalute in Cina.

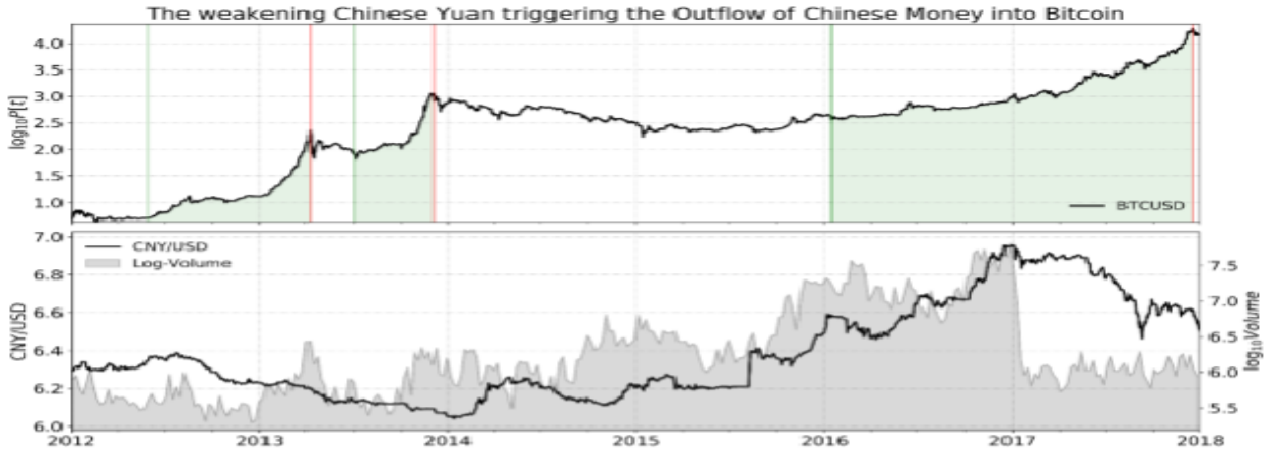

Figura 3.7 Sviluppo Bitcoin rispetto allo Yuan cinese Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

La Figura 3.7 *Sviluppo Bitcoin rispetto allo Yuan cinese* mostra un cambiamento di regime nel tasso di cambio dello Yuan cinese (CNY) rispetto al dollaro statunitense dal 2014 in poi. Nell'agosto 2015, il deprezzamento dello Yuan è stato imposto da una politica basata sulla svalutazione della moneta proposta dalla Banca Popolare Cinese (PBoC). Questa svalutazione è stata motivata dal desiderio di aumentare la competitività delle imprese esportatrici. Da lì in poi, un continuo indebolimento dello Yuan cinese si è sviluppato fino a gennaio 2017. Come reazione al deprezzamento della valuta dal 2014 in poi, gli investitori cinesi hanno cercato di trasferire i propri risparmi verso asset o fondi più sicuri, provocando un deflusso di capitale dalla Cina. Per quanto riguarda l'investitore medio cinese, dato che le prescrizioni in termini di investimenti in valuta estera erano piuttosto restrittive, Bitcoin era una soluzione semplice ed efficiente. Tuttavia, nel gennaio 2017, la PBoC ha obbligato gli Exchange cinesi di Bitcoin, fino ad allora ampiamente non regolamentati, a conformarsi agli istituti finanziari del paese, in quanto sospettava attività di scambio illecito, come il riciclaggio di denaro sporco e la manipolazione dei volumi di scambi, resi possibili dalle commissioni di trading pari a zero. Così, i più grandi Exchange cinesi di Bitcoin, BTCC, Huobi e OKCoin sono stati costretti a introdurre una struttura di commissioni per la negoziazione di criptovalute ed a interrompere il trading con leva. La misura ha portato all'enorme crollo del volume degli scambi, come può essere osservato dalla Figura 3.7 *Sviluppo Bitcoin rispetto allo Yuan cinese.* Contemporaneamente, è scoppiata una bolla breve (la bolla breve 8 nella Figura 3.2 *Caratteristiche delle bolle finanziarie*) che ha fatto perdere a Bitcoin il 30% del suo valore.

A settembre 2017 i regolatori cinesi hanno vietato le cosiddette Initial Coin Offering (ICO). Infine, a metà settembre, la PBoC ha ordinato agli Exchange cinesi di chiudere tutte le attività di trading di monete digitali sul mercato cinese. Questa rapida serie di eventi inaspettati ha praticamente messo fine al commercio di criptovalute in Cina.

