Dipartimento di Economia e Management

Cattedra di Informatica

Criptovalute, Bitcoin e Blockchain: storia, applicazioni attuali e future

Relatore:
Prof. Italiano Giuseppe Francesco

Carlo Vallo,
Matricola 209201

Anno Accademico 2018/2019

Sommario

Introduzione 4
1 – Le criptovalute 6
1.1. Cos'è una criptovaluta 6
1.1.1. Definizione teorica di criptovaluta *6*
1.1.2. Punti di forza e di debolezza delle criptovalute *6*
1.1.3. Le criptovalute possono essere definite "monete"? *7*
1.2. Criptovalute e riciclaggio 8
1.2.1. Le normative antiriciclaggio *8*
1.2.2. Pericolo criptovalute: La V^a Direttiva antiriciclaggio *8*
1.2.3. Perché le criptovalute sono collegate al riciclaggio *10*
1.3. Le principali criptovalute oltre a Bitcoin 10
1.3.1. Gli Altcoin *10*
1.3.2. Litecoin (LTC) *10*
1.3.3. Ethereum (ETH) *11*
1.3.4. Zcash (ZEC) *12*
1.3.5. Dash *12*
1.3.6. Ripple (XRP) *13*
1.3.7. Monero (XMR) *14*
1.3.8. Bitcoin Cash (BCH) *15*
1.3.9. Neo (NEO) *16*
1.3.10. Cardano (ADA) *17*
1.3.11. Eos.io (EOS) *18*
1.3.12. Tether (USDT) *19*
1.3.13. Stellar Lumens (XLM) *20*
1.3.14. Binance Coin (BNB) *20*
1.3.15. Una "classifica" delle criptovalute *21*
2 – Il sistema Bitcoin 22
2.1. Introduzione su Bitcoin 22
2.2. L'era pre-bitcoin e la sua fondazione 23
2.2.1. La profezia di Milton Friedman *23*
2.2.2. Prima applicazione di moneta digitale: il caso di David Chaum *23*
2.2.3. E-gold *24*
2.2.4. Cosa ha imparato il mondo da DigiCash e E-Gold *25*

2.2.5. La cripto-anarchia di Wei Dai *25*
2.3. La nascita di Bitcoin 26
2.3.1. L'annuncio su Metzdowd.com *26*
2.3.2. Il White Paper *27*
2.3.3. La misteriosa identità di Satoshi Nakamoto *29*
2.4. La prima fase di Bitcoin: un milione di capitalizzazione (2008 – 2010) 31
2.4.1. Bitcoin nel 2008 ..... *31*
2.4.2. Bitcoin nel 2009 ..... *31*
2.4.3. Bitcoin nel 2010 ..... *32*
2.5. La seconda fase di Bitcoin: da 0.42 a 1000 USD/BTC (2011 – 2013) 33
2.5.1. Bitcoin nel 2011 ..... *33*
2.5.2. Bitcoin nel 2012 ..... *34*
2.5.3. Bitcoin nel 2013 ..... *35*
2.6. La terza fase di Bitcoin (2014 – 2016) 35
2.6.1. Bitcoin nel 2014 ..... *36*
2.6.2. Bitcoin nel 2015 ..... *37*
2.6.3. Bitcoin nel 2016 ..... *37*
2.7. La quarta fase di Bitcoin (2017 - 2019) 37
2.7.1. Bitcoin nel 2017 ..... *37*
2.7.2. Bitcoin nel 2018 ..... *39*
2.7.3. I motivi del crollo *40*
2.7.4. Il Bitcoin nel 2019 ..... *42*
3 – La Blockchain 43
3.1. Fondamenti teorici della Blockchain 43
3.1.1. Cenni sulla crittografia *43*
3.1.2. L'apporto di Wei Dai *43*
3.1.3. Hashcash *44*
3.2. La Blockchain in Bitcoin 46
3.2.1. Definizione di Blockchain *46*
3.2.2. La difficoltà della Blockchain *46*
3.2.3. Le transazioni *46*
3.2.4. La funzione della Blockchain in Bitcoin *48*
3.2.5. Il mining *48*
3.3. Applicazioni della Blockchain al di fuori di Bitcoin 50
3.3.1. Altre tipologie di Blockchain *50*

3.3.2. Prospetto generale sull'utilizzo della Blockchain *51*
3.3.3. La Blockchain nel settore finanziario *52*
3.3.4. La Blockchain nel settore IP *54*
3.3.5. La Blockchain nella gestione d'impresa *54*
3.3.6. La Blockchain nel settore sanitario *55*
3.3.7. La Blockchain nel settore alimentare *56*
4 – Prospettive future 57
4.1. Il futuro delle criptovalute sul mercato 57
4.1.1. Il futuro di NEO *58*
4.1.2. Il futuro di Ethereum *59*
4.1.3. Il futuro di Ripple *59*
4.2. Il futuro di Bitcoin 60
Conclusione 62
Riferimenti sitografici 63
1 – Le Criptovalute 63
1.2 63
1.3 63
2 - La nascita di Bitcoin 65
2.1 65
2.2 65
2.3 65
2.4 66
2.5 66
2.6 66
2.7 66
3 - La Blockchain 67
3.1 67
3.2 67
3.3 67
4 - Prospettive future 69

Introduzione

La rivoluzione digitale e informatica ha rivoluzionato molti aspetti della vita dell'essere umano, comprese economia e finanza. Oggi viviamo in un'epoca di

grande cambiamento, colma di scoperte tecnologiche che favoriscono continue innovazioni in ogni settore economico. In questo contesto, una delle novità più interessanti dell'ultimo decennio riguarda l'evoluzione dei sistemi di pagamento e, in particolare, le soluzioni legate all'informatica, come le criptovalute. Queste, infatti, hanno catturato un interesse da parte del pubblico sempre maggiore a partire dal 2008, anno in cui il misterioso Satoshi Nakamoto lanciò il sistema Bitcoin.

Da allora, Bitcoin è cresciuto molto arrivando a valere, dicembre 2017, più di 18,000€ per token, e diventando, tempo prima, un esempio illustre di crittografia. Questo è testimoniato anche dal fatto che, dopo Bitcoin, sono nati numerosi altri sistemi di criptovalute basati su meccanismi simili: Ripple, Ethereum e NEO, solo per citarne alcuni tra i più famosi, hanno sconvolto il mercato delle valute virtuali, pur non potendo ancora essere paragonati a Bitcoin in quanto a importanza e valore di mercato. Nel corso del tempo, molti colossi dell'economia mondiale hanno deciso di accettare pagamenti in criptovalute, come ad esempio Apple e Wordpress.

L'elaborato punta a tracciare quella che è stata la storia del sistema Bitcoin nel corso del suo primo decennio di vita e dell'importanza che oggi riveste la tecnologia alla base del sistema: la Blockchain. È stato scelto di suddividere il lavoro in quattro parti: nella prima, si effettuerà una panoramica dell'ambiente delle criptovalute, analizzando le cause e le conseguenze del loro utilizzo, come la legislazione italiana ed europea hanno reagito al fenomeno e analizzando in breve le criptovalute più stimate dal mercato mondiale; la seconda parte riguarda la storia di Bitcoin, a partire dai primi cenni storici riguardanti l'idea di un sistema decentralizzato e anonimo dei pagamenti e dai primi tentativi di realizzazione dello stesso fino all'exploit del 2017 che lo ha reso famoso in tutto il mondo e al conseguente crollo dell'anno successivo; infine, la terza parte riguarda la Blockchain, tecnologia fondamentale per il funzionamento dell'intero sistema, a partire dalle teorie cripto-anarchiche e al suo funzionamento in Bitcoin, per arrivare alle applicazioni di maggior successo di questa tecnologia al di fuori dell'ambiente cripto-valutario.

In chiusura, seguiranno delle brevi considerazioni personali, coadiuvate da dati di riferimento, di quelle che sembrano essere le criptovalute più interessati sul mercato (incluso, ovviamente, Bitcoin) in riferimento agli scenari futuri.

1 – Le criptovalute

1.1. Cos'è una criptovaluta

1.1.1. Definizione teorica di criptovaluta

Una criptovaluta è una valuta digitale e paritaria che non viene emessa da nessuna banca centrale, la cui implementazione avviene su base crittografica, al fine di convalidare le transazioni e di generare token. La rete sulla quale sono generate e trasferite le criptovalute è, generalmente, una rete *peer-to-peer*, ovvero una rete che non possiede nodi gerarchizzati (cioè nodi *client* o nodi *server*), ma un numero indefinito di nodi equivalenti tra loro, ciascuno dei quali può fungere da *client* o da *server* nei confronti degli altri nodi, in modo che ogni nodo sia in grado di avviare o completare una transazione. Solitamente, le regole di emissione delle criptovalute sono basate su un algoritmo *open source*, ovvero su un programma informatico aperto e pubblico che contiene le istruzioni del sistema.

1.1.2. Punti di forza e di debolezza delle criptovalute

I vantaggi di usare una criptovaluta rispetto alle monete sovrane riguardano principalmente i seguenti aspetti:

- Finanziario: a differenza degli scambi monetari o tra valute centralizzate, le criptovalute non presentano generalmente costi di transazione dovuti agli scambi effettuati;
- Politico: non essendo assoggettate a nessun ente politico, poiché decentralizzate, si gode di piena libertà delle criptovalute che si possiedono, si gode di privacy nel corso e al termine degli scambi (variabile a seconda della criptovaluta di riferimento, ma comunque generalmente più alta della privacy di altre valute centralizzate, fatta eccezione per gli scambi in contanti), non è possibile l'intromissione di enti politici (come ad esempio per interventi di *bailout* o per il controllo dell'inflazione);
- Pratico: il principale vantaggio pratico di possedere criptovalute è che si ha la certezza dell'impossibilità di falsificazione;
- Trasparenza: a differenza della moneta, che è anonima e non rintracciabile, dopo esser stata scambiata, le criptovalute godono di pseudo-anonimato, ovvero a ogni operatore corrisponde uno pseudonimo con il quale viene registrato per ogni transazione effettuata, questo fa in modo che tutti gli scambi effettuati attraverso bitcoin siano rintracciabili, anche se l'identità delle parti resta nascosta, appunto, da pseudonimo. Questo garantisce che una persona non ceda più di quanto possegga.

I rischi legati all'uso e al commercio di criptovalute sono vari e, principalmente, sono i seguenti:

- Perdita delle credenziali di accesso al proprio wallet, in quanto questi wallet generalmente custodiscono un ammontare non indifferente di criptovalute e sono, per ciò, protetti da password molto complesse, la cui perdita implica l'irreversibile perdita del portafoglio stesso;

- Sono documentati molti casi in cui i possessori di criptovalute hanno subito attacchi da parte di *hacker*[1];
- Alta volatilità: pur non essendo intrinsecamente uno svantaggio, l'alta volatilità è giudicata molto negativamente dal mercato; l'investimento in criptovalute può generare alti profitti e altrettanto alte perdite, in quanto il loro valore di cambio è pesantemente influenzato da fattori esterni (annunci di regolamentazione, divieti di utilizzo in alcuni stati, …);
- Bassa liquidità: sebbene la liquidità delle criptovalute non sia stata sempre un problema nella storia delle criptovalute, in quanto la domanda è spesso alta, ci sono stati periodi in cui la liquidità è stata molto bassa.

1.1.3. Le criptovalute possono essere definite "monete"?

Rispondiamo subito: no; le criptovalute non possono essere definite come monete digitali. Questo in quanto per moneta elettronica si intende «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento … e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica»[2]. In altri termini, la moneta elettronica deve avere i seguenti requisiti:

- Ci deve essere la presenza di un valore monetario;
- Questo valore deve essere memorizzato elettronicamente e rappresentare un credito verso l'emittente;
- Il valore deve essere stato emesso per consentire operazioni di pagamento (versamento, trasferimento o prelievo di fondi);
- Questo valore rappresenta un credito verso un soggetto emittente (Banca o IMEL[3]);
- Il valore deve essere convenzionalmente accettato, come mezzo di pagamento, da persone diverse dall'emittente (con un potenziale di spendibilità per una serie illimitata di beni o servizi presso una serie illimitata di operatori).

  Un esempio di moneta elettronica può essere una carta prepagata rilasciata da una Banca o da un IMEL. In conclusione, le monete elettroniche sono una rappresentazione digitale delle valute tradizionali a corso legale, come euro, dollari, et cetera.

  Le criptovalute, invece, sono «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»[4], dunque possiamo notare che per le criptovalute manca la caratteristica di titolo di credito nei confronti di un terzo soggetto; inoltre, i soggetti che emettono (in gergo, i *miner*[5]) criptovalute

[1] L'hacker è una persona che trae piacere nell'esplorare i dettagli dei sistemi programmabili e sperimenta come estenderne l'utilizzo, nel mondo dell'informatica viene spesso utilizzato con accezione negativa come una persona che sfrutta debolezze di alcuni programmi per trarne guadagno o per causare problemi a chi gestisce tali sistemi.
[2] Ex art. 2, n. 2, Direttiva 2009/110/CE; seconda direttiva IMEL
[3] Istituto di Moneta Elettronica.
[4] Ex D. Lgs. 25 maggio 2017, n. 90
[5] I miner sono coloro che registrano ogni blocco alla Blockchain, confermando le transazioni attraverso il loro lavoro, in cambio dell'ottenimento di un premio in BTC una volta convalidato il blocco.

non rientrano nelle categorie di soggetti a cui è riservata e riconosciuta per legge l'emissione di moneta elettronica ex art. 114-bis, Testo Unico Bancario. In caso di rapporti di credito-debito, se non diversamente specificato, il creditore non è quindi legalmente vincolato ad accettare una criptovaluta come strumento di pagamento, pur essendoci, ovviamente, la possibilità di accettarla.

1.2. Criptovalute e riciclaggio

1.2.1. Le normative antiriciclaggio

Dalla nascita dell'UE fino a oggi, gli organi competenti comunitari e nazionali si sono mossi per sfavorire le pratiche, considerate ovviamente illegali, di riciclaggio. La I^{a} Direttiva antiriciclaggio risale al 1991, fu pubblicata dalla CE e riguardava obblighi di identificazione, segnalazione e registrazione di qualunque operazione finanziaria sospetta, a carico di enti creditizi e finanziari; la IIa Direttiva antiriciclaggio venne pubblicata dieci anni più tardi, nel 2001, e allargava la competenza di tali obblighi anche ai professionisti; la III^{a} Direttiva, risalente al 2005, applicò al terrorismo le metodologie e gli obblighi già in vigore contro il riciclaggio; la IV^{a} Direttiva, infine, nel 2015, seguì le raccomandazioni del Gruppo d'Azione Finanziaria Internazionale (GAFI) e introdusse novità di sistema, come ad esempio la presenza di controlli ai movimenti finanziari di personaggi politici, la criminalizzazione di reati fiscali e l'istituzione di un registro nazionale degli effettivi beneficiari di transazioni sospette. Il quadro antiriciclaggio al 2016, dunque, era rappresentato da due strumenti giuridici: la quarta Direttiva UE 2015/849, (recepita dall'Italia con il d.lgs. n. 90/2017) e il Regolamento sui trasferimenti di fondi 2015/847, adottati il 20 maggio 2015.

1.2.2. Pericolo criptovalute: La V^{a} Direttiva antiriciclaggio

Il 3 Aprile 2016 sono stati pubblicati i c.d. *Panama Papers*, ovvero un corposo fascicolo di oltre 11 milioni di documenti che contengono informazioni dettagliate su oltre 200mila società offshore e relativi organigrammi. Il nome di questa inchiesta è dovuto allo studio legale *Mossack Fonseca*, che ha sede a Panama per l'appunto. Questo studio riportò nomi e somme di denaro di personaggi pubblici, politici e di soggetti attivi nel campo dell'economia privata e della finanza, compresi manager italiani, i quali dovranno rispondere dell'accusa di evasione fiscale. I dati raccolti iniziano dal 1970 e arrivano al 2015. Oltre 400 giornalisti, attivi in più di 80 paesi, hanno analizzato il fascicolo.

Già prima di ciò, tuttavia, gli organismi e le autorità nazionali e internazionali di tutto il mondo avevano iniziato a porre la loro attenzione sulle valute virtuali, che permettevano una negoziazione pseudo-anonima priva di ogni intermediazione da parte di enti controllati dalle suddette autorità; la preoccupazione maggiore riguardava, appunto, il riciclaggio e il finanziamento al terrorismo. Il GAFI pubblicò, nel giugno 2014 un report chiamato *Virtual Currencies – Potential AML/CFT risks*, nel quale auspicava un intervento delle istituzioni europee a riguardo dei rischi potenziali che le criptovalute potessero portare al sistema economico-finanziario europeo e mondiale.

Il mese successivo, anche la European Banking Authority (EBA) pubblicò un report dal nome *Opinion on virtual currencies,* nel quale individuava i rischi che potesse portare la negoziazione di criptovalute per utilizzatori, partecipanti al mercato,

integrità e stabilità del sistema nel suo complesso. Il fine del documento redatto dall'EBA era identico a quello del GAFI: entrambi chiedevano a gran voce un intervento delle istituzioni al fine di regolare l'utilizzo di criptovalute.

In Italia si pronunciarono su questo argomento sia Banca d'Italia che l'UIF[6]. Banca d'Italia guardava soprattutto ai rischi per gli operatori da essa vigilati in considerazione a una potenziale violazione della riserva di legge sulla raccolta del risparmio e sui servizi di pagamento. L'UIF, invece, pubblicò il documento *Utilizzo anonimo delle valute virtuali*, in cui si evidenziava l'effetto che le criptovalute potessero avere sul riciclaggio e sul finanziamento del terrorismo, effetto causato dall'anonimato e dall'operatività online e decentralizzata.

A seguito di ciò, la Commissione presentò, nel luglio 2016, una nuova proposta al fine di rafforzare il quadro normativo vigente riguardo all'antiriciclaggio e di garantire una maggiore trasparenza finanziaria. Questa proposta è stata a lungo discussa e si è concretizzata, poi, nella V^{a} Direttiva antiriciclaggio, per la quale, a causa della particolare gravità dei rischi che ne hanno spinto la nascita, se ne chiedeva il recepimento entro un termine massimo di 18 mesi, a differenza dei soliti due anni. Questa direttiva mirava a chiarire e regolare diversi punti riguardanti l'utilizzo di piattaforme online e di valute "alternative", in particolare:

- Regolamentazione contro i rischi di finanziamento del terrorismo attraverso l'inclusione delle piattaforme di scambio di valute virtuali (piattaforme di *exchange*) e dei servizi di portafoglio digitale (*e-wallet*), i quali avrebbero dovuto applicare gli obblighi di verifica della clientela alle operazioni, ponendo di fatto fine all'anonimato. In corso di stesura, venne fatta particolare menzione anche degli attacchi informatici degli hacker ai portafogli elettronici e della possibilità di smarrimento delle chiavi crittografiche personali e segrete necessarie per accedere ai portafogli;
- Rafforzamento dei poteri delle UIF dell'UE e l'implementazione della cooperazione con Autorità a livello nazionale e internazionale, tramite ampliamento della gamma di informazioni, rendendo accessibili al pubblico i registri di titolari effettivi di società e trust, anche passivi, con conseguente armonizzazione della regolamentazione sui reati tributari, criminalizzati dalla IV^{a} Direttiva ma caratterizzati da soglie diverse nei vari paesi membri;
- Un'interconnessione comunitaria di informazioni su società e trust e una centralizzazione nazionale sui beneficiari effettivi di conti bancari e cassette di sicurezza, per garantire sicurezza agli investitori ed evitare l'occultamento di attività criminali. Questi registri dei beneficiari effettivi sono stati estesi a tutti i trust e agli istituti giuridici affini, rendendo disponibili tali informazioni al pubblico e a qualunque persona fisica o giuridica che possa dimostrare un legittimo interesse (dunque anche autorità fiscali, di vigilanza, di antiriciclaggio, organi giudiziari, et cetera);
  Tale direttiva dovrà essere recepita entro il 10 Gennaio 2020.

[6] Unità di Informazione Finanziaria.

1.2.3. Perché le criptovalute sono collegate al riciclaggio

Abbiamo già spiegato come lo pseudo-anonimato e la mancanza di intermediazione rendono le criptovalute un pericolo. Tuttavia, perché preferirle al contante? La risposta a questa domanda sta nella grande facilità e velocità di spostamento, minore per le brevissime distanze, ma sicuramente significativa se si pensa a scambi internazionali, e nello pseudo-anonimato che, seppur non garantisce un anonimato completo come il contante, è quasi comparabile.

1.3. Le principali criptovalute oltre a Bitcoin

1.3.1. Gli Altcoin

Il Bitcoin ha dato via a un trend che ha causato la nascita di molte altre criptovalute, le quali prendono il nome di *altcoin*. Generalizzando, si può dire che la maggior parte di loro si presentano come varianti di Bitcoin (in quanto spesso sono ottenuto attraverso modifiche del codice dello stesso) con elementi di differenza che rispetto in un'ottica di perfezionamento della criptovaluta.

Rispetto a Bitcoin, la maggior parte delle altre criptovalute sono più facili da ottenere (sia acquistandole, sia attraverso il mining), ma presentano dei lati negativi: hanno una minore liquidità, sono meno accettate per i pagamenti e hanno una volatilità più alta.

Si stima ci siano oltre 1.600 criptovalute sul mercato e ognuna di loro ha una sua nicchia di mercato, pertanto è difficile compilare una lista che risulti oggettiva e completa riguardo ciò. Inoltre, è difficile dare un valore che sia "di mercato" alle varie criptovalute: l'approccio dominante tra gli analisti è di tipo relativo, ovvero si mettono in relazione tra loro i prezzi delle varie criptovalute e si misura l'andamento relativo di una valuta rispetto a un'altra o rispetto a un indice (che spesso viene definito come media tra più valute). Secondo questo approccio, sono presentate di seguito le criptovalute più importanti fatta eccezione per Bitcoin. I dati relativi alle criptovalute sono, per natura dinamici, per tanto quando ritenuto conveniente verranno utilizzate medie di breve periodo piuttosto che dati precisi, in quanto quest'ultimi potrebbero essere fuorvianti. Per quanto si cerchi di dare un range ai valori osservati, piuttosto che un dato preciso, l'alta volatilità delle criptovalute può far sì che tali valori cambino in modo radicale e repentino anche a distanza di poche ore. I dati quantitativi presentati in questo capitolo sono raccolti da CoinMarketCap, che segue l'andamento delle criptovalute sul mercato in tempo reale e si riferiscono alla prima metà del mese di aprile 2019.

1.3.2. Litecoin (LTC)

Litecoin nasce nel 2011 e fa parte della prima ondata di criptovalute che è seguita a Bitcoin. Venne definita dallo stesso creatore come l'argento delle criptovalute, con riferimento proprio a Bitcoin, che sarebbe in questa metafora l'oro. LTC è basata su un network di pagamenti globali open-source non controllato da alcuna autorità centrale e viene emesso grazie alle procedure di mining, che, come per Bitcoin, implicano la risoluzione di problemi matematici; in particolare, ogni blocco della catena, generato dal network ogni 2,5 minuti, garantisce a colui che lo risolve 50 litecoin. Il numero di Litecoin in circolazione è stato fissato al momento della sua creazione ed è pari a 84 milioni.

Il Litecoin ha un tasso di cambio effettivo con l'euro e con il dollaro statunitense e questo ha permesso alla criptovaluta di avere molto successo in paesi come Olanda, Repubblica Ceca, Finlandia e Russia.

Avendo il Litecoin, rispetto al Bitcoin, un limite di circolazione più alto (84 milioni contro 21 milioni), è intuitivo che i tempi di mining sono minori nella stessa proporzione: se per Bitcoin ci vogliono 10 minuti per generare un blocco, a Litecoin ne bastano 2,5, dunque la conferma delle operazioni risulta essere più rapida. Un'ulteriore differenza riguarda l'algoritmo utilizzato: Litecoin utilizza, infatti, l'algoritmo Scrypt, una funzione sequenziale memory-hard, la quale richiede più memoria.

La quotazione massima raggiunta da Litecoin è stata 300$, raggiunta nel dicembre 2017, a cui è seguito un calo. Il prezzo registrato tra marzo e aprile 2019 oscilla tra gli 85$ e i 95$.

