Università
Ca'Foscari
Venezia

Corso di Laurea magistrale

in

Amministrazione, finanza e controllo

(ordinamento ex D.M. 270/2004)

Tesi di Laurea

Le Cryptocurrency: un'analisi puntuale e prospettica sul criptomondo

Relatore
Ch. Prof. Renato Rizzini

Correlatore
Ch. Prof. Moreno Mancin

Laureando
Marco Bruno
Matricola 859449

Anno Accademico
2017 / 2018

“Alla mia Famiglia che ha reso possibile questo mio traguardo, in particolar modo:
a Giulio e Maria, i mei genitori, che hanno reso possibile la trasformazione di un sogno in realtà,
a Daniele, mio fratello, come fonte di risolutezza e determinazione,
a Elena e Alberto, mia sorella e mio cognato, che hanno avuto l’enorme pazienza nel sorreggermi in questo elaborato,
a Federico, mio nipote nonché amore incondizionato della mia vita, nella speranza di un mondo migliore,
a Nonna Caterina, che mi ha sempre coccolato con le sue dolci parole,
a Ylenia, la mia stella polare, che mi ha sopportato e supportato di fronte ad ogni ostacolo che mi è stato posto.

Infine, a Venezia e al Popolo veneto, che mi ha accolto e mi ha dato la fierezza di essere un italiano e un cittadino del mondo”

Indice

Introduzione

Ho deciso di trattare questo argomento perché è estremamente attuale, infatti tutto il mondo sta cercando di capire se questa innovazione possa soppiantare radicalmente tutto il sistema finanziario tradizionale, quello che siamo comunamente abituati ad utilizzare. Attualmente, tutto il mondo sta prendendo coscienza delle valute digitali, specialmente dal 2017, anno in cui si è registrata la più ampia diffusione di questo tema tra l'audience pubblica, ossia tra chi realmente sta scommettendo consapevolmente in questo settore in chiave prospettica, o a chi semplicemente punta ad una mera speculazione finanziaria. Capire le concrete opportunità o rischi che il criptomondo possa portare, è uno degli scopi di questo elaborato, nonché anche analizzare come realmente il mondo si sta muovendo verso questo settore, per poi comprendere se e in che modo potrà ancora evolvere il criptomondo nel futuro.

Sono passati quasi dieci anni dalla nascita di *Bitcoin*, la prima valuta digitale decentralizzata; quel momento è l'anno zero delle valute digitali. Infatti, da lì a poco sono sarebbero state inventate e "coniate" altre monete di questo genere che sono definite dagli esperti *Altcoins*. Questa nuova tipologia di valute non poteva essere ascritta in nessun ambiente già esistente, quindi è stato necessario coniare un nuovo termine il *Criptomondo*.

Queste criptovalute hanno la particolarità di funzionare in maniera del tutto decentralizzata, ovvero è il primo sistema di pagamento in cui non vengono chiamati in causa gli intermediari finanziari. Inoltre, il processo di coniazione non è più lasciato in mano alle Banche Centrali, così come il procedimento di garanzia delle transazioni non è trasferito alle banche, infatti tali meccanismi vengono lasciati agli utenti delle apposite piattaforme.

In tale meccanismo, la crittografia e la piattaforma sottostante hanno preso il ruolo di un'Autorità centrale, ovvero nella finanza tradizionale la fiducia era ben riposta nelle Banche Centrali, le quali ne controllavano l'ammontare e il valore delle stesse. Nel criptomondo non è più così, la fiducia viene rimessa nella crittografia e nei complessi calcoli matematici. Bitcoin è nato per rendere le transazioni più veloci e sicure rispetto a quanto non fosse prima, sganciandole dal controllo di un'Autorità centrale per fornirlo

così agli utilizzatori delle stesse. Non a caso è stato scelto l'anno 2008 come data di lancio, anno dello scoppio di una delle più grandi crisi finanziarie mondiale di tutti i tempi.
Nel corso dell'elaborato, verrà descritto il funzionamento sottostante alle criptovalute, che garantisce altissimi standard di sicurezza ed affidabilità. Nella fattispecie, verrà illustrato come gli utenti riescono a sopperire alla mancanza degli intermediari, da una parte attraverso uno speciale network in cui tutti gli utenti possono prenderne parte liberamente così facendo si possono effettuare le transazioni con tali valute (in realtà esistono due tipi diversi di network, nei quali viene lasciata più o meno libertà di accesso); mentre dall'altra grazie all'intervento della crittografia viene garantita l'anonimità e sicurezza. Per quanto riguarda l'attività di validazione e registrazione delle transazioni viene adibita ai partecipanti stessi delle piattaforme. Inoltre, anche questa funzione viene realizzata con sistemi e modi differenti, dipendentemente dal tipo sistema di convalidazione che la criptovaluta ha deciso di utilizzare.
Questo fenomeno è diventato virale, specialmente nel 2017 dove si è registrato il picco massimo di capitalizzazione del cripto-settore: raggiungendo nella metà di dicembre quasi i $ 600 miliardi. A fine gennaio 2018 il criptomondo era composto da 1,600 valute digitali, per un controvalore di $ 600 miliardi. Successivamente, il primo semestre del 2018 è caratterizzato da una discesa per tutto il settore, registrando valori antecedenti a quelli di dicembre, facendo intendere che probabilmente il criptomondo è stato sopravvalutato, specialmente il Bitcoin. Attualmente, il settore ha una capitalizzazione di circa $ 279 miliardi[1] per 1629 criptovalute.

L'obiettivo della mia analisi è inquadrare il fenomeno in tutti i suoi aspetti, da quelli meramente tecnici a quelli economici e fiscali. Inoltre, per una migliore argomentazione, si è scelto di analizzare cinque criptovalute, prendendo quelle che per motivi di maggiore diffusione ed incrementi tecnologici, possono rappresentare il criptomondo nel suo vero insieme. Inoltre, dallo studio di queste cinque l'intento è di evidenziare i loro punti di forza e debolezze, così verificando se realmente ci potranno essere nuove valute digitali in un futuro prossimo, che riusciranno a superare quelle presenti sul mercato.

[1] Fonte Url: "https://coinmarketcap.com/", in data 16 giugno 2018, ore 10:50.

Inoltre, partendo dall'analisi del loro sistema sottostante, quale secondo gli esperti rappresenta probabilmente la "vera" rivoluzione che ha portato il criptomondo, si vorrà capire se realmente questa sarà adibita anche a scopi ulteriori che da quella per cui è stata inventata.

Infine, lo scopo ultimo dell'elaborato è cercar di prevedere i possibili scenari futuri, attraverso un'analisi prospettica dei temi analizzati del criptomondo.

Per raggiungere tali obiettivi, l'elaborato sarà così strutturato:

- 1° Capitolo: sarà descritto il criptomondo, facendo un'analisi analitica sulla storia della moneta e sull'avvento della prima valuta digitale decentralizzata, successivamente si illustreranno le cinque criptomonete prese in esame, ed infine si farà un breve confronto tra le criptovalute e le valute tradizionali;
- 2° Capitolo: verterà sul funzionamento sottostante, inizialmente evidenziando le innovazioni tecnologiche che hanno permesso la realizzazione di tali innovazioni *disruptive*, successivamente quest'analisi continuerà con le singole valute digitali prese in considerazione;
- 3° Capitolo: esplicherà l'economia del criptomondo, descrivendo quali soggetti coinvolge e quale impatto ha avuto e sta avendo sull'economia reale;
- 4° Capitolo: verranno descritte le attuali e future regolamentazioni delle criptovalute, inizialmente si farà un inquadramento mondiale per poi concentrarsi dettagliatamente sulla normativa italiana;
- 5° Capitolo: infine qui verrà trattato l'argomento facendo una sintesi dell'elaborato, mettendo in luce i vantaggi e gli svantaggi che caratterizzano (intrinsecamente) il criptomondo e le innovazioni connesse, infine si cercherà di fare delle ipotesi sui possibili scenari futuri.

Capitolo I – Che cosa sono le Criptovalute

Una Prima Definizione

La criptovaluta è uno "strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta; denaro, moneta virtuale"[2].

Con il termine criptovaluta (o in accezione anglosassone *cryptocurrency*) si identifica un nuovo strumento di transazione che opera attraverso valute digitali. In questo momento storico la finanza digitale sta ricoprendo un ruolo fondamentale. In particolare, si stanno profilando due scenari: nel primo si assisterà probabilmente a un cambiamento talmente radicale da cui difficilmente si potrà più far ritorno; o viceversa, come viene sostenuto da molte figure di spicco della finanza internazionale, tra cui Warren Buffet[3], si assisterà ad un disastro finanziario globale. Come verrà illustrato nell'elaborato, il termine di *cryptocurrency* identifica tutto il mondo delle *cyber-valute*, iniziando dalla primogenita bitcoin fino ad arrivare alle altre che nel gergo tecnico vengono definite *Altcoins*.

In realtà non si può confermare una tesi invece di un'altra, ma quello che risulta certo è l'estrema difficoltà nello studio e gestione di questo complesso argomento.

A tal proposito, si può citare questo piccolo estratto del Il Sole24h: "l'unica certezza che c'è oggi sui Bitcoin e sulle criptovalute è la difficoltà di gestire in modo ordinato lo sviluppo di una nuova generazione di strumenti finanziari e di pagamento digitale le cui straordinarie peculiarità tecnologiche ne rappresentano la forza e il limite"[4].

A tale riguardo le criptovalute sono viste in maniera assai positiva dalle nuove generazioni della *digital economy*, infatti vengono sostenute per i loro punti di forza, tra i quali l'indipendenza dalle banche centrali e quindi da qualsiasi andamento dei tassi di interesse e dei cicli economici. Per gli stessi motivi sono visti negativamente, quasi con timore e paura, dagli Stati e dalle autorità di vigilanza. La vigilanza di queste risulta essenziale per il controllo delle transazioni sul web, al fine di evitare infiltrazioni criminali con lo scopo di riciclare denaro ed evadere fiscalmente.

---

[2] Definizione presa dal dizionario Treccani:
"http://www.treccani.it/vocabolario/criptovaluta_%28Neologismi%29/".

[3] Tratta da: "http://www.corriere.it/economia/18_gennaio_10/buffett-le-criptovalute-faranno-brutta-fine-81090898-f622-11e7-9b06-fe054c3be5b2.shtml".

[4] Tratta dall'Ebook del Sole24h: "Bitcoin Generation la rivoluzione delle criptovalute".

Inoltre, non da ultimo, aver la possibilità di utilizzare i *token*[5] per le transazioni di prodotti e servizi illegali sul *dark web*[6].

La mancata regolamentazione di questi strumenti altamente innovativi ha creato confusione; non esiste ancora una classificazione giuridica di queste valute digitali, quindi non si sa se siano monete virtuali adibite a strumento di scambio nel commercio o delle semplici *commodities*.

In questa confusione planetaria, i governi di Cina e Corea del sud, che nel passato lasciavano utilizzare liberamente questo strumento (che forse veniva usato per eludere i capitali), stanno cercando di vietarne lo scambio; negli Stati Uniti vengono trattati come *commodity*, mentre in Giappone vengono considerati al pari dello yen. L'Europa si sta ancora interrogando su cosa sia questo fenomeno, anche se la BCE ha confermato che le criptovalute non sono riconosciute come una moneta con corso legale.

Cenni Storici

Breve storia della Moneta

La definizione di moneta è essenziale per lo studio che si sta affrontando, qui il Treccani può esser d'aiuto: "dall'originario significato di dischetto di metallo coniato per le necessità degli scambi, avente lega, titolo, peso e valore stabiliti, per estensione tutto ciò che, nei vari periodi e paesi, funge da intermediario degli scambi e da comune misura[7]".

Da questa prima definizione fornita dal dizionario Treccani, si pensa la moneta come uno strumento di pagamento in quanto svolge la funzione di scambio per le transazioni fra le persone.

A riguardo si può citare la definizione del premio Nobel Samuelson: "La moneta, in quanto moneta e non in quanto merce, è voluta non per il suo valore intrinseco, ma per le cose che consente di acquistare"[8].

---

[5] Token: Letteralmente Token significa gettone, quindi nell'ambito delle monete digitali, i token sono le monete vere e proprie.

[6] Dark Web: "The Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. While it's most famously been used for black market drug sales and even child pornography, the Dark Web also enables anonymous whistleblowing and protects users from surveillance and censorship", Fonte Url: "https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/".

[7] Definizione dal dizionario Treccani:
"http://www.treccani.it/enciclopedia/moneta/#origineefunzionedellamoneta-1".

[8] Tratto da: Samuelson, Economia, Zanichelli 1989, pag. 255.

Originariamente però non era intesa in questo modo, anzi assumeva tutt'altro valore. Infatti, nell'antichità si parla di *economia naturale* per intendere quella che non utilizzava la moneta, a cui si contrappone l'*economia monetaria*. Questa classificazione può essere usata per determinare lo stato di avanzamento dell'economia dei popoli, in quanto la moneta riscuoteva una grande importanza nell'organizzazione economica dei popoli[9]. Lo storico austriaco Dopsch sostiene che l'economia monetaria ha un orizzonte temporale molto più esteso di quello che altri storici ed economisti pensano, sostiene inoltre che il passaggio tra le due economie non sia stato netto e irreversibile. Ad ogni modo, si può affermare che la prima forma di scambio tra i primitivi è stato il *baratto* che consiste nello scambio di beni o servizi. Secondo la tesi di Dopsch, questa fase è riconducibile agli albori dell'umanità, perché proprio tra i primitivi si sarebbe praticato lo scambio di merce. Solo in seguito si passa alla cosiddetta *moneta merce* che favoriva gli scambi che consistevano in merci costituite da ocra rossa, lance, scudi, conchiglie. In tal modo si ottiene una netta separazione dal sistema precedente attribuendo ad ogni bene o servizio un valore misurabile in una convenzionale unità di misura. Questa antica forma di pagamento è stata usata fino in periodi recenti: dai popoli nell'area del pacifico fino alla metà del Novecento, in Giappone fino al 1868[10], in Islanda fino al XIX secolo, in Cina fino agli anni '30 del Novecento. In questa forma di pagamento rientra anche l'uso dei metalli preziosi, a tal riguardo: "Le monete-utensili non svolgono la funzione di unità di misura, ma solo quelle di riserva di valore e mezzo di pagamento"[11]. Dunque, questa è una forma di pagamento astratta e più evoluta rispetto al baratto che offre molti vantaggi, tra cui: la non deperibilità, la disponibilità, la verificabilità e la divisibilità del bene. Difatti, inizialmente c'era una difficoltà nella valutazione di questi metalli, di conseguenza questi vennero fusi in forma di utensili (per esempio un'ascia), quindi la moneta veniva valutata sulla base della dimensione-capacità.

Lo sviluppo successivo è stato l'uso dei metalli preziosi per il conio di monete e i principali minerali erano oro, argento e rame. Ogni civiltà ha avuto un diverso tempo di

[9] A riguardo si possono citare i seguenti libri: Dopsh, "Economia naturale ed economa monetaria nella storia universale", Sansoni, 1930; Romano e Tucci, "Storia d'Italia - Economia naturale, economia monetaria", Annali 6, Einaudi, 1983.

[10] In questo contesto, nel paese del Sol Levante, l'economia naturale è perdurata fino al XVIII secolo, proprio per il contesto culturale del suo popolo, perché come afferma Dopsh: "un samurai riteneva vergognoso toccare moneta, e se questa gli veniva donata considerava ciò come un grave oltraggio". Fonte: Dopsh, cit., pag. 46.

[11] Fonte tratta dal libro: Franco Spinelli, "La moneta dall'oro all'euro – un viaggio fra storia e teoria", Etas, 1999, pag. 10.

maturazione per l'adozione delle monete. L'invenzione del conio è avvenuta nella Babilonia del III millennio a.C. e successivamente si è spostata verso occidente, grazie alle conquiste di Alessandro Magno e alla diffusione dell'Impero Romano. È interessante notare che in tutte le società, di ogni parte del Mondo, la coniazione è stata voluta e garantita da un'autorità centrale, infatti:

- L'antico Oriente: Cina: III millennio a.C. compare la moneta metallica di argento, rame e ferro, e già nel II secolo d.C. compare la moneta di carta (portando il sigillo del Gran Khan, aventi corso legale). Giappone: V secolo d.C. compare la moneta di rame e nel VII quella d'argento (dapprima gestiti da importanti famiglie, poi dall'imperatore). India: I millennio a.C. anche se l'economia naturale rimane un caposaldo. Babilonia e Assiria sistema misto, tra le varie monete vi è un rapporto fisso ufficiale disciplinato dal codice di Hammurabi nel 2100 a.C., garanzia fornita dai sacerdoti prima e poi dallo Stato con i sigilli dopo. Persia al tempo di Dario, nel 500 a.C., sistema di pagamento misto, in più per la coniazione d'oro era riservato al re. Nella civiltà egizia la coniazione delle monete la troviamo solo nel IV secolo a.C. con l'arrivo di Alessandro Magno e per via del ruolo limitato del commercio, l'economia naturale perdurò molto di più.
- L'antica Grecia e Roma: la civiltà egea usa le monete di rame dal II millennio a.C., ma con la riforma di Solone nel 594 a.C. è imposta l'uso di moneta coniata. A Roma si inizia a usare il bestiame e il sale[12] come moneta, ma con la legge del 430 a.C. si passa al pagamento delle multe con la moneta metallica (la prima fu quella in rame).

Ogni popolo della Terra ha conosciuto periodi di evoluzione del sistema di scambio soprattutto tra Asia ed Europa[13]. Indubbiamente gli scambi commerciali che hanno interessato questi due continenti hanno accelerato questo processo arrivando a influenzarsi reciprocamente.

Bisogna aspettare l'arrivo dell'età moderna per poter parlare dell'economia monetaria per come la intendiamo noi oggi. I fattori che hanno contribuito all'evoluzione del sistema monetario sono molteplici e complementari, ricordiamo: il commercio che si sviluppa enormemente e che non conosce più confini (basti pensare all'importanza delle

[12] Per questo motivo si derivano i noti termini latini: pecunia e salarium.
[13] Come viene spiegato dettagliatamente nel libro: Franco Spinelli, "La moneta dall'oro all'euro – un viaggio fra storia e teoria", Etas, 1999, pag. 6 e pag. 47.

repubbliche marinare e specialmente il peso politico-economico che aveva assunto la repubblica Serenissima di Venezia con l'estremo oriente), dalla creazione e diffusione capillare delle banche e da ultimo la scoperta dell'America che porta grosse quantità di metallo prezioso e non.

A riguardo, vale la pena di citare lo studio etnologico-storico di Einzig:

"l'approccio etnologico:

- Oceania: a Samoa: stuoie di diversa natura, Hawaii: legno di sandalo, Palau: perle, noci, stuoie, gusci di tartaruga e tabacco. Santa Cruz: piume di pappagallo. Nuova Guinea: zanne di cinghiale e conchiglie.
- Asia: Filippine: riso, la cui unità è definita da una mazzolina di spighe. Alor: tamburi di metallo, gong di ottone e frecce. Cambogia: bufali, buoi, asce e treppiedi. Siam: Conchiglie e gettoni da gioco in ceramica. Malesia: polvere d'oro e lingotti di stagno. Mongolia: pani di tè, pecore e pelli di scoiattolo. India: grano, riso e sale. Siberia: renne, pelli e tè. Sri Lanka, Maldive e Arabia: semi di piante particolari, conchiglie, ami e cammelli.
- Africa: Sudan: ferro a forma di zappa. Etiopia: sale. Kenya: bestiame. Tanzania: perle. Nigeria: conchiglie, schiavi, tessuti e gin. Ghana: polvere d'oro. Congo: barre d'ottone. Sudafrica: bestiame e perle.
- America: Alaska: pellicce, polvere d'oro e conchiglie. Canada: wampum, pellicce, coperte, rum e schiavi. Messico: grani di cacao. Guatemala: mais. Brasile: frecce e fucili. Paraguay: gusci di lumaca.

L'approccio storico:

- Preistoria: Gallia: bestiame, barre di metallo, anelli e metallo fuso a forma di ascia celtica. Germania: bestiame e anelli. Inghilterra: schiavi e barre di metallo nel Galles e metallo coniato sotto forma di spade e anelli altrove. Irlanda: bestiame e schiavi, grano o orzo per i piccoli pagamenti.
- Medioevo: Inghilterra: come mezzo di scambio anelli, monete coniate e bestiame, mentre l'unità di misura *pound* indica un certo peso di argento che non viene mai coniato. Irlanda: il bestiame è la moneta più usata e anche come unità di conto, ma non scompare l'uso di schiave (scambiate con le mucche in un rapporto di 1 a 3). Islanda: da bestiame a stoffa, pesce secco ed anelli metallici. Danimarca: da bestiame ai metalli coniati. Svezia e Norvegia: da bestiame, burro, pelli e stoffa alla moneta coniata. Ungheria e Russia: da bestiame all'oro e alle pellicce.

- Periodo moderno: Inghilterra: chiodi di ferro, uova e uccelli. Irlanda: bestiame. Canada: grano, pellicce e pesce secco. Barbados: cotone, tabacco, zucchero e poi la moneta coniata. Bermude: tabacco. Honduras: pezzi di legno di mogano. Russia: pellicce, poi metallo coniato, ma l'argento coniato mantiene un ruolo significativo. Francia: sospeso l'uso degli asssignats di carta, nel 1795 si torna al grano ed argento. Austria: al termine del primo conflitto mondiale si usano burro e avena. India: nocciole"[14].

Aver riportato questi studi all'interno di questo elaborato è servito a mettere in luce certi aspetti, che hanno giocato un ruolo fondamentale per lo sviluppo dell'economia monetaria a livello globale. Innanzitutto, si evince che l'economia monetaria perdura per molto tempo, ed è avvenuta in tutte le società, specialmente in quelle più primitive e anche nelle condizioni socioeconomiche più difficili. Come si può constatare, molte volte c'è una razionalità nella scelta di una determinata merce adibita alla moneta: ossia si scelgono merci che hanno una valenza pratica nella vita quotidiana; altre volte è vista come una conseguenza dell'estensione geografica dell'area commerciale. In tutte le società si sceglie di passare alla moneta di metallo e alcune di esse le danno un nome proprio spesso coincidente con quelle dell'unità di peso (talento, lira, pound). Si privilegia ad utilizzare metalli preziosi come merce-moneta, ad alto valore intrinseco. Cionondimeno, in ogni società c'è sempre l'autorità preposta (politica, militare o religiosa), che ha il compito decisionale ed autoritario nella scelta della moneta da far accettare agli utilizzatori.
Il passo successivo è stato il passaggio dalla merce-moneta (metallica) alla carta-moneta. Come si è illustrato precedentemente le prime forme note di questa tipologia di moneta sono da localizzarsi in Oriente mentre in Europa l'arrivo della carta moneta è da attribuirsi al mondo islamico con l'avvento delle crociate qualche secolo più tardi (anche se una sostanziale diffusione si avrà solo qualche secolo più tardi). Ci sono diverse ragioni che favoriscono la forte diffusione della carta moneta tra le quali la sua praticità. Grazie a questa tipologia di moneta i governi nazionali hanno potuto emettere debito pubblico, infatti la liquidità del biglietto di banca non possiede valore intrinseco come il metallo, ma esso dipende solamente dalla credibilità del Paese. Proprio per questo motivo, solo con la nascita di autorità nazionali riconosciute, si manifesta la sua piena accettazione ed

[14] Questi studi sono riportati nel libro: Franco Spinelli, cit., pag. 17-18.

utilizzo[15]. La carta-moneta ha un ulteriore vantaggio: non è costosa e non ha un costo-opportunità e per questo motivo, con la stampa di carta-moneta, si libera il metallo che può essere impiegato più fruttuosamente.

Nel 1867 si creò il cosiddetto *Gold Standard* noto anche come *sistema aureo*; questo principio consente di trasformare l'oro in riserva per le banche centrali, e viene usato per regolare i deficit delle bilance commerciali. Le autorità monetarie possono emettere moneta fino a un limite (pari ad alcune volte il valore dell'oro detenuto nei forzieri). Così facendo l'argento perde importanza come metallo monetario. In tal modo i Paesi hanno legato le loro politiche monetarie (specialmente quelle espansive), alle quantità di riserva d'oro presenti nei loro caveau. Facile intuire che se il paese grava in situazione di crisi economica che perdura per parecchio tempo, le riserve auree scendono drasticamente. Per evitare ciò si usa la pratica delle svalutazioni della propria valuta. Il deprezzamento porta effetti collaterali anche alle altre monete. Ad ogni modo, ci sono monete che sono state prese come riferimento, tra cui la sterlina, che all'epoca era la più forte.

Il *Gold Standard* fu messo in crisi tra le due guerre mondiali, fino all'abbandono definitivo avvenuto con gli accordi *Bretton Woods*, perché in tale sistema gli Stati erano limitati dalle sole riserve auree che possedevano, mentre in realtà avevano da una parte l'esigenza di finanziare le ingenti spese belliche, e dall'altra sostenere le proprie economie affossate dalla grande depressione. Purtroppo, questo sistema aggravava la situazione, impedendo interventi espansivi delle *policy makers*.

Con gli accordi di Bretton Woods, avvenuti il 22 luglio 1944, è stato deciso congiuntamente alla fondazione del Fondo Monetario Internazionale (FMI) e della Banca Mondiale, l'abolizione dell'apparato precedente. Il nuovo sistema prevede una struttura di cambi fissi rispetto al Dollaro, il quale diventa la nuova moneta di riferimento. Di conseguenza, le riserve auree delle banche centrali perdono importanza rispetto al dollaro americano.

Questa soluzione che ha funzionato solo nel breve periodo, perché permetteva più flessibilità agli altri Paesi che hanno potuto quindi attuare politiche monetarie espansive

[15] Sarebbe stato difficilmente realizzabile nei secoli precedenti. Le singole città stato o piccoli regni, avrebbero avuto difficoltà a far accettare moneta priva di valore intrinseco, e avrebbero innescato la legge di Gresham, dove i sudditi avrebbero conservato moneta estera se fosse migliore di quella interna, e che quest'ultima sarebbe stata impiegata solamente per il pagamento di tasse, e che quindi ritornavano direttamente al mittente. Legge di Gresham tratta da fonte: "http://www.treccani.it/enciclopedia/sir-thomas-gresham_%28Enciclopedia-Italiana%29/".

grazie alle continue svalutazioni della propria valuta. Questo determina però una cosa inaspettata, il fallimento del sistema stesso. Ovvero quando c'era stato un periodo inflazionistico negli U.S.A. verso la fine degli anni '60, questo aveva avuto l'effetto collaterale (inflazionistico) anche nei paesi in cui la loro valuta era legata al dollaro. Il sistema era crollato definitivamente quando gli U.S.A. erano entrati in recessione e di conseguenza il Dollaro si era deprezzato, cosicché non si poteva più mantenere né il Gold standard per il Dollaro né tantomeno tenere il cambio fisso del dollaro con le altre valute. In definitiva, con l'accordo del 1973 si passa al sistema di cambi flessibili (doveva essere temporaneo ma di fatto diventa perpetuo) dove si lascia libertà ai cambi delle valute di oscillare senza vincoli o restrizioni alcune.

La differenza fra moneta a corso legale rispetto alla *classica* moneta, a cui ci si riferiva prima del 1973, appare adesso più chiara: fino a quell'anno il mondo occidentale usava una moneta che era garantita dalle riserve auree degli Stati Uniti. Da quella data in poi, la moneta è definita a corso legale o moneta *Fiat*, poiché questo strumento di pagamento non è garantito da alcuna riserva aurea e tantomeno dal valore intrinseco della moneta stessa. È lo Stato nazionale a dare valore alla propria valuta e il popolo la usa riponendo la sua fiducia nell'autorità centrale.

Da quello che si è analizzato, si evince che la moneta è un elemento caratterizzato da grande mutevolezza infatti, a seconda delle circostanze (sociali, relazioni internazionali, economiche, culturali), può evolvere in sistemi mai adottati prima o regredire, o addirittura creare un sistema misto in cui coesistono più sistemi differenti tra loro[16]. Si può affermare che le monete siano l'espressione dei popoli, utilizzate per attuare scambi e in più generale impiegate come strumento civile per creare e mantenere stabili i legami nella comunità.

Per i motivi sopra elencati, non si può tralasciare l'evoluzione che ha avuto negli ultimi decenni, in primis con l'avvento dell'euro. Quest'ultima moneta rappresenta l'unità dei Paesi europei, in risposta al cambiamento geopolitico mondiale; anche se attualmente sta vivendo una situazione difficile e di crisi. Senza entrare troppo in dettaglio, l'avvento della crisi del 2008 ha portato fuori i problemi insiti dei singoli Stati membri nonché dei limiti che possa rappresentare questa valuta. Cionondimeno, rappresenta un primo passo per

[16] Quello che è accaduto nel passato, per esempio nell'economia del Giappone fino del XIX secolo, dove coesistevano sia l'economia naturale che l'economia monetaria.

l'unità degli Stati, per raggiungere l'ideale di unità politica sotto forma di Stati Federali Europei.

Un'altra innovazione, che è avvenuta negli ultimi anni, è la digitalizzazione della moneta. Questo fenomeno si è diffuso enormemente, complice anche l'avvento di Internet, e ha modificato radicalmente tutti i settori socioeconomici del Mondo. La moneta elettronica è cominciata da Dee Hock, l'inventore di Visa, oltre cinquant'anni fa. Negli ultimi decenni si è molto sviluppata ed è facile intuire le ragioni: la praticità nel trasporto, la non necessità del cambio valuta, la possibilità di effettuare transazioni a distanza e per ultimo la possibilità di pagamenti periodici. Inoltre, ci sono dei vantaggi anche da parte dell'autorità, quali ad esempio la tracciabilità, fornendo così alla finanza un sistema di controllo ineccepibile.

Tuttavia, questo sistema di pagamento, non ha soppiantato completamente il denaro contante che continua ad essere utilizzato senza problemi. Questo è avvenuto per due motivi principali: il primo è la necessità di avere un conto in banca e il secondo è l'anonimità dei contraenti, con più tutela della privacy. Attualmente si sta vivendo un'epoca particolare in cui sia la moneta fisica che la moneta elettronica convivono proprio perché hanno diverse caratteristiche e le si possono alternare a seconda che ci sia un'esigenza invece di un'altra. Amato e Fantacci[17] sostengono che non si possono usare entrambe nello stesso momento e questa possibilità si è verificata solo con l'arrivo di bitcoin. Come si vedrà nei paragrafi successivi, l'arrivo della moneta digitale ha generato numerose di queste monete che vogliono soppiantare il sistema finanziario tradizionale o quantomeno migliorarlo. Ad ogni modo non ci è dato sapere se queste valute digitali soppianteranno quelle tradizionali, ma sicuramente stanno creando preoccupazione tra le istituzioni finanziarie.

Prima dell'avvento della digitalizzazione delle monete

L'avvento della digitalizzazione delle monete viene spesso associata alla creazione del bitcoin, nel 2008-2009. In realtà questa affermazione è inesatta in quanto bitcoin incorpora nel proprio sistema informatico decenni di studi che ne hanno permesso la nascita; infatti, il vero problema che cercano di risolvere i sistemi monetari decentralizzati

[17] Gli autori del libro: "Per un pugno di Bitcoin", 2016, Università Bocconi.

è il double-spending18. Bitcoin non è stata la prima moneta decentralizzata che è riuscita in questo intento, ma è stata la prima che, seppur scegliendo adeguatamente il timing perfetto per il suo lancio19, è riuscita a farsi apprezzare dal grande pubblico. Il sistema Bitcoin incorpora molte soluzioni trovate dalle precedenti valute elettroniche sviluppate da crittografi che erano intenti nello sviluppo di un sistema valutario decentralizzato, sin dai primordi di internet. Prima di passare in rassegna gli antenati della moneta digitale più famosa al mondo si cercherà di evidenziare chi e cosa abbia influenzato quest'era delle criptomonete.