Anche se, verso la fine del 2017, il commercio di criptovalute è stato proclamato "Ufficialmente morto in Cina",[49] le azioni intraprese dalla PBoC hanno portato a due effetti: uno spostamento del trading nei mercati OTC e lo spostamento all'estero dell'attività di scambio di criptomonete da parte dei maggiori Exchange cinesi. In questo modo, sebbene la PBoC sia riuscita a prevenire il trading di monete virtuali basato sullo Yuan, la domanda di Bitcoin fu ancora maggiore e reindirizzata verso altri mercati. Pertanto, i vincoli normativi imposti non hanno avuto un'influenza permanente sull'evoluzione globale del prezzo del Bitcoin. Infatti, durante tutto il 2017, il suo valore si è ripreso rapidamente dai crolli derivanti dalle notizie negative relative alla Cina.

Oltre alla grande influenza esercitata dalla Cina sul valore del Bitcoin, ci sono stati altri fattori che hanno determinato la crescita della terza lunga bolla; essa è stata caratterizzata da una serie di bolle brevi che sono esplose improvvisamente, seguite però da un rapido recupero del prezzo. Come nel caso della seconda bolla lunga, si assistette ad un aumento dell'hashing power della rete e alla formazione di molte mining pools di Bitcoin. Questo sviluppo produsse un ulteriore pubblicità e invogliò sempre più persone a praticare l'attività

[49] (Raphoza, 2017)

di mining. Inoltre, il fatto che i guadagni derivanti da questa attività fossero ripartiti proporzionalmente tra i minatori in base al contributo in termini di potenza di calcolo dei loro computer, fornì un grande incentivo, specialmente per i minatori più deboli.

Tuttavia, la caratteristica più evidente che ha guidato l'accelerazione del prezzo di Bitcoin, dopo la chiusura della borsa cinese, è stata la crescita dell'intero mercato delle monete virtuali. In risposta alla crescente domanda da parte degli investitori di investimenti alternativi nel mercato delle criptovalute, sono nate nuove monete digitali. Nel corso del 2017, il mercato delle criptomonete ha cambiato la sua struttura: mentre prima era dominato dal Bitcoin, con il tempo si è sempre più diversificato, con lo sviluppo di numerose valute dotate di tecnologie e protocolli differenti.

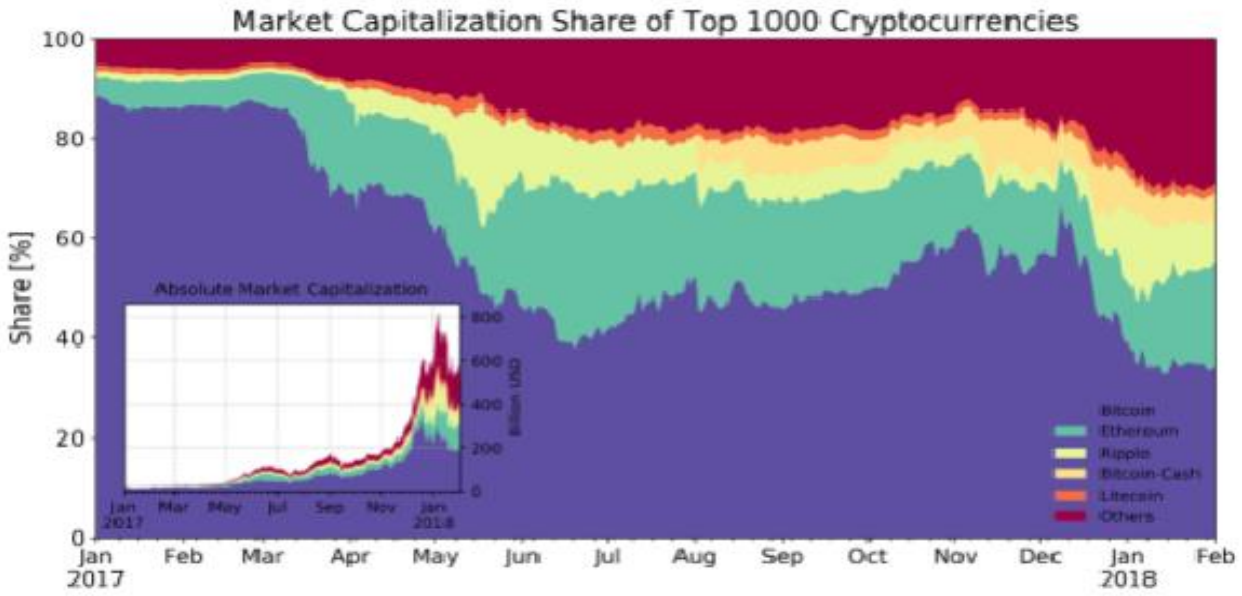

Figura 3.8 Aumento di capitalizzazione di mercato degli altcoin Fonte: Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018