1.3.3. Ethereum (ETH)

Ethereum, nata nel 2015, fa parte della seconda ondata di criptovalute, successiva a quella di Litecoin ed è stata definita da molti come un un'avanguardia nel campo delle criptovalute risultando, a prova di ciò, uno dei mercati crittografici con più alta capitalizzazione. Si basa su un programma il cui input è dato da nodi validatori di una Blockchain, sulla quale questi devono trovare consenso attraverso un algoritmo che garantisca il rispetto delle regole del protocollo e il cambiamento di stato che il programma opera sulla catena. Così come BTC ed LTC, anche Ether, il token di Ethereum, viene rilasciata ai miner attraverso la convalidazione delle transazioni.

Il funzionamento pratico di Ethereum è quello di garantire il funzionamento dei cosiddetti *smart contracts*, "contratti intelligenti", attraverso la sua criptovaluta. Questi contratti per funzionare devono pagare la potenza di calcolo della rete attraverso il token Ether, che funziona come una specie di carburante per Ethereum. Questi contratti, che sono in realtà un linguaggio di programmazione eseguito internamente alla rete, funzionano in modo indipendente e sono utilizzati per molte operazioni diverse tra loro, come ad esempio registrazione di domini e realizzazione di piattaforme di crowfunding. La loro indipendenza è dovuta al fatto che ogni contratto è indipendente dagli altri e contiene le regole per il suo stesso funzionamento, che avviene dunque in modo automatico seguendo la legge iscritta nel codice.

Quello del sistema Ethereum è uno dei mercati crittografici più apprezzati dagli investitori, nonostante il possesso della moneta a fini speculativi (come accade per le altre criptovalute) sia solo uno dei fini del sistema: questa sua duttilità rappresenta il principale punto di forza rispetto a Bitcoin. Il mercato di Ethereum è relativamente giovane, ma è in rapidissima crescita: il massimo storico del valore per token è stato raggiunto nel gennaio 2018, pari a 1300$; successivamente è calato fino a stabilizzarsi tra i 100$ e i 150$ a inizio 2019, mentre la capitalizzazione totale è di circa 12 miliardi.

Nel 2018, Ethereum ha chiuso in seconda posizione nel mercato delle criptovalute, dopo Bitcoin, riuscendo a superare Ripple, un'altra importante criptovaluta che occupava precedentemente il secondo posto. Alcuni analisti, infine, stimano che a

causa del maggiore potenziale, un giorno Ethereum possa superare addirittura il leader di mercato, Bitcoin.

1.3.4. Zcash (ZEC)

Lo Zcash è una delle criptovalute più giovani, il cui lancio risale alla fine del 2016. Per definirsi, lo stesso sistema ha utilizzato un paragone informatico con Bitcoin, ovvero «If bitcoin is like http for money, zcash is https», in cui la "s" sta per *securtiy*. Infatti, la principale novità introdotta da Zcash è un anonimato del 100%, quindi rappresenta, per chi la utilizza, privacy e trasparenza selettiva delle transazioni.

Tale anonimato viene raggiunto attraverso l'omissione di alcuni dettagli riguardanti le transazioni all'interno della Blockchain; in particolare, a differenza delle criptovalute già trattate che utilizzano un meccanismo di pseudo-anonimato attraverso l'uso di *nickname*, Zcash offusca completamente mittente, transazione e destinatario. Tale privacy, comunque, è facoltativa.

Questo è reso possibile dalla *Zero Knowledge Proof*, "dimostrazione senza conoscenza", cioè la tecnologia sul quale si basa il funzionamento di Zcash. Ciò rende possibile l'omissione delle informazioni che, altrimenti, andrebbero rivelate per convalidare le transazioni (come accade nella Blockchain del sistema Bitcoin), permettendo una conferma da parte del sistema senza che nessun dettaglio sia mai rivelato. Questa tecnologia utilizza la sigla Zk-Shark e viene considerata uno degli apici della crittografia, in quanto rende possibile stilare un registro che garantisca contemporaneamente privacy e sicurezza.

Questo rende il mining di Zcash completamente diverso da quello delle altre criptovalute. La capacità di estrazione dello Zcash non dipende infatti dalla potenza di calcolo dei processori, bensì dalla RAM presente all'interno del proprio computer, rendendola "minabile" anche da computer meno potenti. La quantità circolante di Zcash è pari a quella del Bitcoin, ovvero 21 milioni di unità.

Il prezzo di Zcash è cresciuto, nel 2017, del 440%, registrando così una performance superiore a quella di altre criptovalute più celebri. Il suo massimo storico è stato di ben 3'192$, valore registrato nell'ottobre del 2016, solo un giorno dopo il suo lancio. Attualmente, ad aprile 2019, il suo valore oscilla tra i 65$ e i 75$, mentre la sua capitalizzazione è pari a 451 milioni di dollari circa.

1.3.5. Dash

Dash nasce da una modifica del codice già utilizzato per i Bitcoin, ma con l'aggiunta di nuove funzionalità; il nome viene dalla crasi della locuzione *Digital Cash*. La criptovaluta era nota inizialmente come XCoin, ma diventò famosa con il nome di Darkcoin. Nacque nel 2014 con l'obiettivo di essere il successore e, contemporaneamente, un'alternativa a Bitcoin: questo perché, essendo definito come Digital Cash dai suoi stessi creatori, si propone come un vero e proprio contante digitale da sostituire alle monete sovrane; questo avviene grazie a una piattaforma di sviluppo di denaro elettronico per scambi di tipo peer-to-peer completamente open-source, che si avvale di un sistema che rende le transazioni molto più veloci e con costi di transazione perfettamente trascurabili rispetto al sistema Bitcoin.

La rete di Dash si articola su due livelli: sul primo livello, la creazione di nuovi blocchi viene gestita dai minatori, mentre il secondo livello della rete è gestito dai *masternode*, strumenti che portano a termine vari compiti attraverso l'esecuzione di funzioni di governance. Tali compiti hanno un costo e, pertanto, ai *masternode* è garantito un premio definito in percentuale del premio di blocco. Sulla piattaforma esistono due tipi di transazioni:

- *InstantSend*: sono transazioni istantanee i cui input possono essere bloccati su specifiche transazioni e controllati attraverso una verifica del livello *masternode* della rete;
- *PrivateSend*: viene definito come un servizio di *coin-mixing*[7] incentrato su CoinJoin (un metodo che prevede un'unica transazione collettiva invece che più transazioni singole per garantire un livello più alto di privacy); per questo tipo di transazioni, è previsto un cap di mille Dash. La privacy degli utenti su questa rete è più alta rispetto agli standard in quanto il sistema PrivateSend mescola le criptovalute attraverso i *masternode* e rende impossibile il tracciamento di una transazione dalla sua fase iniziale a quella finale.

In conclusione, possiamo affermare che Dash garantisce un sistema di transazioni molto più rapido (a livello di tempistiche parliamo di tempi inferiori al secondo per confermare una transazione, mentre Bitcoin impiega alcuni minuti), con una privacy leggermente più estesa e con tasse di transazioni minime.

Il massimale circolante di Dash è fissato a 18,9 milioni e verrà raggiunto soltanto nel 2030. La remunerazione per blocco è variabile e diminuisce del 7,1% ogni anno, con un tempo medio di estrazione del blocco pari a 2,5 minuti.

La capitalizzazione di mercato di Dash oggi si attesta intorno a 1 miliardo di dollari. La quotazione di ogni singolo Dash è partita, come molte criptovalute, a un valore vicino a 1€, alzandosi in seguito, ma senza mai superare i 15€. Successivamente, la quotazione ha iniziato a lievitare a causa di un crescente numero di utenti interessati, aumentando di pari passo le transazioni: il prezzo di un token ha raggiunto quota 100€ per Dash nel marzo 2017. Nei mesi successivi si sono registrate rapide e ampie oscillazioni di prezzo, fino a quando non è iniziato un trend rialzista che ha fatto raggiungere a Dash una quotazione di 464€ a novembre dello stesso anno. Solo un mese dopo, il 20 dicembre, ha raggiunto la sua massima quotazione pari a 1494$. Il prezzo, attualmente, si aggira in un intorno di 130$.

1.3.6. Ripple (XRP)

Ripple è una criptovaluta nata nel 2013 e rappresenta, insieme al progetto Ethereum, la fonte principale di competizione nei confronti del Bitcoin, posizione avvalorata dalle stesse affermazioni dei suoi creatori, che sostengono di voler superare i punti di debolezza di Bitcoin. L'idea di base di Ripple è quella di un sistema monetario peer-to-peer che punta a eliminare o abbassare i costi di intermediazione finanziaria (ad esempio quelli applicati da banche o carte di credito). La rete Ripple opera su una piattaforma decentralizzata e su una rete open-source e le sue transazioni sono istantanee, gratuite e irreversibili.

[7] Un sistema simile a una gestione collettiva di fondi.

Un'importante differenza tra XRP e BTC è data dalla presenza dei *ledger*, ovvero registri di transazione che permettono di monitorare gli scambi e completare le transazioni nel giro di pochi secondi, garantendo un grado di maggiore trasparenza e di maggiore rapidità. Attraverso la rete Ripple è, inoltre, possibile trasferire pagamenti senza continuità di forma, permettendo al beneficiario di ricevere dollari anche se la transazione è stata fatta in euro.

È possibile vedere la rete Ripple come una versione più moderna dell'attuale sistema di intermediazione finanziaria: il paragone nasce dalla fiducia di base che dà valore tanto alle monete sovrane quanto alla valuta Ripple. In particolare, tale rete si compone di tre parti: un network di pagamenti, una borsa propria e la già citata valuta.
Il network di pagamento funziona attraverso dei crediti IOU (*I Owe You)*, che rappresentano le monete reali e sono ciò che di fatto viene scambiato sulla rete, valutate sulla base di valuta XRP. Se A deve pagare B in USD ma ha soltanto EUR, il destinatario compra l'IOU in euro pagando XRP e vende IOU in dollari ricevendo altrettanti XRP.

Il quantitativo massimo di Ripple in circolazione è pari a cento miliardi di unità ed è già stato raggiunto; inoltre, la distribuzione è affidata a OneCoin, la società che ha ideato la rete e non è prevista distribuzione tramite mining. Il market cap attuale è di circa 14 miliardi, con un valore per XRP pari 0,33$ circa. Il massimo valore raggiunto da XRP è stato di 1.93$, nel dicembre 2017.

1.3.7. Monero (XMR)

Monero nasce nell'aprile 2014 con il nome di BitMonero e, come la maggior parte delle criptovalute, utilizza un sistema Blockchain completamente decentralizzato per validare le transazioni, molto meno trasparente ma garante di un livello superiore di privacy rispetto alla media. Il suo funzionamento si basa su un protocollo detto CryptoNote, un insieme di algoritmi che è stato elogiato anche da Van der Laan, un'autorità del settore e sviluppatore di Bitcoin Core.
Tale sistema si basa essenzialmente su tre misure:

- *Ring Signature:* la prima di queste tre misure serve a nascondere la provenienza dei soldi in una transazione effettuata con Monero e consiste nell'inserimento di ogni transazione all'interno di un gruppo di transazioni simili in modo che a un osservatore esterno risulti impossibile capire quale sia la chiave del mittente, essendo all'interno di un gruppo di chiavi;
- *Stealth Address:* la seconda misura tutela, invece, il destinatario della transazione attraverso la creazione, da parte del mittente, di un indirizzo casuale valido esclusivamente per la singola transazione. Questo fa sì che si ricevano soldi sempre su indirizzi diversi, ognuno noto solo al mittente e al destinatario della singola transazione;
- *Ring Confidential Transaction (RTC):* l'ultima misura è atta a nascondere l'importo scambiato. Grazie all'RTC il mittente inserisce come input il suo intero wallet e come output inserisce l'importo che desidera inviare e il restante importo del suo wallet, che riceverà come sotto forma di resto. In questo modo la transazione viene verificata attraverso l'equazione che lega la somma degli output all'input, provando così che non sono stati creati nuovi Monero. Tali informazioni non sono visibili ai

terzi.

La capitalizzazione di Monero è attualmente a circa 950 milioni di euro, con un prezzo per unità che si aggira intorno tra i 50€ e i 60€. Il suo massimo è stato raggiunto in data 7/1/2018 ed è pari a 440€.

1.3.8. Bitcoin Cash (BCH)

Bitcoin Cash nasce nell'agosto 2017 da una costola di Bitcoin e per volere dei suoi stessi sviluppatori, i quali ritenevano di poter riuscire a superare dei limiti di Bitcoin attraverso la creazione di questa nuova moneta. Questo provocò una rottura nel gruppo di sviluppatori di Bitcoin, in quanto solo alcuni volevano modificare alcune specifiche tecniche del software; questi si staccarono, dunque, dal gruppo originale e attraverso un *hard fork*[8] di Bitcoin fecero partire Bitcoin Cash. Al lancio, le opinioni degli investitori erano eterogenee: alcuni la ritenevano un'occasione di investimento importante, mentre altri erano del pensiero che fosse solo una mossa speculativa: nonostante tutto, esso raggiunse da subito un discreto successo.

Come le altre criptovalute, Bitcoin Cash è una valuta virtuale decentralizzata, che mira a risolvere principalmente due problemi del Bitcoin: quello dei *mining pool*, (ovvero il monopolio virtuale instaurato dai miners, che ha fatto perdere a Bitcoin, in alcuni periodi, la sua decentralizzazione) e quello riguardante la lentezza con il quale i blocchi venivano validati sulla catena. Quest'ultimo problema era causato dal limite di 1Mb come dimensione massima dei blocchi imposto dal codice per la catena di Bitcoin, il che permette un massimo di tre transazioni validate al secondo, creando un effetto a "collo di bottiglia" nella rete, che non solo provocava una lunga attesa per la validazione delle transazioni, ma lasciava queste completamente in mano ai miners, creando di fatto un monopolio virtuale. Furono proposte varie soluzioni, in quanto gli sviluppatori erano restii a creare una nuova criptovaluta, ma nessuna di queste sembrava risolvere il problema. Questa è stata definita come una «ideological battle over Bitcoin's future»[9], ovvero una battaglia ideologica, più che tecnica, sul futuro di Bitcoin.

La maggior parte degli sviluppatori volevano adottare una modifica chiamata SegWit, abbreviazione di *Segregated Witness*[10], che aveva come obiettivo il ripristino della decentralizzazione di Bitcoin, piuttosto che il conferimento di maggior potere nelle mani dei miners e sarebbe stata valida per circa il 10% delle transazioni totali su Bitcoin. Questo sarebbe avvenuto attraverso un alleggerimento delle transazioni causato dall'omissione di alcuni dettagli (come ad esempio le firme) e dalla possibilità di effettuare transazioni *off-chain*, al di fuori della Blockchain, in modo che non appesantissero i blocchi. In parallelo alla SegWit, era previsto l'aumento delle commissioni per traslare bitcoin, fino a 83 centesimi ad operazione (tali commissioni non sono obbligatorie, ma possono essere pagate dagli utenti per

[8] Un software costruito sulla base del codice originale di Bitcoin che divide da un certo punto in poi la Blockchain in due parti, in modo che su una parte siano validate le transazioni confermate da nodi non aggiornati alla nuova versione del protocollo, mentre sull'altra sono validate solo le transazioni confermate da nodi aggiornati.

[9] Oscar Williams-Grut e Rob Price, *A Bitcoin civil war is threatening to tear the digital currency in 2 — here's what you need to know*, BUSINESS INSIDER [26/03/2017]

[10] In italiano "testimone segregato".

velocizzare la transazione) e un raddoppio della capacità dei blocchi a 2 Mb. Ovviamente, i miners, erano in una situazione di profondo disaccordo rispetto alla SegWit, ma la proposta, denominata *BIP 91*, fu accettata. Questo gruppo di sviluppatori, che si è distaccato da Bitcoin era dell'opinione che quest'ultimo avesse tradito il suo ideale di democrazia, in quanto i mining pool erano in grado di detenere fino al 20% dei bitcoin in circolazione con la conseguenza di creare disparità di potere politico (direttamente proporzionale alla quantità di bitcoin detenuta) all'interno della Blockchain.

Questi, allora, decisero di distaccarsi e di creare BitcoinCash, che condivide con Bitcoin le specifiche tecniche riguardo all'algoritmo di hashing, alla proof of work, al numero massimo di monete e agli indirizzi. Le principali differenze riguardano invece una maggiore sicurezza per chi detiene BCH riguardo a situazioni di *re-play* e *wipeout* (ovvero rispettivamente, la replicazione di una transazione avvenuta in un ramo della catena su un altro ramo e la cancellazione di alcune transazioni effettuate su un ramo attraverso altre transazioni) e la presenza, sempre per quest'ultimo, di un mercato attivo basato su contratti futures, oltre a quella più importante, ovvero l'aumento della dimensione massima da 1Mb (o 2Mb nel caso di SegWit) a 8Mb. Inoltre, inizialmente chi possedeva Bitcoin possedeva lo stesso ammontare di Bitcoin Cash e questo è stato fondamentale per avere uno slancio iniziale; successivamente alla scissione, anche le due monete si sono divise permettendo ai possessori di effettuare transazioni separate.

La capitalizzazione di mercato di BCH, ad aprile 2019, è pari a 4.345.452.439€, mentre il suo prezzo si aggira tra i 240€ e i 250€. Il massimo valore per unità raggiunto è stato pari a 3.851,67€, registrato in data 20/12/2017.

1.3.9. Neo (NEO)

Neo, il cui nome nasce dal greco e significa "novità", è una criptovaluta nata nel 2014 con una mission ben precisa: quella di rivoluzionare l'economia attraverso la velocizzazione del passaggio alla *smart economy*. Precedentemente nota come Antshare, Neo è stata la prima Blockchain open-source cinese e il suo valore riuscì passare in pochissimo tempo da 1$ a quasi 48$ nel giro di soli tre mesi.

Viene spesso paragonata e contrapposta ad Ether (la già citata criptovaluta di Ethereum), in quanto essendo molto simile ne risulta essere il principale competitor. La moneta ha cambiato nome nel mese di giugno 2017, mese in cui ha apportato le principali modifiche alla Blockchain distaccandosi da una sostanziale somiglianza con Ethereum. Neo gestisce contratti intelligenti (già trattati nel paragrafo riguardante Ethereum) e identità digitali all'interno della sua piattaforma attraverso il pagamento in criptovaluta, pur vantando, nell'opinione degli stessi sviluppatori, una Blockchain superiore rispetto a scalabilità[11] e linguaggi di programmazione, in quanto Neo supporta i linguaggi informatici comuni come Microsoft.net, Java e Python, mentre Ethereum supporta solo un linguaggio non molto comune, Solidity, che richiede grandi capacità di programmazione (per altro, supportato anche da Neo). Un'altra importante caratteristica di Neo è che le operazioni possono essere, a scelta degli utenti, rese invisibili.

[11] La scalabilità è la capacità di una piattaforma di resistere ad aumenti di transazioni e in termini di compatibilità.

L’economia intelligente che Neo permette di sfruttare è possibile definirla come “implementata”, in quanto consente operazioni di scambio (tra criptovalute, con beni e servizi, ma anche con monete reali) basate su rapidità e sicurezza.

Il grande successo riscosso da Neo ha come base un’alta credibilità del team di sviluppo: mentre la maggior parte delle criptovalute fallisce perché durante la prima fase di *Initial Coin Offerings* (d’ora in avanti ICO) si espone sulla pre-vendita della moneta e sul valore potenziale, NEO ha lasciato parlare l’esperienza del suo team di suoi sviluppatori, i quali si sono sempre occupati di applicazioni tecnologiche nel mondo reale e risulta, per tanto, molto più affidabile di una “cambiale in bianco senza garanzia”, come vengono spesso definite le ICO o i *white paper* lanciati da potenziali truffatori.

La sua capitalizzazione di mercato è pari a oltre 6 milioni di euro, con un prezzo per unità che si aggira intorno ai 9,70€. Il suo punto di massimo è stato pari a 174,08€ in data 15/01/2018.

1.3.10. Cardano (ADA)

Cardano nasce nel settembre 2017 ed è stata creata dall’azienda di sviluppo Blockchain Input Output Hong Kong (IOHK) ma portata avanti da Charles Hoskinson, un co-fondatore di Ethereum. Egli stesso l’ha definita una criptovaluta di terza generazione, dopo Bitcoin ed Ethereum. Questa, infatti, riprende molto dal progetto Ethereum (che a sua volta non sarebbe stato possibile senza l’esistenza di Bitcoin) e ciò si può vedere già dalle funzioni designate come obiettivo del progetto, che rappresentano sostanzialmente un’implementazione delle funzioni della piattaforma di Ethereum.

Anche in questa piattaforma i token vengono estratti tramite il processo di mining, ma le decisioni sui blocchi della catena vengono prese sulla base di un algoritmo chiamato Ouroboros di tipo *proof-of-stake* e non *proof-of-work* come avviene per la maggior parte delle altre criptovalute: questo algoritmo consente di validare i blocchi basandosi sul voto dei possessori di ADA e all’interno di questo protocollo, i nuovi blocchi sono generati e verificati dagli slot-leader, titolo che può essere raggiunto da chiunque possegga ADA. Questo meccanismo ha permesso la creazione di una Blockchain più efficiente, rispetto a molte altre, in termini di costi e risorse, anche se perde a livello di sicurezza.

Mentre ADA opera sulla sua Blockchain, chiamata Cardano Settlment Layer (CSL), i contratti intelligenti e le applicazioni decentralizzate operano su un altro livello chiamato Cardano Computation Layer (CCL); questa architettura multistrato rende possibili gli aggiornamenti attraverso *soft-fork*, cosa che Ethereum non permette, in quanto nella sua architettura questi due livelli sono intrecciati e non separati.

Un altro obiettivo di Cardano, che lo pone come un progetto all’avanguardia anche nello stesso campo delle criptovalute, è la creazione delle *sidechain*, ovvero delle Blockchain secondarie da affiancare alla Blockchain principale, in modo da creare un sistema completamente decentralizzato che permetta di eseguire velocemente transazioni anche tra criptovalute, senza la presenza di broker o altri intermediari.

La capitalizzazione di mercato di Cardano è pari a circa 2 miliardi di euro, con un valore per unità che oscilla tra i 0,05€ e i 0,10€, dovuto all'alto quantitativo di token presenti sul mercato, circa 25 milioni, che sono poco più della metà del totale previsto, 45 milioni. Il prezzo più alto registrato sul mercato risale a 1,17€ registrato in data 04/01/2018.

1.3.11. Eos.io (EOS)

Eos.io rappresenta un progetto innovativo, la cui caratteristica principale è rappresentata da una semplificazione e, contemporaneamente, un'implementazione dell'esecuzione di *smart contract* e di applicazioni decentralizzate. Formalmente, Eos.io è una piattaforma Blockchain open-source che fornisce un OS per applicazioni decentralizzate focalizzate sul web, con servizi personalizzabili. Gli account degli utenti hanno un alto grado di personalizzazione e di protezione, con possibilità di condivisione (sia attraverso servizi cloud, sia attraverso server hosting) di database, con dati archiviabili anche al di fuori della Blockchain. Un altro importante servizio che offre la piattaforma è quello di scambi decentralizzati con fine ultimo l'eliminazione di ogni commissione.

EOS è una piattaforma sviluppata all'inizio del 2017 da Block One, una società condotta a Dan Lirmer e Brendan Bloomer, nomi noti nell'ambiente crittografico in grado di garantire esperienza concreta; EOS è stata resa disponibile da giugno 2018. Il protocollo utilizzato per validare le transazioni è di tipo proof-of-stake, in particolare è chiamato *delegated proof-of-stake* (Dpos), in quanto è un'evoluzione più sicura e contemporaneamente più snella del protocollo tradizionale. EOS non è minabile e il limite di circolante è stato fissato a 1 miliardo di token.

I suoi principali punti di forza riguardano la scalabilità (dovuta al protocollo Dpos) e la flessibilità, la quale permette di annullare una transazione, caratteristica molto utile in caso di furto o di errore; ma, quello che da molti è definito come il principale vantaggio di Eos.io è la facilità di uso della piattaforma, una delle più *user-friendly* nel campo delle criptovalute.

Tuttavia, il protocollo Dpos ha provocato a Eos.io forti critiche: molti accusano, infatti, il sistema di "elitarismo" nella convalidazione delle transazioni, rendendo di fatto fittizia la decentralizzazione. Questo accade perché il Dpos permette che a validare i blocchi sia solo un gruppo ristretto di utenti, che vengono eletti dalla rete in modo democratico, con potere politico degli utenti proporzionale al numero di token EOS detenuti. Questo fa sì che il vero potere decisionale della piattaforma sia in mano a pochi che gestiscono un grande quantitativo di token.