Negli '70 del Novecento, nell'ambito della crittografia, la ricerca condusse a sostanziali sviluppi che avevano lo scopo di migliorare la sicurezza e la privacy individuale; queste erano prerogative dei Governi per la sicurezza delle comunicazioni.

Grazie a questi studi sono stati creati alcuni sistemi monetari anonimi digitali, simili al Bitcoin. Il loro funzionamento consisteva da aggregati di unità di valute indipendenti l'una dall'altra e questo permetteva una grandissima divisibilità; le transazioni erano registrate in un libro mastro. Questi sistemi erano ancora centralizzati. Fra i più famosi si può citare: *DigiCash*, una società fondata nel 1989 da David Chaum che è riuscita a creare un sistema anonimo di denaro digitale per governi e banche allo scopo di vincere la corruzione e il crimine organizzato. Tecnicamente la maggiore innovazione di questa valuta era che le transazioni avvenivano per mezzo di un sistema *wireless* per questo motivo un primo utilizzo fu il pagamento dei pedaggi autostradali. Ci furono numerose banche e multinazionali che si interessarono a questo sistema, tra cui: Deutsche Bank e Credit Suisse, Visa e Microsoft. Nel 1990 fallì il sistema e la società, la valuta continuò ad essere utilizzata fino al 1997 da parte di una banca americana. Nel 1990 vide la luce un sistema di moneta digitale sviluppato dalla Citibank, con il nome di Citibank's e-cash; l'obiettivo di questa valuta era di impedire il riciclaggio, in quanto il titolare della moneta, avrebbe dovuto comunicare alla banca di sostituire i diversi tipi di monete. Ci furono dei test nel 1997 e 2001, anno in cui il progetto fu abbandonato dai manager della Citigroup.

Di seguito sono elencate le tecnologie che hanno permesso lo sviluppo dell'algoritmo utilizzato da Bitcoin. La prima tecnologia che si deve citare è l'hashcash definito per la

[18] Definizione: "Se un utente malintenzionato prova a spendere i propri bitcoin verso due diversi riceventi contemporaneamente, si tratta di doppia spesa. Il mining di Bitcoin e la blockchain esistono per creare un consenso sulla rete, per decidere quale delle due transazioni sia considerata valida", Fonte Url: "https://bitcoin.org/it/glossario".

[19] Come verrà esplicato nei paragrafi più avanti di questo capitolo.

prima volta da Adam Beck nel 1997; tale sistema è basato sul *prof-of-work*[20] il cui scopo è la prevenzione di spam nelle e-mail facendo compiere un dispendioso lavoro al computer mittente prima dell'invio. Questo sistema è fallito in quanto presentava molte difficoltà di adozione e un elevato consumo energetico per il computer e tutto questo al solo scopo di tutelare un servizio di secondaria importanza. Nel 1998 Wei Dai sviluppa B-money un sistema monetario digitale decentralizzato che permette l'anonimato nelle transazioni peer-to-peer. Il sistema era tenuto in piedi da un fondo di deposito dei partecipanti che ricevevano sanzioni e premi in base alla loro condotta; il maggiore problema di questa moneta era la mancanza di un'autorità centrale in grado di sanzionare le cattive condotte. Nel 2005 Nick Szabo sviluppa Bit-gold, questo sistema utilizzava il *proof-of-work* per registrare i passaggi di proprietà. I Bit-gold venivano creati tramite la risoluzione dei blocchi ma non era stato esplicato chiaramente come venivano gestiti. Secondo Szabo, il mercato si sarebbe aggiustato con la potenza computazionale dei computer. In definitiva, questi sistemi erano per lo più idee e teorie ma non erano mai state concretizzati per le numerose difficoltà riscontrate nella loro implementazione. Ad ogni modo, quest'ultime due *primordiali* monete digitali, avevano lo stesso scopo del Bitcoin: garantire l'anonimato delle transazioni.

Bitcoin prende alcuni spunti delle monete precedentemente citate e li combina tra loro per creare il suo *core*. Molti di questi elementi sono comuni in diversi progetti come ad esempio il *peer-to-peer*[21] e l'uso della crittografia a chiave asimmetrica. Il vero colpo genio del creatore fu ideare un sistema che combinava la *Blockchain* e il *Mining*[22]. Con la combinazione delle caratteristiche di entrambe, si poté finalmente tenere correttamente il sistema e allo stesso tempo, tenere sotto controllo dagli attacchi degli hackers.

---

[20] Definizione PoW: "il Proof-of-Work è usata in molte criptovalute. L'applicazione più famosa di PoW è Bitcoin. È stato Bitcoin a porre le basi per questo tipo di consenso. Il puzzle è Hashcash. Questo algoritmo consente di modificare la complessità di un puzzle in base alla potenza totale della rete. Per il Bitcoin tempo medio di formazione del blocco è di 10 minuti", Fonte Url: "https://www.lecriptovalute.org/2018/01/19/proof-of-work-significato-cos-e-pow-e-il-proof-of-stake-guida/".

[21] "Rete informatica nella quale i computer degli utenti connessi fungono nello stesso tempo da client e da server. In tal modo, gli utenti sono in grado di accedere direttamente l'uno al computer dell'altro, visionando e prelevando i file presenti nelle memorie di massa e mettendo a loro volta a disposizione i file che desiderano condividere. Le reti peer-to-peer sono usate in partic. per scambiare file audio o video (come nel caso di Napster ')", Definizione tratta dal dizionario Treccani, Url: "http://www.treccani.it/enciclopedia/peer-to-peer/".

[22] Sia per la tecnologia Blockchain che di Mining, verranno definite qualche paragrafo più di questo capitolo.

Giappone 2008

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution"[23].

Con questa dichiarazione esordisce l'inventore del Bitcoin e, quindi più in generale, dell'universo delle criptovalute. Infatti, la nascita delle criptovalute si identifica con la creazione del *Bitcoin*. Quest'ultimo è stato creato da Satoshi Nakamoto[24] nel 2008. L'ultima apparizione è stata nel 2011, quando ha lasciato il controllo totale del dominio *Bitcoin.org* ad altri sviluppatori tra cui il principale Gavin Andresen.

Ci sono state molte ipotesi dietro a questa identità: inizialmente si sospettava fosse Michael Clear, un laureato in crittografia al Trinity College che ha immediatamente smentito. Molte testate giornalistiche hanno cercato invano di identificare l'inventore servendosi di diversi stratagemmi tra i quali l'analisi dell'inglese utilizzato per capire se fosse un madrelingua o ancora la verifica degli orari delle modifiche al software al fine di identificare il più probabile fuso orario e quindi il paese di origine. Da queste indagini è risultato che potrebbe essere una persona di lingua inglese e di origini americane. Quello che rimane un caposaldo è il suo lavoro, dalla sua prima pubblicazione "*Chryptograhy Mailing List*" del 2008, fino al 2011, anno in cui si ritirò "per curare altre cose". Detto questo non si può affermare precisamente di quale nazionalità e sesso sia, e se pure sia un singolo individuo o un gruppo di programmatori. Come viene riportato da Il Sole 24 ORE, si è cercato di analizzare il suo nome allo scopo di trovare alcuni indizi riguardanti l'identità. Da questa analisi è risultato che il suo nome avrebbe questi significati: *Satoshi*: per intendere intelligente e saggio, *Naka*: mezzo, relazione e *Moto*: origine, fondamento[25].

L'ultima rivelazione degna di nota risale nel dicembre 2015 quando la testata giornalistica *Wired* e *Gizmodo*[26] teorizzavano che dietro alla famosa moneta elettronica ci fosse in realtà Craig Steven Wright, un imprenditore australiano esperto di sicurezza delle informazioni. Tra le prove annoverate la più importante fu la scoperta di un fondo denominato Tulip Trust nel quale Nakamoto aveva depositato all'inizio della creazione del Bitcoin circa un milione di monete digitali. Tale fondo se convertito al momento della

[23] Citazione presa dal primo documento di Satoshi Nakamoto: "Bitcoin: A Peer-to-Peer Electronic Cash System, October 31, 2008".

[24] In realtà questo è uno Pseudonimo, perché non si sa chi si cela dietro a questa figura. Infatti, questo è rimasto ancora un mistero.

[25] Fonte Il Sole 24 ORE: "Sulle tracce del geniale Nakamoto" Edizione 10/2015 pag. 14 - 4 ottobre 2015.

[26] Gizmodo: è un blog sulla tecnologia elettronica di consumo. Fa parte del gruppo Gawker Media gestito da Nick Denton, ed è conosciuto per l'aggiornamento e la copertura sul settore tecnologico.

pubblicazione dell'articolo avrebbe fruttato oltre un miliardo di dollari[27]; oggi ha un valore di oltre i dieci miliardi di dollari[28].

In seguito, Andrew O'Hagan pubblica un articolo sul London Review of Books[29], che racconta la storia di Nakamoto nel quale mette in dubbio il coinvolgimento di Wright per via delle troppe incongruenze.

Nel 2016 Wright afferma:

"Ci sono un sacco di storie in circolazione e non mi va che coinvolgano persone a cui voglio bene. Non voglio che nessuna di loro sia toccata da questa vicenda. Non voglio essere il volto pubblico di qualcosa. Avrei preferito non averlo dovuto fare. Voglio lavorare, voglio continuare a fare ciò che voglio. Non voglio denaro. Non voglio fama. Non voglio essere venerato. Voglio solo essere lasciato in pace"[30].

È interessante evidenziare che la dichiarazione sia arrivata dopo una perquisizione nella casa di Wright, eseguita dalla polizia australiana nel dicembre 2015, con l'obiettivo di trovare documentazioni riguardanti la criptovaluta, anche se le motivazioni ufficiali riguardavano l'evasione fiscale. Curioso notare che queste indagini furono eseguite sottopressioni della Fed americana, che come la Bce, era contraria a una moneta decentralizzata.

Senza continuare ad elencare ulteriori nomi ed ipotesi, c'è da porsi almeno tre domande:

1. Perché la scelta di rimanere segregato ed abbandonare ad un certo punto il progetto?
2. Perché scegliere un nome di origine giapponese?
3. Perché esporsi nel 2008 anno dello scoppio della più grande crisi finanziaria di tutti i tempi?

Probabilmente queste domande rimarranno senza risposta, ma si possono fare alcune ipotesi. In molti si sono chiesti il motivo di tutta questa segretezza. Secondo il premio Nobel Robert Shiller, la segretezza può essere un possibile motivo che ha portato al successo questa moneta digitale[31] e aggiunge:

---

[27] Fonte Il Sole 24 ORE: "Da Nakamoto a Wright: chi si cela dietro l'inventore" Edizione 02/2017 pag. 31 – 24 febbraio 2017.

[28] Quotazione di mercato pari a: 10.439,60 $, 23 febbraio 2018, ore 17:13, Fonte: "https://coinmarketcap.com/".

[29] Articolo pubblicato dal "London Review of Books" autore: "Andrew O'Hagan".

[30] Fonte Il Sole 24 ORE: "Da Nakamoto a Wright: chi si cela dietro l'inventore" Edizione 02/2017 pag. 31 – 24 febbraio 2017.

[31] Fonte WIRED: "https://www.wired.it/economia/finanza/2018/01/12/satoshi-nakamoto-bitcoin/".

"It has no value at all unless there is some common consensus that it has value. Other things like gold would at least have some value if people didn't see it as an investment, Shiller told CNBC in an interview ahead of the World Economic Forum in Davos, Switzerland, where he will be speaking next week. It reminds me of the Tulip mania in Holland in the 1640s, and so the question is did that collapse? We still pay for tulips even now and sometimes they get expensive. (Bitcoin) might totally collapse and be forgotten and I think that's a good likely outcome but it could linger on for a good long time, it could be here in 100 years"[32].

Si può ipotizzare, tentando di rispondere alla terza domanda, che la data di lancio di questa moneta digitale non sia stata lasciata al caso: il principale nemico delle criptovalute sono le monete tradizionali, e il lancio, in un momento storico a valle delle crisi finanziarie del 2008, nel quale la credibilità globale delle tradizionali valute risultava deteriorata, ha consentito alla moneta elettronica di avere un trend positivo.

Lo sviluppatore è stato capace di dare un valore aggiunto alla moneta cavalcando l'onda di sfiducia globale verso monete centralizzate e gestite da enti governativi; infatti un sistema di tipo peer-to-peer riesce ad attrarre le persone grazie al suo carattere *anarchico* e decentralizzato, quindi ad oggi ci sono sempre più persone che investono in questo settore. È quindi possibile ipotizzare che la data di lancio di questa criptovaluta, che ha dato il via poi a tutte le altre, non sia stata lasciata al caso.

La nascita degli "Altcoins"

Dal 1 di gennaio del 2009 al 27 di febbraio del 2018 sono state sviluppate 1580 criptovalute con un valore complessivo di circa 462 $ miliardi[33]. Questi numeri spaventano le grandi istituzioni finanziarie, in primis la BCE e la FED, tanto che più volte si sono pronunciate negativamente e ne stanno monitorando il fenomeno. Dalla creazione del Bitcoin si è assistito alla nascita di nuove monete digitali; alcune di esse hanno tentato di migliorare il core dei Bitcoin diventandone competitor diretti, altre invece hanno cercato di trovare strade alternative.

[32] Fonte CNBC: "https://www.cnbc.com/2018/01/19/bitcoin-likely-to-totally-collapse-nobel-laureate-robert-shiller-says.html".

[33] Fonte url: "https://it.investing.com/crypto/", 27 febbraio 2018, ore 11:36.

Il vero boom di queste monete è stato nell'anno 2017 quando si sono registrati numeri da record: in questo anno si è registrato il prezzo record del Bitcoin (per ora[34]) e cioè 19,665.39[35] $.

La spaventosa crescita delle criptovalute ha portato effetti collaterali devastanti in alcuni settori correlati. Come si vedrà poi nel prossimo capitolo, la creazione delle monete digitali avviene per mezzo di un procedimento denominato *Mining*; tale processo necessita di computers con componenti hardware sviluppate appositamente come ad esempio le schede video.

L'*effetto Mining* ha portato conseguenze negative per i *gamers*[36] in quanto si è registrato un importante incremento del prezzo delle schede video. Recentemente l'azienda Nvidia ha sviluppato una scheda madre dedicata ai miners[37], che permette di svolgere un enorme quantità di calcoli; tale scheda madre consente di montare fino a 19 moduli VRAM.

Un altro effetto collaterale è il consumo spropositato di energia elettrica dovuta al funzionamento di questi potenti calcolatori: si stima che venga utilizzata una quantità di energia elettrica pari al consumo della Danimarca[38].

Recentemente l'Islanda è divenuta il migliore paese per ospitare i server del Bitcoin. Il boom di miner ha fatto lievitare enormemente la domanda di energia elettrica, tanto da superare i consumi elettrici dei privati; la società erogatrice è in allerta perché non sa se riuscirà ad offrire elettricità per tutto il paese. Questa corsa frenetica è stata denominata *corsa all'oro del XXI° secolo*. Il motivo di attrazione per questo paese è dovuto principalmente a due fattori: il primo è la presenza di stazioni idroelettriche che producono l'80% dell'energia ad un costo accessibile, il secondo è il clima rigido, condizione fondamentale per limitare i costi di raffreddamento dei server.

La creazione e lo sviluppo di queste cripto monete è in continua evoluzione, e in alcuni casi può sembrare fuori controllo: si noti che le prime dieci sono quelle più importanti e diffuse sul mercato hanno capitalizzazione pari a $ 371,41 miliardi, cioè pari al 82% di tutto il settore. Si deve scendere fino alla ventiseiesima posizione della classifica per

---

[34] Data odierna: 27 febbraio 2018, ore 11:57.
[35] Fonte url: "https://www.coingecko.com/it/grafici_del_prezzo/bitcoin/usd", 16/12/2017, ore 01:00.
[36] Definizione: "qualcuno che gioca ai videogiochi", Fonte Url: "https://dictionary.cambridge.org/it/dizionario/inglese/gamer".
[37] Fonte Url: "http://www.dday.it/redazione/25507/nvidia-chi-vuole-arricchirsi-coi-bitcoin-fa-salire-il-prezzo-delle-gpu".
[38] Fonte Url: http://www.infodata.ilsole24ore.com/2017/12/30/bitcoin-quanta-energia-elettrica-consumano/.

trovarne una la cui capitalizzazione sia inferiore al miliardo di dollari, e fino alla due centoquindicesima per scendere sotti i 50 milioni di dollari[39].

Il mercato delle criptomonete, pur avendo terminato il 2017 con un trend positivo, ha subito un arresto durante i primi mesi del 2018. In primis lo stesso Bitcoin, che pur avendo raggiunto un prezzo da capogiro nella metà di dicembre, ha registrato una fortissima contrazione sfiorando i 6,852 $ il 6 febbraio 2018, ritornando al prezzo del 13 novembre.

L'arresto era imprevedibile infatti il trend di crescita sembrava inarrestabile. Proprio per questo motivo nel 2017, in piena fase di boom del mercato delle criptovalute, molte società hanno investito creando metodi di finanziamento destinati alla raccolta di capitale attraverso la messa in circolazione di monete digitali. Tali metodi di finanziamento sono denominati *Ico*[40]. Le nuove monete digitali hanno avuto un risultato contrario a quello sperato, secondo i dati raccolti dal portale Bitcoin.com che ha analizzato i trends forniti da *Tokendata*[41]. Le analisi effettuate hanno messo in risalto che il 46% delle 902 nuove criptovalute sviluppate durante lo scorso anno sono state inefficaci: 142 non hanno mai raggiunto la soglia sperata e 276 sono scomparse.

Nel prossimo paragrafo si analizzeranno dieci delle più importanti e diffuse criptovalute sul mercato, senza dimenticare però che, per motivi di volatilità, questa *top ten* è destinata a mutare velocemente.

Le diverse Criptovalute: dal "Bitcoin" agli "Altcoins"

In questo paragrafo si analizzeranno le dieci criptovalute che al momento della stesura di questo lavoro, possono essere considerate le più importanti e diffuse sul mercato. Come spiegato precedentemente, si deve tenere presente che la loro capitalizzazione è circa l'82% di tutto l'ecosistema delle monete digitali e che per molti studiosi queste saranno

[39] Fonte Url: "https://it.investing.com/crypto/currencies", 27 febbraio 2018, ore 17:22.

[40] Ico (*Initial Coin Offering*): "Le offerte iniziali di valuta (Ico) rappresentano il modo per finanziare nuove attività in ambito blockchain. Le società lanciano l'Ico emettendo un "token", un gettone digitale pagato in criptovalute (la più utilizzata è Ethereum), che permette di accedere a un servizio o di avere una quota nella società che si va a finanziare. Si tratta di una sorta di crowdfunding del criptomondo, letteralmente esploso nella seconda metà del 2017: nell'intero anno sono stati raccolti fondi pari a oltre sei miliardi di dollari via Ico". Definizione tratta dall'ebook: *Bitcoin Generation – la rivoluzione delle criptovalute*, Nòva, Il Sole 24h, 9 marzo 2018, pag. 57.

[41] Tratto da Url: "https://www.tokendata.io/".

negli anni avvenire la vera rivoluzione del XXI° secolo dopo la diffusione di internet. La seguente analisi è così strutturata: verranno analizzate accuratamente le prime cinque, alle quali si darà maggiore attenzione perché per diverse ragioni, saranno quelle che prenderanno campo nel prossimo futuro. Nella seconda parte del paragrafo saranno elencate quelle che si posizionano nei posti inferiori della classifica.

Bitcoin (BTC)

Non si può che partire da questa moneta digitale in quanto è considerata la primogenita, dal punto di vista della sua diffusione a larga scala, perché come si è illustrato precedentemente non è la prima in termini anagrafici. Come si è già detto in precedenza, questa fu ideata da Satoshi Nakamoto. In seguito, si sono susseguiti diversi programmatori tra cui Gavin Andresen. Sul sito Bitcoin.org[42] si può trovare l'elenco degli sviluppatori e gli incarichi che stanno svolgendo. L'algoritmo dei Bitcoin è rilasciato sotto licenza *open source*[43].

La nascita della moneta può essere identificata il 31 ottobre 2008 giorno di pubblicazione del *white paper* "Bitcoin: a peer-to-peer electronic cash system", mentre il 3 gennaio del 2009 vede la luce il primo Bitcoin.

Dando una nomenclatura più precisa, con il termine 'Bitcoin' (con la lettera iniziale maiuscola) si intende alla tecnologia di pagamento e registrazione crittografica di informazioni, mentre con il temine 'bitcoin' (con lettera iniziale minuscola) si fa riferimento alla moneta o *token*, che circola per mezzo della tecnologia Bitcoin[44].

Ma realmente come si può definire il Bitcoin? Secondo Amato e Fantacci[45] è un sistema di pagamento molto innovativo con grandi potenzialità: lo si può definire come contante digitale, perché unisce i vantaggi della moneta elettronica a quelli del contante, perché attraverso di esso è possibile sostenere delle transazioni oltreconfine, senza comportare dei costi aggiuntivi, sia da parte del mittente che del destinatario. Il tutto è guidato dall'ideologia (quale il suo carattere anonimo ed anarchico contro i grandi intermediari),

[42] Url: "https://bitcoin.org/it/sviluppo".

[43] Definizione dal dizionario Treccani: software di cui l'utente finale, che può liberamente accedere al file sorgente, è in grado di modificare a suo piacimento il funzionamento, correggere eventuali errori, ridistribuire a sua volta la versione da lui elaborata. L'esempio più noto è il sistema operativo Linux. La distribuzione di un software in formato o. presuppone la rinuncia da parte dei programmatori al diritto di proprietà intellettuale. Fonte Url: "http://www.treccani.it/enciclopedia/open-source/".

[44] Tratta dal libro: Massimo Amato e Luca Fantacci, *Per un pugno di Bitcoin*, Università Bocconi Editore, pag. 7.

[45] Autore del libro: Massimo Amato e Luca Fantacci, cit.

che riesce a sorreggere tutto il sistema e che ha permesso, negli ultimi nove anni, di incrementare sia l'utilizzo che l'accettazione di questa criptomoneta, nonché la sua capitalizzazione, portandola ad essere la "regina" delle criptovalute.

Nel libro *The Bitcoin Bible* Satoshi Nakamoto viene paragonato a Martin Lutero[46]; mentre altri lo hanno definito *Cyber Cristo*, per la *liberazione 2.0* dell'umanità da parte di tutti gli obblighi del sistema tradizionale; con il termine liberazione si intende l'abolizione del controllo verticale e dell'autorità in favore della libertà orizzontale del *peer to peer*[47].

Nel libro sopracitato, viene ripreso il discorso del filoso tedesco Max Weber, che ha studiato il rapporto fra protestantesimo e capitalismo: secondo Weber c'era un paradosso del movimento religioso, nato dalla volontà di liberare l'uomo dall'istituzionalità della fede, ma che ha invece contribuito alla genesi del capitalismo. Secondo Weber tale sistema economico è assai infido, perché è capace di oppressioni inimmaginabili attraverso ad una *pietrificazione meccanizzata*[48]. Difatti, in base a questa teoria, il protestantesimo è all'origine del capitalismo. Questo è successo, pur non volendo, per eccesso di razionalismo. Ad ogni modo, ritornando al discorso del Bitcoin, il contesto è differente, perché è un'innovazione tecnologica politicamente neutrale, dovuta al fatto che è puramente tecnica.

Inoltre, questi concetti vengono rimandati al discorso che Papa Francesco tenne ad una conferenza inerente all'economia del denaro e della finanza. Il discorso è come segue:

"La crisi mondiale che tocca la finanza e l'economia sembra mettere in luce le loro deformità e soprattutto la grave carenza della loro prospettiva antropologica, che riduce l'uomo a una sola delle sue esigenze: il consumo. E peggio ancora, oggi l'essere umano è considerato egli stesso come un bene di consumo che si può usare e poi gettare. Abbiamo incominciato questa cultura dello scarto. Questa deriva si riscontra a livello individuale e sociale; e viene favorita! In un tale contesto, la solidarietà, che è un tesoro dei poveri, è spesso considerata controproducente, contraria alla razionalità finanziaria ed economica. Mentre il reddito di una minoranza cresce in maniera esponenziale, quello della maggioranza si indebolisce. Questo squilibrio deriva da ideologie che promuovono

[46] *The Bitcoin Bible* è un libro scritto da Benjamin Guttman nel 2013, il quale è stato tradotto in lingua italiana nel 2014, denominato: *Bitcoin. Guida Completa*.

[47] Peer-to-Peer: "Etimologia: 'pari (peer) a pari (to peer)'; si dice di rete locale in cui ognuno dei computer collegati ha al pari di tutti gli altri accesso alle risorse comuni, senza che vi sia un'unità di controllo dedicata come server; si dice di software che permette di scambiarsi file fra utenti collegati a Internet", Fonte Url: "https://www.garzantilinguistica.it/ricerca/?q=peer-to-peer".

[48] Ossia a un meccanismo che non abbisogna più di alcun fondamento spirituale per potersi perpetuare.

l'autonomia assoluta dei mercati e la speculazione finanziaria, negando così il diritto di controllo agli Stati pur incaricati di provvedere al bene comune. Si instaura una nuova tirannia invisibile, a volte virtuale, che impone unilateralmente e senza rimedio possibile le sue leggi e le sue regole"[49].

A questo discorso viene contestata la sua posizione, o meglio a chi viene rivolto. Secondo l'autore del testo, il cambiamento deve arrivare dal basso, ossia il papa non può chiedere che i governi debbano controllare i mercati. Secondo l'autore la risposta al pericolo della riduzione dell'uomo a un bene di consumo è l'autonomia assoluta dell'individuo. Quindi nel discorso di questa moneta digitale, il Santo Padre non vedrebbe la differenza che c'è tra il denaro dall'alto e il denaro dal basso. Di conseguenza, secondo Guttman[50], il problema non è il denaro che è uno strumento, ma: "il modo in cui viene creata la fiat money, chi ne controlla l'emissione e coloro in favore dei quali viene emessa"[51]. L'autore afferma che se il Papa conoscesse il significato di *moneta sana*, riuscirebbe a capire la tecnologia *disruptive* di Bitcoin, intesa come un sistema monetario privato e decentrato, e come questa possa riuscire dove le leggi hanno fallito, ossia ad impedire molti crimini finanziari. Guttman sostiene che le banche siano un residuo di *papismo* all'interno dell'economia capitalista e che abbiano il monopolio nella creazione della moneta, e si interpongano fra il denaro e i suoi legittimi possessori. Questo viene estrapolato da:

"Il Martin Lutero di oggi è Satoshi Nakamoto. Lutero pubblicò le sue 95 tesi nel 1517 e Satoshi ha rilasciato il suo codice 'open source' per Bitcoin nel 2009. Il monaco tedesco contestava aspramente che la libertà dalla punizione divina per i peccati potesse essere comprata con il denaro. Nakamoto voleva dare alla gente la possibilità di spostare denaro senza l'uso delle banche, e fare ciò è come parlare con Dio senza un prete"[52].

Si può affermare che il protestantesimo privi la chiesa del ruolo di intermediario, allo stesso modo il Bitcoin, e in più in generale la maggior parte delle altre criptovalute, sta cercando di fare instaurando un rapporto diretto tra l'individuo e il denaro.

Si può affermare senza dubbi che la data di lancio del Bitcoin non è stata affatto casuale, infatti è avvenuta nel 2008, proprio a seguito della più grande crisi finanziaria di tutti i

[49] Tratta dal discorso del Santo Padre Francesco ai nuovi ambasciatori di Kyrgyzstan, Antigua e Barbuda, Lussemburgo, Botswana accreditati presso la Santa Sede, Sala Clementina, giovedì 16 maggio 2013; Fonte Url: "https://w2.vatican.va/content/francesco/it/speeches/2013/may/documents/papa-francesco_20130516_nuovi-ambascaitori.html".

[50] Autore del libro: *Bitcoin: The Bible*.

[51] Guttmann 2013, pag. 367.

[52] Guttmann 2013, pag. 368

tempi che ha coinvolto tutto il sistema finanziario tradizionale. Il white-paper è stato reso pubblico poco più di un mese dopo il fallimento di Lehman Brothers[53] che è la causa delle prime disastrose conseguenze della crisi. Come sostengono gli autori del libro: *Per un pugno di Bitcoin*, il 2008 viene definito come lo *Annus Horribilis* del sistema finanziario globale in quanto viene messo in evidenza il sistema fragile ed oligopolistico delle banche, che tra bancherotte e salvataggi, sono state beneficiarie di aiuti statali immeritati giustificati soltanto dal fatto di esercitare una funzione pubblica essenziale.

Il 3 gennaio 2009 viene "minato" il primo bitcoin soprannominato *genesis block* che ha dato proprio origine a Bitcoin. Successivamente il creatore ha minato un milione di bitcoin nei primi giorni, per poi ritirarsi fino a lasciare definitivamente la comunità a dicembre 2010. Nakamoto riesce a trovare la soluzione al problema del *double spending*, ossia riesce ad evitare che la valuta possa essere copiata.

Oltre alla creazione del token lo sviluppatore del Bitcoin ha introdotto alcune nuovi algoritmi che permettono di gestire transazioni internazionali, decentralizzate e sicure. Infatti, grazie questa innovazione tecnologica il Bitcoin e stato copiato al fine di creare altre monete digitali.

Di fatto il meccanismo di creazione di bitcoin è fissato dall'algoritmo di Satoshi Nakamoto e il numero massimo di monete creabili è 21 milioni[54]: tale soglia, secondo le attuali stime, sarà raggiunta nel 2130[55]. Come viene descritta dagli autori del libro "Bitcoin Generation, la rivoluzione delle criptovalute", il processo di *Mining* consiste nella decodifica di stringa di numeri, che può essere paragonata al complesso rompicapo crittografico, che vengono concatenati immutabilmente sotto forma di blocchi di bit nella Blockchain che possono essere conservate dai proprietari grazie ad un *Wallet*.

Prima di spiegare il funzionamento e la tecnologia che sorregge il Bitcoin e i suoi token è necessario fornire alcune definizioni. Con il termine di *Mining* si intende: "il cuore del sistema della blockchain: i miners sono gli operatori che garantiscono l'autenticità e la veridicità delle transazioni, svolgendo il ruolo dei tradizionali intermediari. In compenso

---

[53] Fallimento Lehman Brothers: "http://www.corriere.it/economia/08_settembre_15/lehman_brothers_banca_crisi_credito_Usa_b8805f84-82b3-11dd-9b8b-00144f02aabc.shtml".

[54] Tutt'ora si è arrivati alla creazione di quasi 17 milioni, tratto dall'ebook, Nòva, Il Sole 24h, cit.

[55] L'estrazione dell'ultima moneta è prevista nel 2130, ma il 99% sarà minato entro il 2027, comunque dipenderà dal successo dei computer quantistici, che potrebbero risolvere l'algoritmo del bitcoin molto più velocemente, ovviamente a scapito di un consumo energico maggiore. Fonte Url: "https://it.businessinsider.com/estrarre-bitcoin-e-sempre-piu-costoso-un-esperto-spiega-fino-a-quando-sara-redditizio/".

questi ricevono i nuovi bitcoin minati"[56]. La Blockchain, o *catena dei blocchi*, "è il registro distribuito e trasparente dentro il quale sono trascritte in modo immodificabile tutte le transazioni effettuate sotto forma di blocchi: i miners si occupano di agganciare i nuovi blocchi alla catena. Il registro è replicato in tutti i nodi della blockchain"[57]. Una volta creati o comprati i bitcoin vengono conservati in un *Wallet* che altro che non è un portafoglio digitale.