La Figura 3.8 *Aumento di capitalizzazione di mercato degli altcoin* mostra la posizione dominante di Bitcoin all'inizio del 2017 con una quota di mercato che arrivava fino al 90%. A maggio 2017, la sua quota di mercato è diminuita del 50%, mentre la sua capitalizzazione di mercato e quella delle altre criptovalute hanno continuato a crescere ad un ritmo elevato fino a dicembre 2017. Durante gli ultimi due mesi del 2017, la capitalizzazione complessiva del cripto-mercato si è quadruplicata.

Tuttavia, con il crollo successivo al 18 dicembre 2017, il valore di Bitcoin e quello di molte criptovalute è diminuito, con Bitcoin che ha perso il 60% del suo valore totale (a febbraio 2018), portando la sua quota di mercato ai minimi storici.[50] Non esiste un'unica causa, globalmente riconosciuta, che giustifichi l'imponente discesa del prezzo; esistono piuttosto una serie di differenti motivi.

[50] (Gerlach, 2018)

Tra questi:

-l'effetto Corea del Sud, in quanto il Ministro della Giustizia coreano dichiarò di voler chiudere i siti di Exchange del paese. Considerando che la Corea del Sud era il terzo paese al mondo per scambi di monete virtuali, il messaggio fu recepito in maniera molto negativa dal mercato

-l'apertura da parte di Coinbase, uno dei più grandi Exchange al mondo, a Bitcoin Cash. Tale decisione portò moltissimi investitori a vendere Bitcoin per acquistare Bitcoin Cash, in grado, secondo loro, di superare i problemi di scalabilità di Bitcoin. In poche ore Bitcoin Cash arrivò a triplicare il suo valore e ciò portò Coinbase a sospendere gli scambi e avviare un'inchiesta per insider trading

-la possibilità, esternata da parte degli sviluppatori di SegWit2X (visto in precedenza), di realizzare un nuovo hard fork sulla blockchain di Bitcoin

-i continui tentativi di regolamentazione da parte di molti paesi che crearono incertezza sul futuro delle monete virtuali: il governo israeliano annunciò di voler bandire dalla borsa di Tel Aviv tutte le società il cui core business si basava sulle criptomonete. Il Ministro francese dichiarò di aver creato un gruppo di lavoro per legiferare sulle criptovalute. Si diffuse la notizia che il governo cinese volesse limitare l'attività di mining del paese. Tutte queste comunicazioni incrementarono l'incertezza sul settore delle monete virtuali, incentivando gli investitori a vendere

-effetto gennaio del Bitcoin, infatti dal 2015, nel mese di gennaio, Bitcoin tradizionalmente perde valore

-attività di trading da parte di grossi detentori di Bitcoin. E' stato ipotizzato che grandi possessori di Bitcoin, avendo intuito i segnali di un crollo, avessero venduto molti token per far scendere il valore di Bitcoin e ricomprarli ad un prezzo inferiore

-Forbes ipotizza addirittura che molte persone che guadagnarono grazie a Bitcoin decisero di venderli per sostenere le spese natalizie.[51]

[51] (Soldavini, 2017)

Conclusioni

Le criptovalute sono un settore in continua espansione in cui novità, nuovi progetti, impieghi da parte di società ma anche problemi, attacchi hacker, crolli di prezzo sono all'ordine del giorno. Quotidianamente nascono nuove monete digitali, grandi imprese decidono di trasformare i loro database contenenti milioni di dati utilizzando una tecnologia basata sulla blockchain, gli intermediari finanziari cercano di offrire agli investitori la possibilità di fare trading con le criptovalute e sempre più società, negozi, università, eventi pubblici accettano pagamenti in Bitcoin. Le monete digitali sono uno strumento che divide il mondo dell'economia: alcuni economisti sono a favore poichè le considerano mezzi di pagamento in grado di superare l'intermediazione da parte degli intermediari finanziari e di non essere soggetti al potere delle banche centrali, mentre altri le considerano enormi truffe destinate rapidamente a scomparire. E' difficile trovare un economista che assuma una posizione intermedia: o si è a favore o si è contrari.