Un importante progetto portato avanti da Eos.io è chiamato *Everipedia*, che come suggerisce il nome stesso, riprende Wikipedia. Si tratta, cioè, di una enciclopedia libera (permessa dalla decentralizzazione dei contenuti della piattaforma), che impedisce il blocco ai cittadini da parte di paesi non sempre democratici: nella sua storia, l'enciclopedia gestita da WikiMedia Group è stata oscurata in vari paesi del mondo, integralmente o parzialmente (attualmente risulta oscurata in Turchia). Per quanto si possa essere o meno d'accordo sull'utilizzo del Dpos, bisogna dare atto a Eos.io di dare opportunità, se non infinite, quantomeno indeterminate, che possono

avere risvolti sociali e politici importanti, schierandosi su temi centrali dello sviluppo del mondo intero, come ad esempio, appunto, libertà di stampa e di espressione.

Attualmente, la capitalizzazione di mercato di EOS è di oltre 4 miliardi di euro, con un prezzo per token abbastanza volatile (ma da inizio 2019 in trend positivo) che si aggira intorno ai 4,20€. Il valore massimo raggiunto da EOS è stato di 20,24€ in data 29 aprile 2018.

1.3.12. Tether (USDT)

Tether è una criptovaluta molto particolare, che rientra nel contesto degli *stablecoin*, criptovalute ancorate a un valore stabile. Già l'abbreviazione, USDT, suona familiare: infatti, questa criptovaluta ha un rapporto di sostanziale parità con il dollaro, la cui sigla è USD, a cui si aggiunge la "T" di Tether. Questa criptovaluta esiste grazie al protocollo Omni, un software open-source che si interfaccia con la Blockchain legando il tether al dollaro. Anche Tether è una criptovaluta decentralizzata le cui transazioni sono permanenti, prive di commissioni e molto veloci rispetto a Bitcoin.

La principale caratteristica che distingue questa criptovaluta dalle altre è la stabilità: la sua oscillazione massima è stata inferiore ai 20 centesimi nell'arco di mesi ed è stabilmente ancorato alla soglia di un dollaro. Questo avviene perché la società che si occupa dell'emissione di tether, la Tether Limited, lo fa solo se ogni unità è coperta da un'unità di dollaro americano nelle proprie riserve, legando sostanzialmente la propria stabilità a quella del dollaro.

Il tether è utilizzato prevalentemente da utenti di piattaforme di exchange per uscire momentaneamente dalle fluttuazioni di criptovalute in momenti di alta tensione, senza bisogno di conversione delle stesse in valute ufficiali, oppure per trasferire fondi da una piattaforma a un'altra, in quanto non sempre le piattaforme accettano le stesse criptovalute. Le piattaforme stesse, talvolta, lo utilizzano al posto del dollaro per i conti dei clienti o per scambiare importi tra esse senza il bisogno di avere conti in moneta reale.

Poiché il valore della stessa deve restare costante, nei periodi di alta domanda, bisogna aumentare conseguentemente l'offerta, idem nel caso in cui la domanda si abbassi. Questo ha portato qualcuno a pensare che, forse, non tutte le emissioni sono coperte da riserve in dollari: la community degli investitori in criptovalute ha iniziato a sospettare di ciò successivamente a un rapporto anonimo diffuso sul web, il quale sostiene e dimostra che le maggiori emissioni di tether coincidano con la caduta dei prezzi dei bitcoin e che tali valute siano state utilizzate per acquistare proprio bitcoin a basso costo. Inoltre, l'aumento del valore di tether successivo a questa manovra si è registrato dopo l'arrivo di un grande quantitativo di tether nel wallet di Bitinfex, una piattaforma di exchange che condivide il CEO e il direttore generale con la Tether Unlimited.

L'attuale capitalizzazione di mercato di Tether è di oltre due milioni di euro, con un prezzo per token che si aggira intorno al dollaro (e quindi in euro si esprime solitamente attraverso al tasso di cambio EUR/USD). Il massimo raggiunto è stato di soli 1,09$, mentre il minimo è stato di 0,92.

1.3.13. Stellar Lumens (XLM)

Stellar Lumens è un progetto nato da un fork di Ripple, avvenuto nel 2017. La locuzione "Stellar Lumens" identifica l'intero sistema rete-criptovaluta, i cui nomi sono rispettivamente "Stellar" e "Lumen". Il network è indipendente dalla valuta ed è in grado di supportare le transazioni di qualsiasi tipo di valuta.

I principali vantaggi di questa valuta sono sicuramente la velocità di conferma delle transazioni (inferiore ai 5 secondi) e la grande mole di transazioni che si possono elaborare al secondo (al punto da essere stata paragonata a VISA, con la quale ha stretto una partnership[12]). I blocchi sono validati attraverso un protocollo chiamato *Stellar Consensus Protocol* (SCP) che non è del tipo POW e che esclude quindi il mining, così come accade per Ripple: questo protocollo prevede che ogni server cerchi di verificare la transazione e ciò accade solo quando i diversi nodi concordano sulla validità, ma non attraverso la fiducia dei server, bensì attraverso l'assunzione che dei server non stiano collaborando per validare transazioni false; la piattaforma, inoltre, permette la realizzazione di contratti intelligenti.

I lumen sono i token creati dalla piattaforma e hanno, all'interno di questa, una duplice funzione: la prima è quella di valuta d'intermediazione nello scambio tra diverse valute, la seconda è di disincentivare lo spam, in quanto per ogni transazione si paga una quota fissa di 0.01 XLM, impedendo così che il sistema si intasi con transazioni fittizie. Nel sistema sono stati creati circa 100 miliardi di lumen, di cui solo il 5% è detenuto dalla fondazione no-profit Stellar Lumens e il restante è stato distribuito ai proprietari di Bitcoin o Ripple, a chi ha aperto un account su Stellar o ad altre organizzazioni no-profit. Nuovi lumen sono immessi sul mercato a un tasso dell'1% annuo.

Attualmente Stellar è visto come un progetto ambizioso, ma con solide fondamenta, in quanto offre le commissioni più basse e le transazioni più veloci all'interno dell'intero mondo delle criptovalute. Tuttavia, ci sono dubbi sulla sua effettiva decentralizzazione, a causa del fondamentale ruolo che i *gateway* hanno nel sistema, ovvero terze parti che ricevono il denaro da parte dell'utente al momento dell'iscrizione e lo registrano come credito nel proprio account.

Attualmente, la capitalizzazione di Stellar è di quasi 2 miliardi di euro, con un valore per token pari a 0,10€ circa. Non è previsto un limite di circolante. Il valore più alto raggiunto è stato di 0,83€ in data 4/1/2018.

1.3.14. Binance Coin (BNB)

Binance Coin nasce nel 2017 insieme alla piattaforma Binance (il cui nome deriva dalla crasi tra *Binary* e *Finance*), dalla holding Beijie Technology, una società cinese con sede in Giappone, in seguito alla politica cinese avversa all'utilizzo delle criptovalute. Dal 2017 a oggi è cresciuta a ritmi impressionanti, fino a diventare una delle piattaforme exchange più attive, performanti e utilizzate nell'intero mercato mondiale.

[12] Michael del Castillo, *Visa-Backed Blockchain Firm Embraces Stellar Cryptocurrency Via Merger*, FORBES [28/9/2018]

La moneta BNB nasce come token della piattaforma, utile sia per pagare le commissioni delle transazioni, sia come mezzo di scambio nel passaggio da una valuta a un'altra (o da una criptovaluta a un'altra) nel corso di una transazione. Il principale vantaggio nell'utilizzo del token è che, se utilizzato per pagare le commissioni, offre su queste uno sconto (che è stato del 50% nell'anno di lancio, quota che si dimezza di anno in anno fino a diventare lo 0% nel 2022), quindi da molti utenti viene preferito in quanto permette di ottenere un valore maggiore a fronte dello stesso pagamento.

Il successo del token è dovuto, in realtà, al successo della piattaforma (che ad oggi si trova a gestire in alcuni periodi il maggior volume di scambi a livello mondiale), in quanto la maggior parte del suo funzionamento replica quello di Ether, il già discusso token di Ethereum, essendo basato anche sulla stessa Blockchain, in attesa dello sviluppo di una propria, nella fase iniziale. I Binance Coin non sono minabili, in quanto sono stati emessi e distribuiti al completo al momento del lancio a coloro i quali avevano contribuito alla ICO e agli investitori più importanti.

Attualmente un Binance Coin quota intorno ai 17€, con un trend fortemente rialzista nel 2019. La capitalizzazione totale di mercato ammonta a quasi 2.5 miliardi di euro, a fronte di un circolante di 150 milioni di token all'incirca. Non è previsto un limite al circolante, ma non essendo minabile spetta a Binance l'emissione dei token. Il valore massimo raggiunto da BNB è stato di 22.03€ in data 12/01/2018.

1.3.15. Una "classifica" delle criptovalute

Tutte queste criptovalute sono quelle che, attualmente, ricoprono le posizioni più alte nel mercato. In particolare, sempre secondo dati CoinMarketCap, la classifica per capitalizzazione di mercato delle criptovalute, ad aprile 2019, risulta essere la seguente:

1. Bitcoin
2. Ethereum
3. Ripple
4. Bitcoin Cash
5. EOS
6. Litecoin
7. Binance Coin
8. Tether
9. Stellar
10. Cardano

Con Monero, Dash e NEO che occupano rispettivamente la tredicesima, quattordicesima e sedicesima posizione.

2 – Il sistema Bitcoin

2.1. Introduzione su Bitcoin

Prima di procedere a un'analisi storica di quello che è stato, è tutt'ora e, secondo molte stime, sarà il Bitcoin, si ritiene necessario darne una definizione precisa. Il Bitcoin (sigla BTC) è una valuta virtuale che, differentemente dalle altre monete (come ad esempio l'Euro o il Dollaro US) ha una circolazione che non dipende da una Banca centrale; questa proprietà del Bitcoin, e di molte altre criptovalute, è detta "decentralizzazione". Il Bitcoin viene messo ufficialmente in circolazione nel 2009 da una persona (o più persone) che rispondono allo pseudonimo di Satoshi Nakamoto.

Il funzionamento di Bitcoin, che andremo ad approfondire ulteriormente nel corso dell'elaborato, si basa fondamentalmente su due princìpi: un network di nodi peer-to-peer e l'utilizzo di una crittografia complessa per validare e rendere sicure le transazioni.

Il valore del Bitcoin è passato da €0, alla data di lancio, fino ad arrivare a un valore massimo per-token di €17,932.61 (in data 17/12/2017). Nel momento in cui scriviamo, il suo valore si aggira intorno agli 8000$ per token, con una capitalizzazione di mercato di circa 140 miliardi di dollari. Il totale circolante massimo di token raggiungibile è pari 21 milioni, mentre attualmente esistono sul mercato 17,701,637 token di BTC.

Ma, di fatto, come si fa a possedere Bitcoin? «Per poter acquistare Bitcoin è necessario aprire un portafoglio/conto virtuale dopodiché occorre collegarsi ai numerosi siti che offrono la valuta virtuale in cambio di denaro (pagamento attraverso bonifico, carte ricaricabili). I Bitcoin possono essere scambiati o spesi (sono accettati da numerose attività commerciali sia virtuali che fisiche)»[13].

Come già analizzato nel precedente capitolo relativo alle criptovalute[14], l'utilizzo di Bitcoin ha dei pro e dei contro, rispetto alle monete sovrane; da una parte è una moneta che permette scambi a bassi costi di transazione, con l'impossibilità di falsificazione da parte di enti terzi, che permette un livello alto di privacy grazie a un meccanismo di pseudoanonimato e la piena proprietà del token stesso, non essendo assoggettato alle politiche di alcuna banca centrale. Dall'altro lato della medaglia, tuttavia, la volatilità di questa valuta è molto alta (tanto che il suo valore può dimezzarsi o raddoppiare nel giro di poche settimane) ed è possibile, inoltre, perdere l'intero wallet a causa di attacchi da parte di hacker o di perdita delle credenziali d'accesso.

Attualmente, a livello mondiale, è assente una corrente di pensiero univoca che porti all'armonizzazione della regolamentazione governativa riguardo al Bitcoin e alle altre criptovalute; in Italia la legislazione vigente è già stata trattata[15], ma ci sono anche altre correnti di pensiero al di fuori dell'UE: il governo cinese, ad esempio, ha proibito alle proprie banche di usare Bitcoin negli scambi interni per prevenire il

[13] *Bitcoin: cos'è e come funziona*, Borsa Italiana S.r.l. [08/01/2019]
[14] Sottoparagrafo 2.1.2.
[15] Paragrafo 2.2.

rischio di riciclaggio ed evitare l'instabilità finanziaria inevitabilmente connessa a essi, nonostante la Cina stessa, secondo Borsa Italiana S.r.l., sia il primo mercato mondiale di Bitcoin, con un terzo circa degli scambi totali al suo interno. Jerome Powell, attuale presidente della Federal Reserve, guarda positivamente al Bitcoin in una prospettiva di lungo termine in relazione a un sistema dei pagamenti più efficace, efficiente e sicuro, ammettendo tuttavia che attualmente la volatilità, dovuta alla mancanza di un valore intrinseco delle criptovalute, è un rischio rilevante di cui bisogna aver conto se si vuole utilizzare questo strumento[1].

2.2. L'era pre-bitcoin e la sua fondazione

2.2.1. La profezia di Milton Friedman

Nonostante si senta spesso definire Bitcoin come "la prima criptovaluta", ciò a livello cronologico non è del tutto vero: certo, è stata senz'altro la prima criptovaluta a utilizzare il sistema crittografico della Blockchain ed è stata la prima criptovaluta ad avere un successo così vasto, ma certamente non è stato il primo tentativo di creazione di un sistema che permettesse gli scambi in anonimato attraverso transazioni online.

A questo proposito, l'economista americano vincitore del premio Nobel per le scienze economiche, Milton Friedman, già dava un'opinione nel corso di un'intervista condotta da NTU / F nel 1999[16], nella quale dichiarò: «l'unica cosa che manca, ma che sarà presto sviluppata, è un sistema e-cash affidabile. Un metodo con cui acquistare su Internet e trasferire fondi da A a B, senza che A conosca B o B conosca A. Il modo in cui posso prendere da un conto 20 dollari e consegnarti a te senza tracciamento del punto di partenza. E tu puoi farlo senza sapere quale sia. Questa modalità di transazione si svilupperà su Internet»[17].

2.2.2. Prima applicazione di moneta digitale: il caso di David Chaum

Il primo a parlare di monete digitali, tuttavia, è stato David Chaum nel lontano 1983. Lo studente, all'epoca ventottenne, pubblicò un paper in quell'anno in cui descriveva la "digital money" come mezzo di pagamento, la cui differenza sostanziale dalle carte di credito consisteva dell'anonimato. Nella sua idea, questo consentiva alla banca di sapere che due persone si sono scambiate un certo importo di denaro, ma senza sapere per cosa fosse stato usato.
La valuta a cui pensava Chaum non sfruttava la tecnologia Blockchain, ma era scambiata attraverso un meccanismo simile a quello con cui avvengono le elezioni: la tessera elettorale, che garantisce il diritto di accesso è assimilabile a una firma virtuale, mentre la transazione è rappresentata dalla scheda elettorale. In questo modo si è certi che chi ha condotto l'operazione ne aveva il diritto, ma al contempo, non si sa come abbia speso quei soldi.
Dunque, allo stesso modo in cui i voti vengono scrutinati, l'ente che gestisce il sistema di pagamenti riceve l'ordine e lo finalizza, senza avere caratteristiche identificative della persona da cui questo proviene.
Lo studioso concretizzò questi fondamenti teorici nel 1989, fondando una società e inventando la valuta digitale DigiCash, che permetteva scambi sicuri e convenienti

[16] L'intervista è facilmente reperibile su YouTube
[5] https://www.dailymail.co.uk/sciencetech/article-5000260/Bitcoin-predicted-Milton-Friedman-18-years-ago.html

per beni e servizi attraverso Internet. Ci sono voluti circa dieci anni affinché DigiCash fosse accettato da banche e utenti, in quanto una forte spinta alla domanda venne data dai primi siti di e-commerce, che nacquero proprio nella seconda metà degli anni ’90.

Il problema di DigiCash era fondamentalmente dovuto al fatto che il vantaggio principale del sistema, l’anonimato, non era percepito dai consumatori come un vantaggio tale da spingerli a utilizzare DigiCash piuttosto che le normali carte di credito, con le quali si sentivano più al sicuro. Alla mancata fortuna, contribuì anche il carattere di Chaum, che fu definito da Raymond Stofberg (CFO di DigiCash fino al ’96) «so paranoid that he always thought something was wrong»[18], in relazione a delle negoziazioni con la Dutch ING Bank durate mesi, per poi vedere Chaum ritirarsi e annullare tutte le trattazioni senza fornire una motivazione. Ricevette anche un’offerta da 100 milioni di dollari da parte di Bill Gates, che voleva integrare DigiCash nel suo OS Windows 95, prontamente rifiutata.

Nel 1999, infine, sia perché la gente non vedeva problemi di sicurezza nelle carte di credito e sia perché c’era diffidenza riguardo a questo nuovo metodo di pagamento, la società andò in bancarotta e la valuta scomparve.

2.2.3. E-gold

Il secondo progetto nel campo criptovalute arrivò nel 1996 da Douglas Jackson e Barry Downey, di professione rispettivamente oncologo e avvocato. La loro idea era più semplice rispetto a DigiCash e consisteva nell’ancorare una valuta digitale al prezzo dell’oro.
Questo avveniva comprando un certo quantitativo di oro (tenuto al sicuro in un deposito a Melbourne, Florida) e vendendo frazioni digitali di questo attraverso un sito web. Queste parti digitali di oro erano rappresentate da token chiamati, per l’appunto, “e-gold”.

Nell’arco temporale che va dalla creazione della piattaforma al nuovo millennio, e-gold riscosse un successo sorprendente, raggiungendo oltre un milione di persone che ne facevano utilizzo. Fu, inoltre, il primo pagamento che non prevedesse carte di credito ad essere integrato in siti di e-commerce, ancor prima del più celebre PayPal, nato nel 1999.

Inizialmente, e-gold fu utilizzato solo dai trader di metalli preziosi, in seguito anche da investitori generici, case d’asta, casinò online, organizzazioni politiche e ONP. La forza di questo sistema era dovuta al fatto che, al contrario di quanto si pensi parlando di oro, era comodo da utilizzare anche per microtransazioni, in quanto le frazioni digitali avevano un valore minimo di un centinaio di grammo d’oro, diventando così il primo sistema efficiente di micropagamento (le carte di credito e altri sistemi imponevano ancora costi di transazione molto alti).

Nel momento di capitalizzazione più alta, e-gold raggiunse i due miliardi di dollari. Tuttavia, vi erano falle abbastanza importanti nel sistema per quel che riguarda la sicurezza, tanto che molti investitori furono vittime di attacchi hacker senza poter

[18] “Così paranoico da pensare ci fosse sempre qualcosa di sbagliato”.

fare appello alla giustizia statunitense perché, *de facto*, e-cash non era riconosciuta dalla legge come "moneta".

Inoltre, dopo l'attentato alle Torri Gemelle (9 settembre 2001) il governo USA introdusse il "Patriot Act", un provvedimento che permetteva la sospensione di alcuni diritti civili nei casi previsti dalla legge. All'interno di questo provvedimento venne cambiata, con effetti retroattivi, la legislazione riguardante lo scambio di denaro, portando Jackson e Downey in tribunale perché in difetto di una licenza; le autorità congelarono le riserve di oro e molti utenti abbandonarono la piattaforma. E-gold, dunque, dovette dichiararsi colpevole di riciclaggio di denaro sporco e richiedere una licenza. Dopo aver pagato la multa e aver fatto 300 ore di lavoro socialmente utile, la licenza fu negata in quanto i criminali, per la legge americana, non posso avere una licenza che gli permetta di svolgere il lavoro di *money transfer*.

2.2.4. Cosa ha imparato il mondo da DigiCash e E-Gold

DigiCash insegnerà al mondo delle criptovalute una lezione: il visionario progetto di Chaum fallì perché lui stesso aveva la paranoia per i diritti di proprietà intellettuale e, anche a causa di tale comportamento, il suo sistema non si sparse mai tra il pubblico.

E-Gold, invece, ha sofferto di vari problemi: in primis, il fatto che vi fosse un'autorità centrale ha reso il sistema vulnerabile ad attacchi hacker, dando così zero vantaggi dal punto di vista della sicurezza rispetto ai metodi tradizionali; poi, in generale, un sistema monetario basato su un rapporto di valore con l'oro potrebbe essere facilmente controllato da autorità statali, conseguenza che si amplifica se la società che costruisce il sistema ha sede legale in uno Stato in cui, per ovvi motivi, la legislazione può variare improvvisamente; creare questo tipo di sistema rivelando la propria identità potrebbe portare a conseguenze spiacevoli, come accaduto a Jackson e Downey.

Satoshi Nakamoto, l'inventore di Bitcoin, imparò la lezione: infatti, la tecnologia Bitcoin, meno di dieci anni rispetto al fallimento di DigiCash e poco più rispetto alla creazione di E-Gold, risolverà questi problemi grazie al sistema a cui abbiamo già accennato in apertura del capitolo e che spiegheremo in dettaglio successivamente. In particolare, risolse il problema di DigiCash grazie alla caratteristica dell'open-source (che da una parte aumenta la concorrenza dalla parte dell'offerta, ma dall'altra permette che gli investitori siano sempre più attratti da questo mercato) ed evitò i problemi di E-Gold grazie all'anonimato, in quanto il creatore è celato dietro lo pseudonimo di Satoshi Nakamoto, e alla tecnologia Blockchain, la quale prevede la decentralizzazione e un grado di sicurezza molto elevato del sistema.

2.2.5. La cripto-anarchia di Wei Dai

Nel 1998, uno scienziato cripto-anarchico (seguace, cioè, di una corrente chiamata "cripto-anarchia" portata avanti da Tim May) di nome Wei Dai pubblicò un documento con i dettagli di una moneta decentralizzata dal nome "B-money". Nel suo articolo, l'ingegnere informatico cinese sognava un mondo in cui la violenza non sarebbe stata possibile. Ma come si collega questo al mondo delle criptovalute?

Secondo Wei Dai, in un mondo in cui le posizioni fisiche e le identità reali degli individui sono oscurati dalla conoscenza pubblica, la violenza non sarebbe possibile e, senza la violenza, anche la ragion d'esistere primaria dei governi non avrebbe

senso, portando dunque a un'anarchia causata non dall'esclusione o dalla distruzione di potere governativo, ma da una mancanza della sua necessità di esistere.

Riconobbe che, affinché il suo sogno diventasse realtà, sarebbe stato necessario che il mondo si evolvesse nei modi di comunicare e negoziare in un enorme sistema peer-to-peer. All'epoca, nel suo documento, facilmente reperibile su Internet e riportato in sitografia, Dai disse: «fino a ora non è chiaro, anche teoricamente, come potrebbe funzionare una simile comunità. Una comunità è definita dalla cooperazione dei suoi partecipanti e una cooperazione efficiente richiede un mezzo di scambio (denaro) e un modo per far rispettare i contratti. Tradizionalmente questi servizi sono stati forniti dal governo o dalle istituzioni sponsorizzate dal governo e solo dalle persone giuridiche»[19].

Dunque, iniziò a discutere due protocolli attraverso i quali sarebbe stato possibile fornire un mezzo di scambio e un metodo di far rispettare i contratti all'interno di una comunità, pur mantenendo la privacy di chi ne fa parte. Il primo era, a sua stessa opinione, impraticabile, in quanto faceva uso di un irrealistico canale broadcast anonimo, ma era necessario per motivare il secondo protocollo, che era invece più pratico.

Questi due protocolli sono stati realizzati, in pratica, da Bitcoin. In particolare, gli aspetti che nel lavoro di Wei Dai restavano teorici e hanno visto la luce grazie a Bitcoin sono il concetto di prova del lavoro (algoritmo *proof-of-work*), trasmissione e firma delle transazioni, l'incentivazione a creare valuta e la presenza di un libro mastro decentralizzato.

Questo stesso documento fu citato come riferimento da Satoshi Nakamoto al momento della creazione di Bitcoin.

2.3. La nascita di Bitcoin

2.3.1. L'annuncio su Metzdowd.com

La prima notizia della nascita di Bitcoin si ha il 31 ottobre 2008. Il sito "metzdowd.com" aveva una mailing list in cui chiunque poteva inserire il suo indirizzo e-mail per scambiare opinioni e informazioni sul mondo della crittografia. Tale servizio, che contava solo poche centinaia di interessati, quel giorno vide arrivare una mail da parte di un certo Satoshi Nakamoto, con scritto:

«I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. […] A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network»[20].