Senza entrare troppo nel dettaglio, cosa che si farà nel secondo capitolo, è utile ricordare che questa criptovaluta si basa sul Mining che è una procedura molto costosa a livello energetico. Questo perché l'algoritmo redatto da Nakamoto è pensato per permettere che un blocco venga minato ogni dieci minuti. In aggiunta, il protocollo è dinamico, ossia si adegua al numero di partecipanti al sistema, e che quindi di conseguenza deve essere adeguato all'aumento della capacità di computazionale per mantenere invariato questo rate. Per questo motivo serve una potenza di calcolo crescente man mano che si va avanti con il mining dei blocchi. Ogni quattro anni la quantità di bitcoin contenuta in un blocco, che può essere considerata come il premio per i *miners*, si dimezza: nel 2009 comprendeva 50 bitcoin dati mentre oggi 12.5[58].

Terminando il discorso, questo sistema di funzionamento è detto *decentrato*, perché invece di basarsi su una struttura gerarchica di computer, dove all'apice si trova il server dell'autorità centrale, si fonda su un network peer-to-peer, dove all'interno tutti i nodi sono sullo stesso livello. Ogni computer prende parte alla conoscenza globale ossia mantiene una copia della blockchain che viene replicata per tutti i computer collegati alla rete. Questa è una vera e propria rivoluzione in quanto la blockchain è conservata da ogni computer, o nodo, in un registro pubblico allo scopo di mantenere un'informazione decentrata e facilmente fruibile da ciascun altro nodo. Questo registro pubblico viene aggiornato dal lavoro dei miners che si occupano di garantire l'autenticità di ogni singola transazione in cambio di bitcoin.

Inizialmente i bitcoin venivano usati per illeciti quali ad esempio acquisti su siti internet come *Silk Road*[59], perché come si vedrà nel prossimo capitolo, una delle sue caratteristiche

[56] Definizione tratta dall'ebook Nòva, Il Sole 24h, cit., pag. 9.
[57] Definizione tratta dall'ebook Nòva, Il Sole 24h, cit., pag. 10.
[58] Data: 9 marzo 2018.
[59] Silk Road: "si tratta di un vero e proprio mercato nero della droga, al quale si accede coperti da anonimato, grazie al programma Tor che funziona come una rete parallela, completamente anonima e irrintracciabile. Non a caso è lo stesso programma utilizzato in giro per il mondo da diversi attivisti per la difesa dei diritti umani che possono così portare avanti le loro battaglie sul web senza essere individuati. Ulbricht - preso dagli agenti federali in California, all'interno di una biblioteca pubblica di San Francisco - aveva creato un

più importanti è che riesce a garantire l'anonimato della transazione. Proprio per questo che viene rimandata alla similitudine della banconota. Il punto cruciale per questa moneta digitale, ma in generale per tutto questo mercato, è l'accettazione di esse. Proprio per questo motivo, quando è stata accettata dai primi negozianti "normali", il prezzo scambiato per l'acquisito è cresciuto nel tempo. Basti pensare che nel 2010, lo sviluppatore Laszlo Hanyecz, per dimostrare la possibilità di utilizzare questa forma di moneta, acquistò due pizze da Papa Johnsper, per la 'modica' cifra di 10,000 bitcoin (pari ad un valore odierno di $ 96,000,000[60]).

Parecchie figure si sono espresse durante gli anni, da scettiche e riluttanti agli albori, a curiose e ben disposte dopo, durante il boom dei prezzi. Infatti, da settembre 2017, quando iniziò la fortissima impennata dei prezzi, forse dovuta a una speculazione inaudita, molte di queste figure si dovute ricredete. Si può citare: Jamie Dimon[61], il quale dopo essersi rimangiato le sue parole, ha sottolineato una cosa assai importante e fondamentale: l'innovazione che porterà la Blockchain. Difatti, il mondo non ha potuto essere contrario o scettico ad essa. Questa piattaforma digitale, il libro mastro delle transazioni, è stato preso da assalto dalle grandi multinazionali e società finanziarie di tutto il mondo, le quali hanno visto le grandissime potenzialità che essa può portare.

Tutt'ora, questa criptomoneta è la prima per capitalizzazione del settore, pari a circa $ 163.01 miliardi, con un prezzo di circa: $ 9,600[62]. Come si vedrà più avanti, questa ha avuto nell'ultimo anno (da inizio 2017 fino al 11 marzo 2018), una elevatissima variabilità, dovuta ad una fortissima speculazione che la ha portata a sfiorare circa 20,000$ nella metà di dicembre 2017, per poi scendere a quasi alla metà ai primi di marzo 2018. Secondo alcuni, questo effetto ha portato a una "scrematura" degli utilizzatori. Come si vedrà nei prossimi capitoli, ci sono state anche delle ingenti truffe da parte di

---

vero e proprio impero, con un giro di affari che si aggira sui due milioni di dollari l'anno". Fonte Url: "http://www.corriere.it/tecnologia/13_ottobre_02/chiuso-silk-road-ebay-droghe-df97b220-2b8c-11e3-93f8-300eb3d838ac.shtml".

[60] Fonte Url: "https://www.investing.com/crypto/", prezzo di 9,600 $, 11 marzo 2018, ore 19:46.

[61] Presidente e Ceo di JP Morgan Chase, il quale disse pubblicamente: "Mi scuso per aver commentato che bitcoin è una frode. La Blockchain è una realtà" era il 9 gennaio 2018. Rimangiandosi quanto detto nel settembre 2017, nel corso di una conferenza tenutasi a New York, il quale aveva definito bitcoin come "una bolla, peggiore dei tulipani", Fonte Url: "http://www.wallstreetitalia.com/bitcoin-dimon-di-jp-morgan-pentito-di-averlo-definito-frode/".

Inoltre, come fatto assai curioso non si può non dire quello che il Ceo di JP Morgan Chase ha fatto, dopo la dichiarazione negativa di settembre 2017. Infatti, secondo l'articolo del Sole24h, La banca di investimento americana, insieme alla Morgan Stanley, hanno fatto acquisti per un totale di circa tre milioni di euro, questo proprio quando il prezzo del bitcoin era piombato ai minimi storici di quei mesi.

[62] Fronte Url: "https://www.investing.com/crypto/", 11 marzo 2018, ore 19:46.

cybercriminali che hanno causato disastri economici nei possessori dei bitcoin[63]. Questo per ribadire nuovamente, che questa criptomoneta è rimasta, e rimane sempre come oggetto di studio, sia tra i regolatori, sia tra i consumatori.

Ethereum (ETH)

Nel 2013 il programma-tore russo-canadese Vitalik Buterin ha presentato il *white paper* di Ethereum nel quale era spiegato dettagliatamente il funzionamento. Questa criptovaluta può essere considerata un'evoluzione del Bitcoin. Grazie a questa pubblicazione ha vinto, nel 2014, la *Theil Fellowship*[64] ricevendo un premio di $ 100,000 che gli ha permesso di dedicarsi completamente al progetto.

Buterin, intuendo le potenzialità della Blockchain, aveva capito che si poteva migliorare il core del Bitcoin creando una struttura che consentisse lo sviluppo di applicazioni decentralizzare con ampie capacità cioè un sistema che non si limitasse solo a transazioni finanziarie peer-to-peer. A differenza di Bitcoin, qui non si voleva solo eliminare gli intermediari finanziari per gli scambi di denaro ma si voleva utilizzare la criptovaluta per rappresentare merci, derivati ed azioni immobiliari. Lo scopo di Buterin è quello di eliminare i vincoli arbitrari fiduciari, tramite lo sviluppo di applicazioni, cambiando così il modo delle transazioni fiduciarie senza l'utilizzo di quei sistemi legali e burocratici lenti e complessi.

Alla fine del 2014 il progetto vede la luce tramite la prima ICO per mezzo della quale vengono venduti i primi *Ether*. Come negli altri sistemi di pagamento elettronico, Ethereum rappresenta un sistema di funzionamento in cui viene utilizzato un nuovo tipo di Blockchain, mentre Ether è la valuta digitale utilizzata dal sistema stesso. Le prime vendite del token risalgono ai mesi di luglio e agosto del 2014; il cui ricavato di tali vendite permette di finanziare ulteriormente il progetto del software.

La prima versione ufficiale di Ethereum viene lanciata il 30 luglio 2015. Tutt'ora Ethereum è guidata da un team centrale di sviluppatori tra i quali figura Buterin. Questo progetto è gestito da una fondazione svizzera no profit: la Ethereum Foundation. Qui si trova la

[63] Fonte Url: "http://www.fastweb.it/web-e-digital/truffe-furti-bitcoin/".

[64] La Theil Fellowship: "is intended for students under the age of 23 and offers them a total of $100,000 over two years, as well as guidance and other resources, to drop out of school and pursue other work, which could involve scientific research, creating a start-up, or working on a social movement", Fonte Url: "https://en.wikipedia.org/wiki/Thiel_Fellowship".

prima differenza con Bitcoin, ossia Ethereum viene identificata con la figura chiave del suo fondatore. Un altro elemento che differisce dalla capostipite è la piattaforma che secondo alcuni può essere paragonata ad un *Framework*[65] in quanto fornisce la possibilità di creare applicazioni blockchain decentralizzate in grado di funzionare autonomamente. Secondo alcuni analisti questo sistema è ancora agli albori e questo perché non è ancora ad un livello di stabilità, scalabilità e sicurezza desiderabili per reggere il confronto con altre applicazioni blockchain decentralizzate.

Nel contesto storico in cui viviamo, c'è una proliferazione di nuove criptovalute che rispetto all'originaria si differenziano proprio nella piattaforma che li sorregge. Nella maggior parte dei casi, si assiste a un miglioramento di questa piattaforma, assolvendo così a propri scopi specifici. Nel caso di Bitcoin, la blockchain ha lo scopo di consentire transizioni internazionali finanziare sicure basate sul sistema peer-to-peer, eliminando la necessità di fiducia di un intermediario finanziario. Invece, nel caso di Ethereum, Buterin ha ideato una piattaforma aperta al pubblico, dove chiunque può costruire un'applicazione blockchain per l'esecuzione di qualsiasi funzione. Invece di memorizzare solo i dati delle transazioni finanziarie, la blockchain di Ethereum è ideata per eseguire un codice basato su transazioni verificate. Per questo motivo le transazioni all'interno di questo sistema, vengono definite *smart contracts*, ossia contratti intelligenti basati su blockchain. Gli smart contracts sono programmi per computer e possono essere considerate come la vera essenza di Ethereum. Il sistema degli *smart contracts* è stato inventato nel 1993 da Nick Szabo[66], il quale li considerava come un "distributore automatico digitale". Per tali motivi, Ethereum è stata a lungo considerata come una perfetta competitor, che potesse surclassare (cosa che non è ancora avvenuta) il Bitcoin. Per le sue caratteristiche, riesce ad attrarre campi molto diversi come ad esempio le imprese, la politica fino ad arrivare alla *supply chain*; a proposito di queste aree di interesse si possono citare alcuni esempi: per le imprese può essere utilizzato per trasferire proprietà, per la politica può servire per l'esercizio del voto in quanto la

[65] Framework: "insieme di elementi software che un programmatore può usare o modificare per realizzare un programma", definizione tratta dal dizionario: "https://www.garzantilinguistica.it/ricerca/?q=framework".

[66] Un crittografo che ideò per primo questo sistema, dove venne ripreso dall'esplosione delle criptovalute. Inoltre, a questa figura gli si era anche associato il nome di Satoshi Nakamoto, infatti per alcuni lui era il creatore di Bitcoin, fonte tratta da Wired, Url: "https://www.wired.it/attualita/tech/2014/04/22/bitcoin-creatore-nick-szabo/".

blockchain è intrinsecamente inattaccabile, nel caso della supply chain può sostituire la burocrazia cartacea, garantendo così compiti e pagamenti nei tempi prefissati.

Ethereum, come per le altre criptovalute soffre periodi di volatilità, ciononostante è diventata une delle più pregiate monete virtuali. Basti pensare che godeva di una capitalizzazione di $ 84 miliardi l'8 marzo 2018, per poi quasi dimezzarsi ed arrivare a $ 47 miliardi il 18 marzo 2018[67].

Come per il Bitcoin, anche qui viene utilizzata la tecnologia *Proof-of-Work* per la convalidazione di ogni nuovo blocco che viene aggiunto alla blockchain. Esattamente come si era visto per il Bitcoin, la creazione gestione dell'infrastruttura è fatta utilizzando algoritmi di mining, per questo motivo per il corretto funzionamento di questa criptovaluta, è richiesto un enorme consumo di energia elettrica e di un'alta capacità computazionale dei computer. Si stima che sia per Bitcoin che per Ethereum, vengano sostenuti dei costi pari a più di $ 1 milione al giorno.

All'inizio del 2017, il creatore di Ethereum ha annunciato che questa criptovaluta si sposterà dal *Proof-of-Work* al *Proof-of-Stake*. Nel maggio 2017 Buterin aveva pubblicato un *white paper* in cui spiegava l'implementazione del nuovo algoritmo del PoS denominato Casper. Rispetto al PoW che utilizzano i computer dei minatori per risolvere un blocco attraverso calcoli complessi e privi di significato, qui il PoS utilizza i partecipanti del sistema Ethereum per la validazione dei singoli blocchi.

Proof-of-Stake potrebbe essere implementato nei mesi successivi in quanto potrebbe portare parecchi vantaggi, dall'eliminazione dei costi esorbitanti ad un miglioramento al livello di sicurezza e scalabilità, nonché velocità nelle transazioni. Ad ogni modo si dovrà aspettare per giudicare come realmente questo impatterà sul sistema poiché gli algoritmi di consenso sono da sempre un problema tecnico all'interno di un ambiente blockchain decentralizzato, nonostante sia un elemento fondamentale per le criptovalute.

[67] Fonte Url: "https://www.investing.com/", 18 marzo 2018, ore 18:55h.

Ripple (XRP)

Ripple è una valuta digitale creata nel 2012 da Chris Larsen e da Jed McCaleb che si basa sul protocollo *OpenCoin*[68]. Il token di Ripple è chiamato *XRP* mentre con il termine Ripple si intende l'intero sistema; questa moneta al momento dell'analisi occupa la terza posizione per capitalizzazione[69]. OpenCoin è stato progettato dall'omonima start-up di San Francisco (ora rinomianta in Ripple Labs) che ha stabilito che il numero massimo di queste monete digitali sia pari a 100 miliardi di XRP; tale numero è già stato raggiunto. È importante far notare che oltre la metà delle monete è ancora in mano a OpenCoin che ne rilascia un po' per volta; ad oggi, in circolazione, se ne contano 38 miliardi. A differenza del Bitcoin, XRP è scambiata per soli $ 0.90 cent[70], e vuole imporsi come moneta digitale alternativa alla capostipite (Bitcoin). Ripple è stata lanciata allo scopo di garantire transazioni finanziarie globali sicure, istantanee (appena 4 secondi) e quasi gratuite di qualsiasi valuta e senza storni di addebito. Si riesce a fare ciò grazie alla tecnologia della blockchain, che però a differenza del Bitcoin, i token di Ripple sono tecnicamente di proprietà della società omonimo, quindi si può affermare che è una valuta semi-decentralizzata, anche se il fondatore preferisce definire XLM come decentralizzata perché il token potrebbe essere scambiato autonomamente anche senza la presenza della società. Questa è stata la ragione del suo boom a fine 2017, quando il valore di questa moneta elettronica è cresciuto oltre il 36,000% in dodici mesi.

Ripple è di proprietà della omonima società (Ripple Labs) che possiede circa il 61% degli XRP. Come detto in precedenza non si deve fare l'operazione *Mining* perché la convalida delle transazioni avviene senza i *miner* e perciò garantisce rapidità e costi energetici pressoché nulli. Come le altre criptovalute utilizza un blockchain decentralizzata, dove le transazioni vengono certificate da alcuni grandi nodi della rete, come ad esempio gli operatori telefonici o le istituzioni accademiche[71] riuscendo così a superare i limiti del sistema finanziario tradizionale, ossia gestire una costosa server farm per difendere le informazioni[72]; in più riesce ad essere trasparente e non "rivoluzionario" contro il sistema

[68] OpenCoin è un progetto partito nel 2007 da David Chaum, volto a creare un sistema monetario digitale, tramite una versione open source. Fonte url: "https://opencoin.org/Members/jhb/opencoin-and-ripple".
[69] Capitalizzazione pari a $ 35,74 miliardi, 01 marzo 2018, ore 12:54h.
[70] Prezzo datato: 1° marzo 2018, ore 12:59h, Fonte Url: "https://it.investing.com/crypto/currencies".
[71] In questo caso: il Mit di Boston.
[72] Come tutt'ora fanno: banche, le società delle carte di credito come Visa, MasterCard e Amex, e anche le nuove realtà come PayPal. Fonte Url: "http://www.corriere.it/economia/18_gennaio_02/scalata-ripple-l-anti-bitcoin-ecco-perche-ora-piace-banche-97077066-f001-11e7-ae90-7494db7ac3d7.shtml".

come il Bitcoin. Infatti, per quest'ultimo motivo, per alcuni Ripple non ha l'ideologia delle altre criptomonete, ma anzi riesce in tal modo ad avvicinarsi alle grandi istituzioni finanziarie, come banche e grandi società, che ancora oggi utilizzano sistemi più antiquati. Questa cripto valuta ha come il vantaggio la "Rapidità" nelle transazioni:

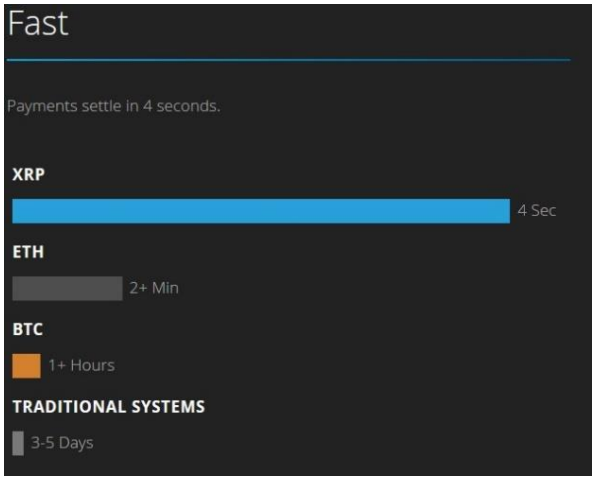


Figure 1.1 Velocità nelle transazioni, fonte Url: "https://ripple.com/xrp/".

Inoltre, XRP è più ecologico[73] e per ottenerlo l'unico modo è acquistarlo normalmente, o coloro che donano alla ricerca scientifica la propria potenza computazionale alla Ripple Lab. La potenzialità di questo sistema e della sua criptovaluta, sta proprio nella sua fondamento, ossia è possibile fare uno scambio tra valute tradizionali, senza passare da una banca centralizzata; in aggiunta è possibile anche fare lo stesso anche tra le altre valute digitali.

Il punto di debolezza di questa moneta digitale è che per ora non è utilizzata per i pagamenti infatti la piattaforma Ripple è adoperata per i trasferimenti in tutte le valute. Probabilmente OpenCoin sta cercando di diffondere una nuova tecnologia che utilizza solo XRP per gli scambi[74].

In definitiva questa criptomoneta vuole imporsi come alternativa e non come diretta competitor del Bitcoin, in quanto Ripple mira a collaborare con il sistema finanziario esistente.

[73] Ogni operazione in Bitcoin corrisponde un consumo di 100kWh, Fonte Url: "https://www.panorama.it/economia/soldi/tutto-quello-che-ce-da-sapere-sulla-criptovaluta-ripple/".
[74] Fonte Idem.

Stellar (XLM)

"Stellar is a common financial platform that is designed to be open and accessible to everyone"[75].

Con questa definizione, la *Stellar Development Foundation*[76] descrive le caratteristiche e gli obiettivo di Stellar. Con il termine Stellar si definisce sia il network Stellar che il protocollo Stellar, mentre con il termine *Lumen* ci si riferisce al token, anche noto con il simbolo *XLM*. Nata agli inizi del 2014 da Jed McCaleb[77] e Joyce Kim, il protocollo *open source* è supportato da un'organizzazione no profit "SDF". Questa fondazione no profit si trova nello stato americano del Delaware e non ha azioni, né profitti concessi a privati, né investimenti privati.

La piattaforma Stellar è basata sulla tecnologia blockchain ed è sviluppata in linguaggio C++ e rispetto a Ripple, è completamente decentralizzata. Questa moneta digitale è un'alternativa rispetto alle altre, ed è complementare a Ripple[78]. Stellar ha una piattaforma tramite la quale chiunque ha la possibilità di immettere nel sistema la propria valuta *Fiat* (Euro, Dollaro, Yen...) e ricevere Lumen (XLM) che potranno essere inviati immediatamente, sostenendo costi irrisori, direttamente nel wallet del destinatario, in qualsiasi paese del mondo. Dopodiché i Lumen ricevuti potranno essere convertiti nella valuta desiderata. A differenza dei Bitcoin non c'è il Mining, infatti la convalida delle transazioni avviene diversamente e in più i token sono stati creati dalla piattaforma.

Trattandosi di un'organizzazione no profit, la SDF si è prefissata di non trarre profitto dalle commissioni di transazione su Stellar, pertanto si finanzia tramite:

"a. 5% of the initially created lumens on Stellar. We periodically auction these lumens on various exchanges;

b. Charitable contributions from companies or individuals;

c. Foundation membership;

---

[75]Definizione tratta dal mandato, fonte Url: "https://www.stellar.org/about/mandate/#Held_by_Foundation".

[76] Per semplicità è nota anche con l'acronimo: "SDF".

[77] Jed McCaleb è un programmatore informatico, noto per aver creato: le tecnologie 'peer-to-peer eDonkey', 'Mt. Gox' un sito che gestiva lo scambio bitcoin (poi venduto a Mark Karpelès poco prima di fare bancarotta), co-fondatore di Ripple nel 2011, che ha lasciato nel 2013 per sviluppare Stellar nel 2014. Tuttavia, pur avendo restrizioni di vendita di XRP, nel gennaio 2018 è stata stimata da 'Fores' la proprietà di token di Ripple (XRP), pari ad un valore di $ 20 miliardi, portandolo al 40° posto nell'elenco delle persone più ricche al mondo. Tuttora, in Stellar ricopre la carica di Chief technology officer.

[78] Ripple punta a connettere le banche di tutto il mondo, Stellar è più al servizio di colossi multinazionali. Fonte Url: "https://www.borsainside.com/criptovalute/67342-ripple-e-stellar-oggi-rimbalzano-previsioni-positive-su-quotazioni-2018-grazie-alle-grandi-aziende/".

d. In 2014, SDF received a loan of $3,000,000 from Stripe[79] which was subsequently repaid with 2B lumens"[80].

Dalla sua creazione sono stati "coniati" 100 miliardi di XLM, com'era specificato nel protocollo. Di questi, 95 miliardi sono stati distribuiti nel mondo, i rimanenti 5 miliardi sono rimasti all'interno della piattaforma Stellar. Come imposto dal suo mandato, la fondazione SDF è incaricata di sorvegliare e gestire l'esecuzione della distribuzione dei Lumen (XLM).

I Lumen iniziali detenuti dalla SDF devono essere distribuiti in questo modo:

"a. 50% for distribution via the Direct Sign-up Program;

b. 25% for distribution via the Partnership Program;

c. 20% for distribution via the Bitcoin Program;

d. 5% held by SDF to support operational costs"[81].

Il secondo punto è degno di essere analizzato: il 'Partnership Program' che ha lo scopo di finanziare, tramite sovvenzioni, imprese, governi, istituzioni o organizzazioni no profit, poiché l'obiettivo è di incoraggiare l'adozione e la crescita di XML. In tal modo, si premieranno le istituzioni che contribuiranno all'ecosistema Stellar, sia in termini di incentivo nell'adozione sia estendendo la portata della rete a popolazioni meno sviluppate o escluse finanziariamente.

Mentre il terzo punto, il *Bitcoin Program* è stato completato in due tempi: uno ad ottobre 2016 e l'altro ad agosto 2017 e questo programma consiste nel distribuire gratuitamente Lumen ai possessori Bitcoin e XRP (19% per Bitcoin e 1% per XRP), con lo scopo di incoraggiare i titolari di queste due criptomonete, ad esplorare e utilizzare Stellar.

Da evidenziare la volontà dei fondatori di SDF e Stirpe[82], di non vendere i Lumen inizialmente ricevuti per almeno cinque anni, al fine di garantire la stabilità del mercato dei XML. Tuttavia, Stirpe si è valsa la possibilità di venderle all'asta ma solo per i destinatari che concordino di non venderle per cinque anni e in ogni caso gli utili netti saranno restituiti alla fondazione.

Per evitare che ci sia un'inflazione troppo elevata per XML, nel network di Stellar pone un limite fisso ad essa. I nuovi XML vengono aggiunti alla rete al ritmo dell'1% all'anno, e ogni

[79] Questa è un'azienda dove crea e gestisce le piattaforme sul web, volte a gestire la loro attività su internet, quali ad esempio i pagamenti online, Url: "https://stripe.com/it".
[80] Fonte Url: "https://www.stellar.org/about/mandate/#Held_by_Foundation".
[81] Fonte Url: "https://www.stellar.org/about/mandate/#Held_by_Foundation".
[82] Stripe: Investment company, Url: "https://stripe.com/it".

settimana, il protocollo distribuisce questi Lumen su qualsiasi account che superi lo 0,05% dei voti da altri account nella rete.

Questa cripto moneta è l'ottava per capitalizzazione pari a $ 6,05 miliardi, con un valore di mercato di $ 0,32[83] l'una. Questa moneta digitale potrà mai soppiantare le altre? Questo è uno dei più grandi interrogativi fin da quando è stata creata ed è degna di nota sia per motivi tecnici sia per importanti partnership internazionali.

"New digital currency aims to unite every money system on earth"[84], inizia così l'articolo della testata: 'Wired", ma lo è realmente? Ebbene ci sono parecchi aspetti che meritano di essere menzionati. Nel 2014, Rodrigo Batista[85] si indirizzò subito dopo il lancio, verso questa cripto valuta. Forse proprio perché rispetto alle altre è stata lanciata e gestita da una fondazione no profit, con lo scopo di connettere le persone, specialmente poco abbienti, tra di loro. Come sostiene Wired, Stellar svolge molteplici funzioni ma ha come obiettivo cardine quello di creare una rete mondiale che consenta a chiunque di inviare qualsiasi valuta e riceverla come qualsiasi altra valuta, ad esempio: inviare bitcoin e riceverli come dollari, oppure pagare qualcuno in euro che verranno ricevuti dal destinatario come Litecoin. Per questi motivi Batista si è subito lanciato in Stellar, perché questa valuta digitale può superare i "limiti" di altre già affermate (quali Bitcoin e Litecoin), fondendola con monete *Fiat* e così estendendo i suoi vantaggi al consumatore medio. Proprio per questo motivo che Patrick Collision di Stirpe ha creduto nel progetto Stellar, per creare qualcosa che unisca le diverse piattaforme e tecnologie.

Ovviamente, anche i fondatori di questa moneta digitale prestano cautela, lo stesso Jeb McCaleb, lo sviluppatore principale di Stellar, è prudente in quanto ha già provato in prima persona, con Ripple, che ci sono dei limiti da superare: infatti secondo il suo parere Stellar è un tentativo di correggere alcuni problemi che si trovano nelle altre criptovalute, incluso il bitcoin. Come si è detto in precedenza, il Bitcoin è guidato da una rete mondiale di computer che consentono, oltre ad archiviare la valuta digitale, anche di inviarla facilmente da un luogo all'altro, senza sostenere costi esorbitanti e saltando gli intermediari. Inoltre, può essere utilizzata anche per pagare beni e servizi, sia online che nei negozi tramite device quali smartphone. McCaleb, con la creazione di Ripple, mira ad estendere questa opportunità a tutte le valute, incluse le *Fiat*. Per fare ciò è stata coniato

[83] Fonte Url: "https://it.investing.com/crypto/", del 07/03/2018 – ore 11:23.

[84] Questa definizione viene data dal giornalista Robert McMillan, di Wired, Fonte Url: "https://www.wired.com/2014/08/new-digital-currency-aims-to-unite-every-money-system-on-earth/?mbid=email_onsiteshare".

[85] Ceo di Mercado Bitcoin, il primo exchange brasiliano di Bitcoin, e uno dei più grandi dell'America Latina.

il token "XRP", che viene usato per gli scambi in rete. Se si vuole scambiare il bitcoin con il dollaro, la rete cerca qualcuno che può convertire il bitcoin in XRP, quindi qualcun altro che scambi l'XRP in dollari. Tutto questo ha causato un problema di fiducia, infatti alcuni hanno ipotizzato che i fondatori, tra cui McCaleb, cercassero solo di arricchirsi con la creazione di una la tecnologia Ripple Labs. Ad ogni modo McCaleb abbandonò definitivamente il progetto Ripple per riavviarlo nel sistema Stellar.

La società Ripple Labs afferma: "Stellar is a fork of Ripple, so the code is practically identical", e questo lo hanno fatto per renderlo così più attrattivo per la grande comunità di valute digitali, così come per le normali imprese e il pubblico in generale.

Come si è detto precedente, il punto di forza è chi controlla questa valuta digitale, ed è una fondazione no profit, piuttosto che una società privata. Inoltre, la gestione della distribuzione dei token viene controllata dalla fondazione stessa, con i parametri sopracitati. Altro punto a suo favore è la velocità di trasferimento di denaro, che è molto più elevata rispetto al bitcoin, e in più il network di Stellar continuerà a generare Lumen, rispetto alle cifre bloccate di Bitcoin[86] e Ripple[87]. Questo perché rispetto alle altre, si tratta di una "valuta inflazionistica", perché la filosofia che sta a monte è quella per cui questa moneta digitale possa essere utilizzata nel futuro e che le persone siano incoraggiate a spenderla effettivamente, piuttosto che limitarsi come mero strumento di investimento. In tal modo, si sono concentrati sulle persone, le quali effettivamente vogliono utilizzare la moneta digitale. A tal proposito non si può non citare l'affermazione di Patrick Collison[88]: "The motivation was, in part, to have people focus a bit less on digital currency as something to hoard or a store of value".

Non da ultimo bisogna tenere a mente che il sistema Bitcoin distribuisce la valuta a persone che aiutano a gestire la propria rete mondiale con piattaforme hardware complesse, invece Stellar si pone come una valuta che possa essere d'aiuto a chi ne ha interesse. A questo interviene anche Joyce Kim[89] che afferma che bisogna sostenere e dare una possibilità anche alle persone più in difficoltà che non dispongono grossi capitali iniziali.

In definitiva, l'obiettivo più grande è la creazione di un modo universale per spostare i soldi, non solo i Lumen, ed è qui che si insidiano le difficoltà: il progetto deve coinvolgere

[86] Bitcoin numero massimo: 21 milioni nel 2130.
[87] Ripple numero massimo: 100 miliardi, già coniati.
[88] Patrick Collison è il Ceo di Stripe.
[89] Joyce Kim è un'addetta nella venture capitalist e amica di lunga data di McCaleb, che all'epoca stava supervisionando il sistema Stellar.

le organizzazioni a configurare i *gateway*[90] di valuta digitale che guideranno il network Stellar. In tal modo, sarà possibile archiviare i dollari in un gateway e questi potranno essere utilizzati per pagare qualcuno in euro, perciò il gateway convertirà inizialmente i dollari in Lumen e poi li invierà ad un altro gateway in grado di convertirli in euro. Per far sì che il progetto funzioni, dovranno partecipare anche le banche tradizionali e le compagnie di carte di credito, che mantengono grandi capitali, che potrebbero essere riluttanti a partecipare in un'area che è ancora offuscata dalle normative.