Nel primo capitolo sono state descritte cinque differenti monete virtuali. Questo è risultato utile oltre che per informare il lettore, anche per stimolarlo a riflettere sul fatto che oggi, rispetto a qualche anno fa, il termine "criptovaluta" stia diventando troppo vago per un settore così ampio e variegato: poche sono le caratteristiche comuni tra Iota e Bitcoin, così come tra Ripple e Monero ecc.

Nel secondo capitolo è stato descritto l'impatto finanziario delle monete virtuali che possono essere considerate un interessante investimento per il portafoglio di ogni investitore. Ovviamente è ben specificato come esse siano un asset ad alto rischio così come alti possano essere i suoi profitti. Basti pensare che chi acquistò un bitcoin il 22 settembre 2013 lo pagò 127,31 dollari. Oggi, 22 settembre 2018, a 5 anni di distanza lo stesso bitcoin vale 6698,56 dollari, circa 53 volte in più!

Nel terzo capitolo sono state analizzate le ampie oscillazioni di prezzo di Bitcoin, che hanno portato alla formazione di tre macro-bolle finanziarie. Queste grandi variazioni di prezzo potevano essere facilmente desunte sia dall'elevata deviazione standard descritta nel capitolo 2 sia dalle incognite che negli anni hanno destabilizzato le valute digitali: tuttavia questo è abbastanza comprensibile in un settore totalmente nuovo. Le criptovalute devono essere collocate a cavallo tra il settore informatico ed economico, due mondi in cui per definizione vi è incertezza. Se a questo si aggiunge che le principali innovazioni sono la disintermediazione, l'assenza di un organo di controllo e la parità tra i nodi della rete si può capire il perché di qualche problema in fase di assestamento.

Un'ultima riflessione riguarda il ruolo dell'innovazione: negli ultimi anni, particolarmente dopo la crisi dell'Euro, c'è stato un grandissimo progresso tecnologico che sta trasformando processi che una volta venivano svolti dall'uomo in sistemi meccanicizzati. Industria 4.0, Big Data, Internet of Things, criptomonete e blockchain sono solo alcune delle tantissime innovazioni che stanno per rivoluzionare la nostra quotidianità. Mentre nel passato le macchine sostituivano principalmente i processi meccanici che prima venivano svolti dall'uomo (tipico è l'esempio dell'aratro sostituito dal trattore oppure le innovazioni in campo industriale), oggi siamo arrivati all'incredibile paradosso per cui le macchine sostituiscono anche la fiducia tra le persone.

La grande innovazione della blockchain è proprio questa: mentre finora il trasferimento di una certa somma di denaro dal soggetto A al soggetto B doveva essere certificato da parte di un istituto finanziario, attraverso la blockchain questo potrebbe non servire più. Similmente si comportano gli smart contracts su Ethereum. Se prima un contratto tra due parti doveva essere ricevuto da un'autorità competente, in futuro questo potrebbe non essere più necessario.

Ancora più incredibile è ciò che riuscirà a fare l'Internet of Things; esso sarà in grado di sopperire a qualsiasi mancanza di un individuo poichè le macchine provvederanno per esso. Quando non ci sarà più latte, il frigorifero ne percepirà la mancanza e comunicherà direttamente al frigorifero del supermercato di spedirlo ad un dato indirizzo e ad una data ora: il pagamento verrà eseguito tra macchine in criptomonete. Quando la mattina un individuo dovrà andare al lavoro, non sarà più lui a dover guidare ma la sua automobile si muoverà autonomamente verso l'ufficio. Quando per casa si vorrà dialogare o serviranno alcune informazioni ci sarà un "robot da compagnia" in grado di riferirci il meteo per il giorno successivo, ricordarci gli impegni o giocare con i bambini.

Il rischio è quello che non sia più l'uomo a controllare la macchina ma la macchina a controllare l'uomo. Senza la fiducia, il dialogo, le interazioni tra persone cade il concetto di società. Si potrebbe arrivare a percepire sbagliato ciò che è in contrasto con il volere della macchina e questo potrebbe iniziare a limitare la nostra libertà senza che noi ce ne accorgeremo.