Satoshi Nakamoto spiegò, in maniera estremamente sintetica, il funzionamento del sistema Bitcoin e, in particolare, le novità previste dall'algoritmo proof-of-work della

[19] http://www.weidai.com/bmoney.txt

[20] https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Blockchain. Vi era, inoltre, un link a un testo in formato pdf che spiegava nel dettaglio il funzionamento del sistema. Tale link era, molto semplicemente, http://www.bitcoin.org/bitcoin.pdf, il link ancora funzionate del white paper di Bitcoin.

2.3.2. Il White Paper

Cos'è un "white paper"? Un white paper, in italiano "libro bianco" è una «raccolta di documenti e testimonianze che associazioni, comitati, partiti, ecc. pubblicano al fine di denunciare (sensibilizzando così la pubblica opinione) gravi fenomeni sociali, la degradazione di certe istituzioni, il cattivo funzionamento di pubblici enti e servizî»[21]. Proseguendo sul sito si legge che «l'espressione, è attestata per la prima volta nell'italiano scritto agli inizi del secolo XX (1906). Alcuni studiosi ipotizzano che libro bianco possa in qualche modo rifarsi all'album latino, cioè alla tavola imbiancata sulla cui superficie i Romani trascrivevano gli editti dei pretori; altri pensano che libro bianco derivi il proprio attributo dal colore della legatura che usualmente si adopera per questo genere di raccolta di relazioni e allegate documentazioni»[7].

In pratica, nel mondo del web, la parola indica dei documenti redatti da professionisti o autorità del settore che spiegano in modo preciso e dettagliato il funzionamento di un prodotto, una tecnologia o un servizio a un pubblico interessato. Quasi tutte le criptovalute hanno un loro white paper che ne spiega il funzionamento.

Satoshi Nakamoto registrò il dominio "Bitcoin.org" due mesi prima, rendendo disponibile allo stesso tempo il download del white paper in formato PDF. In apertura del documento, si legge un sommario che spiega con poche parole il progetto che si andrà a esaminare nelle pagine successive:

«Una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un soggetto a un altro senza passare attraverso alcuna istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, in quanto si hanno ben pochi benefici se è necessaria la presenza di un terzo fiduciario per prevenire la doppia spesa. Proponiamo una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer. La rete stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash, formando una registrazione che non può essere modificata senza rifare la proof-of-work. La catena più lunga non solo serve come prova della sequenza di eventi ai quali si è assistito, ma anche come prova che essa proviene dal gruppo più grande di potenza CPU. Fino a quando la maggior parte della potenza CPU è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su base best-effort e i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quello che è avvenuto mentre erano non erano presenti»[22].

Procedendo a quello che è il capitolo 1, si legge la "mission" del progetto:

[21] http://www.treccani.it/magazine/lingua_italiana/domande_e_risposte/lessico/lessico_067.html
[22] Satoshi Nakamoto, *White Paper*, http://www.bitcoin.org/bitcoin.pdf cap. "Introduzione"

«Il commercio su Internet fa affidamento quasi esclusivamente sulle istituzioni finanziarie che servono come terze parti di fiducia per elaborare i pagamenti elettronici. Nonostante il sistema funzioni abbastanza bene per la maggior parte delle transazioni, esso soffre ancora delle debolezze intrinseche di un modello basato sulla fiducia. Transazioni totalmente irreversibili non sono realmente possibili, dal momento che le istituzioni finanziarie non possono evitare le dispute di mediazione. Il costo dell'intermediazione aumenta i costi di transazione, limitando la dimensione minima delle transazioni praticabili ed escludendo la possibilità di piccole transazioni occasionali, e c'è un costo più ampio collegato alla perdita della capacità di effettuare pagamenti irreversibili per quei servizi che sono anch'essi irreversibili. Con la possibilità di reversibilità, si diffonde la necessità di fiducia. I commercianti devono diffidare dei loro clienti, tormentandoli con maggiori richieste di informazioni rispetto a quanto non sarebbe altrimenti necessario. Una certa percentuale di frodi è accettata come inevitabile. Tali costi e le incertezze di pagamento possono essere evitati utilizzando moneta fisica di persona, ma non esiste alcun meccanismo per effettuare pagamenti attraverso un mezzo di comunicazione senza un'entità di fiducia.

È dunque necessario un sistema di pagamento elettronico basato su prova crittografica invece che sulla fiducia, che consenta a due controparti qualsiasi negoziare direttamente tra loro senza la necessità di una terza parte di fiducia. Le transazioni che sono computazionalmente impraticabili da invertire proteggerebbero i venditori dalle frodi, inoltre altri meccanismi consuetudinari di deposito di garanzia potrebbero essere facilmente implementati per proteggere gli acquirenti. In questo lavoro, proponiamo una soluzione al problema della doppia spesa utilizzando un server di marcatura temporale distribuito peer-to-peer per generare la prova computazionale dell'ordine cronologico delle transazioni. Il sistema è sicuro finché i nodi onesti controllano collettivamente più potenza CPU rispetto a qualsiasi gruppo collaborativo di nodi attaccanti»[9].

I restanti capitoli del white paper di Bitcoin riguardano le modalità di funzionamento delle transazioni, dei server, dell'algoritmo *proof-of-work*, della rete, del mining, della verifica dei pagamenti e la privacy del sistema.

La sua conclusione, invece, sintetizza ulteriormente ciò che è detto nelle poche pagine del paper:

«Abbiamo proposto un sistema per le transazioni elettroniche non basato sulla fiducia. Abbiamo iniziato con il *framework* abituale delle valute basate su firme digitali, che prevede un forte controllo sulla proprietà, ma è incompleto non avendo modo di prevenire la doppia spesa. Per risolvere questo problema, abbiamo proposto una rete *peer-to-peer* che utilizza la *proof-of-work* per registrare una storia pubblica delle transazioni, la cui modifica diventa rapidamente computazionalmente impraticabile per un utente malintenzionato se i nodi onesti controllano la maggioranza della potenza della CPU. La rete è robusta nella sua semplicità non strutturata. I nodi lavorano tutti insieme con poca coordinazione. Non hanno bisogno di essere identificati, dal momento che i messaggi non vengono instradati in qualche direzione particolare ma vengono solo consegnati su base *best-effort*. I nodi possono lasciare e ricongiungersi con la rete a piacimento, accettando la catena *proof-of-work*

come prova di quello che è successo mentre erano assenti. Essi votano con la loro potenza di CPU, esprimendo la loro accettazione di blocchi validi mediante il lavoro che compiono sulla loro estensione e respingendo i blocchi non validi tramite il rifiuto di lavorare sugli stessi. Tutte le regole e gli incentivi necessari possono essere applicati mediante questo meccanismo di consenso»[23].

Il primo blocco di Bitcoin è stato minato da Satoshi Nakamoto stesso il 3 gennaio 2009.

2.3.3. La misteriosa identità di Satoshi Nakamoto

Il white paper ha le pregevoli caratteristiche di un documento chiaro, conciso, essenziale e allo stesso tempo completo. Non lascia, in altre parole, alcun dubbio sul funzionamento del sistema Bitcoin. L'unico dubbio che viene spontaneo è uno: chi è Satoshi Nakamoto?

Solitamente, il proprietario di un dominio registrato può essere cercato in database disponibili s online, ma Bitcoin.org è stato registrato attraverso un servizio che nasconde l'identità del proprietario. Questi servizi sono utilizzati solitamente da soggetti politicamente coinvolti o criminali. Su una cosa si è ormai certi: non esiste una persona chiamata Satoshi Nakamoto, per cui non esiste alcuna certezza su chi si nasconda dietro a questo pseudonimo; addirittura, non si sa neanche se sia una sola persona o un gruppo di persone.
Inoltre, in giapponese Satoshi Nakamoto si traduce come "pensiero scaltro nella fondazione"[24]. Se non si fosse certi sia uno pseudonimo, si direbbe uno pseudonimo perfetto per il profilo.

A sua detta, Satoshi Nakamoto è un uomo giapponese, nato il 5 aprile 1975. Il nome è di origine giapponese, il che potrebbe portare a pensare che sia effettivamente di origini giapponesi, ma le opinioni della "crypto-community" non sono d'accordo: si sostiene, infatti, che più probabilmente dietro Satoshi Nakamoto si nasconda (almeno) una persona vissuta in un paese anglofono, in quanto il suo uso dell'inglese è molto preciso e, analizzandolo da un punto di vista linguistico, emerge un utilizzo sia di American English che di British English, nonché di espressioni del parlato comune che si trovano di rado su libri accademici (come ad esempio l'espressione "bloody hard"[25], utilizzata da Satoshi nella sezione di commenti del codice sorgente della Blockchain); inoltre, non è stata ritrovata online nessuna documentazione originale in giapponese o proveniente dal Giappone.
Sul sito BitcoinTalk, un utente dal nome Satoshi Nakamoto partecipava attivamente alle discussioni fino al 2010, ma a giudicare dall'orario delle pubblicazioni, si ritiene molto più probabile vivesse in una nazione che appartiene ai fusi orari americani, piuttosto che asiatici.
Inoltre, l'indirizzo da cui scrisse le prime mail proviene da un servizio di e-mail gratuito di origine tedesca e, prima delle suddette mail, non vi era nessuno che conoscesse Satoshi, in quanto non si trova online alcuna notizia della sua esistenza precedente al 31 ottobre 2008.

[23] Satoshi Nakamoto, *White paper*, http://www.bitcoin.org/bitcoin.pdf cap. "Conclusione"
[24] https://www.coindesk.com/information/who-is-satoshi-nakamoto
[25] https://bitcointalk.org/index.php?topic=234.msg1976#msg1976

Ovviamente, esistono tante persone che nel corso degli ultimi dieci anni sono state ipotizzate nascondersi dietro lo pseudonimo di Satoshi, ma la maggior parte di queste hanno smentito. Alcuni dei nomi più accreditati sono i seguenti:

- Michael Clear: uno studente irlandese di informatica al Trinity College che è stato assunto da Allied Irish Banks per migliorare il proprio software di trading basato su valute, il quale è, inoltre, autore di un paper accademico sulla tecnologia peer-to-peer. Egli ha negato di essere Satoshi Nakamoto più volte sul suo blog e davanti alla stampa irlandese, affermando di non essere mai stato molto interessato al mondo dell'economia;
- Vili Lehdonvirta: un programmatore di giochi finlandese, il cui nome è stato collegato per la prima volta a quello di Satoshi proprio da Micheal Clear, in una mail diretta a Joshua Davis, redattore per "The New Yorker" a caccia dell'identità di Satoshi, dopo aver fatto luce proprio su Clear. La risposta del finlandese fu contemporaneamente una negazione della tesi di Clear e Davis (a sua detta, a causa della sua scarsa preparazione sul tema crittografia), un attestato di stima nei confronti di Nakamoto e la grande preoccupazione che il sistema Bitcoin sia usato per motivi criminali. Entrambi i nomi appaiono su un articolo redatto proprio da Davis per il sopracitato giornale, dal nome "The Crypto-Currency", pubblicato il 3 ottobre 2011;
- Nick Szabo: come sostiene Nathaniel Popper, giornalista del "New York Times", le sue ricerche indicano che dietro al nome di Satoshi Nakamoto si nasconda un uomo solitario di origine ungherese ma di cittadinanza americana, Nick Szabo. In un articolo dal nome "Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin", pubblicato sul New York Times il 15 maggio 2015, il giornalista sostiene fermamente questa ipotesi, pur ammettendo una netta negazione da parte di Szabo, che affermava di essere permanentemente impegnato nel campo telecomunicazioni. Il nome di Szabo è stato pensato dal giornalista in quanto gli si deve una notevole contribuzione al progetto Bitcoin, poiché ideatore di Bit Gold, un sistema che ha raggiunto gli stessi obiettivi di Bitcoin tempo prima e, seppur non raffinato quanto Bitcoin, quest'ultimo incorpora molte delle idee messe in codice da Szabo. Nel 2014 egli, inoltre, si unì a una start-up basata sull'utilizzo di Bitcoin chiamata Varum, che si proponeva di costruire una piattaforma migliore per lo scambio di Bitcoin, e fece cambiare direzione organizzativa all'intera impresa, portando un profitto di circa 12 milioni di dollari grazie all'utilizzo degli *smart contract*, già analizzati nel capitolo precedente, che il sistema Bitcoin permette di risolvere. Szabo affermerà, inoltre, in un post su un suo blog nel 2011, che le uniche persone oltre a lui stesso a cui inizialmente piacesse l'idea di Bitcoin erano il cripto-anarchico Wei Dai, di cui abbiamo già discusso nel capitolo precedente, e Hal Finney, aggiungendo che quest'ultimo fosse l'unico, insieme a Nakamoto, abbastanza motivato da implementare un sistema così complesso;
- Hal Finney: quest'uomo è stato il primo a ricevere una transazione Bitcoin, da Satoshi Nakamoto in persona. Nelle sue dichiarazioni pubbliche (come si può vedere dal suo profilo twitter), è sempre stato entusiasta del progetto Bitcoin. Egli scriverà anche numerosi post su Twitter in cui afferma di lavorare effettivamente al progetto, come ad esempio un tweet in cui sostiene di cercare modi per implementare l'anonimato del sistema[26] e un altro in cui affermava di voler diminuire le emissioni

[26] https://twitter.com/halfin/status/1136749815?ref_src=twsrc%5Etfw

di CO_2 causate dal mining di Bitcoin[27].
Hal Finney morì il 28 agosto 2014 della malattia di Lou Gehrig.

- Neal King, Vladimir Oksman, Charles Bry: questi tre nomi, appartenenti a tre crittografi, sono stati fatti da Adam Penenberg il 10 novembre 2011 in un articolo chiamato "The Bitcoin Crypto-Currency Mystery Reopened", pubblicato da Fast Company. Egli riprende (ed elogia) il lavoro di Joshua Davis, dunque racconta una sua ricerca svolta nel web cercando documenti che contenessero espressioni simili a quelle utilizzate nel white paper di Bitcoin; in particolare, trovò che la locuzione "computationally impractical to reverse" portava a 26 risultati, di cui 25 posteriori alla nascita del Bitcoin e uno datato esattamente tre giorni prima alla nascita della piattaforma, avvenuta il 18 agosto 2008: questo risultato era una pagina web che descriveva un brevetto dal nome "system and method for providing secure communications" di proprietà dei tre crittografi. Un'altra coincidenza si trova nel fatto che il dominio Bitcoin.org è stato registrato da un provider finlandese ed è stato documentato un viaggio in Finlandia da parte di Bry circa sei mesi prima dell'agosto 2008.
  Ovviamente, ognuno di loro ha declinato una qualunque affiliazione al progetto Bitcoin.

2.4. La prima fase di Bitcoin: un milione di capitalizzazione (2008 – 2010)

In questa fase della vita di Bitcoin, esso era utilizzato prevalentemente da chi si interessasse del mondo della crittografia. A partire dalla sua nascita, nel 2008, Bitcoin inizia attraverso un processo lento, ma continuo, a diffondersi, fino ad arrivare, alla fine del 2010, ad avere una capitalizzazione totale di mercato stimata intorno a 1 milione di dollari US.

Purtroppo, essendo poco documentati i primi movimenti, è impossibile stabilire esattamente l'andamento del valore di un singolo token BTC in questa fase di vita, se non estrapolando dei tassi di cambio con il dollaro dalle transazioni di cui abbiamo traccia, operazione che verrà svolta nel corso del paragrafo.

2.4.1. Bitcoin nel 2008

Come già detto, le prime tre date importanti da ricordare per Bitcoin sono il 18 agosto 2008 (giorno in cui è stato registrato il dominio Bitcoin.org), il 31 ottobre 2008 (giorno in cui, attraverso una mail a metzdowd.com da Satoshi Nakamoto, è stato reso pubblico il white paper di Bitcoin) e il 3 gennaio 2009 (data della creazione del "blocco di genesi" della catena da parte dello stesso Satoshi). La validazione della prima transazione ha portato alla creazione di 50 bitcoin, un evento passato in sordina nel mondo intero ma che, giudicando a posteriori, ha cambiato la storia della crittografia e, forse, del mondo intero.

2.4.2. Bitcoin nel 2009

Il 9 gennaio 2009 viene rilasciato il primo client Bitcoin Open Source, la famosa "versione 0.1" e, tre giorni dopo, avviene la prima transazione su Bitcoin: 10 bitcoin sono stati mandati dallo stesso Satoshi Nakamoto ad Hal Finney. Nell'ottobre dello stesso anno, ci fu il primo tasso di cambio con il dollaro USA: tale cambio era fissato a 1.309 BTC/USD ed era calcolato sulla base della potenza computazionale

[27] https://twitter.com/halfin/status/1153096538?ref_src=twsrc%5Etfw

necessaria per ottenere un token. Da qui inizia una lenta ma inesorabile diffusione di Bitcoin, con la nascita del forum BitcoinTalk.org il 22 Novembre dello stesso anno a opera di Satoshi Nakamoto, che sotto l'username "satoshi" pubblicò anche il primo post. Infine, il 16 dicembre fu rilasciata la versione di Bitcoin 0.2.

2.4.3. Bitcoin nel 2010

Nel mese di gennaio 2010 avvenne il primo incremento nella difficoltà della verifica dei blocchi, un incremento pari al 18.3% (che crebbe ulteriormente arrivando al 33.4% entro fine mese; alla fine dell'anno, la difficoltà aumentò, rispetto a 365 giorni prima, del 115,912.9%, a testimonianza di come questo sistema si stesse espandendo a macchia d'olio). Il 22 Maggio successivo è un'altra data storica, conosciuta nell'ambiente ancora oggi come "Bitcoin pizza day", in quanto avvenne, a Jacksonville (Florida), la prima transazione che vedeva nello scambio da una parte bitcoin e dall'altra un bene di consumo: il programmatore Laszlo Hanyecz pagò due pizze 10000 BTC (il tasso di cambio era, allora a 400 BTC/USD, per un costo di circa 25€). Nel corso dell'anno, crebbe notevolmente la fama e l'utilizzo di Bitcoin, grazie ad articoli e discussioni pubblicati sui principali siti d'informazione americana in campo informatico, primo tra tutti slashdot.org, tanto che, nel giro di soli cinque giorni (dal 7/6/2010 al 12/6/2010) il prezzo di Bitcoin crebbe del 1000%, arrivando da 0.008 USD/BTC a 0.080 USD/BTC. Il 17 luglio nacque MtGox, la piattaforma di scambi giapponese, che arrivò a coprire quasi i tre quarti del mercato di criptovalute, fallendo poi nel 2014 dopo aver subito una perdita di 850,000 bitcoin a causa di alcuni hacker (del valore di circa 450 milioni di dollari, che rappresenta tutt'ora il più grande furto di BTC mai registrato). Il primo disastro registrato avvenne il 15 agosto, quando venne sfruttata una vulnerabilità del codice: in unica transazione vennero generati 184 milioni di BTC, inviati a due indirizzi diversi sulla rete. Per risolvere il problema fu necessario un intervento diretto sulla rete che cancellò la transazione sulla Blockchain nel giro di poche ore, risolvendo questo bug con un aggiornamento del protocollo. Nell'ottobre dello stesso anno iniziarono a rivelarsi anche agli organi governativi le potenzialità, ma soprattutto i problemi per la sicurezza legati all'uso delle criptovalute; la Financial Action Task Force scrisse in un documento:

«Virtual currencies, such as Bitcoin, have developed into a powerful payment method with ever growing global acceptance. Virtual currencies offer an innovative, cheap and flexible method of payment. At the same time, the unique and often unfamiliar business model of virtual currencies poses a challenge to regulators around the world who are unsure how to deal with this payment method. The policy responses vary considerably, with some countries embracing this new technology and others severely or totally limiting its legitimate use»[28].

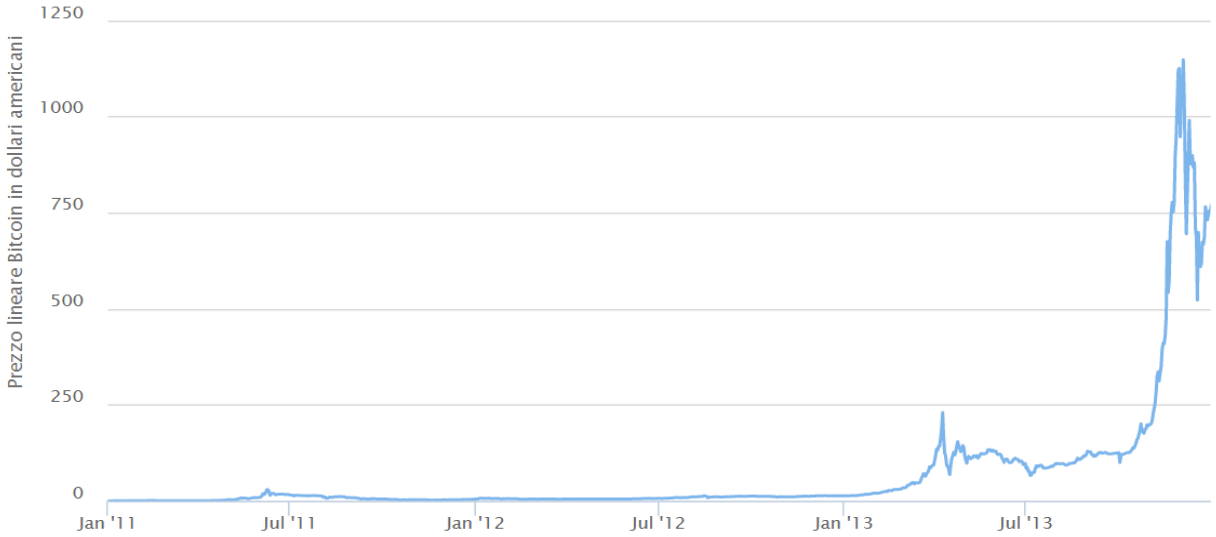
Aggiungendo, però, subito dopo, i problemi legati all'utilizzo di tali tecnologie, di cui si è discusso nel paragrafo 2.2. Nello stesso mese nacque il primo OpenCL (Open Computing Language, un'architettura logica di supporto su cui un software può essere progettato e realizzato in modo facilitato e che può esser eseguito su una molteplicità di piattaforme, CPU, GPU, e altri tipi di processori) dedicato al mining di Bitcoin e per la prima volta una *mining pool* (un insieme di hardware che lavorano insieme attraverso un software per aumentare la loro potenza di calcolo e avere una

[28] FATF report, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* [2014]

maggiore probabilità di risolvere e verificare un blocco della catena) estrae un blocco. Il 12 dicembre, Satoshi Nakamoto pubblica il suo ultimo post su BitcoinTalk[29], dopodiché lo sviluppo di Bitcoin verrà affidato a Gavin Andersen, un noto programmatore americano. Si stima che, alla fine del 2010, la capitalizzazione fosse di circa un milione di dollari.

2.5. La seconda fase di Bitcoin: da 0.42 a 1000 USD/BTC (2011 – 2013)

La seconda fase di Bitcoin fa conoscere definitivamente al mondo questo sistema, che si diffonde senza limiti geografici nei liberi mercati di tutto il mondo. Aumentano i miner, aumentano i servizi che accettano i Bitcoin come pagamento in sostituzione delle monete correnti e aumentano gli utenti del servizio. Alla fine del triennio, il Bitcoin raggiunge un tasso di cambio di mille USD/BTC.



30

2.5.1. Bitcoin nel 2011

Il 2011 iniziò con tre eventi storici nel corso di soli 40 giorni: infatti, in questo periodo fu effettuata la più grande transazione monetaria nella storia di Bitcoin, che vide 3 account dallo Zimbabwe scambiare, su #bitcoin-otc 100 trilioni di dollari zimbabwani con 4 BTC (se si pensa che all'epoca il tasso di cambio con il dollaro era 0.42 USD/BTC, la transazione non sembra avere un valore poi così alto), fu generato il blocco #105000 rilasciando così il 25% della fornitura totale di 21 milioni di BTC, pari circa a 5.24 milioni, e nel giro di due settimane Bitcoin vide raddoppiare il suo valore rispetto al dollaro arrivando per la prima a raggiungere la parità, eventi che accaddero rispettivamente il 27/01, il 28/01 e il 9/02. Negli stessi mesi, il *pooled mining* raggiunse la capacità di dieci Ghash/s e nacque SilkRoad, un e-commerce di merce illegale, nel quale era possibile acquistare droghe, armi e altri prodotti dal commercio limitato o proibito pagando in Bitcoin.