Questa è la grande differenza rispetto a Ripple, infatti come afferma Monica Long[91]: "We think people will interact with Ripple via the financial instruments they already use", ed è per questo che Ripple si è focalizzato a non portare la sua attenzione ai consumatori, ma direttamente alle istituzioni finanziarie, e come si è detto precedentemente, per questo motivo le grandi banche sono state attratte da Ripple. Invece, Stellar ha come obiettivo cardine la piena utilizzabilità da parte di chiunque ed ovviamente trovando il modo di collaborare con i regolatori, ma come appunto afferma Kim che questo progetto deve rimanere aperto a tutti, e che non dia ad un'organizzazione vantaggi e privilegi rispetto ad altre. Inoltre, aggiunge: "Major infrastructure for the world like this, shouldn't be owned by a company".

Come più volte si è detto, quando delle organizzazioni stipulano partnership con queste piattaforme digitali, non fanno che puntare i riflettori su di loro e quanto è più importante il player che stringe l'accordo, maggiore è la fiducia e la autorevolezza che viene infusa nella criptomoneta. Un esempio di questo fenomeno è l'accordo stipulato con l'IBM il 16 ottobre 2017[92], quando l'azienda americana si è dimostrata interessata alla blockchain di Stellar e al suo sistema di pagamento elettronico. In dettaglio, IBM ha annunciato che avrebbe usato questa piattaforma digitale per cooperare con le banche situate nel Pacifico meridionale, con lo scopo di fornire pagamenti transnazionali. Per Stellar è stato un grande momento, e ha fatto apprezzare maggiormente al pubblico il suo token che ha avuto un incremento del 190% in un giorno (dal $ 0,01897 del 15 ottobre al $ 0,03600 del 16 ottobre, e pari al 242% il 17 ottobre 2017) [93]. Da evidenziare che il prezzo non è più sceso sotto questa soglia. Tra i big nelle partnership, non si può dimenticare, che nel

[90] Gateway (dall'inglese: portone, passaggio) è un dispositivo di rete che opera al livello di rete, il suo scopo principale è quello di veicolare i pacchetti di rete all'esterno di una rete locale. Fonte Url: "https://it.wikipedia.org/wiki/Gateway_(informatica)".

[91] Monica Long è la direttrice delle comunicazioni di Ripple Labs.

[92] Fonte Url: "http://www-03.ibm.com/press/us/en/pressrelease/53290.wss".

[93] Fonte url: "https://it.investing.com/crypto/stellar".

maggio 2016, anche l'azienda americana Deloitte ha stretto una partnership con questa piattaforma, per il lancio della: 'Deloitte Digital Bank', con lo scopo di potenziare i pagamenti istantanei attraverso i confini.
Secondo gli esperti di FinTech del sito Finder.com, questa criptovaluta sarà destinata a crescere vertiginosamente entro la fine del 2018, portando la capitalizzazione di mercato pari a $ 183 miliardi, ossia ad un aumento oltre il 1700% nel 2018[94].

Iota (MIOTA)

"THE BACKBONE OF IOT IS HERE - Scalable, Decentralized, Modular, No Fees"[95]
Con IOTA si identifica il registro di distribuzione *open source*, creato per permettere la comunicazione e le transazioni sicure tra un network e prodotti ideati per connettersi e condividere le informazioni. Tale sistema è denominato 'Internet of Thing' (in acronimo: IoT[96]). Inoltre, IOTA identifica sia la criptovaluta che il suo token. Come verrà illustrato in seguito, questa tecnologia è assai differente dalle altre criptovalute, e vuole imporsi come alternativa ad esse. Prima di iniziare l'analisi più dettagliata è necessario inquadrare il sistema 'IoT', visto che questa tecnologia è adibita a soddisfare questo bisogno.
"Internet delle cose" o 'IoT' (acronimo di Internet of Things), è un nuovo vocabolo introdotto da Kevin Ashton, nel 1999. Questo termine si riferisce all'estensione del mondo virtuale di internet nel mondo reale degli oggetti e luoghi concreti. L'obiettivo dell'IoT è di permettere agli oggetti di interagire da remoto usufruendo delle infrastrutture dei network esistenti, allo scopo di fare interagire il mondo fisico con quello digitale. Come descritto dall'articolo di Yahoo Finanza, del 27 febbraio 2018, la tecnologia utilizzata viene usata nei campi più diversi, ad esempio: "impianti di monitoraggio dell'udito, transponder biochip di animali da fattoria, dispositivi di analisi del DNA per il monitoraggio ambientale/alimentare/patogeno e dispositivi operativi che supportano i vigili del fuoco nelle operazioni di ricerca e salvataggio"[97]. In tal modo, le informazioni raccolte da questi dispositivi potranno essere condivise su più sistemi per poi essere elaborate.

[94] Fonte Url: "http://www.wallstreetitalia.com/stellar-lastro-nascente-delle-criptovalute/".
[95] Fonte Url: "https://iota.org/".
[96] Si stima che l'IoT raggiungerà 30 miliardi di oggetti solo nei prossimi anni, pari ad un valore di circa $ 7,1 trilioni.
[97] Fonte Url: "https://it.finance.yahoo.com/notizie/iota-cos-%C3%A8-e-come-082026529.html".

Lo sviluppo di Iota inizia nel 2015, dai fondatori David Sønstebø, Sergey Ivancheglo, Dominik Schiener e Serguei Popov. La sede del team di sviluppo è a Berlino, dove successivamente è stata fondata la *IOTA Foundation*. Questo team è composto dal matematico Popov, che ha ideato il core della criptovaluta chiamato *Tangle*. Come verrà analizzato dettagliatamente nel prossimo capitolo, questa moneta non basa sulla classica Blockchain, ma utilizza una sistema diverso che trae spunto da su una teoria matematica denonimata 'Directed Acyclic Graphs' (DAG). Il vantaggio di questa tecnologia si trova nel processo di verifica: ad ogni nuovo nodo del network è richiesta l'approvazione delle due precedenti transazioni; di conseguenza, qui non sono coinvolti i minatori nel processo di verifica, mentre la crescita e la velocità del network dipendono dal numero di utenti che ne usufruiscono. Questo di fatto sopperisce ai limiti del Bitcoin e dei suoi colli di bottiglia legati alla velocità delle transazioni. Grazie a questa piattaforma, non si applica nessun costo di transazione per l'utilizzo e non soffre delle limitazioni di Bitcoin, illustrate precedentemente.

Come per le altre criptomonete, la fondazione IOTA ha stretto delle partnership con altre 20 società, con l'intendo di sviluppare un mercato decentralizzato, tra cui: Cisco System, Fujitsu, Microsoft e Volkswagen. Proprio per questo motivo alla fine di febbraio questa criptomoneta aveva raggiunto il quarto posto della classifica (superando Ripple e Litecoin), con una capitalizzazione di mercato pari a $ 11.915 miliardi. Ad ora questa impennata sembrerebbe azzerata, e al momento dell'analisi si trova al dodicesimo con una capitalizzazione pari a 3,575$ miliardi[98], con un prezzo di 1,29$ (precedentemente era di 4,87$).

Concludendo, quello che può fare questa tecnologia è sensazionale, ricordando che sostanzialmente l'obiettivo di IOTA è quello di rendere più semplice lo scambio di informazioni tra device con limitate capacità computazionali tipiche del panorama IoT. Pertanto, ad esempio i proprietari di IOTA possono sfruttare la tecnologia *QR*[99], per effettuare acquisti di beni di consumo e farli recapitare a domicilio. Questo è reso possibile grazie all'eliminazione di commissioni e ritardi nell'elaborazioni che invece si verificherebbero utilizzando bitcoin.

[98] Fonte Url: "https://coinmarketcap.com/currencies/iota/#charts", 09 marzo 2018, ore 20:43h.

[99] I codici QR (acronimo di "Quick Response") sono quei simboli "quadrati" che trovi sui siti Internet e sui giornali che, se inquadrati con la fotocamera del cellulare, permettono di accedere a siti Internet, informazioni e video online istantaneamente. Si tratta di codici a barre "con gli steroidi" le cui potenzialità possono essere pressoché infinite; possono essere utilizzati per aprire pagine Web, visualizzare bigliettini da visita digitali e molto altro ancora.

Di seguito verranno prese in analisi altre cinque criptovalute che si trovano nella Top Ten per capitalizzazione ed importanza. A differenza delle precedenti verranno solo brevemente descritte.

Bitcoin Cash (BCH)

Il Bitcoin Cash è una criptovaluta nata dalla scissione del Bitcoin, avvenuta il 1° agosto 2017. Questa valuta digitale è un *hard fork*[100]. Questo è avvenuto perché ci sono state delle diversità di pensiero tra i vari componenti dei team degli sviluppatori. A chi possedeva dei bitcoin nel proprio wallet prima della scissione, gli sviluppatori hanno donato lo stesso numero di bitcoin cash. Questa scissione è stata voluta dalla comunità allo scopo di aumentare la velocità della convalida delle transazioni che risultava troppo lenta per il bitcoin tradizionale.
Il Bitcoin Cash ha una capitalizzazione pari a $ 14.69 miliardi e ad un prezzo di $ 876.74[101]: questi numeri gli permettono di aggiudicarsi la quarta posizione in classifica, subito dietro a Ripple.

Litecoin (LTC)

Litecoin è stato lanciato il 7 ottobre 2011, da Charles Lee, un ex-dipendente di Google. Questa moneta digitale utilizza un protocollo open source, ed è nata per superare i limiti del Bitcoin come ad esempio la velocità di convalida dei blocchi (soli 2.5 minuti, 7.5 in meno rispetto a Bitcoin) e il numero massimo di monete generabili (fino a 84 milioni di monete, quattro volte in più rispetto al Bitcoin). Più volte il software è stato migliorato; questa moneta digitale è stata definita come la possibile alternativa al Bitcoin. Tutt'ora ricopre la quinta posizione della classifica, con una capitalizzazione pari a $ 7.83 miliardi, avente un prezzo pari a $ 142.08[102].

[100] Per Fork di un progetto si intende quando gli sviluppatori copiano il codice sorgente e ne sviluppano un altro indipendente, creando così un altro software.
[101] Fonte Url: "https://www.investing.com/", 18 marzo 2018, ore 19:49h.
[102] Fonte Url: "https://www.investing.com/", 18 marzo 2018, ore 20:05h.

Cardano (ADA)

Cardano ha visto la luce il 29 settembre 2017, è stato creato dalla società sviluppatrice della blockchain: Input Output Hong Kong (IOHK) e da Charles Hoskinson, l'ex co-fondatore di BitShares ed Ethereum. Questo è il primo progetto blockchain che ha mescolato la filosofia scientifica e studi accademici. Questo progetto ha lo scopo di risolvere il uno dei problemi di accettazione della criptovaluta tradizionale, ossia conciliare gli interessi del cliente finale con quelli dell'autorità di regolamentazione. Quindi rispetto alla filosofia del Bitcoin, qui si vuole l'accettazione da parte dei regolatori dell'utilizzo di questa moneta digitale, senza sacrificare l'aninomato e il decentramento. Rispetto alle altre, si è concentrata di più sulla sicurezza del sistema, partendo già dal linguaggio di programmazione *Haskell* che dovrebbe garantire una maggiore robustezza. Come per Ethereum, anche Cardano consente lo sviluppo dei contratti intelligenti.
Attualmente ricopre la settima posizione della classifica, con una capitalizzazione pari a: $ 3.50 miliardi, con un prezzo a $ 0.133[103].

Neo (NEO)

Neo è stata lanciata nel febbraio 2014 da DA Hongfei. Inizialmente, il progetto era stato denominato *AntShares*. Questa piattaforma consente lo sviluppo di contratti intelligenti, come Ethereum. Sono state emesse nel sistema 100 milioni di NEO, e questo ammontare rimane fisso. Uno dei vantaggi di questa moneta è la velocità infatti è in grado di gestire fino a 10,000 transazioni al secondo. La piattaforma gestisce contemporaneamente due monete digitali: NEO e GAS.
Al momento Neo ricopre la sesta posizione della classifica con una capitalizzazione pari a $ 3.54 miliardi e un prezzo di 49.428[104].

[103] Fonte url: "https://www.investing.com/crypto/currencies", 18 marzo 2018, ore 20:22.
[104] Fonte url: "https://www.investing.com/crypto/currencies", 18 marzo 2018, ore 20:31.

Eos (EOS)

Eos è nata a giugno 2017 dalla società Block.one (società registrata presso le Isole Cayman), è attualmente sottosviluppo e il protocollo verrà rilasciato sotto licenza *open source* dal 1° giugno 2018. Questa Criptovaluta ha iniziato a raccogliere fondi emettendo ICO da giugno 2017. Simile al sistema di Ethereum, Eos offre la possibilità di creare *smart contracts*, e consente le transazioni tra differenti valute, senza passare per il dollaro statunitense, come Ripple. Si basa su un nuovo tipo di blockchain, più veloce e sicura in quanto riesce ad evitare che ci siano furti all'interno del proprio *wallet*. L'algoritmo utilizzato per il consenso è il *Delegated Proof of Stake* (DPoS) che funziona come il sopracitato PoS, ma risulta migliorato in termini di sicurezza. Questa moneta digitale riesce a funzionare anche in caso di "guasto" del sistema in quanto la community può eleggere un nuovo produttore, qualora uno fallisse. Oltre a EOS, anche BitShares e Steem utilizzano questo algoritmo.
Attualmente EOS ricopre la decima posizione della classifica, con una capitalizzazione pari a $ 2.99 miliardi e con un prezzo di: $ 4.049[105].

[105] Fonte url: "https://www.investing.com/crypto/currencies", 18 marzo 2018, ore 20:47.

Griglia riepilogativa e Swot Analysis

Analisi attraverso descrittori	Criptovalute				
	Bitcoin	***Etherem***	***Ripple***	***Stellar***	***Iota***
Simbolo					
Nascita	03-gen-09	30-lug-15	2012	2014 (dal protocollo di Ripple)	11-giu-16
Creatore/i	Satoshi Nakamoto (pseudonimo)	Vitalik Buterin	Arthur Britto, David Shwartz, Ryan Fugger	Jed McCaleb e Joyce Kim	David Sønstebø, Sergey Ivancheglo, Dominik Schiener e Serguei Popov
Proprietà	Dominio Pubblico	Fondazione no profit	Public Company	Fondazione no profit	Fondazione no profit
Ideologia	Creazione di sistema di pagamento decentrato, carattere anarchico	Evolvere la Blockchain, per consentire i smart contract	Superare i limiti di Bitcoin	Consentire transazioni internazionali senza cambiare valuta	Interazioni con il mondo 'IoT'
Utilizzo	Sistema di pagamento	Smart Contract	Sistema di pagamento/Forex e rimesse	Settlement/Pagamenti crossborder/Forex e rimesse	Comunicazioni e transazioni nell'ambito 'IoT'
Algoritmo & Sistema sottostante	C++/Blochchain/Proof-of-Work/Mining	C++_Python_Go_Java/ Blockchain 2.0/Proof-of-Work/Mining	C++/Blockchain/Proof of Correctness/No Mining	C++/Blockchain/No Mining	C_Python_Java/Tangle /No Mining
Monete in circolazione	16,9 miliardi Btc	98,3 milioni Eth	39,1 miliardi Xrp	18.5 miliardi Xlm	2.8 miliardi Miota
Prezzo	8,851.16 $	552.74 $	0.711133 $	0.261766 $	1.47 $
Capitalizzazione di Mkt	149,849,917,521 $	54,338,651,810 $	27,801,100,946 $	4,855,478,170 $	4,008,577,865 $
Situazione: 1 Mese Crescita/Stallo/Decrescita	Stallo	Decrescita	Stallo/Decrescita	Crescita	Stallo/Crescita

Tabella 1.1 Griglia comparativa, aggiornata al 20 marzo 2018, alle ore 18:45. Fonte: "https://coinmarketcap.com/".

La Tabella 1.1 mette a confronto le principali criptovalute precedentemente analizzate. Si può notare che ciascuna di esse presenti note distintive sia a livello informatico che di utilizzo. Ognuna criptovaluta mantiene un'ideologia che la tiene in contatto con i propri utilizzatori. Come si è già detto in precedenza, non ci è dato sapere in che modo evolveranno nel futuro, ma sicuramente queste faranno ancora parlare di loro. Nei successivi capitoli, si cercherà di analizzarle sotto ogni punto di vista. È importante sottolineare ancora una volta la caratteristica intrinseca di questo mercato, ossia l'altissima dinamicità, per cui è possibile che queste monete possano essere velocemente soppiantate. Sta di fatto che al di là del loro destino incerto, queste criptomonete attualmente rappresentano la punta di diamante di questo mercato in termini di tecnologia e di consenso tra il pubblico.

Tramite l'analisi Swot[106] si è cercato di mettere in evidenzia i principali aspetti riguardanti questo strumento finanziario. Si sono messi in luce i punti di forza e di debolezza, per quanto riguarda l'analisi dei fattori endogeni, mentre si sono analizzate le opportunità e le minacce per l'analisi dei fattori esogeni. Ovviamente questo è un punto di partenza, perché possono venire fuori altri aspetti, che solo con ulteriori studi si può fare, oppure che ci sia un mutamento che viene direttamente dal mondo cryptocurrency.

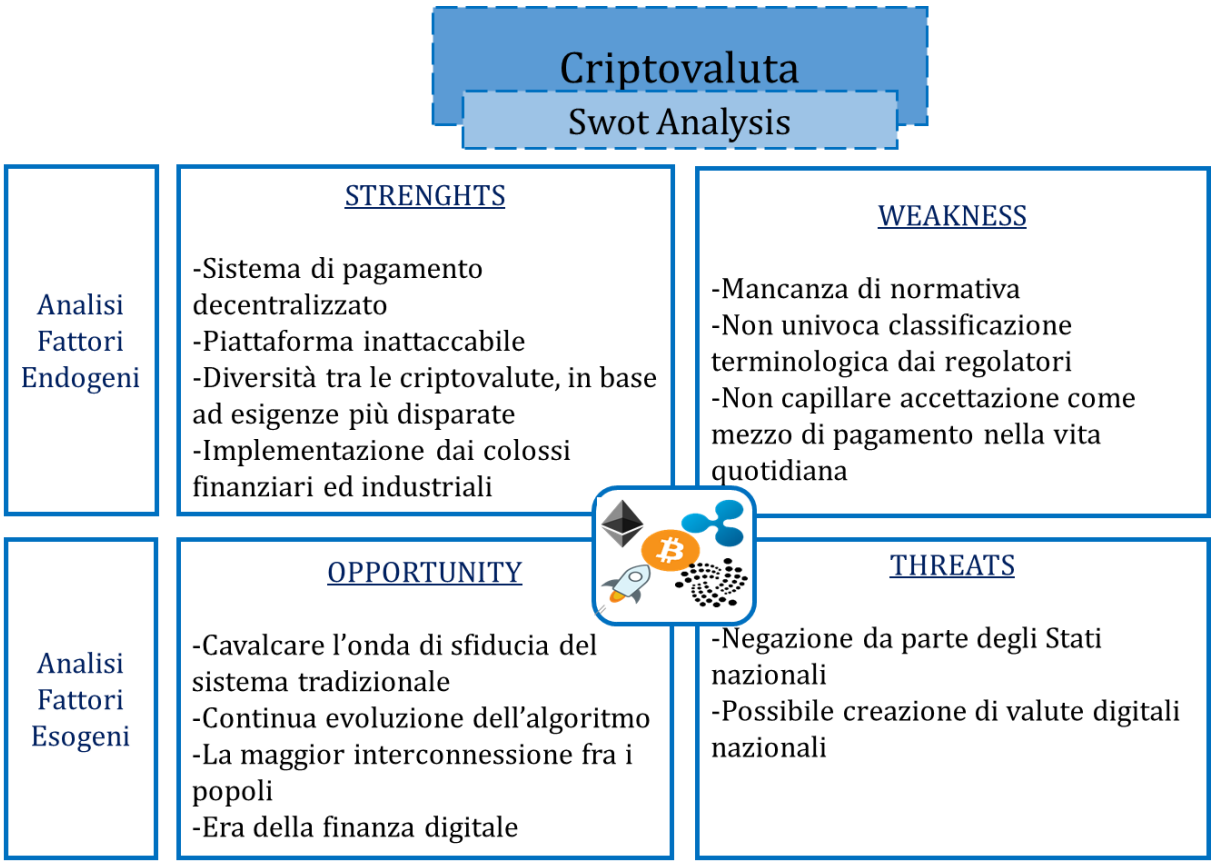


Figura 1.1 Swot Analysis della Criptovaluta

[106] Analisi Swot: "l'analisi SWOT è quella utilizzata per la pianificazione strategica di un progetto o attività e consiste nell'evidenziare i punti di forza, Strenght, di debolezza, Weakness, le opportunità, Opportunity, le minacce, Threat, che si riscontrano per il raggiungimento dell'obiettivo. I punti di forza e di debolezza sono fattori interni all'azienda o attività, mentre le opportunità e le minacce sono fattori esterni. Si tratta di una tecnica di analisi, che ormai è diffusa da oltre mezzo secolo e che consente a un'impresa di capire su quali fattori può fare leva per raggiungere l'obiettivo e quali, invece, rappresentano le debolezze della propria attività", fonte Url: "http://dizionarioeconomico.com/analisi-swot".
"Tale tecnica è attribuita a Albert Humphrey, che ha guidato un progetto di ricerca all'Università di Stanford fra gli anni '60 e '70 utilizzando i dati forniti dalla Fortune 500", fonte Url: "https://it.wikipedia.org/wiki/Analisi_SWOT".

Capitolo II – Il funzionamento sottostante

Inquadramento generale

In questo capitolo si affronteranno i diversi sistemi che sorreggono l'intero sistema delle criptovalute. Come si è potuto vedere nel capitolo precedente, le criptomonete utilizzano diverse tecnologie, che combinate tra di loro, creano il sistema sottostante. Verranno inoltre analizzati in dettaglio i core delle cinque valute digitali descritte nel capitolo precedente. Il capitolo si conclude con una griglia comparativa che riassume le similitudini e le differenze nelle tecnologie utilizzate.

Analisi tecnologica

Questo paragrafo, descrive le diverse tecnologie che sorreggono l'universo delle criptomonete, è diviso in due sotto paragrafi: il primo fornisce una descrizione delle tecniche di crittografia, il secondo fornisce un'analisi della rete peer-to-peer distribuita.

La crittografia

Secondo il dizionario Treccani, La crittografia è la: "Tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario; ciò si può ottenere con due diversi metodi: celando l'esistenza stessa del messaggio o sottoponendo il testo del messaggio a trasformazioni che lo rendano incomprensibile."[107]

Questo termine deriva dalle parole greche: *kryptós* e *graphía*, ossia 'nascosto' e 'scrittura', ed è la scienza che studia le scritture nascoste. Questa tecnica ha origini antichissime, infatti veniva già usata dagli Ebrei con il codice di *atbash*, dagli Spartani con la *scitala* e dai Romani sotto l'imperatore Gaio Giulio Cesare con il cifrario di Cesare. Una maggiore diffusione si può riscontrare a partire dal 1400 d.C. legata all'invio di comunicazioni diplomatiche e militari.

[107] Fonte Url: "http://www.treccani.it/enciclopedia/crittografia/".

Con il susseguirsi dei secoli, questa tecnica si è evoluta con l'invenzione di algoritmi sempre più complessi che però risultavano di difficile applicazione a causa della mancanza di calcolatori. Per questo motivo che questa scienza ha evidenziato un salto evolutivo con l'invenzione delle macchine elettromeccaniche: durante la Seconda guerra mondiale fu sviluppata Enigma, utilizzata dalle forze armate naziste per criptare le comunicazioni militari; per cercare di decodificare tali messaggi venne sviluppata dalle forze alleate la macchina di Turing.

La nascita della criptologia moderna può essere fatta risalire alla pubblicazione dell'articolo *Communication Theory of Secrecy Systems* da parte del matematico ed ingegnere statunitense di Claude Shannon nel 1949 che viene considerato il padre fondatore di questa scienza: in questo articolo si dimostra matematicamente che utilizzando una chiave di criptatura di una lunghezza pari a quella del testo da nascondere, si ha ottiene un livello di sicurezza comprovata; tale tecnica prende il nome di Cifrario di Vernam ed è una tecnica assai laboriosa non è facile da applicare, senza scordare la difficoltà di dove trasmettere la chiave. Questo metodo venne utilizzato durante la guerra fredda.

Nell'era digitale tutte le complessa operazioni vengono svolte dai calcolatori, quindi si possono utilizzare tecniche ce in passato non potevano essere immaginate. Attualmente i sistemi crittografici hanno un ruolo fondamentale per la messa in sicurezza e protezione delle informazioni. Secondo i criteri internazionali dell'ISO (*Internatioanl Organization for Standardization*), ci sono delle caratteristiche che devono essere rispettate e garantite per far sì che un documento sia definito affidabile:

- Confidenzialità: le informazioni scambiate tra mittente e destinatario, non vadano nelle mani di una terza entità non autorizzata; questa è ottenuta tramite tecniche crittografiche.
- Integrità dei dati: le informazioni scambiate vengano alterare durante il passaggio.
- Autenticazione: si garantisce l'accertamento dell'identità attraverso i servizi di autenticazione, quali ad esempio: mediante l'utilizzo di password.
- Controllo degli accessi: dopo che è avvenuto l'autenticazione, c'è la possibilità di controllare gli accessi per verificare che si utilizzino solo i servizi autorizzati.
- Non Ripudiabilità: questo viene utilizzato per garantire che le entità in questione, non possano rifiutare la partecipazione.

L'efficacia dell'algoritmo, definita come probabilità di risalire al testo originale partendo dal testo cifrato, deve essere basata solo sulla segretezza della chiave e non sulla segretezza dell'algoritmo in sé, in quanto non può essere dimostrato matematicamente che sia sicuro.

Gli algoritmi crittografici possono essere suddivisi in tre categorie:

- crittografia Simmetrica (o crittografia a chiave privata);
- crittografia Asimmetrica (o crittografia a chiave pubblica), quella che viene usata dal Bitcoin e dalle altre criptovalute;
- crittografia Ibrida (una combinazione delle precedenti).

Crittografia Simmetrica

La crittografia Simmetrica (o crittografia a chiave privata), veniva utilizzata fino a pochi anni fa, mentre nei moderni sistemi informatici non viene più utilizzata.

Figura 2.1 Schema Crittografia a Chiave Privata - Fonte Url: "https://lamiaprivacy.wordpress.com/2015/03/07/capire_le_basi_della_crittografia/".

Come viene mostrato nella figura soprastante, il mittente cifra con la stessa chiave segreta che il destinatario utilizza per decifrare. Qui sorge il grande problema di come scambiarsi la stessa chiave segreta, senza compromettere tutta la segretezza. Per evitare che terzi possano leggere il contenuto del testo criptato, è opportuno scegliere accuratamente un canale sicuro per inviare la chiave all'altra controparte; L'osservazione che sorge è che questo canale può essere utilizzato per l'invio del testo in chiaro.

Crittografia Asimmetrica

Nella crittografia Asimmetrica (o crittografia a chiave pubblica), si utilizzano cifrari che usano due chiavi diverse, univocamente correlate. Una viene utilizzata per cifrare il testo in chiaro e l'altra per decifrare il testo cifrato con la prima. Da notare che è irrilevante quale delle due venga usata per la prima operazione.
Da tenere a mente:

- Non si può decifrare il documento con la stessa chiave utilizzata per cifrarlo,
- La coppia di chiavi viene generata con la stessa procedura,
- Pur essendo a conoscenza di una, non vi è modo di risalire all'altra.

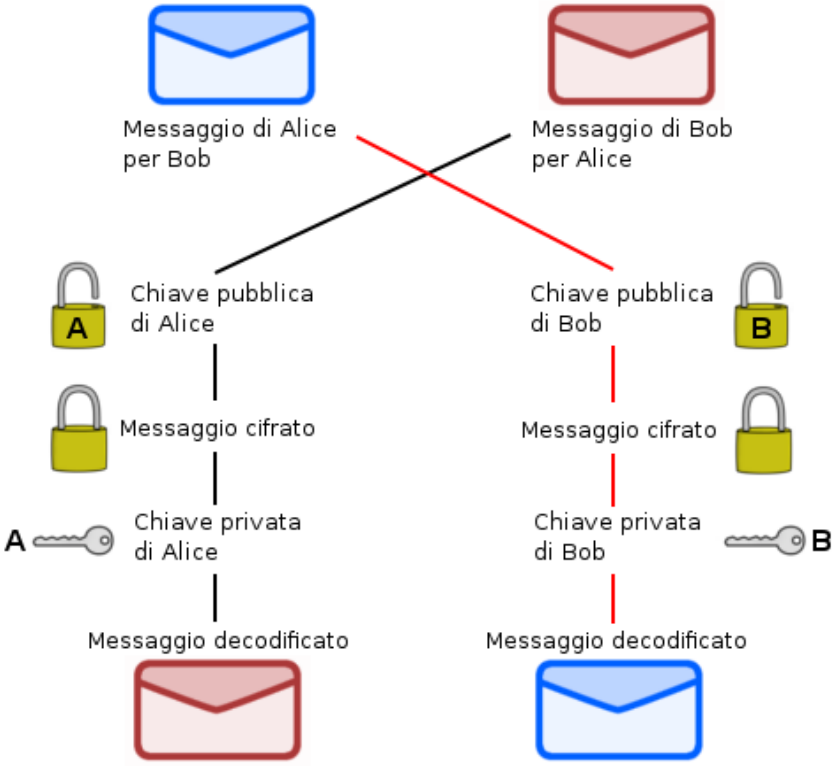


Figura 2.2 Schema Crittografia a Chiave Pubblica - Fonte Url: "https://lamiaprivacy.wordpress.com/2015/03/07/capire_le_basi_della_crittografia/".

Questo algoritmo è stato presentato in un documento nel 1976 redatto dai ricercatori Whitfield Diffie e Martin Hellman. Negli ultimi 40 anni è stato adottato per diverse applicazioni nel settore delle comunicazioni sicure, quali ad esempio: il commercio elettronico e l'home banking.
Come si evince dalla figura 2.2, chiunque può inviare un documento segreto a chi renda pubblica una delle due chiavi. Dunque, si può rendere e disponibile una della coppia di

chiavi (la chiave pubblica) a chiunque, mentre si deve tenere segretamente l'altra (la chiave privata). In questo modo, l'emittente cifra il documento con la chiave pubblica del destinatario e solo il destinatario può decifrarlo, perché nelle sue mani possiede la chiave privata correlata alla chiave pubblica utilizzata nella prima fase dal mittente.

Per comprendere meglio questo procedimento si può citare l'esempio:

"In questa situazione Bob (il destinatario) crea due chiavi. La prima (privata) è segreta e la tiene per sé, gli serve per decifrare i messaggi cifrati con seconda chiave, che è pubblica e viene utilizzata, appunto, per cifrare le informazioni. Bob rende nota la chiave pubblica a tutti coloro che vogliono inviargli un messaggio e non ha paura che questa chiave possa venire scoperta dal *nemico*"[108].