Bibliografia

Back, A. (2002). *Hashcash-A Denial of Service Counter-Measure.* Working paper.

Beck, M. (2017). *Into the Ether with Ethereum Classic.*White paper

Bellini, M. (2018). *Blockchain e Bitcoin.* Milano: Class Editori.

Bhargavan, K. et al. (2016). *Short Paper: Formal Verification of Smart Contracts.*Working paper

BitFury Group in collaborazione con Jeff Garzik (2015). *Public versus Private Blockchains.*White paper

Bonneau, J. (2015). et al. *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. Working paper

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform.*White paper

Clack, C. (2016). et al. *Smart Contract Templates: foundations, design landscape and research directions.*Working paper

Cos'è il Bitcoin Cash. (2018). *Cointelegraph*.

Direttiva 2018/843. (2018). *DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.* Parlamento e Consiglio Europeo.

Dombrovskis, V. (2018). *Remarks by Vice-President Dombrovskis at the Round Table on Cryptocurrencies.* European Commission.

Falkon, S. (2017). The Story of the DAO—Its History and Consequences. *Medium*.

Gaschi, A. (2017). Fenomeno ICO: fino a che punto opportunità, quando rischia di essere truffa. *Blockchain4innovation*.

Gerlach, J.-C. et al. (2018). *Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018.* Working paper

Liew, J. K.-S. (2018). et al. *Crypto-Currency Investing Examined.* Working paper

Liu, Y. (2018). et al. *Risks and Returns of Cryptocurrency.* Working paper

Merkle, R. (2016). *DAOs, Democracy and Governance.* Working paper

Milunovich, G. (2018). *Cryptocurrencies Mainstream Asset Classes and Risk Factors – A Study of Connectedness.* Working paper

Mulders, M. (2018). A comparison between ERC20, ERC223, and the new Ethereum ERC777 token standard. *Cointelligence*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* White paper

Nicotra, M. (2017). ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno. *Blockchain4innovation*.

Nizza, C. (2018). *Token ERC-20: cosa sono e come funzionano.* Working paper

Popov, S. (2018). et al. *Equilibria in the Tangle.* Working paper

Popov, S. (2018). *The Tangle (version 1.4.3).* White paper

Raphoza, K. (2017). Cryptocurrency Exchanges Officially Dead In China. *Forbes*.

Ray, S. (2018). What is DAPP. *Toward Data Science*.

Rivest, R. et al. (2006). *How to leak a secret.* Working paper

Rosic, A. (2018). What is Monero. *Blockgeeks*

Saberhagen, N. v. (2013). *CryptoNote.* White paper

Seng, W. W. et al. (2018). *Cryptocurrency: A new investment opportunity? An investigation of the hedging capability of cryptocurrencies and their influence on stock, bond and gold portfolios.* Working paper

Shahbar, K. et al. (2017). *Weighted Factors for Measuring Anonymity Services: A Case Study on Tor, JonDonym, and I2P*. Working paper

Siegel, D. (2016). Understanding The DAO Attack. *Coindesk.*

Soldavini, P. (2017, Dicembre 22). Bitcoin, crollo del 40% in due giorni. Giù tutte le criptovalute. *ilSole24Ore*.

Sornette, D. et al. (2016). *Early Warning Signals of Financial Crises with Multi-Scale Quantile Regressions of Log-Periodic Power Law Singularities.* Working paper

Swan, M. (2015). *Blockchain-Blueprint for a New Economy.* Newton (MA): O'Reilly Media.

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger EIP-150 revision.*Yellow paper

Sitografia

(2018). Tratto da Iota: www.Iota.org

(2018). Tratto da Monero: www.getmonero.org

(2018). Tratto da Kovri: www.getkovri.org

Ethereum Development Tutorial. (2018). Tratto da Github: www.github.com

Process Payments. (2018). Tratto da Ripple: www.ripple.com

Remix. (2018). Tratto da Github: www.github.com

Ring signature: Untraceable payments. (2018). Tratto da Cryptonote: www.cryptonote.org

The Invisible Internet Project (I2P). (2018). Tratto da I2P: www.geti2p.net

Xrp Concepts. (2018). Tratto da Xrp Ledger Developer Portal: www.developers.ripple.com