Verso la fine di marzo la popolarità di Bitcoin cresceva a dismisura, tanto che vennero aperte Britcoin (una piattaforma che permetteva di scambiare BTC e GBP[31])

[29] https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts
[30] www.buybitcoinworldwide.com/it/prezzi/, grafico dell'andamento del tasso di cambio USD/BTC del triennio 2011-2013

e Bitcoin Brasil (una piattaforma che permetteva di scambiare BTC ed R$[32]), rispettivamente il 27 e il 31 del mese. Altre piattaforme seguirono, tanto che la capitalizzazione di mercato di Bitcoin, nel mese di aprile, si attestava intorno ai 10 miliardi di dollari statunitensi.

Nel giugno 2011 viene attestato il primo furto di Bitcoin per un valore di 375,000.00$ circa (25 BTC) per colpa di una falla nei sistemi di MtGox e MyBitcoin che portò al furto di interi portafogli. A partire da agosto si tennero le prime due conferenze sul Bitcoin (20/8 alla World Expo in New York City, 25/11 a Praga), a testimonianza di quanto nel mondo cresceva l'interesse per il cripto-mondo.

Dopo essere arrivato alla parità di cambio con il dollaro nel mese di febbraio attraversò qualche mese negativo che ne vide scendere il valore del 20%, ma a partire dalla metà di aprile il prezzo risalirà fino ad arrivare al massimo annuale, ben 29.6 USD/BTC. Tuttavia, questo prezzo si pensa sia stato ottenuto artificialmente tramite alcuni bot e come conseguenza scese nel giro di pochi mesi, arrivando al cambio di circa quattro USD/BTC alla fine dell'anno.

2.5.2. Bitcoin nel 2012

L'inizio del 2012 vede Bitcoin citato sul web perlopiù per casi di furto (il 1/03, ad esempio, avviene il più grande furto di BTC, circa 50000 token vengono rubati dopo un aggiornamento di sicurezza su Linode) oppure da siti di informazione che, vedendo crescere l'interesse da parte del pubblico, iniziano a parlarne. A giugno, viene creato il più grande blocco della catena, il #181919, il quale include 1322 transazioni, e viene lanciato Coinbase, che attraverso la collaborazione con autorità legislative appartenenti a varie e diverse giurisdizioni e a vere e proprie partnership con alcune banche, raggiunge il successo come piattaforma di scambio (secondo i dati risalenti a ottobre 2018, la società ha una valutazione di 8 miliardi di dollari)[33]. Grazie a Coinbase e alle crescenti fonti di informazione (degna di nota la Bitcoin Conference tenutasi a Londra nei giorni 15/9 e 16/9), Bitcoin raggiunge sempre un maggior successo e si vede nascere anche la Bitcoin Foundation, creata con lo scopo di "helping to create awareness of the benefits of Bitcoin, how to use it and its related technology requirements, for technologists, regulators, the media and everyone else globally"[34]. A novembre, WordPress[35] inizia ad accettare pagamenti in bitcoin.

I miner, che vengono retribuiti in BTC per il lavoro svolto, necessario al funzionamento del sistema, sono stati pagati 50 BTC per blocco completato. Il sistema prevedeva che, al raggiungimento dei 210000 blocchi minati, avvenisse un evento definitio *halving event*[36], il quale provoca un dimezzamento del premio dato ai miner. Tale evento si è verificato il 28/11, impostando come ricompensa per la validazione un blocco 25 BTC. Il secondo *halving event* si è verificato nel luglio 2016 ed un terzo è stimato per metà 2020.

---

[31] Great Britain Pounds
[32] Brazilian Reals
[33] https://www.businessinsider.com/coinbase-valued-at-8-billion-after-raising-another-mega-round-2018-10?IR=T
[34] https://bitcoinfoundation.org/wp-content/uploads/2017/03/Bitcoin_Foundation_Manifesto.pdf
[35] Wordpress è un software di content management system open source, il quale consente la creazione e distribuzione di un sito Internet formato da contenuti testuali o multimediali, facilmente gestibili ed aggiornabili in maniera dinamica.
[36] Potrebbe essere tradotto in italiano come "Evento dimezzante".

2.5.3. Bitcoin nel 2013

Nel marzo 2013 la Blockchain si divise temporaneamente in due parti indipendenti tra di loro con diverse regole di funzionamento e di accettazione delle trattazioni; questo malfunzionamento, sfociato in due sistemi funzionanti indipendentemente e in parallelo, è durato per sei ore, dopodiché gli sviluppatori sono stati chiamati a sistemare il sistema, fermando le transazioni in corso per operare sulla Blockchain. Questo portò la FinCEN[37] a stabilire delle linee guida[38] sul funzionamento delle "valute virtuali decentralizzate", come per l'appunto Bitcoin. Nello stesso mese, le banche cipriote hanno confiscato i risparmi delle persone nel contesto della crisi finanziaria scoppiata a Cipro nel 2013 e le persone iniziarono a utilizzare, come alternativa al denaro liquido, il Bitcoin. Da quel momento, Bitcoin ha assolto questa funzione in altri contesti simili, come ad esempio nel corso dell'iperinflazione venezuelana avvenuta alla fine del 2016. Il 1/4 il bitcoin supera i 100 dollari di quotazione. Il 9 dello stesso mese costa addirittura 230$, per poi scendere a 60$ nel giro di una settimana e assumere valori compresi tra gli 80 e 110 dollari per qualche mese.

Nel corso dell'anno, comunque, Bitcoin riuscì a ottenere sempre più consensi da parte del mercato, tanto che alcuni servizi (come OkCupid, Foodler, Mega, Wikileaks, Pizzacoin, …) iniziarono ad accettare BTC come pagamento, il che incrementò ulteriormente la sua fama.

Il 2/10 SilkRoad viene chiuso dall'FBI e tutti i fondi in Bitcoin, per un valore totale di circa 26mila BTC, confiscati. Il mercato reagisce con un nuovo calo della moneta, che scende a 109$.
A novembre debutta l'Antminer S1, il primo ASIC[39] di Bitmain con un hashrate di 180 Gh/s. In seguito al crescente supporto del mercato e al crescente numero di miner attivi sulla catena, a novembre, per la prima volta nella storia, il cambio USD/BTC supera il valore di 1000.
A dicembre, la Banca Popolare Cinese[40] proibisce alle istituzioni finanziare di effettuare transazioni in Bitcoin (il loro utilizzo per comprare beni fisici era già stato proibito dal 2009).

2.6. La terza fase di Bitcoin (2014 – 2016)

Questa seconda fase della vita di Bitcoin è caratterizzata da un improvviso shock a inizio 2014 che porta la quotazione di Bitcoin da cifre che oscillavano intorno ai 1000$ nel dicembre 2013 a cifre che si aggireranno intorno ai 500$ nei primi mesi del 2014, per poi proseguire una lenta discesa fino alla metà di gennaio 2015. Da qui parte un periodo di relativa stabilità del valore del token BTC, compreso tra i 200$ e i 400$, al quale segue, da settembre dello stesso anno, un trend positivo che aumenta il valore in modo lento (se paragonato alle oscillazioni successive) ma costante, fino a registrare nel complesso del triennio un aumento di valore, chiudendo il mese di dicembre 2016 sulle stesse cifre del dicembre 2013, pur senza mai toccare la "quota

[37] Financial Crimes Enforcement Network, autorità statunitense di sorveglianza finanziaria
[38] https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities
[39] Application Specific Integrated Circuit, cioè un circuito integrato creato appositamente per risolvere un'applicazione di calcolo ben precisa, detta in gergo *special purpose*, in questo caso il mining di Bitcoin.
[40] Banca centrale della Repubblica Popolare Cinese

1000" registrata in quel mese. Nel frattempo, aumentano le autorità che cercano di regolamentare l'utilizzo delle criptovalute.

41

2.6.1. *Bitcoin nel 2014*

Il 2014 è stato definito come "*annus horribilis* del bitcoin"[42]. A gennaio apre, a Londra, Elliptic Vault, che si definisce come un servizio in grado di identificare attività illecite nel sistema Bitcoin grazie a un'intelligence che comprende specialisti di criptovalute, istituzioni finanziarie e governative. Per usare le loro parole, sono coloro che trovano la verità tra i database[43]. Elliptic Vault prova che le operazioni siano conformi alle normative AML[44] e investiga su eventuali illeciti che coinvolgano l'utilizzo di BTC. Nel frattempo, anche il D Las Vegas Casino Hotel e il Golden Gate Hotel & Casino annunciano di accettare BTC come pagamento[45], così come il The Chicago Sun-Times[46].
Il 27 Gennaio il giornale The Guardian riporta la notizia che il vicepresidente della Bitcoin Foundation è stato arrestato con le accuse di riciclaggio, avendo venduto a operatori di Silk Road circa un milione di dollari di BTC; Bitcoin accusa un brusco decremento di valore (circa del 30%), mantenendo un trend negativo per il resto dell'anno. A febbraio 2014 MtGox sospende le transazioni, chiude il sito ed il servizio di transazioni e dichiara bancarotta[47]. Tra il 31 gennaio e il 21 febbraio il bitcoin passa da 938 a 111 dollari. A fine dicembre, anche Microsoft accetta pagamenti in BTC[48] e il valore di Bitcoin oscilla intorno ai 315$.

---

[41] www.buybitcoinworldwide.com/it/prezzi/, grafico dell'andamento del tasso di cambio USD/BTC del triennio 2011-2013
[42] Eugenio Spagnuolo, *Storia breve del bitcoin*, WIRED [3/01/2019]
[43] "We are the people who find the truth in data" è lo slogan di Elliptic Vault
[44] Anti-Money Laundering, conosciuta in Italia come Normativa Antiriciclaggio, di cui si è già discusso nel paragrafo 2.2.
[45] Nancy Trejos, *Las Vegas casinos adopt new form of currency: Bitcoins*, USA TODAY [23/01/2014]
[46] Rob Wile, *The Chicago Sun-Times Now Accepts Bitcoin*, THE BUSINESS INSIDER, [3/04/2014]
[47] Tim Allman, *MtGox bitcoin exchange files for bankruptcy*, BBC [1/03/2014]
[48] Matthew Sparkes, *Tech giant Microsoft accepts Bitcoin payments*, THE TELEGRAPH [11/12/2014]

2.6.2. Bitcoin nel 2015

Il 2015 è stato un anno relativamente tranquillo per i Bitcoin: non vi è alcuno shock particolarmente forte nell'andamento dei prezzi e non vi sono eventi che modificano radicalmente il modo di vedere o utilizzare il sistema.

L'anno si apre, tuttavia, con uno *shutdown*[49] di Bitstamp, un servizio exchange britannico; sul sito si poteva leggere che la chiusura era dovuta a un probabile furto di 19,000 BTC (circa 5 milioni di dollari)[50] da alcuni account da parte di un hacker. Il sito tornò operativo il 9/01, dopo aver aumentato le misure di sicurezza. A ottobre partì una proposta[51] per inserire un carattere nel sistema Unicode[52] che rappresenti Bitcoin, proposta che viene accettata nel mese successivo, con l'accettazione del simbolo "Ƀ", identificativo di Bitcoin. Il NYDFS[53] applicò una regolazione all'utilizzo di Bitcoin chiama BitLicense[54] e alle piattaforme di exchange, tanto che alcune piattaforme abbandonarono lo Stato.

Il valore dei token si mantiene stabile, eccetto qualche giorno in gennaio, tra i 200$ e i 300$, per poi salire improvvisamente a fine anno; il giorno di Natale, un BTC vale 455$.

2.6.3. Bitcoin nel 2016

L'anno si apre con il governo giapponese che riconosce, nel mese di marzo, Bitcoin come sistema sostitutivo alla moneta[55] e, pochi giorni dopo, Bidorbuy (il principale marketplace sudafricano) approva i bitcoin come metodo di pagamento. Continuano ad esserci attacchi di hacker alle piattaforme di exchange, come ad esempio a Bitfinex, la quale perde quasi 120,000 BTC[56] con un singolo attacco, in agosto; questo causa una perdita di valore di Bitcoin del 20%. Il 9 luglio accade il secondo *halving event* che porta la ricompensa dei miner per il lavoro svolto a 12.5 BTC.

Il trend annuale dei prezzi è, eccezion fatta per agosto, nettamente positivo: l'anno si apre con una quotazione di circa 430$ e si chiude con un aumento maggiore del 100%.

2.7. La quarta fase di Bitcoin (2017 - 2019)

2.7.1. Bitcoin nel 2017

Il 2017 è stato, senza ombra di dubbio, l'anno che ha cambiato la storia di Bitcoin. L'anno inizia con il ritorno del valore a quota 1000$ già nel corso di gennaio, proseguendo il trend positivo iniziato a settembre 2015. Nel mercato internazionale, si espande la categoria di commercianti che accettano il BTC come forma di pagamento sostitutiva della moneta e aumentano i riconoscimenti legislativi

[49] Chiusura temporanea dei servizi
[50] Caleb Chen, *Bitcoin Exchange Bitstamp Confirms Loss of ~18,866 BTC (~$5 million USD) from Hot Wallet,* CCN [6/01/2015]
[51] Ken Shirriff. *Proposal for addition of bitcoin sign*, UNICODE CONSORTIUM [2/10/2015]
[52] L'Unicode è un sistema di codifica che assegna un numero univoco ad ogni carattere usato per la scrittura di testi, in maniera indipendente dalla lingua, dalla piattaforma informatica e dal programma utilizzato.
[53] New York State Department of Financial Services
[54] Davis Polk, *New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal* [5/06/2015]

[55] Mai Ishikawa, *Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case*, JOURNAL OF FINANCIAL REGULATION [4/01/2017]
[56] Frances Coppola, *Theft And Mayhem In The Bitcoin World*, FORBES [6/08/2015]

all'utilizzo delle criptovalute: si stima che in Giappone, nel 2015, fossero circa 260,000 i servizi commerciali che accettavano la criptovaluta[57]. Perfino la Russia, che fino a quel momento aveva mantenuto un certo scetticismo nei confronti delle criptovalute, inizia a considerare l'idea di utilizzarle a livello individuale e governativo: Putin, il 2 giugno, si espresse pubblicamente a favore delle tecnologie che facilitassero la creazione di business model basati sulla digital economy (pur se con dissenso del primo ministro Igor Shuvalov), Elvira Nabiullina (capo della Banca Centrale Russa) disse ai microfoni dell'NBC che era in corso un'analisi dell'eventuale legalizzazione delle criptovalute, mentre Olga Skorobogatova, sua vice, dichiarò pubblicamente che la banca stesse considerando l'idea di lanciare la sua criptovaluta[58]; anche la più grande banca svedese, la Skandiabanken, inizia a integrare account Bitcoin[59]. Nasce nell'agosto 2017, Bitcoin Cash[60], tramite un *hard fork* della catena, precedentemente annunciato, e per volere degli stessi sviluppatori di Bitcoin.

Inoltre, iniziano a guadagnare terreno, oltre ai Bitcoin e ad altre criptovalute simili, gli stablecoin, Tether[61] in primis. Come spiega il Sole24Ore[62], gli stablecoin e i Bitcoin, che sulla carta dovrebbero essere avversari, crescono in parallelo: questo perché la conversione di una criptovaluta in moneta reale è, per ora, un processo lungo e scomodo, se paragonato alla conversione tra due criptovalute. Gli stablecoin sono un modo veloce per convertire una criptovaluta in una riserva di valore, evitando un iter lungo e proteggendosi dall'alta volatilità delle criptovalute. L'articolo continua spiegando che Tether, nonostante non sia l'unico stablecoin sul mercato, nel 2017 «ha gestito sostanzialmente un monopolio che ha influenzato pesantemente l'andamento dei prezzi sui vari exchange, come evidenziato da un'analisi statistica dell'Università di Austin, Texas. Molto è dipeso dal fatto che la società che emetteva i Tether era de facto controllata dalla più grande crypto-exchange dell'Asia, Bitfinex», anche se è difficile affermare con certezza se sia stato Tether a influenzare Bitcoin o viceversa, dato che probabilmente l'effetto è stato reciproco.

Il volume delle transazioni inizia a salire in seguito a questi eventi portando il prezzo a salire incessantemente da maggio, mese che si apre con un prezzo registrato di 1,400$ per BTC. Per capire quanto velocemente salì il prezzo di Bitcoin nei mesi che vanno da maggio a dicembre 2017, basti guardare massimo e minimo del valore nei singoli mesi:

- Maggio: il minimo è registrato in apertura del mese ed è pari a circa 1,400$, mentre il massimo è registrato il 24 ed è pari a 2,400$;
- Giugno: il minimo è pari a 2,450$, registrato il primo giorno del mese, mentre il massimo risale al 14 ed è uguale a circa 3,000$;
- Luglio: i valori di minimo e massimo sono registrati a soli quattro giorni di differenza, il 16 (con un valore di 1,930$) e il 20 (quasi 2,900$);

[57] Business Insider Intelligence, *Bitcoin acceptance growing in Japan*, BUSINESS INSIDER [7/04/2017]
[58] Howard Amos, *Russia Is Becoming a Cryptocurrency Haven*, THE MOSCOW TIMES [12/7/2017]
[59] Rosemary Bigmore, *A decade of cryptocurrency: from bitcoin to mining chips*, THE TELEGRAPH [25/5/2018]
[60] Per una trattazione più approfondita di Bitcoin Cash si rimanda al sottoparagrafo 2.3.8.
[61] Per ulteriori informazioni su Tether, vedasi il sottoparagrafo 2.3.12.
[62] Marcello Minenna, *L'esplosione della bolla Bitcoin: un'autopsia*, SOLE24ORE [31/12/2018]

- Agosto: anche in questo caso il valore minimo, circa 2,730$, è registrato in apertura del mese, mentre il massimo, pari a 4,650 circa si raggiunge il 28;
- Settembre: questo mese rappresenta un'eccezione nel trend positivo del periodo, in quanto il prezzo massimo, che sfiora i 5,000$, si trova al primo giorno del mese, mentre a metà mese, il 14, si ha il valore minimo di 3,200$ (alla fine del mese il valore si attesta intorno ai 4,300$);
- Ottobre: in questo mese, invece, si ritorna al trend solito, con un valore minimo di circa 4,200$ il 5 e un massimo di 6,100 alla fine del mese;
- Novembre: in questo mese si assiste a un brevissimo trend ribassista che dura quattro giorni, chiudendo con il valore minimo registrato, il 12, di 5,800$, mentre il massimo arriva a fine mese, ed è pari a circa 10,000$, senza però raggiungerli;
- Dicembre: in questo mese viene registrato il valore massimo della storia di Bitcoin, pari a 19,783$, mentre il minimo si attesta a inizio mese e supera comunque i 10,000$.[63]

2.7.2. Bitcoin nel 2018

Il 2018 è stato un anno che potremmo definire "tragico" per Bitcoin e per tutti coloro che hanno puntato su questa criptovaluta nei mesi precedenti: il massimo raggiunto nel 2017 non verrà mai più raggiunto e il valore più alto assunto da Bitcoin si colloca cronologicamente il 5 gennaio, pari a circa 17,000$. A questo punto, prende piede un trend negativo che porterà, dopo una stabilità intorno al valore di 6,000$ durata qualche mese, a un valore di 3,700$, con cui si chiuderà l'anno.

Andando con ordine, sono diversi gli eventi del 2018 che possono aver causato una diminuzione del valore di Bitcoin, ma nessuno di loro appare così drastico da causare una riduzione di valore dell'80% nell'arco di 12 mesi. A gennaio, le autorità finanziarie coreane danno il via a un'indagine su alcuni servizi legati alle criptovalute in seguito a una petizione popolare, la quale lamentava un abuso delle criptovalute in manovre illecite e una mancata tutela degli investitori. Tale indagine sfocerà in una regolamentazione ferrea che obbliga gli utenti di Bitcoin e altre criptovalute a identificarsi nell'operazione, mettendo di fatto fine all'anonimato[64]. Anche in Cina, durante il National People's Congress di marzo, è stato dichiarato che le autorità cinesi non riconoscono le valute virtuali come Bitcoin come strumento di

[63] Tutti i riferimenti sono presi dai dati storici registrati da buybitcoinworldwide.com
[64] The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, [7/2018] p. 121

pagamento tradizionale e che, in parallelo a ciò, le banche non accettano alcuna criptovaluta[65].

Verso la fine di gennaio, anche Facebook annuncia di voler bloccare tutto l'*advertising* riguardante le criptovalute, in quanto molte compagnie non operavano in buona fede[66]; Google, meno di due mesi dopo, seguirà le orme di Facebook[67] e qualche giorno dopo anche Twitter e LinkedIn[68].

2.7.3. I motivi del crollo

«Come un anno fa non c'erano motivi specifici per un rialzo che si è rivelato del tutto ingiustificato, oggi non ci sono ragioni specifiche alla base della caduta, che sembra comunque destinata a proseguire», scrive il Sole24Ore[69] a fine 2018. Da una parte, nel 2017 l'aumento vertiginoso della quotazione di Bitcoin era dovuto a una presa di coscienza da parte delle istituzioni, che aveva modificato l'opinione degli investitori: Giappone, Russia e Svezia, tre nazioni notoriamente conservatrici, hanno aperto le frontiere virtuali all'utilizzo di questo nuovo strumento finanziario e questo ha causato un ottimismo intorno alle criptovalute, facendo alzare i valori a dismisura, ma senza un effettivo aumento di valore intrinseco delle stesse. L'effetto, tuttavia, è stato ingigantito dalla mole di investitori "curiosi" al riguardo e dal numero spropositato di criptovalute sul mercato, elementi che si sono autoalimentati nel clima ottimistico che aleggiava nel settore da settembre 2015. Al riguardo, si parla anche di aumenti "artificiali" di valore[70] ottenuti da transazioni fittizie operate dai gestori di Bitinfex, il più grande exchange asiatico nonché gestore del sistema Tether, a causa di un parallelismo tra il periodo di aumento di valore di Bitcoin e l'immissione di token Tether sul mercato, come evidenziato dal grafico.

---

[65] The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, [7/2018] p. 106
[66] Dave Lee, *Facebook bans all crypto-currency ads*, BBC [30/1/2018]
[67] Daisuke Wakabayashi, *Google Bans Bitcoin Advertisements in Policy Change*, THE NEW YORK TIMES [14/3/2018]
[68] Thomas Wilson, *Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind*, THE INDEPENDENT UK [28/3/2018]
[69] Pierangelo Soldavini, *Bitcoin in caduta libera perde il 30% in una settimana: le tre ragioni del crollo*, SOLE24ORE [20/11/2018]
[70] Matt Robinson e Tom Schoenberg, *Bitcoin-Rigging Criminal Probe Focused on Tie to Tether*, BLOOMBERG [20/11/2018]

Alle prime notizie negative (oltre alla regolamentazione ci sono stati attacchi di hacking a varie piattaforme di exchange), il mercato si trovò sorpreso, si scatenò il *panic selling*[71] e la quotazione di Bitcoin (e della maggior parte delle altre criptovalute non ancorate a una moneta reale) precipitò, fino al raggiungere i 3,000$. Nel periodo gennaio-aprile 2018, il calo è stato *demand-driven* e dunque determinato dalla fuga di investitori speculativi dell'ultim'ora, fortemente esposti per via dell'acquisto a prezzi molto elevati e spaventati dall'improvviso *turn-around* del mercato dopo una crescita insostenibile. Inoltre, come si vede dal grafico, in seguito alla diminuzione del valore di Bitcoin, l'emissione di Tether (la cui capitalizzazione, avendo un valore fisso, è costante) ha subito un brusco stop. L'opinione diffusa nei mercati è che i Tether fossero emessi "allo scoperto" per acquistare valute digitali e rivenderle quando il prezzo si fosse alzato, in modo da trarne profitto, ma venendo meno all'aspetto che dà un valore al sistema, ovvero che ad ogni token emesso corrisponda un dollaro nelle casse. Il prezzo di 6,000$ è legato al costo della potenza necessaria per il mining.

Il calo di novembre 2018, invece, è dovuto a un'ulteriore divisione di Bitcoin Cash, che, a differenza di quella che lo ha generato, mette in circolazione una valuta digitale priva di innovazioni, provocando semplicemente un "effetto scossa" nei mercati, che perdono fiducia. In questo caso il fattore è *offer-driven*, in quanto molti miner spostano la loro potenza di calcolo per minare le valute clone, sperando di poter raddoppiare i profitti. Questo ha provocato un calo di supporto al sistema Bitcoin. Anche in questo caso il valore dei token BTC è dovuto al costo della potenza di calcolo necessaria per il mining, che il sistema riduce grazie a un meccanismo di autoregolamentazione.