Per questo motivo, riprendendo gli attori dell'esempio precedente, si può pensare alla chiave pubblica come l'indirizzo di residenza dove abita Bob, il quale può renderla di pubblico dominio, ma che effettivamente nessuno può violare la sua dimora. Invece, si può ricondurre la chiave privata alla serratura della propria porta. Quindi, Bob comunica il proprio indirizzo (chiave pubblica) ad Alice per farsi consegnare un pacchetto. Lei può recarsi direttamente al suo indirizzo, ma effettivamente non può addentrarvi, perché non ha la chiave per aprire la porta (chiave privata).

In definitiva, anche se la crittografia asimmetrica risolve il problema della riservatezza, perché effettivamente il messaggio viene criptato con la chiave pubblica, e solamente il possessore della chiave privata può decriptarlo, non è di certo immune da limiti. Infatti, questa procedura ha dei grossi limiti, come per esempio la mole di lavoro cui è sottoposto calcolatore elettronico per elaborare criptare il testo ed eventualmente creare le chiavi, rendendo pesante ed articolato l'intero lavoro. Una tecnica utilizzata per ovviare a questo problema utilizzare la crittografia asimmetrica solo per trasmettere in modo sicuro la chiave crittografica per poi continuare la comunicazione utilizzando la crittografia simmetrica.

Si dovette aspettare circa un anno per la prima realizzazione empirica del sistema di crittografia asimmetrica. Nell'agosto del 1977, Martin Gardner presentò un algoritmo degli informatici Rivest, Shamir e Adelman (i quali gli diedero il loro nome: RSA). Con questo algoritmo la sicurezza diventò estrema, perché utilizzava una chiave di almeno 1020 bit contro i 128 degli algoritmi a chiave simmetrica. Ovviamente, questo lo rende estremamente complesso e pesante dal punto di vista computazionale. Questo algoritmo

[108] Fonte Url: "https://medium.com/@AndreaFerraresso/la-crittografia-dietro-a-bitcoin-72cc6ad3fa41".

è basato su alcune proprietà dei numeri primi. Senza addentrarci troppo nel dettaglio, occorre aggiungere solo che questo algoritmo alla fine degli anni '80 veniva usato solamente dai Governi e dalle grosse multinazionali che disponevano di calcolatori molto potenti.
Ci fu una più ampia diffusione solo con l'arrivo del sistema freeware PGP (Pretty Good Privacy) di Phil Zimmermann, un algoritmo ibrido che utilizzava sia chiave asimmetrica che simmetrica.
La crittografia asimmetrica può anche essere utilizzata per autenticare la provenienza del messaggio, attraverso il processo inverso delle chiavi. Pertanto, il mittente decifrerà con la propria chiave privata e successivamente, il destinatario decifrerà il messaggio con la chiave pubblica del mittente, in questo modo sarà garantita l'autenticità del messaggio.
Su questo principio che si basa la firma digitale, ma prima di descrivere tale metodo, è opportuno riprendere alcuni concetti, che ruotano attorno a questo meccanismo.

Funzione crittografica di Hash

La funzione crittografica di Hash permette di aggirare i limiti evidenziati precedentemente mantenendo un elevato livello di sicurezza e una maggiore velocità. Tale sistema permette di trasformare un input di informazioni a lunghezza arbitraria, per ottenere un output formato da codici alfanumerici di lunghezza costante (che può variare a seconda dall'algoritmo utilizzato: da 160bit a 512 bit). Questo codice o hash ottenuto viene gergalmente detto impronta (digest o fingerprint). Il vantaggio di questa tecnica è la possibilità di utilizzare questa impronta come un attributo compatto ed univoco del documento stesso, cosicché si firma l'impronta piuttosto che l'intero documento. Per far ciò che questo avvenga, la funzione deve rispettare due proprietà fondamentali: l'incollisionalità e l'unidirezionalità.
Senza elencare dettagliatamente tutte le differenze degli algoritmi creati, è da evidenziare che le funzioni Hash più note sono MD5 e SHA: la prima è lo standard utilizzato sul web la seconda viene usata come standard governativo ed è più sicura e lenta.

Le funzioni Hash - SHA architettate sono: SHA-0/SHA-1/SHA-2/SHA-3. La prima non è più in circolazione, mentre la seconda è stata *bucata* dal team di Google nel febbraio 2017[109] (tema molto attuale perché questo metodo è ampiamente diffuso sul web).
Ricapitolando, le caratteristiche della funzione di Hash sono:

- Irreversibilità: le funzioni di hash sono irreversibili, perché pur conoscendo l'hash (output finale), è quasi impossibile ricavarne le informazioni originali.
- Determinismo: le funzioni di hash sono deterministiche proprio perché è quasi impossibile che input diversi diano lo stesso output, anzi si ricaverà lo stesso output partendo dal medesimo input.
- Lunghezza Fissa: l'output prodotto dalle funzioni di hash ha una lunghezza fissa. In particolare, per il MD5 a 128 bit (16 byte) avrà sempre un hash in output di 32 cifre esadecimali; per il Hash SHA-1 a 160 bit avrà sempre un hash in output di 32 cifre esadecimali.
- Effetto valanga: *the avalanche effect*, è una proprietà fondamentale, per cui anche una piccola modifica nell'input, produce una notevole variazione negli hash. A riguardo, la tabella sottostante riassume questa particolarità.

Hello
f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Hallo
59d9a6df06b9f610f7db8e036896ed03662d168f

Tabella 2.1 Esempi di conversione tramite la funzione crittografica Hash, utilizzando come algoritmo di conversione l'SHA-1 (160 bit).

Nella tabella 2.1 viene fatto un esempio di conversione, utilizzando l'algoritmo SHA-1, che restituisce un hash di 160 bit, ossia 32 cifre esadecimali. Lo scopo di questo esempio è di rendere lampante come *the avalanche effect* possa giocare un ruolo fondamentale.
Concludendo è utile ricordare che più corto è l'output generato da questa funzione crittografica, vale a dire l'hash prodotto, più alta è la probabilità di una collisione. Questo è quello che è stato fatto dal team di ricerca di Google, che ha dimostrato come l'Hash di SHA-1 possa essere rotto, ossia che due input diversi possano avere la stessa identica

[109] Fonte Url: "https://www.hdblog.it/2017/02/24/Google-rompe-per-la-prima-volta-lalgoritmo-di-hashing-SHA-1/".

impronta digitale (lo stesso Hash). Per questo motivo, nel tempo sono stati evoluti questi algoritmi, fino al SHA-3, che genera un hash a 512 bit.

Firma Digitale ed autenticazione dei messaggi

Già Daffie e Hellman si accorsero che non esisteva solo il problema della riservatezza, ma anche dell'autenticazione e l'integrità dei messaggi. I creatori della chiave pubblica si resero conto che si poteva risolvere questo problema attraverso la crittografia asimmetrica. Più precisamente videro la possibilità di effettuare anche il processo inverso oltre al normale processo di criptografico, ossia cifrare con la chiave privata un messaggio, per poi successivamente decifrarlo con la chiave pubblica. Ovviamente questa operazione non offre nessun tipo di sicurezza, perché come si è detto più volte la chiave pubblica è a disposizione a chiunque, però attraverso questo stratagemma si garantisce l'autenticità del messaggio al destinatario, ossia che il messaggio proviene da Bob e che nessuno lo ha manipolato.

Pertanto, i due matematici-informatici idearono di aggiungere questo processo di autenticazione al normale processo di criptazione normale. Dunque, per rendere più chiara la dinamica di questo sistema, è utile citare questo esempio:

Bob (mittente) cifra il messaggio con la chiave pubblica di Alice (destinatario), così garantendo la riservatezza. Bob cifra nuovamente il messaggio, ma con la propria chiave privata, in tal modo questo risulta autenticato/firmato.

A sua volta, inizialmente Alice impiegherà la propria chiave privata per cifrare la prima operazione, in tal modo la sicurezza è stata tutela e protetta. Successivamente, in aggiunta si potrà utilizzare anche la chiave pubblica di Bob, in tal modo si potrà autenticare l'origine del messaggio.

Come si è già detto in precedenza, questo tipo di crittografia può essere molto complessa e richiederebbe una capacità computazionale notevole, considerando che si deve ripetere il processo: prima per firmare e dopo per verificare i documenti, senza dimenticare le dimensioni delle informazioni.

Proprio per tale motivo, che entra in gioco la funzione crittografica di Hash, descritta precedentemente. Di seguito ci sono due figure, in cui vengono rappresentate le due fasi dell'utilizzo della Firma Digitale.

Fase 1:

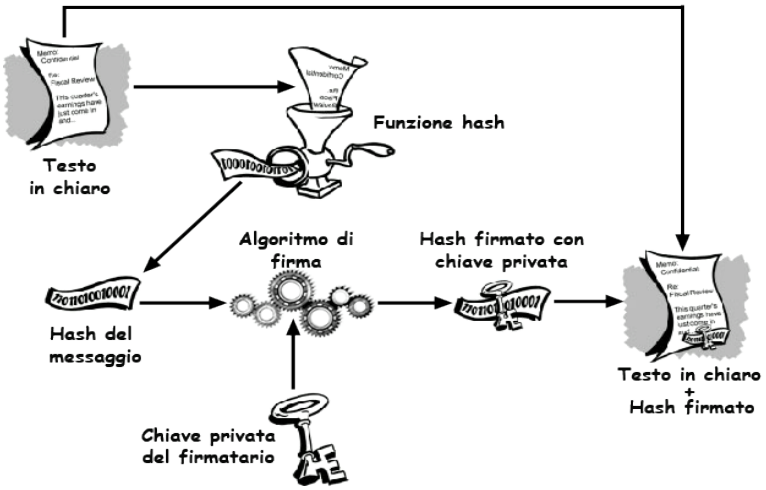


Figura 1.3 Prima fase: Apposizione sul documento della Firma Digitale dell'Emittente. Fonte Url: "http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0304/GnuPG/Gnupg.htm".

Inizialmente il mittente utilizza un algoritmo crittografico di Hash per ottenere un'impronta digitale che viene cifrata con la chiave privata, ed allegata al documento costituendone la firma. Poi invia al destinatario sia il documento che la propria chiave pubblica. Inoltre, in questa fase il mittente può scegliere se criptare ulteriormente il documento con un algoritmo, per renderlo sicuro.

Fase 2:

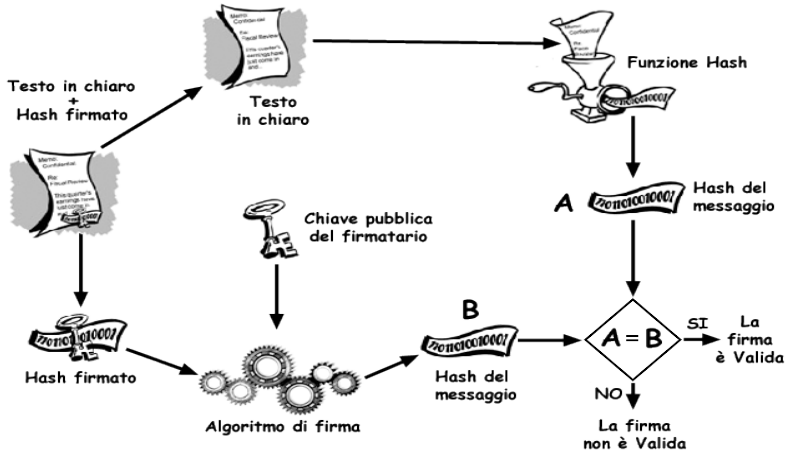


Figura 2.4 Seconda Fase: Controllo della Firma del Destinatario. Fonte Url: "http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-

Successivamente, il destinatario decifrerà il digest con la chiave pubblica del mittente ricevuta insieme al documento, quindi potrà affermare che il documento non sia stato contraffatto. Questa verifica garantisce che sono rispettate le seguenti caratteristiche:

- Autenticità: il destinatario può rimanere sicuro, perché l'identità del mittente è stata confermata e che non vi sia stato nessun impostore;

- Integrità: la certezza che il documento non sia stato in alcun modo modificato e alterato da nessuno.
- Non ripudiabilità: il mittente una volta inviato il documento non potrà negare di averlo fatto.

In conclusione, è utile ricordare che in realtà risulterà più importante non tanto la segretezza in sé del documento, ma l'autenticità perché attraverso questo meccanismo, si è certi dell'identità del mittente e se c'è stata una violazione e modifica. Pertanto, il processo di crittazione dell'intero messaggio per ragioni di sicurezza passerebbe in secondo piano. Inutile ricordare che utilizzando questo metodo, ossia criptando solamente il fingerprint e non l'intero documento, l'operazione risulta semplice e veloce.

La rete peer-to-peer e il calcolo distribuito

La *rete peer-to-peer* (letteralmente: pari-pari o paritario) è una particolare piattaforma di network, nella quale ogni singolo nodo (computer) dialoga direttamente con gli altri, senza che ci sia un nodo centrale (server) adibito al controllo della comunicazione.
Quando gli utenti utilizzano un network peer-to-peer all''interno di esso nessuno è più importante degli altri: tutti hanno lo stesso valore.
Questa nozione è contrapposta al concetto tradizionale di server-client, nella quale si trova un ente di controllo (server), che comunica direttamente con il client. Nella figura sottostante si può vedere intuitivamente, la differenza tra i due diversi network.
Un network che utilizza questa architettura viene definita decentralizzata perché i nodi non sono gerarchizzati sotto un server. Grazie a questo tipo di struttura, vengono superati tutti gli svantaggi dell'architettura *server-client*, quali ad esempio: gli altissimi costi di gestione che sono concentrati nel server, la scalabilità del sistema (all'aumentare del numero dei partecipanti, le prestazioni si degradano), la disponibilità e qualità del servizio (solo il server garantisce il servizio e in caso di blocco, il sistema fallisce). Infatti, nel modello peer-to-peer ogni nodo (peer) partecipata attivamente e contemporaneamente può essere sia client che server.
In particolare, ha trovato maggior applicazione nel campo del *file-sharing*, dove ogni nodo condivide i propri files con tutti gli altri partecipanti. Inoltre, come già prima si è accennato, il sistema può fornire un servizio a calcolo distribuito, dove la capacità del sistema è costituita da un'aggregazione delle risorse computazionali dei singoli nodi.

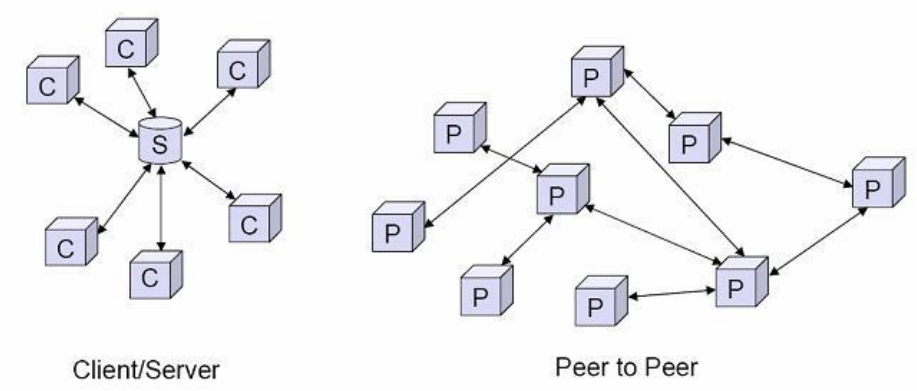


Figura 2.5 A sinistra c'è raffigurato un esempio dell'architettura Client/Server, mentre a destra quella Peer-to-Peer. Fonte Url: "http://www.ragazzieweb.it/?q=node/41".

Le applicazioni che si possono fare con questa architettura sono:

- File Sharing (empiricamente quella più conosciuta ed utilizzata, quali ad esempio: Napster, Gnutella);
- Communication and collaboration;
- Platforms;
- Distributed computing.

Il *Distributed Computing* merita un'analisi più accurata in quanto trova applicazione nel mondo delle criptovalute. Rispetto al File Sharing, dove vengono condivisi i files con gli altri nodi della rete, qui viene condiviso la risorsa computazionale del proprio elaboratore, ossia i cicli di *CPU* (Central Processing Unit) o della GPU (Graphic Processing Unit).

Il sistema che regge l'apparato di molte monete digitali è la Blockchain che ha un'architettura *peer-to-peer distribuito di ledger*. Con il termine *distribuito* si allude alla disposizione spaziale dei singoli calcolatori, che possono trovarsi fisicamente lontani fra loro ed inoltre, possono lavorare in completa autonomia l'uno dall'altro. *Ledger* letteralmente significa libro mastro, cioè un archivio digitale nel quale vengono trascritte tutte le transazioni avvenute fin a quel momento.

Bitcoin e altre criptomonete utilizzano la rete peer-to-peer per il calcolo distribuito per la risoluzione di problemi matematici complessi: i nodi presenti all'interno della rete offrono la propria potenza computazionale. Questa potenza informatica è adibita al sopperimento del ruolo di un server centrale, il quale viene utilizzato tradizionalmente

per tenere traccia su un unico registro centrale delle varie transazioni, al fine di evitare che possa verificarsi il problema del *Double-Spending*[110].
Attraverso questa architettura di rete, ovvero la Blockchain, i registri vengono spartiti all'interno dei partecipanti della rete che utilizzano algoritmi crittografici per garantire la sicurezza dei dati (che non vengano persi o alterati), ed infine nessuno possa accedere alle informazioni senza avere un'autorizzazione.

Analisi tecnica delle diverse Criptovalute

In questo paragrafo verranno elencate ed analizzatele le diverse tecniche che permettono il funzionamento delle criptovalute studiate nel precedente capitolo. Inizialmente, nel primo sotto paragrafo verrà redatto un elenco dal carattere puramente tecnico nel quale ogni singola tecnica verrà studiata separatamente dalle altre. Successivamente, verrà costruita una griglia riepilogativa e comparativa, composta dall'unione di questi metodi utilizzati per il corretto funzionamento di esse.

Chiavi ed indirizzi

Per consentire le transazioni tra un soggetto e l'altro, vengono usate dei particolari strumenti crittografici per evitare che un malintenzionato possa entrare nel sistema e possa appropriarsi di denaro altrui. Come si è detto più volte, non c'è un organismo centrale che possa garantire questo, ma è proprio la rete *peer-to-peer* e la crittografia che possono superare questi limiti.
Dalla creazione di un wallet, si costruisce un'identità digitale sulla blockchain, che si potrebbe paragonare ad un iban bancario, perché entrambi sono anonimi. Ogni identità creata è unica ed è identificata con un proprio codice alfanumerico.
L'apparato delle criptovalute si basa sulla crittografia asimmetrica: ad ogni identità creata nella blockchain viene associata una chiave privata e una chiave pubblica.
Dalla chiave privata si deriva un'unica chiave pubblica: la prima viene utilizzata per confermare le transazioni verso altri indirizzi (transazioni in uscita, output), mentre la seconda è usata per ricevere le criptovalute nel proprio wallet (transazioni in entrata, input). Da evidenziare l'uso differente delle due, dove quella pubblica può essere diffusa

[110] Questo concetto verrà tratta nei prossimi paragrafi di questo capitolo.

tra il pubblico, mentre quella privata deve rimanere segreta e al sicuro da chiunque. Questo perché è proprio attraverso la chiave privata che viene certificata la transazione a favore del destinatario. Questo sistema finora è resistito a qualsiasi attacco i furti vengono commessi quando viene rubata la chiave privata dai cyber-criminali.

Quindi in una transazione tra due soggetti la chiave privata corrisponde al proprietario delle monete digitali che vengono scambiate, mentre la chiave pubblica è riferita all'indirizzo del ricevente.

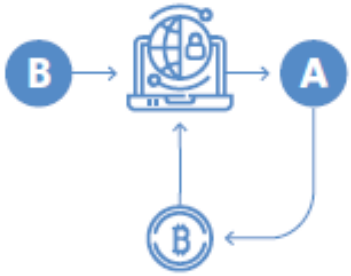


Figura 2.6 La procedura, mentre vengono trasferiti le valute digitali dal soggetto A al soggetto B. Fonte: "Bitcoin Generation" Nòva, Sole 24h.

Come si può vedere dalla figura 2.6, l'utente B crea un indirizzo (che non è altro che la sua chiave pubblica modificata) per l'utente A che vuole trasferire le monete digitali. L'utente A esegue il trasferimento utilizzando il proprio wallet, impiegando per la certificazione, la propria chiave privata. In questo modo, chiunque sulla blockchain può verificarne l'autenticità, attraverso la chiave pubblica dell'utente A.

La *chiave privata* è un codice casuale di 256 bit che serve per firmare digitalmente le transazioni effettuate quindi se un malintenzionato riuscisse ad impossessarsene potrebbe liberamente usufruire delle monete digitali ad essa associate.

Dalla chiave privata, si deriva la *chiave pubblica*. Quest'ultima è formata da un codice di 512 bit, creato dall'algoritmo ECDSA[111] a 512 bit. Come si è detto precedentemente, la chiave pubblica è in mano al ricevente della transazione, con lo scopo di autenticare la firma digitale del mittente. Da evidenziare che la chiave pubblica viene rivelata solamente quando la transazione viene firmata.

[111] ECDSA: "In crittografia, l'Elliptic Curve Digital Signature Algorithm (ECDSA) offre una variante del Digital Signature Algorithm (DSA) usando la crittografia ellittica. Fu proposto la prima volta nel 1992 da Scott Vanstone. Nel 1998 è diventato uno standard ISO (ISO 14888), nel 1999 è stato accettato come standard ANSI (ANSI X9.62) mentre nel 2000 è diventato uno standard IEEE (IEEE P1363 2)". Fonte Url: "https://it.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm".

Il sistema di chiavi dipende dal tipo di wallet che si adopera, nel caso del metodo paper-wallet, si esegue un doppio hash:

- Inizialmente, si calcola un Hash SHA-256(chiave pubblica)
- Successivamente, si esegue Hash RIPEMD-160(SHA-256(Chiave Pubblica));

Infine, il tutto viene codificato in formato ASCII, tramite l'algoritmo Base58Check.

Ottenuto questo indirizzo, risulta impossibile determinare la chiave pubblica o privata partendo da esso. Quindi gli indirizzi che si possono trovare sulla blockchain, non sono altro che gli Hash delle chiavi pubbliche degli utenti. Viene fatto questo meccanismo, al fine di rendere il codice alfanumerici più corto e garantendo maggiore sicurezza contro a malintenzionati.

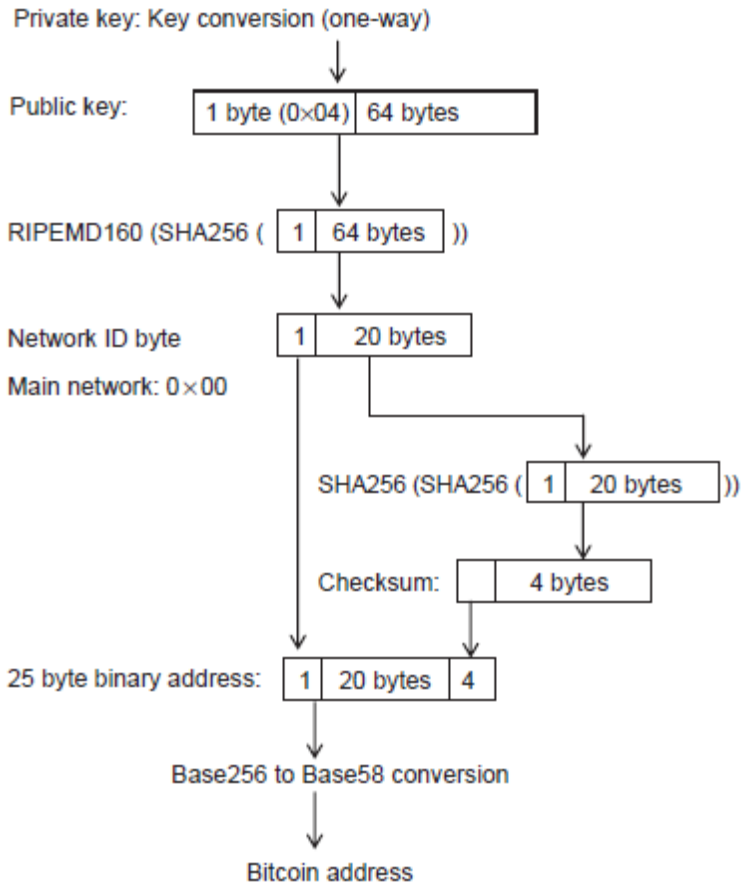


Figura 2.7 Processo di generazione del Bitcoin Indirizzo, Fonte: "Handbook of Digital Currency", David Lee Kuo Chuen, 2015.

La vera rivoluzione: la *Blockchain*

La Blockchain rappresenta la più grande rivoluzione dopo l'avvento del "w.w.w." avvenuta nel 2001. Molte figure internazionali si sono espresse in favore a questa tecnologia che sta ribaltando letteralmente il mondo della finanza e non solo. A differenza del Bitcoin, il quale è stato concepito per ribaltare la finanza tradizionale, invece qui la tecnologia sottostante, che regge il sistema del Bitcoin e della maggior parte dell'universo delle monete digitali, ha un enorme potenziale proprio per quel mondo che il suo token vuole eliminare. Questa tecnologia può essere definita sinteticamente con cinque parole: *sistema peer-to-peer distribuito di ledger*. Dove per ledger si intende un libro mastro cioè una sorta di registro contabile.

Affinché questo registro informatico possa funzionare è indispensabile che ci sia un network appropriato distribuito tra gli utenti che garantisca segretezza, grazie alla crittografia e che permetta transazioni sicure ed affidabili. In particolar modo, la Blockchain riesce a coniugare perfettamente: il network peer-to-peer con l'infrastruttura delle chiavi pubbliche e l'uso della crittografia di Hash.

A riguardo si può citare la definizione che viene data dalla JP Morgan:

"Blockchain (often referred to as distributed ledger technology) is a secure transaction ledger database shared by all parties in a distributed network, which records and stores every transaction that occurs in the network, creating an irrevocable and auditable transaction history. Blockchain can be considered a superior database where the data and access to the data are encrypted. The distributed nature of the Blockchain means it has a built-in redundancy and can survive the loss of one node because the master record is shared or mutualized"[112].

[112] Fonte: "J.P. Morgan Perspectives – Decrypting Cryptocurrencies", J.P. Morgan, 9 febbraio 2018.

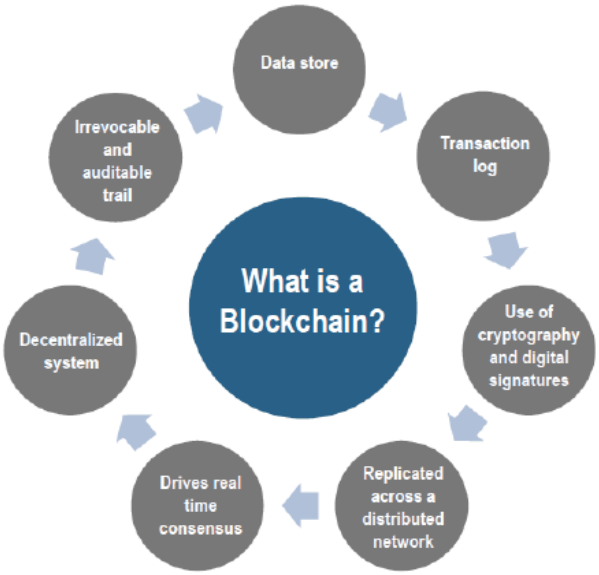


Figura 2.8 Componenti chiave della Blockchain, Fonte: J.P. Morgan

È ampiamente diffuso definire la Blockchain (o Registro distribuito) come un database superiore, in base a queste quattro importanti caratteristiche:

- I dati registrati sono criptati;
- L'accesso ai dati anch'esso è criptato;
- La natura distribuita del sistema, permette di sopravvivere alla perdita di un nodo, per via della ridondanza e dalla condivisione del registro;
- Le transazioni sono tracciate, una volta registrate è impossibile alterarle e modificarle.

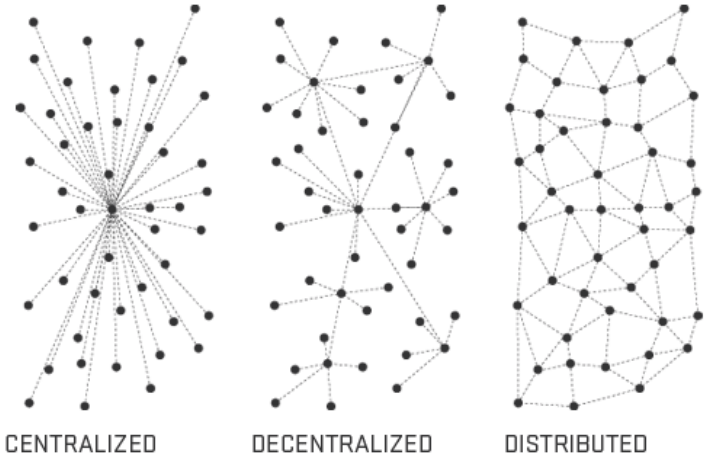


Figura 2.9 Schema differenti tipi di Network, Fonte: "On Distributed Communications Networks", Paul Baran, 1964.

Nel sistema Centralizzato, il controllo è sottoposto ad una singola entità, e quindi la possibilità di fallire viene da un unico punto. Mentre nel sistema Decentralizzato c'è

l'eliminazione di una figura di un'autorità centrale nel processo di autorizzazione delle transazioni. Inoltre, nel sistema di registri Distribuiti (*Distributed Ledgers*) è un tipo di database, dove tutti i nodi all'interno del sistema possono e riescono a collaborare per ottenere il consenso sulla disposizione dei dati condivisi.

Dalla figura 2.9 si può notare la differenza tra i diversi tipi di network. Com'è stato già evidenziato nel paragrafo precedente, le criptovalute utilizzano il registro digitale distribuito (Distributed ledgers). Quando vi è il consenso e la validazione della transazione, questa viene inserita all'interno del sistema, attraverso la creazione di un blocco da parte dei nodi (computer degli utenti). Questo procedimento può avvenire grazie alla struttura della Blockchain, ovvero grazie alla rete peer-to-peer a calcolo distribuito, dove le informazioni vengono copiate e trasmesse attraverso tutti nodi presenti sulla rete. Rispetto al singolo server o database centralizzato, qui il sistema a calcolo distribuito riesce a fare a meno dell'ente centrale per la sicurezza e la certificazione delle transazioni. Di seguito ci sono due figure, dove vengono illustrate da una parte il sistema centralizzato (tradizionale) e dall'altra il sistema distribuito.

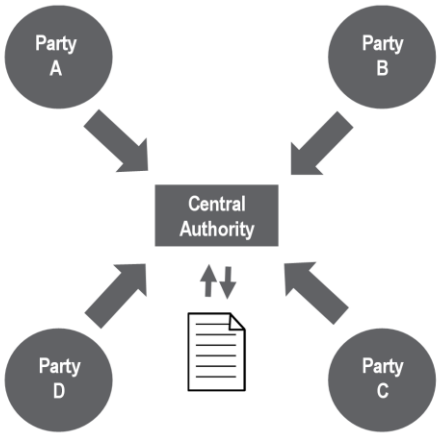


Figura 2.10 Registro centralizzato, fonte: J.P. Morgan.

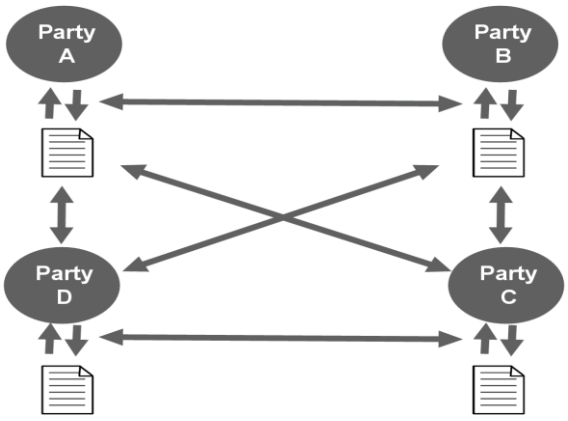


Figura 2.11 Registro distribuito, fonte: J.P. Morgan.

Come si evince nella figura 210, nel sistema centralizzato, avendo un singolo database, la possibilità di fallire è molto alta. In aggiunta, verranno sostenuti anche costi maggiori per la gestione e della sicurezza dei dati, senza contare che è più esposto al cyber crimine. Invece, dalla figura 2.11 si può osservare come un registro distribuito è intrinsecamente più sicuro, in quanto ridondato, quindi l'unico modo per attaccare questo sistema consiste in un attacco simultaneo su tutte le copie presenti sui singoli nodi. Inoltre, come verrà illustrato in seguito, una qualsiasi manomissione o alterazione al database verrà rilevata dai partecipanti.

Tuttavia, è bene ricordare che anche la Blockchain non è completamente immune al cyber-crimine, perché potrebbe esserci una collusione tra gli utenti che potrebbero modificare tutte le copie presenti sui propri registri all'unisono (remota possibilità).
Proprio per questo, che le autorità centralizzate stanno guardando con interesse, la praticità e l'utilizzo di questa tecnologia, come prossima implementazione nei propri sistemi. Per questa ragione, si potrebbe assistere ad un periodo di transizione fra l'infrastruttura esistente e le piattaforme a database distribuiti, ed in tal senso che si deve interpretare gli approcci collaborativi che stanno emergendo nei settori dei servizi finanziari.
Esistono quattro tipi diversi di Blockchain:

- Blockchain pubblica: permette il dialogo fra gli utenti con la possibilità di eseguire le transazioni. Inoltre, gli utenti sono liberi di trasferire valore senza che ci sia un permesso da un operatore della Blockchain.
- Blockchain privata: ci sono delle restrizioni fra il dialogo degli utenti, i quali devono essere preventivamente registrati, assieme ai revisori, sulla lista blockchain. Anche per le transazioni devono rispettare le interfacce preposte.
- Blockchain autorizzata: la costruzione del sistema è limitato dall'entità preposta, che è resa nota pubblicamente ed è la stessa che può limitare l'uso ai partecipanti.
- Blockchain non autorizzata: chiunque è autorizzato a collaborare per la creazione del sistema stesso. Agli utenti è permesso il libero arbitrio per l'entrata e l'uscita.

La Blockchain viene anche denominata: *Catena a blocchi*, proprio per l'unione dei singoli blocchi. Ogni blocco contiene un elenco delle transazioni e un *block header*.
Quest'ultimo è formato da:

- Una struttura contenente i dati delle transazioni nel singolo blocco;
- Una marca temporale relativa all'algoritmo del proof-of-work, per il processo di validazione della transazione;
- Il riferimento al blocco precedente (o parent block) attraverso lo hash.

Quello che ne risulta è una catena a blocchi, che formano la stessa Blockchain, in cui ogni blocco è identificabile attraverso lo hash, del suo relativo header (intestazione). La creazione dei nuovi blocchi avviene tramite la procedura di consenso della transazione attraverso la procedura *Mining*, le nuove transazioni convalidate vengono aggiunte alla catena. Tale sistema riesce ad essere apprezzato ed utilizzato, perché vi è fiducia

nell'utilizzo dei partecipanti (per la sua estrema sicurezza). Per far sì che il sistema funzioni, la Blockchain utilizza la crittografia a chiave pubblica per firmare digitalmente le transazioni.

Inoltre, questa tecnologia crittografica viene usata anche per verificare l'identità, ossia viene creato un timestamp, garantendo così alla transazione presente sulla Blockchain, piena autenticità e che non sia stata alterata o manipolata da nessuno. La caratteristica fondamentale della Blockchain è la distribuzione dei dati, tale per cui viene garantita la piena sicurezza. Infatti, ogni informazione di tutte le nuove transazioni devono essere trasmesse ad ogni nodo presente sulla rete. Questo processo garantisce la sincronia e la coerenza dei dati a livello dell'intero sistema.

La valuta digitale è definita come una catena di firme digitali, dove l'emittente trasferisce denaro al destinatario firmando digitalmente un hash della precedente transazione più la chiave pubblica del prossimo destinatario, queste firme vengono aggiunte alla fine della transazione, in modo tale da provare che è lui il vero proprietario di quella somma di denaro. In definitiva, solo chi è il vero proprietario della chiave privata può creare un'autentica firma digitale, ed essere il vero soggetto autorizzato a spendere quella somma. Infine, il destinatario che riceve la transazione può controllare personalmente l'autenticità delle firme digitali per validare la catena di proprietà. Quindi evitare che il precedente proprietario abbia speso due volte lo stesso ammontare, ossia che abbia fatto il *double-spending*. Per evitare questo, interviene un altro meccanismo: il *timestamp*.

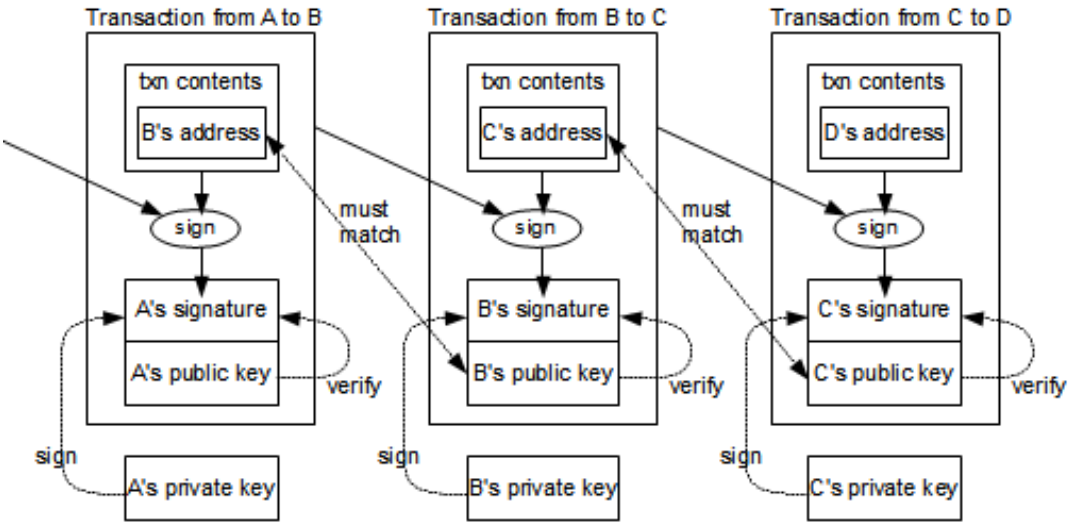


Figura 2.12 Esempio di transazioni tra più utenti, Fonte Url: "http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html".

Nella figura soprastante (2.12), viene illustrata un altro esempio di una transazione tra più utenti della rete. Senza addentrare nel tecnicismo matematico di ogni singola transazione, si può distinguere due componenti fondamentali presenti in ognuna:

- Input: sono le informazioni della precedente transazione, dalla quale proviene quella somma di denaro;
- Output: sono le informazioni del destinatario per il trasferimento del denaro.

Questi componenti giocano un ruolo cruciale per ogni singola transazione, infatti per aggregare o suddividere il valore, le transazioni comprendono molteplici input ed output. In particolare, ogni transazione ha due tipi di vettori dove registrano queste informazioni, nei vettori *vin*, che sono adibiti per le transazioni in ingresso, mentre nei vettori *vout*, per quelle in uscita. In dettaglio, ci possono essere più input che possono raggruppare quantità più piccole, invece al massimo ci potranno essere due output: uno per il pagamento, e l'altro per dare un possibile resto al mittente.

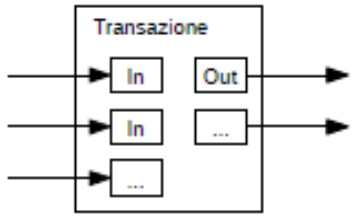


Figura 2.13 Esempio struttura di una transazione.
Fonte "Bitcoin: A peer-to-Peer Electronic Cash System",
Satoshi Nakamoto, 2008.

Quello che emerso è che quando viene creato una valuta digitale (in questo esempio si è trattato di un bitcoin), questa viene trasferita da un proprietario all'altro per effettuare delle transazioni. In questo modo, ogni output di valuta digitale costituirà poi un input per le prossime transazioni. Come si è detto prima, è prevista un preciso output per dare un eventuale resto al mittente, questo per evitare che vadano perse alcuni bitcoin. Quindi se un proprietario deve effettuare un pagamento di più piccola taglia rispetto a quella contenuta negli input, successivamente verrà generato un nuovo indirizzo dove il proprietario dei bitcoin invierà la differenza. Il processo che permette questo procedimento è denominato *change*. Da notare che attraverso questo procedimento,

vengono rinviati parte dell'ammontare al precedente proprietario (all'emittente), quindi questa parte di denaro non è stata effettivamente spesa, ma comunque viene conteggiata nella rilevazione di certe analisi.

Pertanto, conteggiare tutti gli output di tutte le transazioni, senza tenere conto dell'esistenza del secondo output (che ha il compito di eseguire il processo *change*), può sviare certi risultati, in particolare l'analisi sul volume degli scambi presenti sul network della moneta digitale, può essere non conforme con la realtà.

Unità di misura nel sistema Bitcoin			
Unità	*Simbolo*	*Valore Decimale*	*Infomazione*
Mega-bitcoin	MBTC	1,000,000	raro
Kilo-bitcoin	kBTC	1,000	raro
Hecto-bitcoin	hBTC	100	raro
Deca-bitcoin	daBTC	10	raro
bitcoin	BTC	1	unità base
Deci-bitcoin	dBTX	0,1	raro
Centi-bitcoin	cBTC	0,01	in precedenza frequente
Milli-bitcoin	mBTC	0,001	occasionale
Micro-bitcoin	µBTC	0,000001	frequente
Finney	-	0,0000001	-
Satoshi	sat	0,00000001	valore Blockchain
Millisatoshi	msat	0,00000000001	pagamento valore canale

Tabella 2.2 Tabella riassuntiva dell'unità di misura del bitcoin.
Fonte Url: "https://en.bitcoin.it/wiki/Units#cite_note-4".

Inoltre, come si evince dalla tabella 2.2, gli emittenti possono traferire anche solamente una porzione del valore di una transazione presente negli input, questo può avvenire perché c'è la possibilità di suddividere un singolo bitcoin (BTC) in 100,000,000 parti. La più piccola unità utilizzata come pagamento (1/100,000,000) è stato denominata "Satoshi", in memoria del suo inventore.
Ritornando al discorso precedente, si è visto come una singola transazione avviene grazie al meccanismo della crittografia asimmetrica, dove la firma digitale è quella che permette di autenticare ogni singola transazione. Ad ogni modo, servirà il meccanismo del marcatore temporale per evitare che possa esserci il double spending, ossia che si possa effettuare con lo stesso identico ammontare più pagamenti. Prima di entrare in quel discorso, è utile spendere due parole su cosa sia il blocco, visto che è il sistema è retto dall'unione di essi.

Le transazioni sono raggruppate in blocchi, che contengono la storia completa delle transazioni che quindi può essere verificata da chiunque, come il proprietario attuale di ogni singolo ammontare di token. Ogni blocco ha un numero predeterminato di transazioni, in base alla sua dimensione. Il limite del blocco è di 1,000,000 bytes (1 Megabyte), così a supportare una propagazione veloce e ridurre le anomalie. La dimensione di ogni singola transazione è differente dalle altre, perché dipende dal numero di input ed output della transazione stessa.

Version	02000000
Previous block hash (reversed)	17975b97c18ed1f7e255adf297599b553 30edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 C0e19fa6b2b92b3a19c8e6badc141787
Timestamp	358b0553
Bits	535f0119
Nonce	48750833
Transaction count	63
Transaction	

Tabella 2.3 Struttura di un Blocco, Fonte: "Handbook of Digital Currency", David Lee Kuo Chuen, 2015.

Nella tabella 2.3 viene rappresentata la struttura di un blocco, che è composto da due elementi imprescindibili: l'intestazione e il corpo. Nel corpo si trovano le transazioni, mentre l'intestazione (come raffigurata nella tabella soprastante) è suddivisa in sette campi:

- Numero di versione del blocco: dipende dalla versione del software;
- Hash previous block: è un valore di hash a 256 bit e fa riferimento al blocco precedente della blockchain;
- Merkle root[113] (Radice di Merkle): è l'hash di tutti gli hash delle transazioni presenti nel blocco. All'interno di un blocco le transazioni vengono sottoposte ad hashing indirettamente attraverso il Merkle root. Di conseguenza, quando si fa l'hashing di un blocco, anche se per una sola transazione, viene richiesto una potenza computazionale per l'hashing di un blocco con 1000 transazioni;

[113] Merkle root: Il nodo radice di un Merkle Tree, dove discendono tutte le coppie hash nella struttura. Le intestazioni dei blocchi devono includere un root merkle valida derivante da tutte le transazioni in quel blocco. Fonte Url: "https://bitcoin.org/en/glossary/merkle-root".

- Timestamp: rappresenta la marca temporale attuale, dal 1970-01-01T 00:00 UTC (tempo universale coordinato dal 1° gennaio, 1970);
- Campo di bit: rappresenta il valore di destinazione corrente.
- Nonce: è un campo di 8 byte che varia in base al target. Questo valore inizia con 0 e man mano viene incrementato con gli ulteriori hash. In particolare, il valore viene trovato in base a tentativi, vale a dire fin tanto che non si trova l'hash contenente il numero di zeri iniziali richiesti.
- Numero di transazioni: è il campo dove vengono sommate il numero di transazioni presenti nel blocco.

L'intestazione di un blocco utilizza l'hash SHA256 bit, deve essere uguale o inferiore dell'obiettivo corrente perché il blocco sia accettato dalla rete. Per convalidare il blocco, deve essere risolto il rompicapo matematico. Questo enigma matematico è dinamico, vale a dire che il valore target (obiettivo) è inversamente proporzionale all'aumento della difficoltà nel processo di generazione di un blocco. Quindi il valore obiettivo diminuirà con l'aumento della difficoltà. Con il termine difficoltà si allude ad una metrica che indica quanto sia difficile risolvere i blocchi di una transazione, in base al Hashrate[114] della rete.

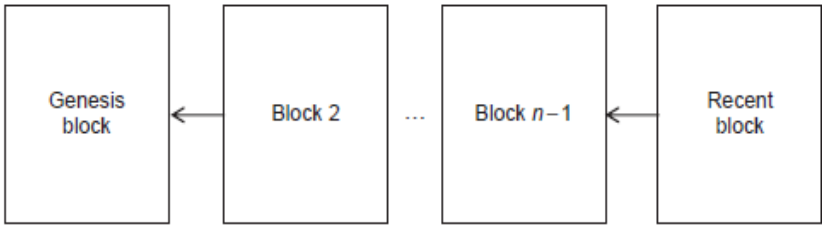


Figura 2.14 Un esempio della struttura Blockchain, Fonte: "Handbook Of Digital Currency", David Lee Kuo Chuen, 2015.

Come raffigurato dalla figura 2.14, si può affermare che la Blockchain è una sequenza di blocchi che registra tutte le transazioni come un pubblico registro. Ogni blocco della catena rappresenta la conferma dell'integrità del precedente, fino ad arrivare al primo blocco, denominato blocco genesi. Nessuno può sovrascrivere ed alterare i blocchi precedenti dal fork della catena. In Bitcoin viene utilizzata la funzione l'Hashcash (doppia-SHA256 bit) per evitare attacchi. Come si è già detto nei paragrafi precedenti, l'SHA256 bit tramuta il messaggio di input in un fingerprint a 256 bit. Per riuscire ad eseguire tutti questi calcoli complessi, è essenziale un buon grado di Hashrate. Infatti, maggiore è questo livello, maggiore è la probabilità di risolvere il blocco della transazione, ma questo

[114] Definizione di Hashrate: "è la misura del numero di calcoli (hash) al secondo che l'hardware può eseguire, mentre cerca di rompere il problema matematico", Fonte "Handbook of Digital Currency" David Lee Kuo Chuen, 2015.

ovviamente viene comparato a quello medio del network. In dettaglio, un nodo inizialmente verifica l'intera blockchain, successivamente prende le nuove transazioni (non ancora confermate) e dichiara al network quale secondo lui dovrebbe essere il nuovo blocco. Così facendo però, vi è la possibilità che più nodi creino simultaneamente dei blocchi simili. Per evitare ciò, nel processo di validazione del blocco ogni nodo deve avere una soluzione al problema matematico. Il primo che riesce a risolvere questo enigma matematico (risolvere il blocco), lo trasmette al network, che lo accettera come il prossimo blocco della catena.

In aggiunta a quanto si è detto, è rimasto un ultimo argomento da trattare, ossia il problema del *Double-Spending*. Nel caso del mondo delle criptovalute, prive di un organo centrale di garanzia (in realtà questo vale per la maggior parte di loro), serve un ulteriore meccanismo che permetta di evitare l'inconveniente che un utente possa spendere la stessa cifra due volte.

Il problema che si ha in questo caso è di coordinare i nodi presenti sul network, con la possibilità che ci siano dei sabotatori, è denominato come il *Problema dei Generali Bizantini*[115].

Come è stato descritto precedentemente i nodi raggruppano le transazioni all'interno dei blocchi (tabella 2.3), i quali sono collegati l'uno all'altro e formano così la blockchain e sono condivisi su tutto il network. Questo processo viene illustrato nella figura 2.14, dove i blocchi aggiunti attendono di essere confermati dal sistema e solo se questo si verifica, vengono accettati alla catena. Ogni blocco ha un Hash del blocco precedente, in tal modo viene rispettato l'ordine cronologico dei blocchi, ma è da ricordare che chiunque può immettere nel sistema un nuovo blocco, per esempio un assalitore potrebbe creare una catena alternativa che rassegni proprietà arbitrariamente. Per evitare ciò, ai nodi di Bitcoin viene richiesto di risolvere un problema complesso di PoW al fine di aggiungere un blocco nella Blockchain. Ogni blocco dipenderà dal suo precedente, che è stato creato tramite questo procedimento. Per sostituire l'intera catena, qualcuno dovrebbe risolvere il problema di PoW per ogni blocco presente nella catena, e questo gli richiederebbe un enorme sforzo computazionale. Un assalitore può anche tentare di cambiare il blocco più

[115] Definizione: "Il problema dei generali bizantini è un problema informatico su come raggiungere consenso in situazioni in cui è possibile la presenza di errori. Il problema consiste nel trovare un accordo, comunicando solo tramite messaggi, tra componenti diversi nel caso in cui siano presenti informazioni discordanti". Fonte Url: "https://it.wikipedia.org/wiki/Problema_dei_generali_bizantini".

recente della blockchain. In questo caso ci dovrebbero essere due blocchi allo stesso punto del precedente, così creando un *fork* all'interno della blockchain.

Tuttavia, questo può succedere anche se ci sono due nodi onesti che incidentalmente creano un blocco contemporaneamente: questo può accadere per via dei ritardi della rete, allora ogni nodo, ossia ogni Miner sceglierà il blocco che ha ricevuto e lavorerà su quello, allungando il più possibile quella catena. Il sistema punterà sempre al maggiore sforzo computazionale, per questo motivo sceglierà sempre la catena più lunga; per cui dopo un certo numero di blocchi, la biforcazione temporaneamente ammessa, verrà eliminata.

In dettaglio, per eliminare questi inconvenienti si esegue la conferma della transazione, in tal modo una volta trasferita la transazione e confermata non potrà più essere spesa. Quindi quando viene inserita una transazione all'interno di un blocco, questa viene denominata conferma della transazione. In particolare, una transazione si dice confermata quando ha almeno 6 conferme.

Infatti, dal proprio wallet si può controllare lo stato della transazione, ovvero se è stata confermata o meno cioè se è stata inserita in almeno 6 blocchi successivi. Ad ogni modo, ogni partecipante al network può decidere in base alla sua propensione al rischio, il numero minimo di conferme per le transazioni che riceve. Certo che abbassare il numero di conferme, può comportare da una parte una rapidità nelle transazioni, ma dall'altra può essere pericoloso (dipenderebbe anche dall'importo della transazione).

Da evidenziare che un blocco per definizione viene creato ogni 10 minuti circa, e quindi se la transazione ha bisogno di ottenere 6 conferme per essere validata, di conseguenza ci vorrà circa un'ora prima che la transazione sia stata confermata, e quindi che il denaro digitale sia stato trasferito.

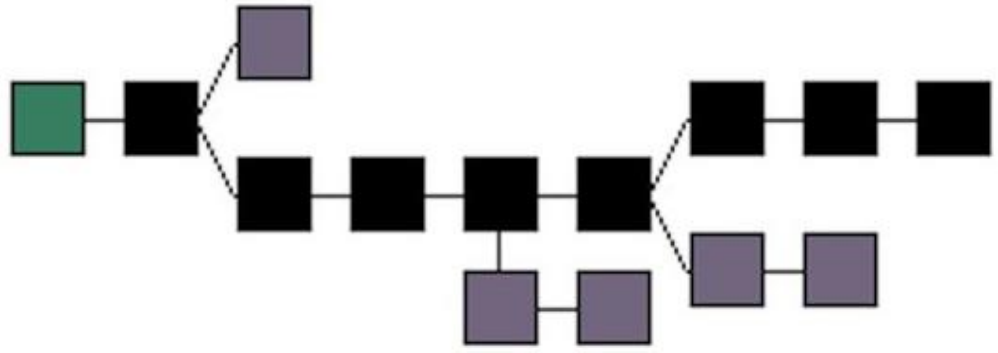


Figura 2.15 Un esempio empirico del funzionamento della Blockchain.
Fonte "Bitcoin Internals: A technical guide to Bitcoin" Chris Clark, 2013.

Come viene mostrato dalla figura 2.15, i blocchi neri raffigurano i rami della catena che sono stati accettati, che sono per definizione i più lunghi. Mentre i blocchi grigi sono mantenuti sulla blockchain, ma sono stati ignorati, perché non sono i rami più lunghi. Inoltre, quest'ultimi vengono definiti blocchi orfani. Il blocco che si trova alla sinistra è il primo blocco della blockchain ed è denominato anche come il *blocco genesis*.

Il *Mining*

Il processo di convalida di ogni singolo blocco, e quindi l'aggiunta nella catena, è denominato *mining*, mentre chi esegue questa operazione è chiamato m*iners*. Questo processo è composto dalle seguenti fasi:

1- Registrare le transazioni, trasmesse dal network, in un blocco. I miners possono decidere arbitrariamente quali transazioni includere nel proprio blocco. Normalmente, ogni transazione ha una piccola commissione, che sarà pagata al miner quando il blocco sarà accettato. Infatti, i miners sono spronati ad includere più transazioni possibili all'interno di esso, fino al limite dimensionale di 1 Megabyte.

2- Verificare l'autenticità di tutte le transazioni.

3- Selezionare la più lunga strada della Blockchain, in corrispondenza dell'ultimo fork, ed inserire l'hash dell'intestazione del nuovo blocco al precedente.

4- Provare a risolvere il problema matematico del PoW; possono accadere due scenari:

   a. Se la soluzione viene trovata, viene aggiunto il nuovo blocco alla catena e viene comunicato all'intero network.

   b. Se il PoW viene risolto prima da un altro nodo (scenario molto frequente), il PoW e la trasmissione del blocco sono controllate per il processo di validazione. Se il controllo va a buon fine, il loro blocco viene aggiunto alla catena ed inoltrato al network; altrimenti questo verrà scartato.

Ogni miners presente sul network proverà all'unisono a risolvere questi calcoli complessi per l'aggiunta dei nuovi blocchi. I nodi non possono comunicare istantaneamente, perché potrebbero avere delle differenti versioni della blockchain, ma ad ogni modo, normalmente la maggioranza dei nodi sarà d'accordo. Questo avviene perché i blocchi

vengono creati regolarmente ad un tasso temporale di circa 10 minuti, invece la comunicazione dei nuovi blocchi sarà solo di pochi secondi. In questo lasso temporale, come si è detto nel precedente paragrafo, tutti i nodi proveranno a risolvere il PoW fintanto che solo causalmente un nodo riuscirà a risolverlo. Quando avviene la creazione di un nuovo blocco, questo verrà comunicato e in pochi secondi tutti i nodi accetteranno e successivamente tutti ripartiranno da quest'ultimo.

Come si è illustrato dalla figura 2.15, quando due nodi creano un nuovo blocco casualmente e allo stesso tempo, viene creata una soft fork (differente da un Hard Fork, come nel caso dei Bitcoin Cash), e da questa alcuni nodi prenderanno una strada piuttosto che un'altra, ma per il sistema vince sempre la difficoltà e la complessità, vale a dire vige la *regola della catena più lunga*. In base a questa regola si garantirà il ritorno al consenso abbastanza velocemente. Questo non è sinonimo di garanzia, perché tutti processeranno simultaneamente le stesse transazioni, perché per l'appunto ognuno può decidere arbitrariamente su quali lavorare. Ad ogni modo si possono verificare due possibili scenari:

- il primo: è che si verifichino delle sovrapposizioni delle transazioni che i miners stanno elaborando in parallelo, perché vogliono includere più transazioni possibili all'interno dei loro blocchi;
- il secondo: nel momento in cui vengono aggiunti i nuovi blocchi alla catena può succedere che qualche porzione di transazioni sia rimasta tagliata fuori dal nuovo blocco. Comunque, quest'ultime saranno riprese e messe insieme a quelle non ancora processate, in modo tale che i miners potranno scegliere se includerle nella creazione del prossimo blocco.

In conclusione, il mining è stato ideato per rendere sicura ed efficiente la Blockchain e questo può essere possibile dalla presenza dei miners. Inoltre, questo è l'unico modo possibile per immettere nel sistema nuovi token.

Proof-of-Work (PoW)

Il PoW si riferisce al processo di lavoro dei Miners, per risolvere i difficili e complessi problemi matematici. I miners seguono questa procedura:

1. incrementano un numero arbitrario scelto casualmente, nell'intestazione del blocco, denominato *nonce*;

2. calcolano l'hash dalla nuova intestazione;
3. controllano se l'hash dell'intestazione (espresso numericamente) è inferiore ad un predeterminato valore obiettivo (target).

Come si era già spiegato nel precedente paragrafo, se la conversione numerica dell'Hash non è inferiore al valore target, il blocco sarà espulso dal network. L'obiettivo di questa procedura (del PoW) è di trovare un blocco che abbia un Hash il cui valore sia il più basso possibile. Nello specifico viene usato l'*Adam Back's Hashcash* (ideato nel 1997). L'Hashcash è un sistema che fa parte della procedura mining che determina il target dal sistema in base alla difficoltà. Nel sistema di Adam Back, viene usato come valore target il numero degli zeri presenti all'inizio del codice binario dell'Hash. Questo concetto è stato ripreso in Bitcoin, in modo tale che attraverso la procedura Hash, viene iterata la generazione del codice fin tanto che non produce un codice hash che ha nella parte inziale del codice binario il numero esatto degli zeri.
Quindi la soluzione del problema del PoW, la sì raggiunge risolvendo:

$$H(x) \leq T$$

Dove x (nonce) verrà aggiunto alla funzione per risolvere il problema, in questo modo la soluzione si troverà andando a tentativi.
Il processo poi continuerà facendo un doppio Hash SHA256 dell'intestazione del blocco:

$$SHA256^2(\text{block header})$$

Per esempio, si vuole trovare un Hash che abbia 9 zeri come prime cifre, partendo da: H("Hello!0").
Per prima cosa verrà aggiunto 0 come valore nonce. L'output hash generato non sarà inferiore al target. Procedendo per tentativi ed incrementando ad ogni tentativo il nonce, si dovrà arrivare alla 9270° iterazione affinché l'uscita determinata sia inferiore all'obiettivo:
SHA256(SHA256(("Hello!0")) =
1312af181c275f94028d480a6adc1e125b1caa44c749ec81976192e2ec934c64
…..
H("Hello!9270") =
0000000002fc32107f1fdc0241fa747ff97342a4714df7cc52ea464e12dcd4e9".
In conclusione, al terzo punto di tale procedura, al momento del controllo, se l'Hash calcolato è inferiore o uguale al valore target, si è risolto il problema e il blocco verrà

aggiunto alla catena. Altrimenti, la soluzione non è stata trovata, per cui si reitererà la procedura ripartendo dal primo punto, ossia aggiungendo un valore al nonce.

La difficoltà del valore Target

La regola fondamentale nella creazione di nuovi blocchi è che non debbano essere creati né troppo velocemente e né troppo lentamente. Pertanto, bisogna trovare un giusto compromesso, perché se venissero aggiunti troppo velocemente rispetto al tempo di distribuzione sul network, la Blockchain diventerebbe piena di *forks*. Questo creerebbe confusione e difficoltà per i nodi nell'ottenimento del consenso, ossia si avrebbero delle difficoltà nel decidere in ramo dirigersi sulla catena. Con l'aumentare del consenso della criptovaluta si sono aggiunti sempre più miners e si è assistito nell'evoluzione della componentistica hardware: per questi motivi il tasso di risoluzione del PoW dovrebbe aumentare. Per evitare questo, il sistema ha la capacità di adattarsi mantenendo costante il tempo tra la creazione dei nuovi blocchi a circa 10 minuti. Questa regolazione viene adattata periodicamente dal valore Hash target per blocchi. Infatti, come si è accennato prima, l'Hash dell'intestazione del blocco deve essere minore o uguale al valore target. Tanto è più basso il valore di target, più difficile sarà trovare dei blocchi. Il sistema è sviluppato per far sì che ogni 2016 blocchi (ossia due settimane, se ogni la creazione di ogni nuovo blocco avviene ogni 10 minuti), i nodi calcoleranno una nuova difficoltà basata sul tempo impiegato a minare i precedenti 2016 blocchi. Attraverso dei calcoli matematici, si può trovare l'intervallo del valore target utilizzato per il mining.

Ricompense del Mining

Risolvere il problema del PoW è un lavoro estremamente laborioso e costoso, sia a livello di potenza computazionale del computer che dal costo energetico. Per questo motivo, è fondamentale il ruolo della ricompensa per incoraggiare le persone a partecipare come miners. Nel Bitcoin vengono rilasciati dei nuovi bitcoin ai miners per ogni blocco minato. Cosicché alla prima transazione di ogni blocco, i miners inseriscono la cosiddetta transazione *coinbase* (o anche detta transazione generazione), cosicché loro stessi si premiano. Difatti, nell'output delle transazioni di coinbase si trova l'indirizzo specifico dei

miners, in tal modo loro potranno ricevere le ricompense se il blocco creato è stato accettato dalla catena. A causa dei problemi, descritti in precedenza, legati al fork non è possibile sapere immediatamente se il nuovo blocco è stato accettato: il sistema richiede 100 blocchi del tempo maturato prima che il coinbase possa essere speso. Per tal motivo la classica transazione ha bisogno di circa 1 ora per effettuare un'altra transazione di quell'ammontare, mentre per le transazioni coinbase necessita di circa 17 ore.