[71] "diluvio di vendite che a volte colpisce un tipo di mercato o una classe di attività, è un tipico esempio di come a cattive notizie o attese, possano corrispondere fenomeni anche turbolenti di vendita" [ex Borsa Italiana, https://www.borsaitaliana.it/notizie/speciali/obbligazioni/strumento-di-investimento/universo-corporate-bond/le-nuove-tendenze-del-mercato.htm)

2.7.4. Il Bitcoin nel 2019

Il 2019 di Bitcoin è iniziato con una ripresa rispetto al 2018, in quanto il valore del token, che nel primo mese è restato stabile tra i 3000$ e i 4000$ (senza mai toccare nessuno dei due estremi), ha iniziato da febbraio un trend positivo che ha portato BTC a raddoppiare il suo valore nel mese di maggio. Nel momento in cui scriviamo, il suo valore si aggira intorno agli 8000$ per token, con una capitalizzazione di mercato di circa 140 miliardi di dollari.

3 – La Blockchain

3.1. Fondamenti teorici della Blockchain

3.1.1. Cenni sulla crittografia

Crittografia in greco significa "scrittura segreta" e rappresenta la tecnica di rendere incomprensibile un messaggio a chi non è autorizzato a leggerlo. Si parla di crittografia non solo nel linguaggio informatico, ma in generale quando ci si riferisce a un messaggio mandato attraverso un codice incomprensibile per chiunque non sia destinatario. Nel caso della Blockchain, la crittografia viene invece utilizzata non per nascondere dati, ma per garantire la sicurezza del sistema e impedire manomissioni. Anzi, un grande pregio della blockchain è che i dati, rappresentati dalle transazioni, non sono nascosti, ma pubblici e condivisi tra tutti i partecipanti della rete: grazie a questo si ottiene la decentralizzazione.

3.1.2. L'apporto di Wei Dai

Come già trattato precedentemente, il Bitcoin non nasce *ex novo* dalla mente di Satoshi Nakamoto, ma riprende idee già discusse nel cripto-mondo[72]. David Chaum, Milton Friedman, Douglas Jackson, Barry Downey e Wei Dai sono le persone che hanno iniziato a costruire le fondamenta teoriche sul quale l'intero palazzo del Bitcoin e delle valute virtuali è stato costruito.

Tuttavia, a eccezione di Wei Dai, nessuno di loro aveva proposto nulla di simile alla Blockchain per far funzionare un sistema dei pagamenti alternativo. Wei Dai, nel suo progetto (sempre rimasto teorico) "B-money", individuò due funzioni fondamentali a cui doveva assolvere un ipotetico nuovo sistema dei pagamenti indipendente da ogni autorità centrale: un mezzo di scambio della moneta e un modo per assicurarsi che i contratti vengano rispettati, funzioni di cui si occupa, fondamentalmente e in misura diversa in ogni parte del mondo, il governo.
Wei Dai assunse per vera un'ipotesi, tutto sommato verosimile, per trattare l'argomento in modo più semplice: l'esistenza di un network non tracciabile che permetta lo pseudoanonimato tra le parti di una trattativa, in cui ogni transazione è firmata dal mittente e decriptata dal destinatario. Dopodiché descrisse un plausibile sistema che funzionasse grazie a due protocolli.

Nel primo protocollo, ogni elemento del sistema conserva un database indipendente in cui registra quanta moneta appartiene a ogni pseudonimo e l'insieme di questi database determina quanta moneta ha ciascuno. Il protocollo riguarda il modo in cui questi quantitativi di moneta virtuale individuale sono aggiornati ed è diviso in punti:

1. la creazione di moneta: tutti possono creare moneta risolvendo un problema computazionale a condizione che sia facile determinare oggettivamente lo sforzo necessario per risolverlo e che il "premio" in moneta concesso a ciascuno sia proporzionale a tale sforzo;
2. il trasferimento di moneta: se la persona che si nasconde dietro lo pseudonimo "A" vuole trasferire una quantità di moneta X al proprietario dello pseudonimo "B", è sufficiente che immetta nel sistema il messaggio "Do a B una quantità di moneta pari

[72] Paragrafo 2.2.

a X" e firmi tale messaggio, in modo che ognuno aggiorni il database per quanto riguarda i profili di A e B, eccetto che questo non porti A alla detenzione di una quantità negativa di monete, in quel caso il messaggio è ignorato;

3. l'effetto dei contratti: un contratto valido deve includere un massimo di risarcimento in caso di fallimento di ogni parte contrattuale, nonché contemplare una terza parte che eseguirà un arbitrato nel caso di contestazioni; tutte le parti di un contratto, incluso l'arbitro, devono inviare in rete le loro firme digitali del contratto prima che questo possa essere considerato valido, dopodiché i partecipanti addebitano il massimo della quota al conto terzo, che si identifica con un hash[73] di sicurezza del contratto; il contratto è efficace se gli addebiti funzionano su tutte le parti contrattuali senza che si verifichi un bilancio negativo per nessuno, nel qual caso il contratto viene ignorato e si ha un *rollback*[74];
4. la conclusione dei contratti: quando il contratto si conclude, ogni parte invia in rete un messaggio firmato in cui si chiarifica il modo con il quale si è concluso (con l'adempimento dell'obbligazione o con disputa) e, una volta arrivate tutte le firme, le parti riprendono la quota versata per l'eventuale inadempimento (se questo non si è verificato) e cancella l'account fittizio del contratto;
5. applicazione dei contratti: se le parti non trovano un accordo sulla conclusione nonostante l'aiuto di un arbitro, ogni parte invia nella rete una proposta di risarcimento o sanzione argomentandola a suo favore e ogni partecipante fa una determinazione in merito, dopodiché modifica il suo database.

Il secondo protocollo di Wei Dai riguarda i conti correnti di ciascuno, localizzati in un sottoinsieme di partecipanti chiamato *server* e non nei database individuali. Questi server sono collegati da una rete di trasmissione di tipo Usenet[75]. Il formato dei messaggi che rappresentano le transazioni resta uguale a quello del primo protocollo, ma i partecipanti al canale dove è stato trasmesso il messaggio devono verificare che questo sia stato ricevuto ed elaborato correttamente in un sottoinsieme casuale di questi server. È necessario un meccanismo per mantenere l'onestà dei server: ad ognuno di loro è richiesto di accreditare una certa quantità di denaro su un conto corrente speciale, il quale rappresenta il risarcimento per multe o il premio per ricompense e, inoltre, ogni server deve pubblicare i propri database aggiornati con le operazioni di creazione e attribuzione di denaro. Ogni partecipante deve verificare che il bilancio del proprio conto corrente sia esatto e che la somma di tutti i bilanci non superi la quantità massimo di denaro, ovvero quella creata, in questo modo anche in caso di collusione totale, è impossibile aumentare costantemente e senza costi la quantità di denaro circolante.

3.1.3. Hashcash

Nel 1992 due ricercatori, di nome Cynthia Dwork e Moni Naor, presentarono alla Conferenza Annuale di Criptologia (tenutasi a Santa Barbara, California) un documento dal nome "Determinazione del prezzo tramite elaborazione o lotta contro la posta indesiderata". Nell'abstract del *white paper* si legge che il contenuto tratta

[73] Un "hash" è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

[74] Tutti i conti correnti vengono ripristinati al valore precedente.

[75] La rete Usenet è una rete mondiale formata da migliaia di server tra loro interconnessi, ognuno dei quali raccoglie dei dati o post che le persone aventi accesso alla rete inviano in una data gerarchia, in un archivio ad accesso pubblico.

una tecnica computazionale per combattere la posta indesiderata in particolare, mentre in generale si tratta di un sistema di controllo di accesso a una risorsa condivisa; per fare questo, sono suggerite, nel corso della trattazione, diverse funzioni di determinazione del prezzo calcolate attraverso la potenza di elaborazione di chi utilizza il sistema: in questo modo, impostando delle funzioni difficili, ma non intrattabili, si raziona l'accesso alla risorsa in quanto un sovraccarico di domanda non rende possibile al computer che la invia il calcolo di così tante funzioni.

Nel 1997, il crittografo Adam Back propose una funzione simile e la chiamò Hashcash, un'iterazione pensata come meccanismo di controllo dell'abuso sistematico di risorse condivise e disponibili a tutti, come il servizio e-mail.

Il sistema Hashcash applicato al servizio e-mail implica che una funzione moderatamente difficile deve essere risolta al fine di mandare una mail, ciò significa che per qualunque computer non è un problema risolvere la funzione e mandare una mail, ma diventa un problema mandarne troppe. In questo modo, gli account di posta elettronica che fanno *spam*[76] sono disincentivati a farlo a causa della potenza computazionale necessaria molto alta. Un codice testuale di un hashcash viene aggiunto all'intestazione dell'e-mail, in modo da provare che il mittente ha impiegato un certo lasso di tempo e di potenza computazionale: attraverso un rapporto tra la difficoltà del problema e il lasso di tempo impiegato per risolverlo è possibile vedere se il mittente sia uno spammer. Il destinatario può, ad un costo di calcolo trascurabile, verificare che il timbro sia valido.

Hashcash utilizza una funzione di hash crittografica denominata "SHA-1" (Secure Hash Algorithm 1); la denominazione "SHA" indica una famiglia di cinque funzioni crittografiche di hash:

- SHA-1;
- SHA-224;
- SHA-256;
- SHA-384;
- SHA-512;

Le ultime quattro vengono indicate, solitamente, sotto il nome comune di SHA-2, per differenziarle dalla prima. SHA-1 produce un digest[77] del messaggio di soli 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla; all'aumentare dei bit da cui è formato il messaggio, aumenta la complessità di decifrazione messaggio.

Una buona funzione di hash ha una serie di proprietà:

- velocità di calcolo: dato un qualunque m, la funzione h(m) è calcolabile in modo veloce ed efficiente;

[76] Messaggio pubblicitario non richiesto, inviato a un numero molto elevato di utenti di Internet tramite posta elettronica. Il termine viene più comunemente utilizzato per indicare l'azione di mandare spam.
[77] "Digest" è l'output dell'applicazione dell'algoritmo hash, rappresentato da una stringa di dimensioni variabili a seconda della funzione crittografica di hash utilizzata, e rappresenta in modo compatto le informazioni originali contenute nel documento firmato. Il digest è ciò che permette la decodifica e, più sono i bit dai cui è composto, più diventa difficile tale decodifica.

- unidirezionalità: dato h(m) è computazionalmente molto difficile tornare a m;
- resistenza alle collisioni: è molto difficile trovare m1 e m2 tali che h(m1) = h(m2).

3.2. La Blockchain in Bitcoin

3.2.1. Definizione di Blockchain

La Blockchain analogamente è una raccolta di operazioni dette "transazioni", effettuate tra gli utenti di uno stesso network. Tecnicamente è un database distribuito in una rete di nodi peer-to-peer. Come ci dice l'etimologia della parola, la Blockchain è una catena di blocchi concatenati tra loro, ciascuno dei quali è costituito da un insieme di transazioni. Il legame tra blocchi è di tipo crittografico: ogni blocco contiene uno speciale riferimento a quello precedente e questo riferimento è dato da una stringa alfanumerica, detta hash, calcolata tramite la funzione crittografica SHA-256, che identifica il blocco precedente.

3.2.2. La difficoltà della Blockchain

La rete di Bitcoin è preimpostata per mantenere il tasso medio di creazione di blocchi a sei all'ora. Pertanto, per garantire che il tasso di creazione di blocchi rimanga invariato nonostante la creazione di potenti apparati minerari, la rete aumenta periodicamente la difficoltà. La difficoltà, come mostrata nel grafico sottostante, riflette quindi l'intensità dell'attività dei miner sulla rete.

78

3.2.3. Le transazioni

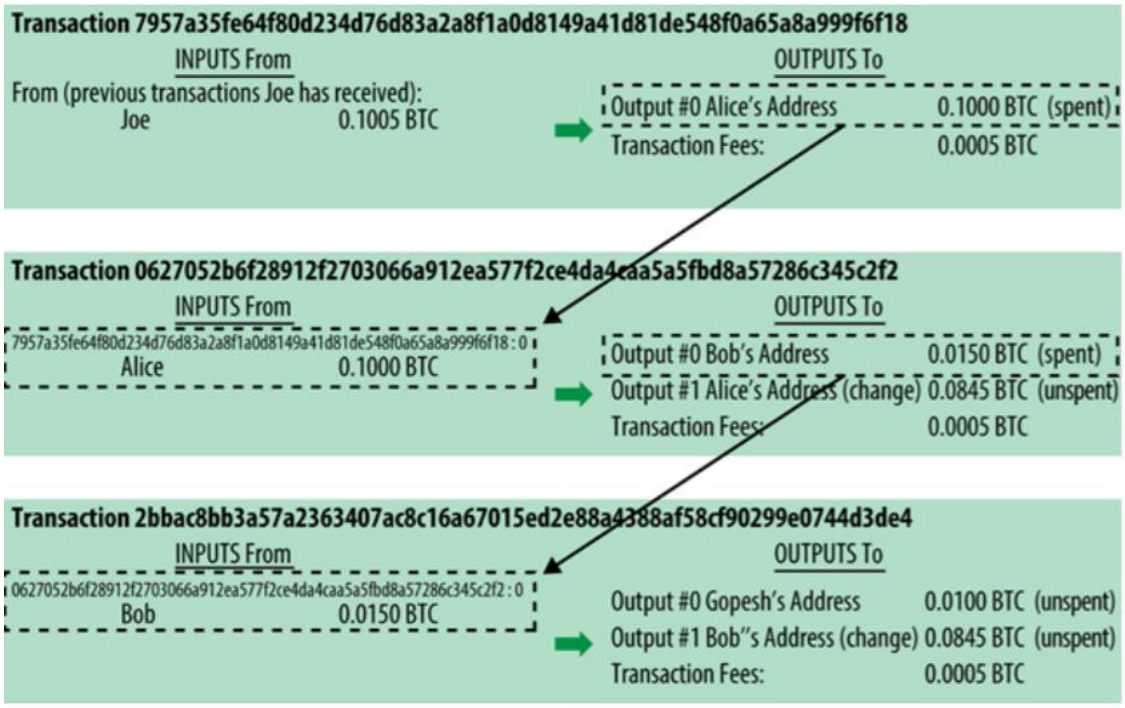
Una transazione, nel caso del sistema Bitcoin, non è altro che uno scambio di informazione tra utenti, in particolare l'informazione è un asset monetario che dopo una transazione subisce un cambio di proprietà, passando da un utente mittente A ad un utente ricevente B. Ogni blocco è formato da quantità variabile di transazioni e la totalità dei blocchi forma blockchain, il libro mastro che tiene traccia di tutti gli scambi avvenuti tra gli utenti, dal blocco genesi fino ad oggi.

Per effettuare una transazione è necessario avere un *wallet*[79] che fornisca una chiave pubblica (quindi conosciuta da tutti) grazie alla quale è possibile ricevere moneta e una chiave privata (conosciuta solo dal proprietario), grazie alla quale è possibile inviare moneta.

Supponendo che A voglia spedire X BTC a B, è necessario che quest'ultimo fornisca il proprio indirizzo pubblico ad A, la quale firmerà un messaggio con la propria chiave privata in cui dichiarerà di voler spedire X BTC a B. Quando il messaggio

[78] Fonte: blockchain.com/it/charts/difficulty
[79] Testualmente, la parola "wallet" si traduce con "portafoglio". In questo caso, tuttavia, un wallet è un software

viene spedito nel network chiunque può verificare che sia stato firmato da A e che la quantità di moneta che intende inviare sia effettivamente in suo possesso. Questa verifica è possibile farla consultando tutte le transazioni che sono state fatte da e verso l'indirizzo pubblico di A e quindi il suo saldo è facilmente ricavabile. In questo modo, a transazione chiusa, è possibile per B spendere questi BTC attraverso un'altra transazione che autorizza il trasferimento a un eventuale utente C e così via. Ogni transazione ha un input, rappresentato dalla chiave privata del mittente, e un output, rappresentato dalla chiave pubblica del destinatario.



80

Il grafico rappresenta un esempio di catena di tranasazioni: nel primo riquadro il wallet di Joe crea una transazione (identificata da un codice hash) che vede l'invio di 0.1005 bitcoin, di cui 0.1000 all'indirizzo di Alice e 0.0005 in *transaction fee*, una commissione pagata per incentivare i miner a convalidare prima la transazione in un blocco. Gli input provengono dall'output di una precedente transazione in cui Joe è stato il beneficiario e vanno a finire negli output riportati a destra. Nella seconda transazione Alice invia 0.1000 bitcoin di cui 0.0150 a Bob, 0.0845 al suo *wallet* (come resto) e 0.0005 in *transaction fee.* La regola è che la somma degli input deve sempre pareggiare quella degli output, ecco il motivo per cui Alice invia un resto al suo stesso *wallet*. In questo caso l'input fa riferimento all'output della transazione in cui Alice ha ricevuto bitcoin da Joe (cioè quella nel primo riquadro) e va a finire nell'output di destra. Infine, nell'ultima transazione, con lo stesso principio, Bob invia della moneta all'indirizzo di Gopesh, della moneta al suo portafoglio come resto e una *transaction fee*.

Una volta creata la transazione, il nodo che l'ha creata la invia ai nodi circostanti facenti parte della stessa rete, affinché venga validata. Se il processo va a buon fine,

[80] Fonte: Mastering Bitcoin

la transazione arriva ad altri nodi e viene restituita una conferma al mittente iniziale. Questo processo di inoltro delle transazioni si chiama *flooding*[81].

3.2.4. La funzione della Blockchain in Bitcoin

Satoshi Nakamoto, nel suo white paper, scriverà: "per implementare un server timestamp distribuito su base peer-to-peer, dovremo utilizzare un sistema di proof-of-work simile all'Hashcash di Adam Back, piuttosto che ai giornali o ai post Usenet. Il proof-of-work implica la scansione di un valore che, con hash, come con SHA-256, l'hash inizia con un numero di bit zero"[82]. SHA-256, tuttavia, non è l'unica funzione di hash utilizzata dal sistema Bitcoin, in quanto oltre a questa viene utilizzata un'altra funzione chiamata RIPEMD-160, simile nelle performance a SHA-1 (anch'essa a 160 bit).

La crittografia utilizzata da Bitcoin è detta "asimmetrica" (o a chiave pubblica/privata), in quanto utilizza due chiavi interdipendenti, una per cifrare i dati, e l'altra per decifrarli (piuttosto che un'unica chiave, come accade per la cifratura "simmetrica"). La crittografia asimmetrica in Bitcoin, per concludere, è impiegata per due scopi: cifrare un messaggio o verificarne l'autenticità. Nel primo caso il mittente cifra il messaggio con la chiave pubblica del destinatario, in modo tale che solo quest'ultimo grazie alla propria chiave privata, possa decifrarlo e leggerlo. Nel secondo caso, quello che interessa Bitcoin, il messaggio viene cifrato dal mittente con la chiave privata in suo possesso e il destinatario può verificarne l'autenticità decifrandolo con la chiave pubblica del mittente. L'algoritmo utilizzato da Bitcoin per generare questa coppia di chiavi è ECDSA (Elliptic Curve Digital Signature Algorithm), un algoritmo di firma digitale[83]. Questo meccanismo permette alla crittografia di avere tre funzioni:

- autorizzazione alla spesa: chi possiede la chiave privata può usarla per spendere i propri fondi;
- non ripudiabilità: le parti che intervengono in un determinato scambio non possono poi negare di aver preso parte allo stesso;
- non modificabilità: una volta che una transazione o parte di essa è firmata, non la si può modificare senza invalidarla.

3.2.5. Il mining

Il mining è definito come un "processo di consenso distribuito"[84], il quale consente al sistema Bitcoin di essere decentralizzato, in quanto assolve al compito che nei sistemi di pagamento tradizionali è affidato all'autorità centrale, cioè quello di autorizzare e validare le transazioni. I miner sono sparsi nel mondo e registrano le transazioni nei blocchi che compongono la Blockchain, quando tali blocchi vengono aggiunti alla catena, i miner hanno anche il compito di garanti della sicurezza del

[81] In italiano, "inondazione"
[82] Satoshi Nakamoto, *White Paper*, p. 3
[83] Una firma digitale è uno schema matematico che serve a dimostrare l'autenticità di un messaggio o di un documento digitale, essa dà la certezza che il mittente abbia inviato il messaggio e che quest'ultimo non sia stato manomesso
[84] Bitcoin.org

sistema, in quanto è nel loro interesse assicurarsi che le transazioni confermate siano valide.

Nella pratica, il mining richiede computer molto potenti che risolvono problemi di calcolo computazionale molto complessi[85]. La parola "mining" indica, in lingua inglese, l'atto del minare una vena d'oro nel terreno: l'associazione deriva da un parallelismo tra le due attività nel lavoro e nella fortuna richiesta per completare il lavoro e dal "premio" che si ottiene, che nel caso di un minatore di oro è un certo valore in oro, mentre nel caso di un miner di bitcoin è un certo valore in BTC.

La ricompensa per la registrazione e la validazione di un intero blocco di transazioni è variabile; in particolare, essa varia con il tempo: il primo *halving event* risale al novembre 2012, mentre il secondo al luglio 2016. Ne è previsto un terzo (che porterà alla ricompensa di 6,25BTC) per la metà del 2020.

Affinché un miner guadagni, è necessario che siano verificate transazioni nella quantità di almeno 1Megabyte (che, teoricamente, può essere solo una, ma nella pratica sono migliaia, a seconda di quante informazioni contenga ogni transazione) e che sia risolto il problema matematico computazionale; questa seconda parte, chiamata "Proof-of-Work", che caratterizza appunto il sistema come un sistema PoW. Ciò che fanno effettivamente i computer dei miner è provare a trovare un numero esadecimale a 64 cifre chiamato "hash". I computer dei miner vanno a una velocità che può essere nell'ordine di Megahash al secondo (MH/s), Gigahash al secondo (GH/s) o, addirittura, Terahash al secondo (TH/s), che identifica il numero di tentativi effettuati in un secondo di indovinare l'hash. La difficoltà identifica il

[85] "complessità", in questo senso, è usata nel significato "impossibili da risolvere senza un computer" in tempi relativamente utili.

reciproco della probabilità che un numero emesso sia minore o uguale al target. La difficoltà varia secondo il sistema già trattato[86].

3.3. Applicazioni della Blockchain al di fuori di Bitcoin

La Blockchain utilizzata nel sistema Bitcoin può concretamente cambiare la nostra vita. Tuttavia, il "come" resta un interrogativo non indifferente. È stato condotto uno studio da parte dell'EPRS[87] che mette ha il compito di approfondimento e sensibilizzare il mondo politico e amministrativo sulle potenzialità della Blockchain, tecnologia particolarmente adatta, ad esempio. per tracciare i prodotti attraverso catene di approvvigionamento e filiere oppure per risolvere problemi quali pirateria di contenuti multimediali.

3.3.1. Altre tipologie di Blockchain

La Blockchain di Bitcoin, così come quella delle altre criptovalute (come ad esempio Ethereum), si presenta come un libro mastro di transazioni raggruppate in blocchi distribuiti in una rete libera[88] di nodi paritari. Questa tipologia di Blockchain prende il nome di *Permissionless*[89].

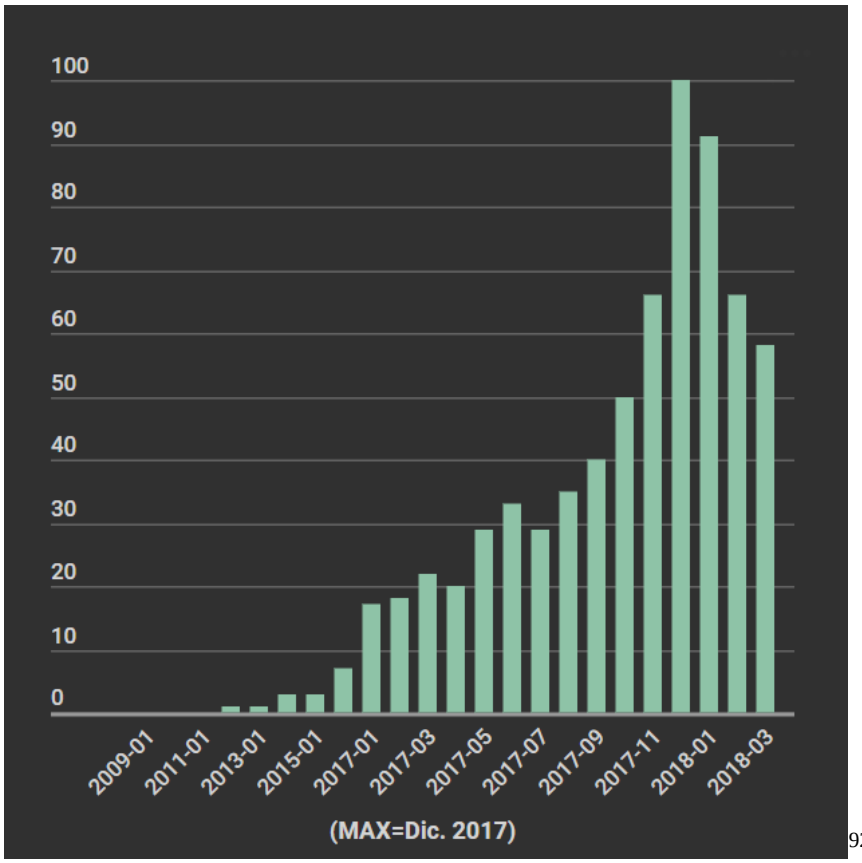
Esiste un'altra tipologia di Blockchain, chiama *Permissioned*, la quale è utilizzata per scambiare informazioni in maniera privata e più efficiente rispetto ad una permissionless, in quanto nelle permissioned non c'è necessità di escogitare un meccanismo artificioso (quale l'algoritmo POW) per eleggere il nodo che dovrà formare un nuovo blocco, in quanto i nodi validatori e creatori vengono scelti dagli amministratori e quando gli utenti scambiano transazioni, si affidano ai *trusted peer*[90], che raggiungono il consenso utilizzando algoritmi più efficienti di quelli usati per le permissionless Blockchain; questo comporta un miglioramento delle prestazioni in termini di velocità delle transazioni.

Oltre ad essere con o senza permessi per entrare nella rete, le Blockchain possono essere raggruppate sotto un'altra classificazione: pubbliche o private. Se la catena è pubblica, i nodi possono consultarla anche senza essere necessariamente parte attiva della rete[91] (come si intuisce, la Blockchain di Bitcoin è pubblica). Se privata, al contrario, può essere consultata solo dai nodi che hanno il permesso di accedere. Mentre le Blockchain permissionless non posso essere per definizione private, una permissioned potrebbe essere sia pubblica che privata, e generalmente sono private.

Dal successo di Bitcoin, la Blockchain ha ricevuto un'attenzione importante da parte dei media e del pubblico, diventando argomento centrale di molte innovazioni in settori anche molto diversi da quello delle criptovalute.

---

[86] 3.2.2.
[87] European Parliamentary Research Service.
[88] Da intendersi come "senza barriere all'ingresso".
[89] In italiano può essere tradotto come "Senza (bisogno) di permessi".
[90] "Nodi fidati"
[91] Il che implicherebbe la validazione o la creazione di blocchi.



[92]

3.3.2. *Prospetto generale sull'utilizzo della Blockchain*

Nonostante la tecnologia Blockchain sia un'implementazione necessaria per migliorare sia la sicurezza che l'affidabilità del sistema di *data storage*, molte imprese sostengono di non fidarsi del sistema. Questo perché alla maggior parte delle persone serve un periodo di utilizzo sperimentale di una nuova tecnologia prima di fidarsi, ancor più se la tecnologia di cui si parla è emergente e non affermata, come il caso della Blockchain; inoltre, molti pensano che ci saranno problemi per quanto riguarda la bassa standardizzazione tra sistemi Blockchain-based in organizzazioni diverse, che impedirebbe l'interoperabilità tra queste catene di dati. Oltre ai problemi che vengono all'emergere di una nuova tecnologia, fa la sua parte anche un *understanding gap*[93]*:* ancora oggi molti organi direzionali non hanno ben chiaro cosa sia una Blockchain e come può modificare il proprio settore.

Inoltre, fino a quando non ci sarà una regolazione ben precisa, probabilmente molti governi preferiscono che questa tecnologia sia utilizzata solo in via sperimentale, poiché sarebbe facile cadere in un vuoto legislativo[94].

Ad ogni modo, tutte le stime dicono che nel futuro prossimo la Blockchain verrà utilizzata da un numero sempre maggiore di imprese e che, probabilmente, la disciplina della gestione d'impresa non potrà prescindere dall'utilizzo di uno strumento così utile. Secondo Frank Xiong, vicepresidente del gruppo di sviluppo

[92] Fonte: http://www.report.rai.it/webdoc/2018-bitcoin/
[93] Un *understanding gap* si ha quando c'è una differenza rilevante tra un concetto, in questo la Blockchain, e come questo viene percepito.
[94] Con l'espressione "vuoto legislativo", in giurisprudenza e in diritto, si indica l'assenza di una normativa legislativa che regolamenti una determinata materia giuridica.

della Blockchain di Oracle, entro pochi anni tra il 50% e il 60% delle imprese nel mondo utilizzeranno la tecnologia Blockchain[95]

Il gruppo di imprese che utilizzano questa tecnologia, tuttavia, non è poi così ridotto: secondo uno studio condotto da PwC[96], circa l'84% delle imprese analizzate (circa 600 in 15 Paesi diversi) sta studiando direttamente la tecnologia Bitcoin per applicarla al proprio business model; in particolare, circa il 20% è in una fase di ricerca, il 32% in fase di sviluppo, il 10% in fase di sperimentazione e il 15% ha già integrato la tecnologia Blockchain nei propri sistemi informatici, il restante 21% ha dichiarato di non aver ancora considerato ufficialmente il progetto oppure di averlo messo in pausa. Il gruppo di imprese che utilizza la Blockchain vede la partecipazione anche marchi di una certa importanza al di fuori del mondo bancario e finanziario, come ad esempio:

- Apple;
- Royal Dutch Shell;
- Toyota Motor Corp;
- Samsung;
- Walmart;
- Nestlé;
- Amazon;
- Walt Disney Company;

La maggior parte di queste utilizza la Blockchain per avere informazioni più precise e attendibili dei propri processi, come ad esempio Toyota, altre la utilizzano per rimuovere dalla catena dei ruoli intermediari ritenuti non necessari, come ad esempio Amazon[97].

3.3.3. La Blockchain nel settore finanziario

La tecnologia Blockchain permette un'ottimizzazione innovativa dell'intero sistema finanziario in quanto permette lo scambio di informazioni in modo efficiente, sicuro e trasparente. Questa nuova tecnologia andrebbe a modificare il modo di scambiare informazioni tra dipendenti in un business, in quanto permette di scambiare informazioni tra il personale con modalità rapide, più efficienti e con un grado maggiore di trasparenza rispetto ai sistemi di IT utilizzati oggi.

Inoltre, utilizzando la Blockchain come sistema di *storage* di informazioni si avrebbe un grado maggiore di sicurezza e si avrebbero vantaggi anche a livelli macroeconomici per quel riguarda la riduzione di costi di controllo. Implementare oggi questa tecnologia potrebbe significare raggiungere un vantaggio competitivo di lungo termine in tutto il settore *services* e la possibilità concreta di mantenere tale vantaggio nel tempo.

---

[95] Monica Melton, *Blockchain Could Be Used By At Least 50% Of All Companies Within 3 Years, Oracle Exec Says,* FORBES [09/4/2019]

[96] Il report, chiamato *Blockchain is here. What's your next move*, è un'esortazione al mondo imprenditoriale a implementare l'utilizzo di Blockchain, in quanto la scarsa fiducia al sistema potrebbe ritardare di parecchio la sua integrazione.

[97] Michael del Castillo, *Big Blockchain: The 50 Largest Public Companies Exploring Blockchain,* FORBES [3/7/2018]

Già nel 2016, secondo degli studi condotti dall'IBM Institute for Business Value (IBV)[98], una buona parte delle banche che hanno un business model orientato verso l'innovazione, chiamate in gergo *early adopter* e nelle indagini IBM *trailblazers*, sono le stesse che hanno un posizionamento in grado di proteggerle dalla minaccia di nuovi entranti. Il 70% delle istituzioni finanziare interpellate ha dichiarato di aver concentrato le risorse destinate allo sviluppo di una Blockchain in quattro aree chiave:

- Compensazione;
- pagamenti all'ingrosso;
- Equity ed emissione di titoli del debito;
- Reference data.

Tra gli istituti bancari intervistati, invece, i *trailblazer* si attendono che i principali benefici legati all'adozione delle Blockchain arriveranno dai reference data (83%), dai pagamenti digitali retail (80%) e dal credito al consumo (79%). Gli ostacoli a una massiccia diffusione della Blockchain riguardano principalmente vincoli di carattere normativo (citati dal 56% del campione preso in esame), l'immaturità della tecnologia (citata dal 54% del campione) e la difficoltà di valutazione del ROI (citata dal 52%). Nel corso delle stesse indagini, Likhit Wagle[99], ha affermato che gli *early adopter* sono fondamentali nell'ambiente, in quanto hanno il potere di definire gli standard del mercato e di creare nuovi modelli di business basati sull'utilizzo della Blockchain destinati a essere utilizzati anche da chi percorrerà questa strada dopo di loro.

Secondo uno studio di European Investment Bank[100], l'applicazione della Blockchain potrebbe facilitare il funzionamento delle Istituzioni Finanziarie Internazionali a causa alla capacità della nuova tecnologia di gestire operazioni come conferma delle transazioni, *data storage*[101], allocazione di risorse, et cetera; questo report incoraggia le IFI a promuovere laboratori Blockchain in modo da garantire progressivamente la comprensione, l'applicazione e l'implementazione di questa tecnologia.

Nella pratica, molte banche rilevanti anche a livello internazionale, stanno stringendo delle partnership con start-up che hanno un business model basato sull'implementazione della Blockchain. È il caso della partnership stretta con Ant Financial da Bank of Nanjing, il cui vicepresidente, Wenkai Zhou, ha dichiarato che è stata stretta quest'alleanza in grado di costruire una piattaforma digitale finanziaria per stare al passo con il rapido sviluppo della tecnologia, in modo da migliorare l'abilità di Bank of Nanjing di sottoscrivere prestiti e stringere altre partnership in aree diverse[102]. Un altro esempio è quello di We.Trade, una piattaforma digitale attiva nel campo dei servizi finanziari basata sulla risoluzione di *smart contract* e

[98] Gli studi di IBM a cui ci riferiamo sono due*: Leading the Pack in Blockchain Banking: Trailblazers Set the Pace* (il quale si basa sulle interviste a un campione di 200 banche mondiali) e *Blockchain Rewires Financial Markets: Trailblazers Take the Lead* (che, invece, ha preso in esame un campione di 200 istituzioni finanziarie globali).
[99] Global Industry General Manager, IBM Banking and Financial Markets.
[100] Emmanouil Davradakis e Ricardo Santos, *Blockchain, FinTechs and their relevance for international financial institutions,* [1/2019]
[101] Processo di archiviazione di file sulla piattaforma.
[102] Comunicato stampa di BUSINESS WIRE, *Ant Financial Launches Ant Financial Technology Brand with Full Suite of Technology Products and Services to Support Growth of Financial Institutions*, [20/9/2018]

sulla Blockchain, che ha come obiettivo quello di permettere alle imprese (in particolare alle PMI) di cercare controparti fidate con cui instaurare rapporti commerciali e di avere in ogni momento completa visibilità sullo stato della transazione e della spedizione, digitalizzando e tracciando l'intero processo dalla creazione dell'ordine alla consegna fino al pagamento; a questa piattaforma partecipano anche banche molto importanti del calibro di Santander, UniCredit (che il 21 marzo 2019 ha eseguito la sua prima transazione su una Blockchain[103]), Societe Generale, Eurobank, Caixabank.

3.3.4. La Blockchain nel settore IP

La Blockchain potrebbe fornire un sistema semplice, efficace e trasparente per gestire le *Intellectual Properties*[104]. Essa, infatti è in grado di proteggere tanto i consumatori quanto gli autori di opere digitali di qualunque tipo, semplicemente registrando in ordine cronologico tutti i passaggi di proprietà di un bene digitale, come ad esempio vendite, ma anche donazioni o prestiti; tali transazioni possono essere confermate dagli utenti e altri attori, permettendo ai clienti di sapere esattamente cosa stanno comprando e a chiunque di verificare i diversi trasferimenti di proprietà, in modo da identificare il proprietario originale dell'opera. Un aspetto da implementare in questo campo è l'utilizzo degli *smart contract*, che sarebbero in grado di gestire l'accesso anche di altre persone con determinate specificità (ad esempio in alcuni periodi dell'anno o al verificarsi di alcune condizioni soggettive) e di automatizzare il pagamento dei diritti d'autore.

In questo modo sarebbe possibile sia disporre legalmente di qualunque opera digitale acquistate (finanche a comprarla di seconda mano o prestarla a un amico come fosse una copia fisica) attraverso una nuova gestione trasparente del settore. La Blockchain è in grado di gestire i diritti di venditori e acquirenti, e di sostenere una rete di attori che comprende il proprietario originale dei contenuti e tutti gli intermediari, comprendendo nella filiera coloro sviluppano e gestiscono la blockchain.

3.3.5. La Blockchain nella gestione d'impresa

La Blockchain è una tecnologia che si è adatta perfettamente a un utilizzo all'interno del campo della gestione d'impresa, in particolare per quanto riguarda il *supply chain management*[105], grazie al suo alto potenziale informativo. La possibilità di eseguire *smart contract*, il grande numero di informazioni che può archiviare, la facilità di accesso e la veridicità, infatti, perfezioneranno la gestione della catena produttiva riducendo costi e rischi e implementando la già esistente IT[106] a riguardo. Utilizzando la Blockchain come sistema informativo automatizzato aumenterà la trasparenza e la sicurezza sia in un'ottica interna rispetto all'impresa produttrice, sia esterna: in questo modo non solo sarà possibile per i manager controllare al meglio il processo produttivo, ma permetterà anche ai consumatori di scegliere il marchio che

[103] Pierangelo Soldavini, *UniCredit esegue la prima transazione commerciale via blockchain con We.trade*, SOLE24ORE, [21/3/2019]
[104] In italiano "Proprietà Intellettuale", legata a idee come invenzioni, lavori artistici, disegni, simboli, nomi e immagini usati in contesti aziendali.
[105] Processo di management di tutta la catena produttiva con l'obiettivo di analizzare ogni processo in ottica di aggiunzione di valore al prodotto finale.
[106] Information Technology.

meglio si armonizza con i propri bisogni, essendo più chiara la proposta di valore di ciascuno.

I costi fissi iniziali, tuttavia, sono molto alti e questo è, probabilmente, il motivo per il quale dopo più di dieci anni dalla nascita di Bitcoin e considerata la grande popolarità del sistema, la maggior parte delle imprese ancora oggi non utilizza la Blockchain all'interno della propria produzione. Esistono varie soluzioni per sopperire a questo problema: da una parte, le imprese possono stringere partnership strategiche per acquisire dall'ambiente risorse e conoscenze non presenti all'interno e abbassare così i costi fissi, come hanno fatto Accenture e Microsoft Corporation[107]; in alternativa, è possibile lo sviluppo da parte di enti pubblici o da organi associativi settoriali gestiti da privati di una Blockchain pubblica su cui ogni impresa può lavorare. Oltre alla questione legata ai costi, bisogna anche considerare il tempo che ci vorrà per definire bene obiettivi e standard, nonché introdurre dei vincoli legislativi al suo utilizzo.

3.3.6. La Blockchain nel settore sanitario

Poter avere un registro pubblico e liberamente accessibile, affidabile, sicuro e decentralizzato su cui archiviare le cartelle cliniche dei pazienti è un'idea innovativa, pratica e utile che non può non essere incentrata su Bitcoin; Medicalchain è una piattaforma sanitaria basata su blockchain, il cui obiettivo è creare un sistema di gestione delle cartelle cliniche dei pazienti che si fondi sulle caratteristiche proprie della Blockchain: decentralizzazione, sicurezza e immutabilità dei dati. Gli utenti che si iscrivono alla piattaforma, possono accedere quando vogliono alla loro cartella sanitaria e dare permessi in lettura a parenti e lettura/scrittura ai propri medici. È possibile perciò monitorare la visione dei propri record, stabilire chi può vedere cosa e per quanto tempo.

Tali dati possono essere condivisi non solo con i medici, ma anche con enti assicurativi (in cambio di uno sconto), con ricercatori farmaceutici e laboratori (in modo anonimo e limitato, nel massimo rispetto della privacy) e con il proprio farmacista. Inoltre, i dati possono essere mandati sulla Blockchain attraverso dei dispositivi mobili che monitorino l'attività fisica della persona e gli sviluppatori potranno sviluppare software in grado di dare consigli medici e alimentari sulla base dell'attività fisica quotidiana, delle abitudini e dello stato di salute dell'individuo. La piattaforma utilizza, inoltre, un proprio token per far funzionare il sistema, il MedTokens: questa criptovaluta di proprietà permette lo scambio dei dati personali a fronte di un pagamento, che potrà essere girato a medici o farmacisti (sempre sulla piattaforma) in cambio di servizi.

Gli accessi sono gestiti dalla piattaforma Civic, una blockchain utilizzata per certificare l'identità degli utenti con l'utilizzo della biometria. Le aziende partner di Civic, tra cui Medicalchain appunto, verificano l'identità di un utente iscritto a Civic direttamente sulla sua blockchain. Per assicurare la privacy degli utenti, i record sono criptati con la crittografia a chiave simmetrica. I record vengono salvati *off-chain* in banche dati che fanno parte della giurisdizione dell'utente, ovvero quella del Paese di residenza.

[107] Anna Irrera, *Accenture, Microsoft team up on blockchain-based digital ID network*, REUTERS [19/6/2017]

3.3.7. La Blockchain nel settore alimentare

Oggi, la filiera alimentare internazionale è, spesso, un processo poco chiaro che importa nei paesi industrializzati prodotti che vengono da materie prime di origine straniera. Nonostante in Italia le leggi e i controlli nel settore alimentare siano molto rigidi, non si può dire lo stesso di altre legislazioni, che spesso si ritrovano a mangiare o bere produzioni di cui è difficile sapere la provenienza. Ad esempio, molti stati USA nel 2006 soffrirono un'epidemia di Escherichia Coli[108] che costò la vita a tre persone (un bambino e due donne anziane); dopo aver accettato la natura alimentare dell'epidemia, l'intera industria alimentare entrò in uno stato confusionale. La FDA[109] impiegò due settimane per trovare la fonte dell'epidemia: un solo lotto di spinaci contaminato proveniente da un agricoltore. Un solo lotto bloccò l'intera industria agro-alimentare per due settimane[110]. Questo si sarebbe potuto evitare semplicemente con un sistema di tracciabilità efficace.

Blockchain sembra la tecnologia ideale per garantire trasparenza lungo la filiera alimentare, in quanto sarebbe possibile avere la certezza della veridicità per quanto riguarda i dati su fonte di cibo, qualità, temperatura di transito e freschezza dei prodotti, dando una garanzia di sicurezza a tutti gli agenti della filiera. Questo, soprattutto considerando la progressiva importanza che stanno acquisendo nel mondo la certificazione "Bio", la consapevolezza del cliente sulla fonte del cibo e sul tema della sostenibilità.

Joanne Joliet, senior research director di Gartner, afferma che i negozi di alimentari, poiché obbligati a elevati standard di visibilità e tracciabilità, possono essere trainanti nello sviluppo della Blockchain nell'economia, per poi estenderla a tutti i campi di vendita al dettaglio, predicendo inoltre che entro il 2025 circa il 20% dei più grandi commercianti nel campo agroalimentare utilizzerà sistemi di sicurezza con tecnologia Blockchain[111]. Ad esempio, Walmart ora richiede ai fornitori di verdure a foglia verde di implementare un sistema di tracciamento *farm-to-store* basato su Blockchain. Anche altri negozi alimentari, come Unilever e Nestlé, stanno sfruttando la Blockchain per tracciare la contaminazione degli alimenti.

[108] Escherichia Coli è un noto batterio Gram-negativo.
[109] Food and Drug Administration
[110] *Multistate Outbreak of E. coli O157:H7 Infections Linked to Fresh Spinach (FINAL UPDATE),* CENTERS FOR DISEASE CONTROL AND PREVENTION [6/10/2006]
[111] Gloria Omale, *Gartner Predicts 20% of Top Global Grocers Will Use Blockchain for Food Safety and Traceability by 2025,* GARTNER [30/4/2019]

4 – Prospettive future

4.1. Il futuro delle criptovalute sul mercato

Il mondo delle criptovalute, come abbiamo visto, è un mondo ampio, variegato e che fornisce strumenti in grado di soddisfare la maggior parte dei bisogni degli investitori (valute speculative, stabili, funzionali , et cetera). Se da una parte è chiaro che il passato sia stato turbolento, dall'altra ciò non implica che il futuro lo sarà altrettanto.

Il 2018 ha visto diminuire vertiginosamente la quotazione di tutte le criptovalute, tuttavia la maggior parte di queste ha visto il proprio valore diminuire come riflesso della diminuzione di Bitcoin (così come era aumentato per riflesso dell'aumento di Bitcoin): questo porta alla logica conclusione che alcune criptovalute sono state sottovalutate.

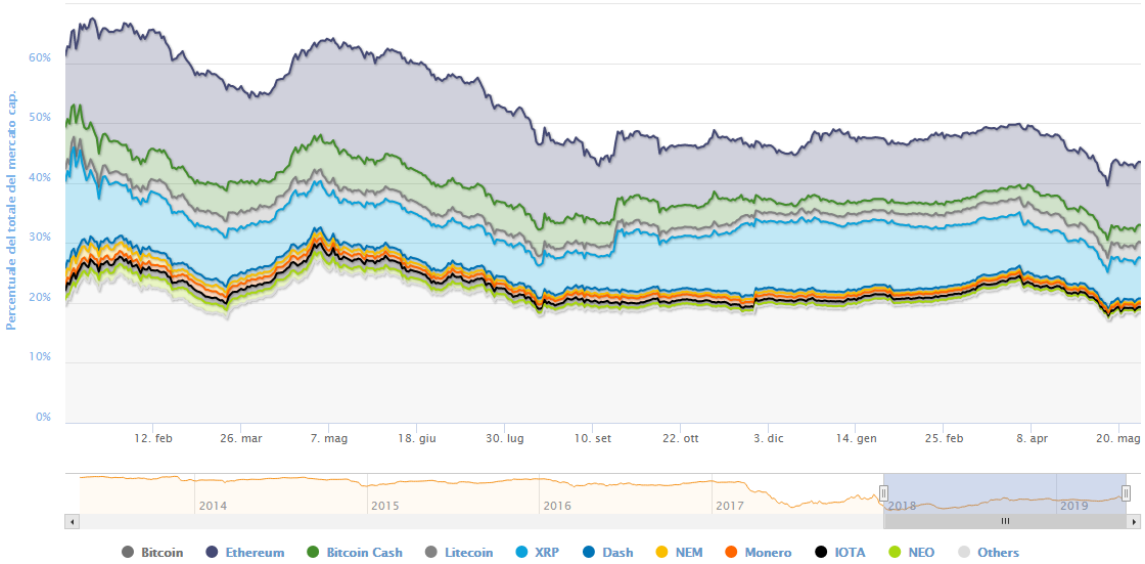
Infatti, dal 2019, è iniziato un trend rialzista in tutto il mondo criptovalute che ha compensato parte della diminuzione dovuta alla sfiducia degli investitori; come spesso succede quando ci sono dei drastici cali di valore di uno strumento, la quotazione di questo tende a scendere al di sotto di quello che sarebbe, in condizioni normali, il suo valore di mercato e, infatti, oggi i prezzi dei token sono in salita; in linea con questo discorso, anche Naval Ravikant[112], sostiene che predire l'andamento delle criptovalute a lungo termine è più facile rispetto al breve termine.

Tuttavia, esistono criptovalute molto diverse tra loro e sarebbe un ragionamento troppo semplicistico accorparle tutte in un'unica trattazione, per tanto andremo in seguito a vedere quali criptovalute, tra quelle esistenti, hanno le prospettive più rosee.

In generale, diciamo che le criptovalute a maggior potenziale sono quelle che rispondono a esigenze ben precise del mercato, quindi ci si può aspettare che la forza di ciascuna criptovaluta sia la sua parte peculiare, piuttosto che ciò che la accomuna alle altre. È per questo che si ritiene che, prima o poi, qualcuna di queste potrebbe superare Bitcoin, un token che può essere visto come un *jack of all trades, but a master of none*[113] e, in futuro, potrebbero essergli preferite altre criptovalute che assolvono a compiti ben precisi nel loro sistema di riferimento.