Da notare che il meccanismo di ricompensa dei miners è l'unico modo possibile per immettere nuova liquidità digitale nel sistema. La remunerazione dei miners è proporzionale all'investimento fatto. Se tutti i bitcoin fossero stati generati all'inizio,

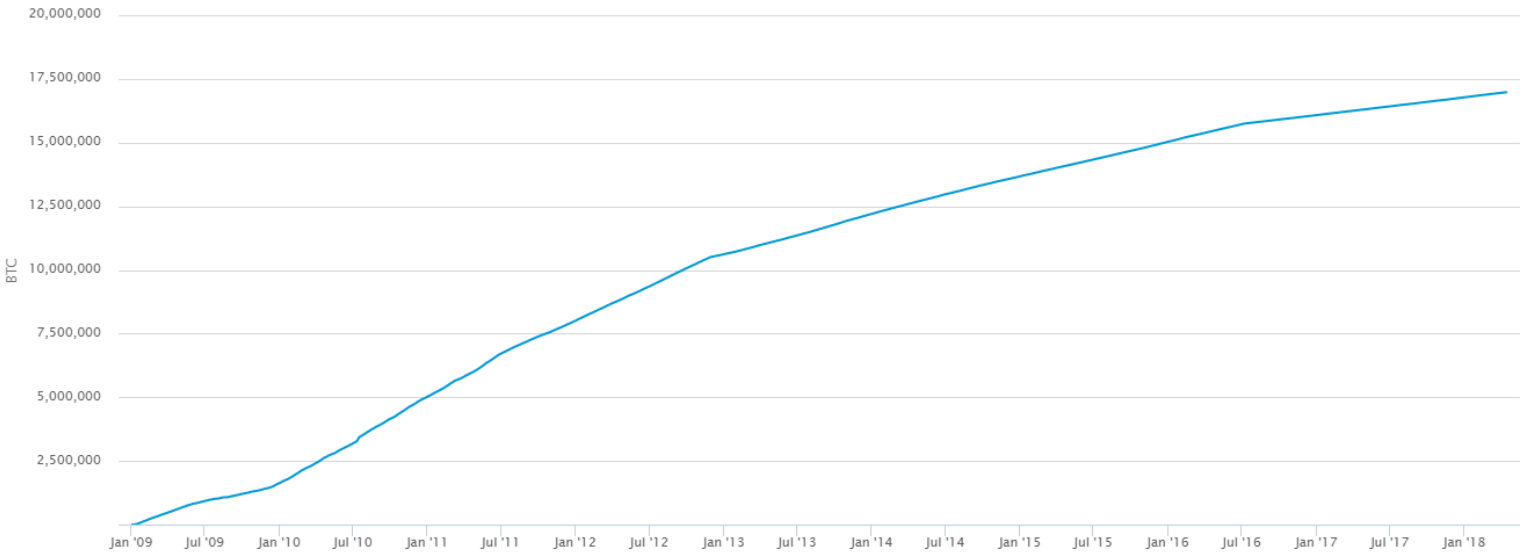


Figura 2.16 Volume di bitcoin estratti fino al 16 aprile 2018. Fonte: "https://blockchain.info", ore 13:11.

probabilmente il creatore avrebbe avuto difficoltà nella loro vendita sul mercato (in altre criptovalute invece sono già state tutte create, e vengono rilasciate in base alla loro richiesta e al tasso d'inflazione). Inizialmente, la ricompensa era di 50 bitcoins per ogni blocco creato e validato: se fosse rimasto a quel tasso di creazione, ci sarebbe stata un'elevatissima inflazione dovuta dall'inserimento dell'offerta monetaria di denaro digitale. Per questo motivo il sistema Bitcoin ha una funzione di adattamento che dipende dal numero di nodi creati finora, in tal modo il sistema è programmato per dimezzare la ricompensa ogni 210,000 blocchi, vale a dire approssimativamente ogni 4 anni circa.

Da qui può si può dedurre che il numero massimo di bitcoin che è possibile estrarre attraverso il mining è 21 milioni: una volta raggiunta tale cifra non sarà più possibile estrarne degli altri. Arrivati a questo traguardo i miners potranno beneficiare come ricompensa solo dalle commissioni sulle transazioni di ogni blocco che hanno minato: queste commissioni esistono già e si ricevono ogni volta quando c'è un eccesso di input

rispetto al valore degli output, e questa plusvalenza va direttamente al miner. Attualmente, il totale delle commissioni è più basso del valore delle transazioni coinbase, ma ad ogni modo quando si invertirà il valore dei due, le commissioni delle transazioni sarà il nuovo profitto dei miners.
Proprio come si vede dalla figura 2.16, attualmente sono stati estratti quasi 17 milioni di token, con una ricompensa di 12.5 bitcoin ad ogni blocco convalidato. Da evidenziare che il termine estrazione di bitcoin è paragonabile all'estrazione dell'oro, infatti l'offerta di bitcoin è collegata al suo processo di mining, anziché dalla sua domanda.
In conclusione, è da riportare che il fattore fondamentale di questo processo è la potenza computazionale messa a disposizione dal miner che determina il successo del lavoro.

Hardware Mining

L'hardware determina il successo dell'operazione di mining: Satoshi Nakamoto estrasse i primi bitcoin con il suo computer personale, ad oggi sono necessarie componentistiche dedicate definite hardware da Mining. Precedentemente, venivano usate le GPUs (Graphics Processing Unit) che hanno il vantaggio di poter eseguire un elevato numero di calcoli in parallelo e sono più veloci delle CPUs. Successivamente sono stati sviluppati nuovi hardware dedicati tra cui lo ASICs (Application-Specific Integrated Circuits) caratterizzati da velocità ordini di grandezza più veloci delle GPUs. I miners devono, per poter essere competitivi, devono disporre di componentistiche di ultima generazione.

Differenti modi per fare il Mining

Ci sono tre modi per fare il Mining: Mining individuale, Pools Mining e Mining Contracts.

Mining individuale:
Nel mining individuale i miners lavorano in solitaria, risolvendo gli Hash individualmente, con lo scopo di trovare la soluzione al problema matematico del PoW, per poi ricevere la ricompensa spettagli. La probabilità di riuscirci è molto bassa in quanto, solitamente, la potenza computazionale non è sufficiente. Nel 2015 il tempo medio di un miner solitario per accaparrarsi la ricompensa era di tre mesi. Non dimenticando che il processo è casuale e non tiene conto dei progressi raggiunti, alla fine dei tre mesi non è detto che possa

farcela. In aggiunta, la singola potenza di calcolo con la relativa potenza di hashing è direttamente proporzionale con l'aumento della difficoltà. Nel 2015 per riuscire a risolvere un blocco con una potenza di 1 GH/s serviva in media 70 anni.

$$\text{Time} = \frac{\text{Difficulty} \times (2^{32})}{\text{Hashrate}}$$

Figura 2.17 Fonte: "Handbook of Digital Currency" David Lee Kuo Chuen, 2015.

Come si può vedere dalla figura 2.17, il tempo è rapportato dalla difficoltà e dal Hashrate.

Pools Mining:

Invece che minare individualmente nuovi blocchi, lo si può fare anche unendo le risorse collettivamente, attraverso la formazione di gruppi. Questi sono formati da un insieme di miners con lo scopo di generare una potenza di Hashing più elevata. La potenza computazionale complessiva è la somma delle singole, mentre la ricompensa è proporzionale alla potenza messa a disposizione del gruppo. Per questo motivo il reddito del miner è minore, ma costante nel tempo.

Contracts Mining:

Utilizzato da coloro che vorrebbero investire nel mining, ma non hanno le risorse per l'investimento inziale, quindi affittano, attraverso apposite infrastrutture, le risorse necessarie per minare nuovi blocchi.

Ci sono tre tipi di Contracts Mining: l'Hosted mining, Virtual hosted mining e il Leased hashing power. Questa forma di mining ha importati vantaggi, quali: nessun costo aggiuntivo di energia elettrica, attrezzatura informatiche e costruzione del sistema software. L'aspetto negativo di questo approccio è la minore redditività.

Onestà e disonestà dei nodi: Attacchi possibili al sistema

Come in ogni sistema sociale e maggiormente qui nel mondo delle criptovalute, è essenziale il corretto comportamento dei nodi. Ovviamente qui acquisisce maggior importanza, perché il sistema sottostante è privo di un organo centralizzato adibito per il controllo, ma sono i singoli nodi ad autogestirsi. Un nodo si dice onesto quando impiega il proprio lavoro computazionale al fine di risolvere il problema del PoW, ed aggiungere dei

blocchi all'interno della catena. Tuttavia, può esserci il caso che qualcuno voglia compiere degli atti adibiti ad aggirare il sistema, e quindi sottrarre il denaro digitale ai legittimi possessori. Si è già illustrato come il meccanismo del mining sia il rimedio al *double-spending* e che la Blockchain segue sempre la catena più lunga, per evitare possibili fork non corrette, tuttavia esistono dei sistemi per aggirare il sistema.
La crittografia che protegge le chiavi private è ineludibile e quindi nessuno può violare il sistema per accreditarsi i fondi non propri. Senza dimenticare che è impossibile derivare la chiave privata partendo dalla chiave pubblica o dall'indirizzo. L'unico modo per rubare le valute elettroniche è quello di accedere ai servizi complementari al sistema Bitcoin, come i wallet o gli Exchange, com'è capitato già più di una volta negli anni passati. Eludendo questi sistemi, i cyber-criminali sono così liberi di rubare la chiave privata. Come è stato detto, non è la Blockchain che viene attaccata, ma bensì gli strumenti dov'è depositata la chiave privata.
Ad ogni modo ci possono essere tre modi per cui il sistema può vacillare:

<u>L'attacco a collisione</u>:
Con l'attacco a collisione si cerca di trovare due input che producono lo stesso risultato Hash. Nel paragrafo della crittografia è stato spiegato come è quasi impossibile trovare lo stesso Hash (output), partendo da due input differenti.
Per esempio, l'algoritmo SHA-1 è stato crackato dal team di Google, utilizzando dei calcolatori appositi e un team iper-specializzato. Nel sistema di Bitcoin vengono utilizzate la crittografia SHA-256 bit ed ECDSA, considerati fra i più sicuri al mondo. Ciononostante, gli algoritmi crittografici di Hash non sono nati per essere sicuri al 100%, ma il loro scopo è quello di disincentivare i malintenzionati ad intraprendere la frode digitale, lo sforzo computazionale per bucare questo algoritmo è maggiore del beneficio economico derivato. Una importante svolta potrebbe accadere con l'utilizzo dei nuovi computer quantistici, e della crittografia quantistica.

<u>Il Double-Spending</u>:
Con questo tipo di attacco, il malintenzionato vuole utilizzare lo stesso denaro digitale per più pagamenti. Come si è già visto precedentemente la Blockchain e in particolare il Mining cercano di evitare questa eventualità, tuttavia può essere effettuato un attacco di questo tipo. Quando si trova una soluzione al problema del PoW di un blocco, questo viene

aggiunto insieme alle transazioni in esso contenute, al quale vengono concatenati ulteriori blocchi partendo da questo. Quando si raggiungono 6 conferme (cinque dopo quella che si è emessa), si ha la conferma del blocco inserito, e quindi delle transazioni contenute. Come si era illustrato nei paragrafi precedenti, esiste la possibilità che sorgano dei fork durante questo processo, dove per la regola della catena più lunga, si sceglie di perseguire quella che ha avuto più conferme. Così facendo si evita il double-spending.

Tutto questo funziona, se il malintenzionato non vuole effettuare due pagamenti senza aspettare la conferma del primo. In particolare, il malfattore effettua il primo pagamento ad un altro utente (ad esempio un negoziante), il secondo utente non aspetta i sei blocchi di conferma (1 ora di attesa) e quindi invia ignaramente il bene. Nel frattempo, il malfattore utilizza la stessa moneta per la seconda transazione, utilizzando la strategia del *Selfish-mining*. In base a questa strategia, è proprio il miner che intenzionalmente crea una fork, per risolvere i blocchi successivi al primo pagamento, senza però comunicarli nel network. Quando avrà risolto un certo numero di blocchi concatenati tra loro, li comunicherà tutti insieme alla rete, in modo tale che saranno accettati senza condizione. A questo punto la catena sarà più lunga dov'è situato il secondo blocco, contenente la seconda transazione, mentre il primo blocco (contenente la prima transazione fasulla), verrà abbandonata, così diventando orfana.

Questo tipo di cyber-attacco è molto improbabile secondo il fondatore di Bitcoin, perché richiederebbe una potenza computazionale elevata, ossia dipenderebbe dalla potenza del nodo/client del suo Hashrate e dal numero di conferme che ha scelto il destinatario della prima transazione. Se il nodo/client ha il 51% dell'Hashrate totale del network, l'attacco può avvenire senza problemi (si veda sotto). Ovviamente, se l'Hashrate è inferiore al 50% e il numero di conferme sono elevate, sarà molto più difficile che questo attacco vada a buon fine.

Il 51% Attack:

Questo è uno fra gli attacchi più conosciuti all'interno del sistema Bitcoin. L'attacco al 51% è un attacco diretto al sistema, dove chi possiede dal 51% (la maggioranza assoluta del sistema) di tutta la potenza computazionale del sistema (hashrate[116]), può alterare le transazioni arbitrariamente. Questa azione può essere condotta da un singolo o da un gruppo di malfattori.

Come si è poc'anzi detto, nel momento in cui si crea un fork, è l'aggiunta dei blocchi concatenati che determinano l'accettazione nella Blockchain, convalidandoli.

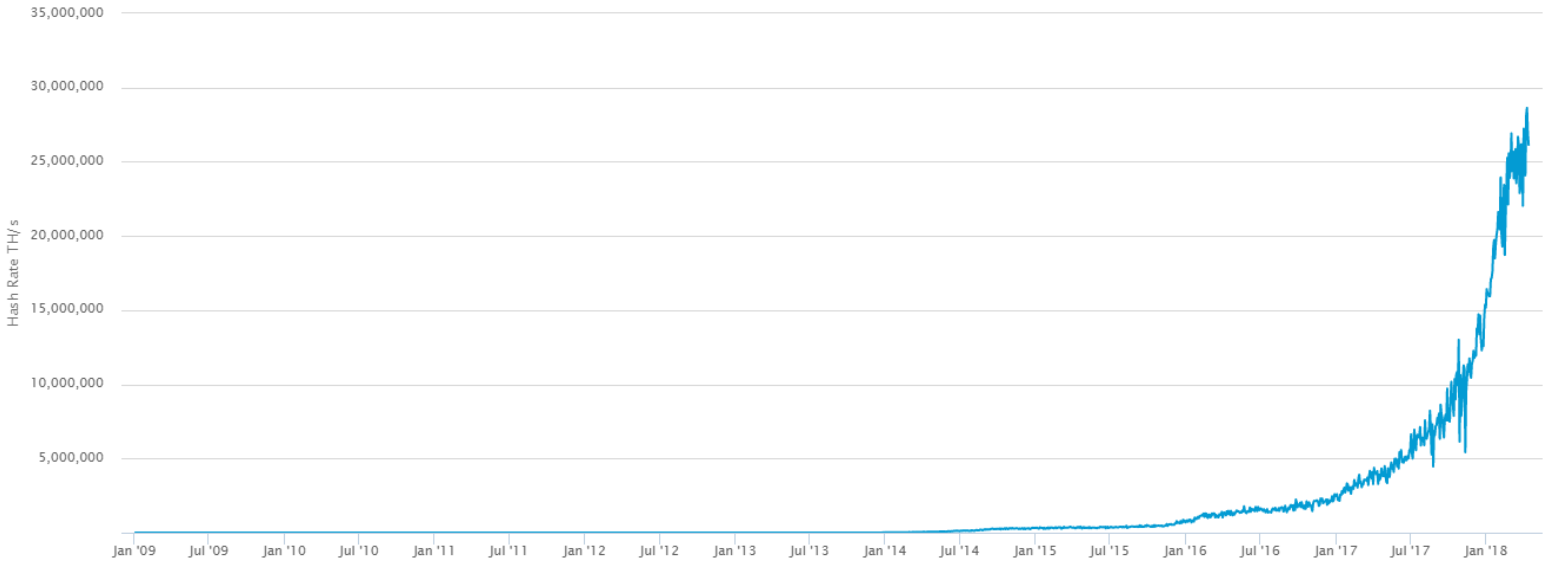


Figura 2.18 Raffigurazione dell'Hashrate totale del sistema Bitcoin: 26.15 EH/s
Fonte Url: "https://blockchain.info/it/charts/hash-rate?timespan=all"., 14 aprile 2018, ore: 02:00.

Tuttavia, se qualcuno riuscisse ad avere il 51% dell'Hashrate totale potrebbe riuscire a creare nuovi blocchi in successione prima degli altri miners. Ad oggi, il 51% dell'Hashrate equivale a 13,334,932.77 TH/s, una cifra enorme che potrebbe essere generata utilizzando degli elaboratori costosissimi e dei costi energetici esorbitanti. Per tale motivo il creatore e più in generale tutta la comunità del criptomondo ritiene che questo tipo di attacco sia molto improbabile.

[116] Hashrate definizione: "Per hashrate si intende l'unità di misura della potenza di elaborazione della rete Bitcoin. Quando la rete raggiunge un hashrate di 10 Th/s, significa che può realizzare un trilione di calcoli al secondo", Fonte Url: "https://bitcoin.org/it/glossario".
Questa potenza è calcolata come il numero di Hash che un elaboratore, o un network di computer, può calcolare in un secondo. Quindi è la potenza che viene adibita per l'inserimento delle transazioni, con la conseguenza di creare dei blocchi genuini.

Smart contracts - Blockchain 2.0

Questo paragrafo descrive l'evoluzione della Blockchain, infatti col tempo quest'architettura è stata studiata, per esplorare il vero potenziale, ossia permettere di raggiungere degli scopi specifici. Nel 2013 Buterin, un giovane programmatore, ha visto queste enormi potenzialità, immaginando un sistema simile a Bitcoin, ma adibito anche per altre funzioni. Buterin ha fondato Ethereum che permette la creazione e lo sviluppo di applicazioni decentralizzate con molteplici funzionalità. La Blockchain di Ethereum è progettata per permettere l'esecuzione di un codice fondato su transazioni verificate. Quindi, invece di trasferire solo i fondi da un utente all'altro, la piattaforma consente l'esecuzione di altri svariati eventi, come ad esempio: trasferimento di titoli di proprietà, gestire la registrazione degli elettori o consentire l'esecuzione di contratti sicuri tra le parti. Le transazioni presenti su questo tipo di Blockchain prendono il nome di *Smart Contracts* (o contratti intelligenti).

Gli Smart Contracts possono essere definiti come contratti intelligenti, ossia dei veri propri programmi o applicazioni. Ogni ripetizione dello stato[117] dell'applicazione è registrata sulla blockchain. Per tale motivo, questa nuova implementazione della classica Blockchain, viene denominata anche *Blockchain 2.0.*

In dettaglio, all'interno di queste applicazioni, il codice software può essere avviato ed eseguito, quando si ha una transazione: lo stato dell'applicazione può modificarsi, e questo viene subito registrato all'interno della Blockchain. Così facendo, si potrà avere tutta la cronologa dell'esecuzione delle applicazioni ed impiegarla per verificare le transazioni. Questo aspetto della registrazione cronologica di una applicazione è fondamentale per il corretto funzionamento dei contratti intelligenti.

Ovviamente, tutto ciò è possibile grazie alla rete peer-to-peer decentralizzata, proprio come quella di Bitcoin, dove vengono sostenuti i calcoli distribuiti dai nodi presenti sulla stessa. Questo network può essere pensato come un unico computer, nel quale tutti gli elaboratori presenti sulla rete si fondono insieme e prende il nome di *Ethereum Virtual Machine* (EVM), dove le Virtual Machines[118] (o VM), sono dei sistemi informatici emulati, in termini di calcolo.

---

[117] Per stato si riferisce a ciò che accade all'interno di un programmo o applicazione in un dato istante.

[118] Definizione di Vitual Machine (VM): "In informatica il termine macchina virtuale (VM) indica un software che, attraverso un processo di virtualizzazione, crea un ambiente virtuale che emula tipicamente il comportamento di una macchina fisica (PC client o server) grazie all'assegnazione di risorse hardware (porzioni di disco rigido, RAM e risorse di processamento) ed in cui alcune applicazioni possono essere

Figura 2.19 Rappresentazione di una Virtual Machine

EVM rappresenta l'ambiante di Runtime per gli smart contracts, in cui ogni nodo presente sul network esegue un'implementazione dell'EVM. Pertanto, i contratti intelligenti verranno eseguiti in questo ambiente virtualizzato. La differenza tra la piattaforma di Bitcoin ed Ethereum, è che nella seconda viene utilizzato un nuovo principio matematico che prende il nome di *l'Albero Merkle Patricia*, che permette di memorizzare i dati (ovvero i blocchi come un insieme di coppie di *chiave/valore*). Utilizzando questo sistema si incrementa l'efficienza e la scalabilità. L'accoppiamento di Chiavi e Valori avviene tramite un metodo matematico, che permette di generare univocamente la chiave partendo dal valore. Inoltre, la particolarità di questo meccanismo è la parte *Patricia* dell'albero: questa caratteristica definisce il posizionamento delle chiavi all'interno della piattaforma.
In generale, sarà proprio il sistema a decidere il modo di unire e gestire i dati memorizzati nei blocchi, attraverso dei prefissi di ciascuna chiave. Questo viene tradotto dai nodi che potranno procedere all'autenticazione, senza effettuare il download dell'intera blockchain. In aggiunta, i nodi non dovranno accedere all'interno sistema per eseguire un calcolo, infatti, questi scaricheranno solo quello che è realmente necessario, ossia lo stato parziale e il processo di verifica di quel pezzo di codice, avverrà con il controllo delle chiavi, in rapporto ai rami circostanti (che si riferiranno fino alla radice, ovvero alla prima transazione). Questo processo garantisce delle transazioni molto più veloci rispetto al Bitcoin, inoltre il sistema è più efficiente e consente una maggior scalabilità, quindi più transazioni in minor tempo.

---

eseguite come se interagissero con tale macchina; infatti se dovesse andare fuori uso il sistema operativo che gira sulla macchina virtuale, il sistema di base non ne risentirebbe affatto. Tra i vantaggi vi è il fatto di poter offrire contemporaneamente ed efficientemente a più utenti diversi ambienti operativi separati, ciascuno attivabile su effettiva richiesta, senza sporcare il sistema fisico reale con il partizionamento del disco rigido oppure fornire ambienti clusterizzati su sistemi server", Fonte Url: "https://it.wikipedia.org/wiki/Macchina_virtuale".

Illustrato questo meccanismo, è utile riprendere il concetto degli smart contracts, intesi come:

"Repeatable and modular scripts run on the Blockchain, to facilitate autonomous transactions between parties once certain criteria have been met"[119].

Questa tecnologia ha portato la Blockchain sotto i riflettori, proprio per la possibilità dell'uso degli smart contracts, per cui le istruzioni commerciali sono sottointese all'interno di un contratto, queste sono programmate nella Blockchain e vengono eseguite insieme ad una transazione.

Questi contratti intelligenti sono l'esempio perfetto di applicazioni distribuite (dApps), che possono essere creati sulla Blockchain.

Le condizioni sono codificate nel linguaggio di programmazione, e sono eseguite automaticamente quando vengono soddisfatte determinate condizioni. Pertanto, la programmazione viene adibita a copiare gli accordi commerciali convenzionali mediante la digitalizzazione delle transazioni all'interno della piattaforma, dove successivamente verrà autenticata attraverso la Blockchain. Una volta registrati nel registro digitale, gli smart contracts diverranno irrevocabili. La figura 2.20 rappresenta il processo degli smart contracts.

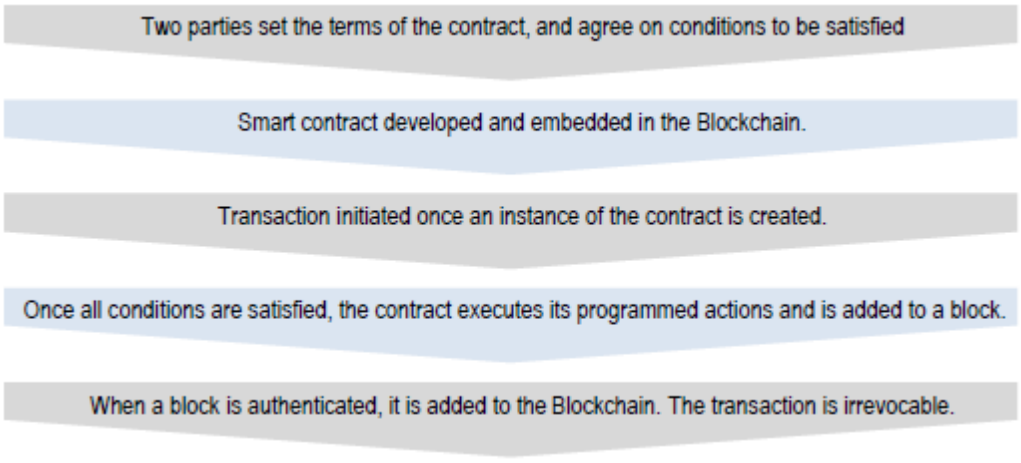


Figura 2.20 Rappresentazione del processo degli Smart Contracts, Fonte J.P. Morgan.

[119] Definizione tratta dal: "J.P. Morgan Perspectives – Decrypting Cryptocurrencies", J.P. Morgan, pag. 11.

Tangle - Blockchain 3.0

Questa piattaforma tecnologica si basa su un network di registri distribuiti, proprio come le altre Blockchain, ma con la differenza che non vengono usati i blocchi, e proprio per questo che non è propriamente corretto denominarla come una Blockchain.
Questa tecnologia deriva dal *Direct Acyclic Graphs* (DAG), della quale non esiste il concetto di miners. Il Tangle di IOTA (la criptovaluta che utilizza questa nuova tecnologia) è un network peer-to-peer, nella quale, ogni volta che una transazione viene registrata, è richiesto che ne vengano confermate due precedenti del tutto causali. Ovviamente per realizzare ciò, intervengono algoritmi crittografici.
Con la tecnologia DAG il processo di conferma delle transazioni è molto veloce: chiunque sul network può verificare le transazioni su qualsiasi elaboratore. In aggiunta, attraverso di essa, vengono permesse due caratteristiche: la possibilità di micro-transazioni e l'estrema velocità del processo. In questo sistema, non essendoci miners che devono validare la transazione ricevendo in cambio una ricompensa economica, possono essere effettuate delle micro-transazioni (ad esempio il pagamento di un caffè). Inoltre, rispetto alle altre criptovalute, qui il sistema risulta estremamente veloce e viene misurato in termini di transazioni per secondo (TPS). La velocità del sistema è direttamente proporzionale al numero di utilizzatori superando così il grande limite della precedente blockchain. Dunque, per terminare la transazione, non si deve aspettare delle ore. Inoltre, la caratteristica più importante di Tangle è che riesce a facilitare le interazioni tra due macchine, ossia permettere l'economia *machine-to-machine* (M2M) che favorisce il protocollo sottostante dell'*Internet of Things* (IoT). In questo sistema si trovano gli Iota come token, e il loro ammontare è fissato ed è privo di costi di inflazione. Un'altra differenza rispetto alla blockchain di Bitcoin, è che qui è presente la IOTA Foundation, un'organizzazione non-governativa registrata in Germania nell'ottobre 2017.

Caratteristiche di Tangle

Transazioni a zero commissione: il sistema offre transazioni nulle, grazie all'eliminazione del mining della valuta e quindi gli utenti non dovranno pagare le commissioni sulle transazioni.

Transazioni veloci: non esiste un limite numerico delle transazioni che possono essere confermate al secondo. Il *throughput* (capacità effettiva di trasmissione) è incrementato proporzionalmente dall'aumento degli utenti presenti sul network. Anche il problema della scalata è eliminato. Quindi ci saranno più transazioni in base a quanti utenti saranno presenti sul network, ed inoltre saranno processate più velocemente.

L'assenza dei Miners: rispetto alle precedenti Blockchains (Blockchain 1.0 e Blockchain 2.0), qui non esiste la figura del miner. In Tangle sono gli utenti a confermare la transazione.

Focalizzazione sull'economia machine-to-machine: Tangle è molto adatta a migliorare le interazioni tra le macchine, che si prefigge di raggiungere questi scopi:

- Migliorare le transazioni machine-to-machine;
- Facilitare l'IoT;
- Supportare l'integrità delle informazioni;
- Permettere i micro-pagamenti a livello planetario;
- Fornire un'infrastruttura comune alle applicazioni bisognose di scalabilità e di sistema decentralizzato.

La criptovaluta Iota: l'utilizzo della criptovaluta Iota vuole essere intesa come il miglior sistema, in termini di affidabilità, decentralità ed efficienza nelle transazioni (M2M). Attraverso questo token, viene sostituita la Blockchain con la tecnologia DAG. Pertanto, si risconteranno benefici di zero commissioni e elevata scalabilità.

Scalabilità: Tangle è un sistema molto scalabile, nel quale ogni nuova transazione emetterà l'autenticazione di due precedenti. In questo modo, si creerà un network che per definizione è altamente scalabile. Inoltre, il sistema sarà sempre più efficiente a man mano

che si aggiungono nuovi utenti, a differenza della blockchain che diventa sempre più complesso ogni volta che viene aggiunto un nuovo blocco.

Transazioni Offline: Tangle permette le transazioni offline. Queste sono permesse attraverso l'uso di sub-tangles, che può permettere il riattacco al Tangle principale una volta che il nodo potrà ritornare online.

Rischi di attacco sulle Blockchains: come si è visto precedentemente, si possono insinuare nel network dei nodi disonesti, per attaccare la blockchain con il double-spending. In Tangle questo è impossibile, grazie alle sue proprietà resistenti quantistiche. Infatti, l'assenza dei miners può essere vista come un a garanzia all'attacco del sistema e quindi che il network sia molto sicuro.

Evoluzione della Blockchain

Nei paragrafi precedenti si è illustrato quanto sia fondamentale l'utilizzo della Blockchain all'interno del criptomondo e come questa tecnologia si stia affermando in tutti i settori industriali, finanziari e governativi.
Concludendo è utile riepilogare l'evoluzione di questa tecnologia *disruptive*:

- Blockchain 1.0: questa tecnologia supporta le criptomonete come bitcoin; è definita dagli esperti in materia come una grande innovazione che rivoluzionerà il modo di gestire gli affari economici dei governi e delle istituzioni;
- Blockchain 2.0: questa è un'evoluzione della precedente, e viene adibita agli *smart contracts* su Ethereum. Su questa piattaforma è possibile definire un'applicazione, e farla funzionare all'interno della Blockchain. Quest'innovazione ha ampissime opportunità che possono migliorare la diffusione della ricchezza e ridurre il protezionismo. Inoltre, può offrire soluzioni per la vita reale, ad esempio registrare i voti durante una campagna elettorale, mettendo a disposizione transazioni trasparenti e molto altro;
- Blockchain 3.0: qui la tecnologia precedente mantiene le sue specificità, ma ha avuto un'evoluzione interessante per quanto riguardo il consenso. Infatti, vengono eliminati i miners nella fase di consenso e viene applicata la tecnologia DAG. Qui la Blockchain prende il nome di Tangle, creata dall'informatico canadese Buterin. Inoltre, questa tecnologia ha la pretesa di allacciarsi con l'IoT, creando così un mondo più interconnesso.