[112] Conosciuto per la sua grande esperienza nell'*angel investment* e per la sua partecipazione al progetto ZCash.

[113] "Jack of all trades" indica qualcuno o qualcosa con la caratteristica di essere molto duttile e versatile in vari campi; il proverbio inglese dice "A jack of all trades, but a master of none", che può essere tradotto come "un tuttofare non sarà mai eccellente in qualcosa".



114

Dal grafico, che indica l'andamento delle criptovalute a più alta capitalizzazione nel mercato, vediamo che nel concreto hanno avuto tutte lo stesso trend, discorso inclusivo di Bitcoin (non evidenziato nel grafico). Questo perché l'opinione degli investitori non specializzati è quella di un mondo di strumenti molto simili tra loro, pur non essendo ciò del tutto vero, e le variazioni di valore di una criptovaluta non riflettono solo caratteristiche della stessa, ma soprattutto rappresentano una reazione agli eventi che influenzano il mondo criptovalute.

4.1.1. Il futuro di NEO

Neo, di cui abbiamo già discusso le caratteristiche di base nel sottoparagrafo dedicato[115], rappresenta probabilmente la criptovaluta a potenziale più elevato tra quelle a maggior capitalizzazione di mercato (si stima che il mercato di NEO rappresenti lo 0,3% del mercato delle criptovalute, un valore che può sembrare basso, ma acquisisce importanza considerando che ne esistono più di 1600)[116].
Riassumendo le sue caratteristiche base, ricordiamo che il progetto NEO rappresenta il principale competitor di Ethereum, in quanto deriva da un'implementazione della stessa Blockchain su cui si basa quel sistema, più forte da un punto di vista di scalabilità, linguaggi di programmazione, rapidità del sistema di scambio e sicurezza. Oggi Ethereum rappresenta la prima forza nel campo criptovalute oltre a Bitcoin: non c'è motivo di non credere che con il tempo NEO possa prendere il posto di Ethereum.

La piattaforma di NEO, oltre a essere ben costruita, ha una possibilità se non infinita, quantomeno indeterminata di oggetti di scambio: si possono scambiare automobili, smartphone, proprietà e qualunque altro asset che possa essere digitalizzato.

Con l'implementazione di NEO, in futuro sarà possibile effettuare microtransazioni di oggetti a livello internazionale senza dover pagare commissioni alte, acquistare proprietà senza l'aiuto di intermediazione di terzi e condividere facilmente asset digitali. NEO sembra esattamente ciò di cui l'economia ha bisogno per diventare

[114] Fonte: coinmarketcap
[115] 1.3.9.
[116] Fonte: coinmarketcap

definitivamente *smart*, ovvero una rete in grado di connettere tutto il mondo con facilità, rapidità e sicurezza.

In aggiunta a ciò, la rete NEO ha due proprietà importanti che influiscono positivamente sulla sua considerazione da parte del mercato: è in grado di esguire efficientemente contratti intelligenti ed è cinese, il che rende ciò molto facile che riesca a diventare la prima criptovaluta in quel mercato, che rappresenta più di un terzo del mercato mondiale.

Infine, NEO rappresenta un competitor di Ethereum, cioè la criptovaluta a più alta capitalizzazione sul mercato dopo Bitcoin: questo vuol dire, anche in un'ottica di diversificazione di portafoglio, comprare token di entrambe le piattaforme sarebbe lo scenario più probabile, facendo corrispondere a una crescita nel breve periodo di Ethereum una crescita di NEO. Nulla toglie che, nel medio-lungo periodo, la situazione possa invertirsi portando Ethereum a crescere a ritmi sostenuti dalla crescita di NEO, pur mantenendo una capitalizzazione maggiore.

4.1.2. Il futuro di Ethereum

Riprendendo alcuni concetti dal paragrafo precedente, Ethereum oggi inizia a sentire la pressione della concorrenza, essendo passato in poco tempo da innovatore a quasi obsoleto come sistema, in quanto tutto ciò che può fare Ethereum, NEO lo fa meglio. È difficile capire come si evolverà la capitalizzazione del sistema, ma è ragionevole pensare che fino a quando il trend criptovalutario spinge verso l'alto, Ethereum continui a essere la principale forza economica dopo Bitcoin, seppur non sarebbe inverosimile vedere una crescita a ritmi decrescenti, se paragonata a quella di altre valute.

La situazione, tuttavia, potrebbe cambiare nel caso in cui ci sia un *turn-around* nel trend, che oggi appare poco probabile nel brevissimo termine. In tal caso, molto investitori "occasionali" che detengono criptovalute per fini speculativi senza avere una reale cultura a riguardo, sarebbero spinti a liquidare il proprio patrimonio di Ether, mentre gli investitori più attenti potrebbero semplicemente virare su altri strumenti.

Si parla da tempo, infatti, di un'innovazione al sistema che oggi sembra più che mai necessaria: fino a quando le aspettative degli investitori continuano a essere positive, non ci sarà alcun problema, ma in caso contrario Ether potrebbe essere uno dei token a più alto potenziale di perdita.

Il co-fondatore di Ethereum, Vitalik Buterin, sembra cosciente di ciò, in quanto nel corso del 2019 sono già apparse delle idee da parte sua per implementare sicurezza e gestione delle transazioni sulla piattaforma[117].

4.1.3. Il futuro di Ripple

Difficile parlare di criptovalute ad alto potenziale senza citare Ripple, quella che sembra oggi la criptovaluta più accettata e utilizzata a livello istituzionale. Si

[117] Adrian Zmudzinski, *Ethereum Co-Founder Vitalik Buterin Proposes Creating On-Chain Ether Mixer*, COIN TELEGRAPH [24/5/2019]

inserisce in un contesto diverso rispetto alle precedenti in quanto viene utilizzata principalmente nelle istituzioni finanziarie, avendo stretto partnership con numerosi istituti finanziari[118], tra i quali figura anche Western Union. Difficilmente ci sarà un'inversione di rotta per questo il token di Ripple, ADA, in quanto la fiducia è data da enti istituzionali o comunque con una certa autorità all'interno dei mercati, per tanto è ragionevole credere che il suo valore, anche in caso di *turn-around* subisca variazioni negative sensibilmente minori rispetto ad altri token, mettendolo probabilmente al primo posto tra le monete su cui vale la pena investire a lungo termine se si cerca un buon rapporto rendimento/rischio.

4.2. Il futuro di Bitcoin

Gli analisti stanno iniziando a chiedersi cosa succederà a Bitcoin nel futuro prossimo. Nonostante sia, per la natura stessa del sistema, molto difficile determinare le variazioni di valore del BTC anche a distanza di pochi giorni o settimane, c'è un evento che dovrebbe mettere sull'attenti gli investitori: nel 2020, infatti, è previsto il terzo *halving event*, che porterà i miner a essere ricompensati 6,25 BTC per il loro lavoro, rispetto ai 12.5 BTC attuali e i 50 BTC di partenza.

Molto è cambiato dalla nascita di Bitcoin e probabilmente entro il 2020 potremmo assistere a nuovi cambiamenti, ma gli analisti fanno notare un dato importante sotto il profilo storico: dopo un anno dal primo *halving event* del 28/11/12 il prezzo aumentò in modo inaspettato facendo quello che sarebbe stato (e rimasto per qualche anno) il record di valore: 1000$ per token; dopo poco più di un anno dal secondo evento, avvenuto il 9 luglio 2016, il BTC ha iniziato a salire di valore, fino ad arrivare nel dicembre 2017 al suo record, non ancora superato, di oltre 19,000$.

119

Molti specialisti della finanza sostengono che il prezzo di Bitcoin aumenterebbe a metà 2020 a causa di un fattore *offer-driven*: in seguito agli *halving event* i miner sono meno incentivati a lavorare e, se la domanda resta costante (o diminuisce in percentuale minore rispetto all'offerta) il valore di un BTC salirà, magari superando il suo precedente record del 2017.

[118] Tim Copeland, *Everything we know about who's using Ripple's most XRP-intensive product*, DECRYPT [22/2/2019]
[119] Fonte: Coindesk

Tuttavia, questa teoria non è segreta e molti investitori potrebbero voler trarre profitto da questa situazione, comprando effettivamente prima che l'ultimo *halving event* si realizzi e facendo aumentare il prezzo in modo più lento e costante rispetto ai due eventi precedenti.

Garrick Hileman, ricercatore di Blockchain e della London School of Economics, sostiene che i mercati di criptovalute sono spesso "*event-driven*"[120] e che, avvicinandoci al prossimo dimezzamento di ricompensa dei miner, il prezzo di un BTC riceverà una spinta verso l'alto da coloro che anticipano la riduzione dell'offerta[121].

Le opinioni celebri sul futuro di Bitcoin sono variegate e vanno dalla delusione e dal pessimismo di Warren Buffet all'entusiasmo di Elon Musk[122]. Il The Guardian, tuttavia, sostiene che bisogna porre l'attenzione sul grande spreco di energia dovuto al mining di Bitcoin[123]: le stime dicono, infatti, che il mining spreca la stessa energia di un piccolo Stato (utilizza poco più dell'energia utilizzata da Cuba e poco meno dell'energia utilizzata dall'Islanda), assimilando l'inquinamento dovuto al Bitcoin a quello del petrolio (paragone forse azzardato, ma comunque eloquente). Tuttavia, non considerando Bitcoin in senso assoluto, ma in paragone alle istituzioni finanziarie, il sistema spreca un terzo dell'energia elettrica sprecata dal sistema finanziario mondiale[124]. Nonostante questo, il Bitcoin è ben lungi dall'arrivare a sostituire il sistema finanziario a causa della mole di transazioni estremamente ridotta di transazioni che permette il sistema (10 al secondo, contro le 24,000 di VISA).

[120] Con quotazioni guidate da eventi che influenzano direttamente domanda e offerta
[121] Billy Bambrough, *A Bitcoin Halvening Is Two Years Away -- Here's What'll Happen To The Bitcoin Price*, FORBES [29/5/2018]
[122] R.R. Hauxley, *The Truth about Bitcoin's Future*, CRYPTOMANIAKS [22/4/2019]
[123] Ethan Lou, *Bitcoin as big oil: the next big environmental fight?*, THE GUARDIAN [17/1/2019]
[124] Katrina Kelly-Pitrou, *Stop worrying about how much energy bitcoin uses*, THE CONVERSATION [20/8/2019]

Conclusione

Proprio nell'epoca della crisi economico-finanziaria mondiale, Bitcoin si è proposto come un sistema alternativo che nel tempo ha scardinato equilibri economici, politici e tecnologici. Nonostante siano ancora lontani dall'imporsi come sistema alternativo, Bitcoin e il mondo delle criptovalute in generale hanno mosso una critica consistente al sistema di pagamenti attuale che, a confronto, sembra sia necessario si rinnovi. Attraverso un sistema peer-to-peer regolato da un protocollo informatico, Bitcoin si presenta come una valuta-unità di conto ed un sistema di pagamento indipendente da ogni controllo centralizzato, ponendo al centro del suo funzionamento l'intera community degli utilizzatori, i nodi della rete.

Tuttavia, lo scenario aperto da Bitcoin e dalle altre valute virtuali genera allo stesso tempo delle opportunità e dei rischi, in quanto se da una parte il sistema garantisce trasparenza ed efficienza, lo strumento che utilizza è caratterizzato da una volatilità troppo alta per poter essere considerato come alternativa alla moneta sovrana. L'obiettivo dell'elaborato era di ottenere un quadro di un mondo complesso e dinamico quale quello delle criptovalute. A tal fine, nel primo capitolo è stato trattato il mondo criptovalutario nel complesso, facendo riferimento al quadro legislativo all'interno del quale si colloca e ai sistemi di criptovalute più ricercati dal mercato, fatta eccezione per Bitcoin, il quale viene ampiamente trattato nel secondo capitolo con un approccio storico-finanziario, delineando tutta la sua storia dalla pubblicazione e dalla pubblicità su Metzdowd del white paper, fino alla metà del Maggio 2019, periodo in cui l'elaborato è stato concluso, e con un prospetto analitico del futuro prossimo. Il terzo capitolo esula dall'aspetto strettamente economico-finanziario dello strumento e guarda alla tecnologia della Blockchain, la quale offre funzionalità inedite che possono essere utilizzate in vari campi; per tanto, si vede la sua applicazione in Bitcoin a cui segue una visione di quello che è l'attuale e il probabile futuro utilizzo di questa tecnologia in diversi settori dell'economia, come la gestione dei diritti di proprietà intellettuale, il *supply chain management*, un nuovo approccio alla settore sanitario e la tracciabilità dei prodotti agricoli lungo la filiera alimentare.
Nel quarto capitolo, infine, viene tracciato un prospetto di quello che potrebbe essere il futuro di NEO, Ethereum, Ripple e Bitcoin in uno scenario verosimile, che tenga conto delle situazioni attuali senza grossi shock sul mercato.

Riferimenti sitografici

1 – Le Criptovalute

1.2.

https://www.wallstreetitalia.com/trend/panama-papers/

http://www.dirittoegiustizia.it/allegati_sp/15/0000082509/Nascita_delle_cripto_valute_e_dei_connessi_rischi_di_riciclaggio.html

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32015L0849&from=IT

http://www.dirittoegiustizia.it/allegati_sp/15/0000082510/Quinta_direttiva_principali_innovazioni.html

https://www.agendadigitale.eu/cultura-digitale/criptovalute-e-riciclaggio-ecco-lillegalita-che-affligge-il-cuore-dei-bitcoin-e-affini/

http://www.consob.it/web/area-pubblica/antiriciclaggio-normativa-europea

https://www.diritto.it/ecco-perche-i-bitcoin-e-le-criptovalute-non-sono-moneta-elettronica/

1.3.

https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

https://coinmarketcap.com/it/

https://nextgenerationcurrency.com/litecoin/

https://litecoin.org/it/

https://www.criptovalute24.com/ethereum/

https://github.com/ethereum/wiki/wiki/%5BItalian%5D-Libro-Bianco

https://www.mercati24.com/zcash-criptovaluta-cose-come-funziona-valore-quotazione-news/

https://whitepaperdatabase.com/zcash-zec-whitepaper/

https://docs.dash.org/en/stable/introduction/about.html

https://www.icer.it/dash-criptovaluta/

https://www.criptovaluta.it/dash

https://www.coingecko.com/it/monete/dash

https://whitepaperdatabase.com/ripple-xrp-whitepaper/

https://www.money.it/Ripple-cos-e-come-funziona-differenze-con-Bitcoin-guida

https://whitepaperdatabase.com/monero-xmr-whitepaper/

https://www.criptovaluta.it/monero-come-funziona

https://coinmarketcap.com/it/currencies/monero/historical-data/

https://coinmarketcap.com/it/currencies/bitcoin-cash/

https://www.comefaretradingonline.com/criptovalute/bitcoin-cash.php

https://www.businessinsider.com/bitcoins-hard-fork-bitcoin-unlimited-segregated-witness-explained-2017-3?IR=T

https://www.cryptoground.com/bitcoin-cash-white-paper

https://www.criptovalute24.com/neo-la-criptovaluta-cinese-paura/

https://coinmarketcap.com/it/currencies/neo/

https://docs.neo.org/en-us/whitepaper.html

https://www.criptovalute24.com/cardano-ada/

https://coinmarketcap.com/it/currencies/cardano/

https://whycardano.com/

https://whitepaperdatabase.com/cardano-ada-whitepaper/

https://coinmarketcap.com/it/currencies/eos/

https://whitepaperdatabase.com/eos-whitepaper/

https://www.criptovaluta.it/eos

https://valutevirtuali.com/2018/10/24/eos-cose-come-funzione-e-quali-caratteristiche-ha-questa-criptovaluta/

https://coinmarketcap.com/it/currencies/tether/

https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

https://www.webeconomia.it/tether-criptovaluta-cose-funziona-conviene-investire/15719/

https://www.ilsole24ore.com/art/notizie/2018-02-09/cos-e-tether-criptovaluta-legata-dollaro-che-fa-tremare-bitcoin-182417.shtml?uuid=AELm3WxD

https://www.criptopedia.info/stellar-xlm/

https://www.forbes.com/sites/michaeldelcastillo/2018/09/10/visa-backed-blockchain-firm-embraces-stellar-cryptocurrency-via-merger/#25013ccd74c2

https://coinmarketcap.com/it/currencies/stellar/

https://whitepaperdatabase.com/stellar-lumens-xlm-whitepaper/

https://www.criptovalute24.com/stellar/

2 - La nascita di Bitcoin

2.1.

https://www.borsaitaliana.it/notizie/sotto-la-lente/bitcoin-172.htm

https://coinmarketcap.com/it/currencies/bitcoin/

2.2.

https://hackernoon.com/the-amazing-story-of-cryptocurrencies-before-bitcoin-fe1b0e55155b

https://www.ilbitcoin.news/premio-nobel-milton-friedman-predetto-bitcoin-17-anni/

https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/

https://monetevirtuali.pro/la-storia-di-bitcoin-parte-3-cose-b-money/

http://www.weidai.com/bmoney.txt

https://www.chaum.com/ecash/

2.3.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875

https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

http://www.treccani.it/magazine/lingua_italiana/domande_e_risposte/lessico/lessico_067.html

https://archive.org/stream/pdfy-MHvlymfJYU05yELW/Gold%20Confiscation%20fdr-executive-order-6102_djvu.txt

https://web.archive.org/web/20111001215655/http://p2pfoundation.ning.com/forum/topic/listForContributor?user=0ye0gncqg772o

https://www.coindesk.com/information/who-is-satoshi-nakamoto

https://bitcointalk.org/index.php?topic=234.msg1976#msg1976

https://www.businessinsider.com/michael-clear-denies-creating-bitcoin-2013-4?IR=T

https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html

https://www.fastcompany.com/1785445/bitcoin-crypto-currency-mystery-reopened

https://www.econopoly.ilsole24ore.com/2019/01/06/bitcoin-anno-10-silk-road/

https://www.swansea.ac.uk/media/Silk-Road-and-Bitcoin.pdf

2.4.

https://blockexplorer.com/news/bitcoin-history-timeline/

http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

https://www.ilsole24ore.com/art/tecnologie/2018-06-29/bitcoin-piu-grande-furto-storia-emerge-tesoretto-un-miliardo-dollari-184422.shtml?uuid=AEYnTnEF

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875

2.5.

https://www.businessinsider.com/coinbase-valued-at-8-billion-after-raising-another-mega-round-2018-10?IR=T

https://bitcoinfoundation.org/wp-content/uploads/2017/03/Bitcoin_Foundation_Manifesto.pdf

https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities

https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities

2.6.

https://eu.usatoday.com/story/dispatches/2014/01/21/las-vegas-casinos-accepting-bitcoins/4713243/

https://www.theguardian.com/technology/2014/jan/27/bitcoin-foundation-vice-chair-arrested-money-laundering

https://www.businessinsider.com/the-chicago-sun-times-will-now-take-bitcoin-payments-2014-4?IR=T

https://www.telegraph.co.uk/technology/news/11286998/Tech-giant-Microsoft-accepts-Bitcoin-payments.html

https://www.bbc.com/news/av/business-26394986/mtgox-bitcoin-exchange-files-for-bankruptcy

https://www.ccn.com/bitcoin-exchange-bitstamp-confirms-loss-of-18886-btc-5-million-usd-from-hot-wallet

https://www.unicode.org/L2/L2015/15229-bitcoin-sign.pdf

https://www.newsbtc.com/2016/03/04/cabinet-of-japan-greenlights-bitcoin-as-payment-method/

https://academic.oup.com/jfr/article/3/1/125/2838368

2.7.

https://www.businessinsider.com/bitcoin-acceptance-growing-in-japan-2017-4?IR=T

https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/

https://www.themoscowtimes.com/2017/06/12/russia-is-becoming-a-cryptocurrency-haven-a58175

https://dailyhodl.com/2018/07/20/south-korea-makes-2018-the-year-of-bitcoin-and-cryptocurrency-acceptance/

http://www1.president.go.kr/petitions/76020?navigation=best-petitions

https://www.bbc.com/news/technology-42881892

https://www.independent.co.uk/news/business/analysis-and-features/twitter-ban-cryptocurrency-adverts-regulators-bitcoin-facebook-social-media-a8277176.html

https://www.nytimes.com/2018/03/14/technology/google-bitcoin-advertising.html

https://www.italiaoggi.it/news/il-bitcoin-e-ancora-vivo-e-con-lui-un-sacco-di-altre-criptovalute-2263804?fbclid=IwAR2Bq7fGVjOECrmTMaPwWx9fuU0yt9e1Wr_gG5n8G0u2qPnhqiDjE2G_pYg

https://www.ilsole24ore.com/art/tecnologie/2018-11-20/bitcoin-caduta-libera-perde-30percento-una-settimana-tre-ragioni-crollo-102616.shtml?uuid=AEa1t5jG

https://www.bloomberg.com/news/articles/2018-11-20/bitcoin-rigging-criminal-probe-is-said-to-focus-on-tie-to-tether

https://www.ilsole24ore.com/art/commenti-e-idee/2018-12-30/l-esplosione-bolla-bitcoin-autopsia-154252.shtml?uuid=AEGaGD7G

3 - La Blockchain

3.1.

http://www.weidai.com/bmoney.txt

http://www.hashcash.org/papers/pvp.pdf

http://www.hashcash.org/hashcash.pdf

https://monetevirtuali.pro/la-storia-di-bitcoin-parte-1-cose-hashcash/

3.2.

https://www.investopedia.com/terms/b/bitcoin-mining.asp

https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html

https://www.blockchain.com/charts/difficulty

https://bitcoin.org/en/how-it-works

http://www.report.rai.it/webdoc/2018-bitcoin/

3.3.

https://www.blockchain4innovation.it/esperti/blockchain-governance-ed-applicazioni/

http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

https://ieeexplore.ieee.org/abstract/document/8525392

https://www.blockchain4innovation.it/mercati/banche-e-finanza/blockchain-nel-finance-65-delle-banche-produzione-entro-3-anni/

http://www.ansa.it/sito/notizie/economia/business_wire/news/2018-09-20_1201875859.html

https://www.businesswire.com/news/home/20180920005319/en/Ant-Financial-Launches-Ant-Financial-Technology-Brand

https://www.ilsole24ore.com/art/tecnologie/2019-03-21/unicredit-esegue-prima-transazione-commerciale-via-blockchain-wetrade-165548.shtml?uuid=ABMqyhgB

https://www.ilsole24ore.com/art/tecnologie/2019-03-21/unicredit-esegue-prima-transazione-commerciale-via-blockchain-wetrade-165548.shtml?uuid=ABMqyhgB

https://www.forbes.com/sites/bernardmarr/2017/08/10/practical-examples-of-how-blockchains-are-used-in-banking-and-the-financial-services-sector/#3546bde91a11

https://financialservicesblog.accenture.com/five-use-cases-for-blockchain-in-financial-services

https://www.blockchaintechnologies.com/swiss-bank-julius-baer-partners-with-crypto-banking-startup-to-offer-digital-asset-services/

https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B

https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain/#3554ebfd2b5b

https://www.forbes.com/sites/trevorclawson/2018/08/31/broken-records-uk-entrepreneurs-see-blockchain-as-the-solution-to-the-patient-data-problem/#4c41bd1372ac

https://www.telegraph.co.uk/business/business-reporter/blockchain-trial-in-healthcare/

https://medicalchain.com/it/

https://www.forbes.com/sites/monicamelton/2019/04/09/blockchain-could-be-used-by-at-least-50-of-all-companies-within-3-years-oracle-exec-says/#1360c7b955cf

https://www.cdc.gov/ecoli/2006/spinach-10-2006.html

https://blockgeeks.com/guides/blockchain-and-supply-chain/

https://www.blockchain4innovation.it/ricerche/blockchain-nella-filiera-alimentare-trasparenza-tracciabilita-e-sicurezza/

4 - Prospettive future

https://cointelegraph.com/news/ethereum-co-founder-vitalik-buterin-proposes-creating-on-chain-ether-mixer

https://decrypt.co/5313/complete-ripple-partnerships-xrapid-xrp

https://cryptomaniaks.com/truth-about-bitcoin-future

https://theconversation.com/stop-worrying-about-how-much-energy-bitcoin-uses-97591

https://www.theguardian.com/commentisfree/2019/jan/17/bitcoin-big-oil-environment-energy

https://www.forbes.com/sites/billybambrough/2018/05/29/a-bitcoin-halvening-is-two-years-away-heres-whatll-happen-to-the-bitcoin-price/#6570c3135286