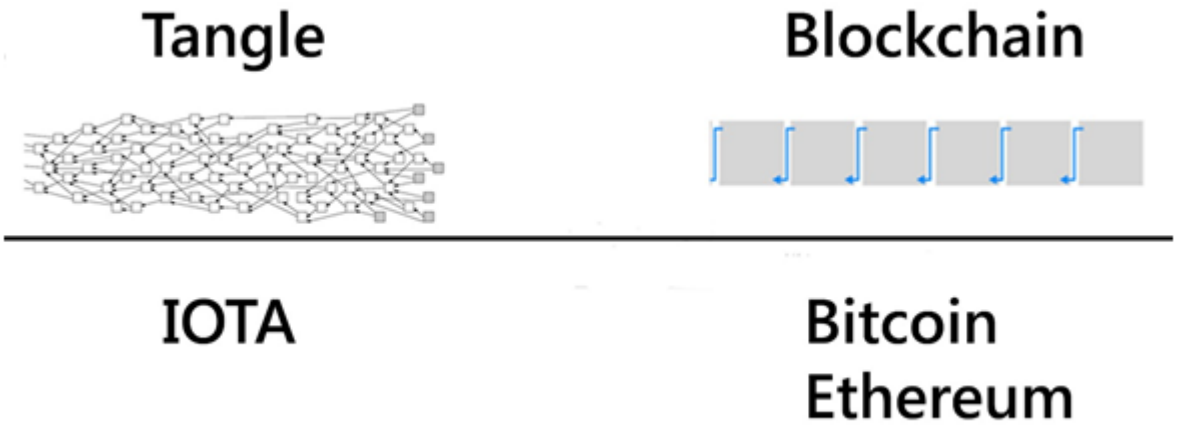


Figura 2.21 Differenze tra le diverse Blockchain. Fonte Url: "https://www.iotaitalia.com/about/".

Proof-of-Stake

Il creatore di Bitcoin, Satoshi Nakamoto, ha rivelato al mondo l'enorme potenzialità della Blockchain. In particolare, quella piattaforma che utilizza per il consenso delle transazioni il PoW. Ci sono state molte critiche su questo tipo di autenticazione, quali ad esempio l'enorme quantità di energia computazionale utilizzata e l'inscalabilità del sistema (la conferma delle transazioni avviene circa dai 10-60 minuti), e la maggior parte del mining avviene in certe parti del mondo, dove l'energia elettrica è economica (Cina e Islanda).
Per questi motivi si è cercato un metodo alternativo per ovviare a questi limiti, e si è creato il *Proof-of-Stake* (PoS).
In questo metodo di consenso un nodo cerca di investire nei token del sistema, piuttosto che investire in elaboratori specifici per l'estrazione dei blocchi. Così diventando il "validatore" del sistema. Da evidenziare che attraverso questo metodo, non esiste più la creazione dei token, ma bensì le monete elettroniche esistono fin dall'inizio e i validatori (chiamati anche stakeholder, perché detengono una partecipazione del sistema), sono remunerati attraverso le commissioni di transazioni. Più specificatamente, la possibilità di un validatore di esser scelto per la creazione di un blocco successivo dipenderà solo dalle monete possedute. Quindi ad esempio uno che possiede 1000 monete avrà una probabilità cinque volte maggiore di esser scelto rispetto ad uno che ne ha 200.
Dopodiché, una volta che il validatore ha creato il blocco, questo sarà aggiunto nella blockchain. A tal proposito, ci sono diversi metodi di PoS. Nel *Tendermint* ogni nodo firmerà sul blocco, fin tanto che non verrà raggiunta la maggioranza dei voti, mentre in altri sistemi verrà scelto un gruppo causale di firmatari.
A questo punto può sorgere il problema del *Nothing-at-Stake* cioè che validatore vuole creare due blocchi e rivendicarne le commissioni delle transazioni e/o un firmatario che vuole firmarli entrambi. Il sistema cerca di scoraggiare questo tipo di ad esempio chiedendo al validatore di bloccare i propri token in un caveau virtuale; se il validatore provasse a raddoppiare o a sborsare il sistema, quelle monete verrebbero prese.
La prima criptovaluta ad adottare questo metodo fu la Peercoin. Attualmente Ethereum sta ancora utilizzando il PoW, ma come si è già accennato nel primo capitolo, anche questa sta pianificando il sistema PoS dagli inizi del 2018.

Proof of Concesum Algorithm

L'algoritmo di consenso di Ripple Protocol (RPCA), viene applicato da tutti i nodi presenti nel network ogni pochi secondi, con lo scopo di mantenerlo corretto. Quando viene raggiunto il consenso, il registro corrente sarà considerato *chiuso* e questo diventerà l'ultimo registro chiuso. Assumendo che il (RPCA) abbia avuto successo, e che non ci sia un fork nel network, l'ultimo registro chiuso sarà mantenuto da tutti i nodi presenti sulla rete e sarà identico. L'RPCA procede ad intervalli (round), definiti come segue:

- inizialmente, ogni server accetta tutte le transazioni valide presenti sul network e che richiedono ancora il consenso (si possono trovare nuove transazioni avviate da utenti finali del server, transazioni detenute da un precedente processo di consenso, ecc.) e li rende pubblici in forma di elenco, denominato *Set Candidato*;
- ogni server quindi fa un aggregato dei set candidati di tutti i server sul suo UNL[120] e vota la veridicità di tutte le transazioni;
- le transazioni che ricevono una percentuale di voti positivi più maggiore di un valore di soglia, passano alla fase successiva, mentre le transazioni che non ricevono abbastanza voti verranno scartati, o inclusi nei set candidati per l'inizio del processo di consenso sul prossimo registro.
- l'ultima fase di consenso richiede una percentuale minima dell'80% di UNL di un server che accetta una transazione. Tutte le transazioni che soddisfano questo requisito sono inserite nel registro che successivamente verrà chiuso, diventando l'ultimo nuovo registro chiuso.

[120] Unique Node List (UNL): Ogni server mantiene un UNL, che è un set di altri servers che sono in coda nella determianzione del consenso. Solo i voti degli altri membri del UNL dei server sono cosniderati quando si determina il consenso (in contrapposizone di ogni nodo sul network). Così il UNL rapresneta un subset del network che quando viene preso collettivamente, è "fidato" dal server non collude ad un tentativo di frodare il network. Fonte "The Ripple Protocol Consensus Algorithm" Schwartz, Yungs, Britto. Pag.3.

Griglia comparativa

Analisi Tecnologica	Criptovalute				
	Bitcoin	***Etherem***	***Ripple***	***Stellar***	***Iota***
Simbolo					
Nascita	03-gen-09	30-lug-15	2012	2014 (dal protocollo di Ripple)	11-giu-16
Blockchain	1.0	2.0	2.0	2.0	3.0
Procedura di Consenso	PoW	PoW	PcA	PoS	DAG
Mining	Sì	Sì	No	No	No

Tabella 2.3 Griglia Comparativa delle diverse tecnologie utilizzate dalle diverse Criptovalute. Analisi del 18 aprile 2018, ore 17:26.

Nella tabella 2.3 vengono comparate le cinque criptovalute in base alla tecnologia impiegata per permettere il loro funzionamento. Quello che emerge è il grado di evoluzione del criptomondo. In particolare, si può notare come la Blockchain, impiegata nel mondo delle monete digitali, si sia evoluta nell'arco di questi nove anni; senza trascurare anche i vari meccanismi di conferma ed autenticazione delle transazioni. Tuttora, il sistema Bitcoin con il suo relativo token, rimane la moneta più diffusa ed utilizzata nel mondo, questo può essere spiegato dal fatto che Bitcoin è stato il precursore di questo mercato. Tuttavia, le altre monete prese in esame, e più in generale tutto il sistema delle criptomonete, potrebbe soppiantarla. Questo può accadere per motivi tecnologici da una parte (il fatto che si aggiunga il termine "1.0-3.0" è un segno distintivo), e dall'altra per motivi di accettazione da parte dei grandi player a livello mondiale (governi e istituzioni), perché hanno un carattere decisamente meno *anarchico*.

Ad ogni modo, quello che risulta lampante è la continua evoluzione della tecnologia, volta a superare i limiti della precedente, puntando sempre di più alla perfezione. Per tali motivi, questa analisi potrà essere soppiantata nel futuro e che quindi potranno sorgere altri sistemi più evoluti e più performanti.

Capitolo III – La Crypto economy

In questo capitolo verrà affrontato l'impatto delle criptovalute sull'economia, nel linguaggio tecnico questo tema viene denominato: Crypto economy.
Come si vedrà nel corso dei paragrafi, le valute digitali hanno intaccato, con profondi cambiamenti, l'economia reale dando vita a un sistema che prima non esisteva.
Inizialmente si studierà com'è composto il criptomondo, ossia di quali figure è costituito il suo ecosistema, per poi analizzare l'utilizzo empirico di una criptovaluta, quindi come ottenerla e come usarla nell'economia reale. Successivamente verranno analizzate le cinque criptomonete prese in esame in termini economici: si esamineranno le componenti di prezzo e capitalizzazione di mercato, cercando di analizzare i comportamenti del mercato. Infine, negli ultimi paragrafi si esaminerà da una parte l'implementazione della tecnologia Blockchain nell'economia e dall'altra un nuovo metodo di finanziamento alternativo a quelli tradizionali, ovvero il crowdfunding delle criptovaluta: la ICO.

L'Ecosistema del Criptomondo

Il criptomondo ha creato un proprio ecosistema, in cui diversi attori interagiscono tra di loro infatti, prima dell'avvento del Bitcoin, non c'era nulla di tutto questo.
Di seguito verranno elencate le principali figure che si trovano per ogni criptovaluta. Ovviamente certe eccezioni che possono variare da una all'altra, come ad esempio i miners che si trovano solamente in alcune di esse.

- Inventori/sviluppatori: sono coloro che creano le monete digitali e sviluppano il network sottostante. In alcuni casi questi vengono identificati sotto delle organizzazioni, mentre in altri rimangono sconosciuti, come per esempio Bitcoin. Questi possono rimanere anche dopo l'avvio della moneta per la gestione e il miglioramento continuo e anche per contribuire al decentramento. Questa funzione può essere svolta anche da enti ben organizzati (fondazioni o società), in cui il decentramento può è essere più o meno accentuato.
- Emittenti: sono coloro che sono in grado di generare dei nuovi token. Il volume totale dell'emissione può essere o predeterminato o dipende dalla domanda. Questo dipende da due fattori:
    - In monete virtuali centralizzate, l'emittente può essere anche l'amministratore e decide lui le regole e ha anche l'autorità per riprendere i token in circolazione. Dopo che sono stati emessi nuovi token, vengono distribuiti agli utenti, tramite la vendita o distribuendoli gratuitamente.
    - In monete virtuali decentralizzate, i nuovi token vengono creati automaticamente, come risultato del lavoro dei miners, i quali riceveranno la loro ricompensa sotto forma di nuovi token.
- Miners: sono persone che rendono disponibile volontariamente il proprio computer per convalidare un insieme di transazioni (denominato *blocco*), fatto con le valute digitali decentralizzate ed aggiunto al registro dei pagamenti (denominato *Blockchain*). I miners possono anche cooperare tra di loro, lavorando in gruppi ben organizzati. Senza i miners, le valute digitali decentralizzate non potrebbero funzionare correttamente perché potrebbero sorgere i problemi della doppia spesa (double-spent) o semplicemente dei falsi token potrebbero facilmente essere immessi nel sistema. Per il loro lavoro vengono ricompensati

tramite il trasferimento di nuovi token. Si adopera il termine *miners* perché viene fatta l'analogia con le persone che spendono tempo ed energia per l'estrazione di minerali preziosi dal sottosuolo. Inoltre, la ricompensa può derivare da una nuova emissione automatica decentralizzata o da un trasferimento dall'emittente. In aggiunta, i miners possono richiedere anche una commissione della transazione da coloro che vogliono fare una verso un altro utente.

- I fornitori di servizi di elaborazione: sono coloro che facilitano il trasferimento di unità da un utente all'altro. Questi li si trova nelle valute digitali centralizzate perché in quelle decentralizzate questi servizi vengono annoverati dal lavoro dei miners.
- Utenti: scelgono di possedere valuta digitale per l'acquisto di beni e servizi sia virtuali che reali da commercianti favorevoli alle criptomonete, possono effettuare transazioni da un utente all'altro anche da enormi distanze (per esempio transfrontaliera) o inviare rimesse o per scopi di investimento (inclusa la speculazione).

  Ci sono cinque modi per ottenere token:

  - acquistarli;
  - lavorare in attività che vengono remunerate con valute digitali (ad esempio: compilando sondaggi);
  - svolgere l'attività del miner, svolgendo il mining, cosicché da auto-generare nuovi token;
  - ricevere token come mezzo di pagamento;
  - ricevere token come donazione o regalo.
- I fornitori di wallet: offrono agli utenti un portafoglio digitale per conservare le loro chiavi crittografiche della valuta digitale e codici di autenticazione delle transazioni avvenute. Ci sono due tipi di portafoglio, che differiscono per la loro immediata usabilità contro la loro sicurezza dal cyber-crimine:

  - portafogli online (archiviazione a caldo);
  - Portafogli offline (archiviazione a freddo).

  Funzionalmente questi servizi sono offerti per pc, mobili e applicazioni che utilizzano il cloud. Ad ogni modo, gli utenti possono utilizzare un proprio portafoglio senza fare uso di un fornitore di portafoglio.

- Exchanges: offrono servizi di trading agli utenti, quotando i tassi di cambio con i quali lo scambio comprerà/venderà valuta digitale rispetto alle principali valute tradizionali (Dollaro americano, Renmimbi, Yen, Euro), o contro altre valute digitali. Generalmente, questi exchanges accettano una vasta gamma di opzioni per il pagamento, tra cui contanti, bonifici e pagamenti con altre valute digitali. Inoltre, questi exchanges offrono servizi statistici (quali ad esempio: volumi scambiati e volatilità).
- Le piattaforme di trading: funzionano come i mercati, dove gli acquirenti e venditori di criptovalute si incontrato e gli viene fornito una piattaforma su cui è possibile contrattare il prezzo. A differenza degli Exchanges, le piattaforme di trading non si impegnano nell'acquistare o vendere loro direttamente. Alcune di esse, come ad esempio: "Localbitcoins.com", offrono il servizio ai loro utenti, di localizzare i potenziali clienti nelle vicinanze.
- Vari altri attori: sono tutti coloro che non sono specificati nell'ambiente del criptomondo, come: commercianti, facilitatori di pagamento (aiutano i commercianti nell'e-commerce, nell'accettazione di monete digitali come metodo di pagamento), sviluppatori di software (per il settore trading e di archiviazione), produttori di hardware per i computer (per il settore Mining), produttori di ATM, i broker (per il settore finanziario, per agevolare gli investimenti in start-up e progettare specifici prodotti finanziari, ad esempio scambi nei fonti (ETF) o derivati), i tumbler (che forniscono un servizio per aumentare ulteriormente l'anonimato del pagatore, rendendo più difficilmente scopribile la provenienza della transazione avvenuta in valuta digitale).

Criptovaluta in azione

In questo paragrafo verrà analizzata la questione sicurezza in relazione al mondo delle criptovalute. In particolare, questa verrà illustrata nei tre aspetti collegati all'uso di tale valuta: come si ottengono, dove detenerla e come trasferirla. Per facilità espositiva, si farà riferimento principalmente a Bitcoin, essendo quella più diffusa e comune, però verranno riprese anche delle altre criptovalute nel caso ci fosse delle particolarità da rimarcare.

Come si ottengono

Nel paragrafo precedente, si è visto che ci sono cinque modi per ottenere criptovalute:

- acquisto;
- lavorare in attività che vengono remunerate con valute digitali (ad esempio: compilando sondaggi);
- svolgere l'attività da miner, attraverso il mining, cosicché da auto-generare nuovi token;
- ricevere token come mezzo di pagamento;
- ricevere token come donazione o regalo.

In particolare, qui verranno analizzate il primo e il quarto punto perché sono quelli più specifici e anche quelli più significativi.

- **L'acquisto**:

Ci sono due principali modalità di acquisto per una valuta digitale:

  - acquisto diretto;
  - in cambio di beni e servizi (questo verrà ripreso nel paragrafo del trasferimento).

A sua volta l'acquisto diretto può avvenire con differenti modalità tra cui la più diffusa è quella di ricorrere al servizio di cambiavalute (exchange service). In dettaglio, ci possono essere exchange fisici o online, e questi svolgono lo stesso lavoro dei cambiavalute tradizionali, ovvero accettare la valuta fiat per ottenere in cambio quella digitale.

- Exchange online: è la modalità più diffusa e sul web si possono trovare differenti servizi, abbastanza simili tra di loro, ma che presentano differenti standard di affidabilità. Questo perché non esiste un registro pubblico ed ufficiale dei cambia

valute, ad oggi chiunque può svolgere questa attività di intermediazione. Pertanto, bisogna informarsi ex-ante sull'affidabilità del exchange, è molto consigliato verificare sui forum appositi il rating del servizio, quindi ridurre il rischio di possibili truffe. Ad esempio, il gruppo Bitcoin-Italia, rintracciabile sui social network, è un buon modo per iniziare. Ad ogni modo, i più importanti e conosciuti exchange online sono: Bitstamp, The Rock Trading, Coinbase. Ogni servizio è differente dall'altro, dai costi di gestione del servizio al costo di vendita/acquisto delle criptovalute. Infatti, questo ultimo punto è assai cruciale, perché diversamente dalle valute fiat, dove esiste un prezzo universalmente riconosciuto, invece sulle piattaforme che trattano le criptovalute, ci possono essere anche delle importanti differenze di prezzo. In particolare, questo è stato analizzato da uno studio del Sole 24 ORE, nell'articolo di dicembre 2017, in cui si sono analizzate le oscillazioni superiori ai $ 2,000 tra una piattaforma e l'altra.

- Exchange fisici: ovvero sono soggetti fisicamente presenti che svolgono il ruolo di venditore. Questi potrebbero essere delle persone che vendono i propri bitcoin oppure un intermediario che svolge abitualmente questo lavoro, ad ogni modo il rischio è inversamente proporzionale alla loro affidabilità. A venir in soccorso ci sono delle community, come ad esempio *Localbitcoin*, dove è possibile lasciare un feedback garantendo così l'affidabilità dei traders. Qui il prezzo varia in base all'affabilità del venditore e il metodo di pagamento utilizzato. In particolare, è stata creata un'impresa nella provincia di Trento, in cui l'imprenditore vende token ed articoli connessi. L'obiettivo dell'impresa è di diventare un cambiavalute a norma di legge, ossia rispettare le normative più stringenti come ad esempio la compilazione di un documento apposito per acquistare più di € 50 di bitcoin.
- ATM: si tratta di apparecchiature simili agli sportelli bancomat, dove è possibile inserire denaro (o carte di credito) e successivamente verranno inviati bitcoin sul proprio wallet (con o senza registrazione, dipendentemente dal Paese e dal modello di ATM). Questa modalità è ampiamente diffusa all'estero, in Italia ce ne sono a malapena una ventina, e principalmente diffuse nel nord Italia. Questa alternativa offre il vantaggio dell'immediatezza, per contro avere prezzi e commissioni più alte degli exchange.
- In cash: *Bitboat*: esiste un servizio italiano, con sede a Londra, che offre la possibilità di acquistare le valute digitali in contanti, evitando così l'incontro tra

acquirente e venditore, grazie alla piattaforma offerta da *Bitboat*. La piattaforma di scambio consente l'acquisto di più criptovalute di cui è possibile effettuare l'ordine online e successivamente effettuare il pagamento in una ricevitoria convenzionata entro la scadenza dell'ordine.

Come conservarli

Prima di effettuare l'acquisto di una criptovaluta è doveroso fornirsi di un portafoglio elettronico (denominato *Wallet*), in cui possibile conservarli ed effettuare le operazioni. Questo wallet non è altro che l'interfaccia personale dell'utente sulla rete della criptovaluta posseduta, simile al conto corrente, in cui vengono custodite password, codici segreti e stringhe di numeri attraverso cui l'utente può effettuare le operazioni. La conservazione delle criptovalute è uno dei momenti più importanti e delicati, perché chiunque venga a conoscenza della password potrà impiegare irreversibilmente il portafoglio. Similarmente anche lo smarrimento delle credenziali di accesso renderà impossibile l'accesso al contenuto del wallet, proprietari compreso. Giusto per dare un'idea di questo fenomeno, i risultati di uno studio effettuato a novembre e dicembre 2017, hanno riportato lo smarrimento circa tra i 2.78 e i 3.79 milioni di bitcoin, ossia circa il 17% - 23% dei bitcoin esistenti, per un valore odierno che si aggira sui $ 32.696 miliardi[121] .

Lo smarrimento della criptovaluta può avvenire per diversi motivi: dimenticare la password, subire un danno hardware dell'hard disk, smarrire o farsi rubare il device in cui era custodita. Ci sono divere modalità di conservazione delle criptovalute, ognuno di esse è un'alternativa all'altra.

Di seguito vengono elencati i differenti wallet:

Online wallet:

Questo servizio viene offerto dai siti web che permettono di memorizzare e custodite in un server online. Questa può essere una buona alternativa alla problematica dello smarrimento della password, anche se comporta notevoli rischi: pericolo di accessi abusivi, l'affidabilità della piattaforma e la garanzia nel tempo. Come si è già detto più volte, i portali e le piattaforme online sono da sempre nel mirino dei cyber-criminali. A tal

[121] Prezzo di bitcoin: $ 8,626.98, in data 13 maggio 2018, 17:17.

proposito non si può non citare i più importanti e famosi furti di bitcoin sui portali online: agosto 2011 a MyBitcoins (sparizione del exchange), agosto 2012 a Bitcoin Saving and Trust (FBI individua uno schema a Ponzi), febbraio 2014 a Mt. Gox (rubati 700 mila bitcoin), agosto 2016 a Bitfinex (rubate le criptomonete, ma almeno qui gli utenti ricevettero un risarcimento del 36%)[122], dicembre 2017 a NiceHash (vengono rubati token per un valore approssimativo di € 70 milioni) e gennaio 2018 a Coincheck (il più grande maxi-furto della storia di bitcoin fino ad 'ora, per un valore di $ 580 milioni)[123]. Un ulteriore fattore di rischio della piattaforma online è che non sia gestita nel rispetto della legalità, ovvero che vengano agevolate attività criminali e/o commettendo il reato di riciclaggio. Quindi se la piattaforma online dovesse finire sotto sequestro è altamente probabile che il denaro investito diventi indisponibile.

Software Wallet:

Sono portafogli che vengono installati su dispostivi elettronici, come computer, cellulari e tablet. Le password sono dei codici segreti, ma visto che la sicurezza è legata al sistema in cui girano, sono più facili da eludere rispetto ad un hardware wallet. Ci sono differenti wallet, che dipendono dalla scelta: di sistema operativo e dal tipo di criptovaluta utilizzata. Alcuni sono improntati sulla sicurezza, mentre altri sulla privacy degli utenti. Anche in questo caso non sono di certo mancati casi di furto. Inoltre, è da considerare la sicurezza e la stabilità del sistema in cui viene installato il wallet software, in caso di crash del sistema, tutto il wallet sarà perduto, per cui sarà utile fare sistematici backup di sistema.

Hardware wallet:

Probabilmente è uno dei metodi più sicuri, in cui viene utilizzato un dispositivo fisico su cui è possibile gestire direttamente il controllo, ad esempio su una chiavetta USB o proprio i wallet hardware predisposti. Questo portafoglio è un dispositivo elettronico ideato solo allo scopo di utilizzare la criptovaluta. Infatti, antecedentemente al pagamento di una transazione, questa deve essere autorizzata dall'hardware wallet, in cui sono contenute le chiavi private dell'utente. Queste ultime vengono custodite offline, al sicuro e protette da

[122] Per approfondimenti si rimanda a: "http://www.fastweb.it/web-e-digital/truffe-furti-bitcoin/".
[123] Per maggiori approfondimenti si rimanda a: "https://it.businessinsider.com/un-maxifurto-da-500-milioni-di-dollari-in-criptovalute-innesca-la-grande-fuga-da-bitcoin-co/".

possibili attacchi malware. I principali vantaggi dell'utilizzo di questo portafoglio rispetto al software wallet sono:

- le chiavi private sono custodite in un ambiente sicuro e protetto, dove non è possibile esportarle come un testo;
- i device sono immuni ai virus creati per rubare le chiavi dai software wallet;
- piena sicurezza nell'utilizzazione senza dover trascrivere il codice, come viene fatto per la conservazione cartacea;
- utilizzo di software open source;
- possibilità di utilizzare strumenti di recupero in caso di furto, smarrimento o crash hardware.

Tutt'ora è forse il metodo più sicuro tra quelli presenti sul mercato, tuttavia è bene ricordarsi che vi è sempre la possibilità di attacchi come ad esempio sofisticati malware.

Paper Wallet:

Le chiavi possono essere conservate e custodite anche su un supporto cartaceo, cosicché si possa rimanere al sicuro da possibili cyber-attacchi e da possibili malfunzioni hardware. Ci sono due modi per creare un paper wallet: stamparne uno da un Online wallet che ne offre la possibilità, oppure in alternativa utilizzare il sito internet *bitaddress.org*. Nel concreto il paper wallet non è altro che un pezzo di carta, in cui vengono stampati gli indirizzi e le chiavi private. L'indirizzo può essere utilizzato anche solo per conservare le criptovalute e controllare il saldo, semplicemente inserendolo su *blockchain.info*. Attraverso il sito internet: *bitaddress.org*, si può creare un paper wallet senza aver la necessità di installare sul proprio computer un software apposito.

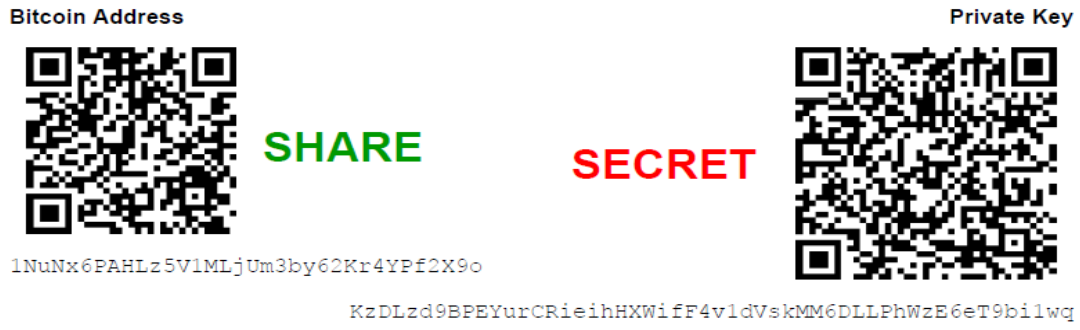


Figura 3.1 Un esempio di un Paper Wallet. Fonte Url: " www.bitaddress.org".

Nella figura 3.1 viene mostrata la generazione della coppia di chiavi, pronta per esser stampata e ponderatamente conservata. Per visionare il saldo del proprio paper wallet si può accedere al sito internet: *blockchain.info*.
Invece, per spendere le monete digitali, si deve utilizzare un software che permetta di effettuare delle transazioni oppure direttamente creando un account sul sito citato in precedenza. Finché il paper stampato rimane al sicuro e nascosto da occhi indiscreti, le criptovalute contenute all'interno del wallet saranno solidamente al sicuro.

Trasferimento

Nella fase di trasferimento il denaro virtuale viene spostato da un conto all'altro seguendo diverse modalità. La transazione va buon fine quando la chiave e l'indirizzo coincidono, tutto questo viene gestito ovviamente dal wallet che rende agevole l'operazione. Infatti, si possono effettuare pagamenti utilizzando il codice QR. Alcune criptovalute riescono a gestire questa fase in maniera del tutto trasparente, infatti chiunque può venire a conoscenza sia del wallet d'origine che del destinatario, come accade per il Bitcoin. Mentre altri riescono a rendere in anonimato o il solo il destinatario, o entrambi.
Da sottolineare che a prescindere dal metodo prescelto, la transazione viene registrata irrevocabilmente, e che quindi non sia più consentito ritornare indietro. Proprio per questo che il tema della sicurezza è un elemento fondamentale, perché in questo settore non esiste sia la tutela del consumatore che del venditore.

L'Escrow:
Per risolvere il problema della fiducia tra il venditore e l'acquirente, nell'attesa temporale della transazione, è nato un servizio di garanzia delle transazioni: l'*escrow* che letteralmente viene tradotto come *deposito di garanzia*. Questo è un servizio del tutto legale e trasparente e viene utilizzato nelle transazioni internazionali. Il suo obiettivo principale è proteggere il livello di fiducia tra l'acquirente e il venditore, specialmente quando non si conoscono. Quindi nel caso specifico, l'acquirente invece di pagare antecedentemente un prodotto, lascerà il denaro in garanzia del pagamento all'escrow, dopodiché il venditore procederà alla consegna del prodotto, e per ultimo il denaro sarà versato dal escrow al venditore dopo che l'acquirente avrà confermato di aver ricevuto il bene. L'*escrow service* è un soggetto bipartisan e per il suo lavoro avrà un compenso monetario in proporzione al valore dell'affare.

Nello specifico ci sono due tipi di escrow: l'*escrow hidden* e per l'appunto *escrow service*. L'unica differenza che si trova nei due è che nel secondo è possibile verificare l'affidabilità dell'escrow stesso, attraverso i feedback lasciati dai precedenti utenti. Questa caratteristica risulta fondamentale nel dark web, dove altrimenti sarebbe troppo rischioso effettuare pagamenti. Ciononostante, non si ha nessuna certezza della sicurezza dell'affare perché è possibile che l'escrow utilizzato sia corrotto e/o colluso.

Criptovalute ed anonimato:

A differenza di quanto si può leggere sul web, non tutte le criptovalute sono dei sistemi di pagamento anonimi. Si può prendere per esempio Bitcoin, il quale non lo è per eccellenza, perché proprio grazie al suo sistema che impedisce il problema del double-spending (ovvero la rete attiva il sistema di marcatura temporale peer-to-peer, assegnando degli identificatori sequenziali ad ognuna transazione, per poi concatenarle nei blocchi), riesce a costruire una sorta di *timeline* di tutti i movimenti di tutti i token generati, dall'indirizzo del loro creatore fino all'ultimo proprietario, così facendo le transazioni sono perfettamente tracciabili.
Tuttavia, esistono due metodi che permettono l'anonimato nelle transazioni:

- il primo è quello di servirsi di nuovi indirizzi per ogni pagamento ricevuto;
- il secondo è quello di utilizzare differenti wallet, rendendo molto più difficile (ma non impossibile) la correlazione trai i vari indirizzi e le transazioni. Questo lo si può attuare grazie ai seguenti strumenti:
    - Dark Wallet: realizzato da Cody Wilson, ed offre un servizio del tutto irrintracciabile delle transazioni in BTC;
    - Mixing service (o Tumbler): sono dei servizi che riescono a mescolare le transazioni di diversi utenti.

Questi servizi, che nel tempo sono stati presi d'assalto dagli utenti che volevano rimanere nell'anonimato, ultimamente hanno avuto un'inversione di tendenza verso altre nuove valute digitali, le quali sono focalizzate verso la tutela della privacy degli utenti. A riguardo si può citare Monero (XMR), questa criptovaluta basa il PoW su un particolare algoritmo: *CryptoNight* e la propria blockchain su *CryptoNote*. Questa particolare blockchain rappresenta un'evoluzione della classica blockchain di Bitcoin ed è orientata verso ad una maggiore tutela alla riservatezza, infatti le transazioni memorizzate sono quasi anonime.

La blockchain è sempre un registro pubblico distribuito e anche se vengono registrate tutte le transazioni dei token, ma non è consentita la tracciabilità degli stessi. Le uniche persone ad avere pieno accesso a tutte le informazioni sono proprio l'acquirente e il venditore.

Il criptomondo nell'economia reale:

Nel corso degli ultimi anni il numero degli esercenti che accettano criptovalute è aumentato esponenzialmente, soprattutto nel corso del 2017 registrando un aumento di circa del 50%. Di seguito verranno mostrate due figure, dove vengono rappresentate il numero degli esercenti: una del 2014 e l'altra in data attuale.

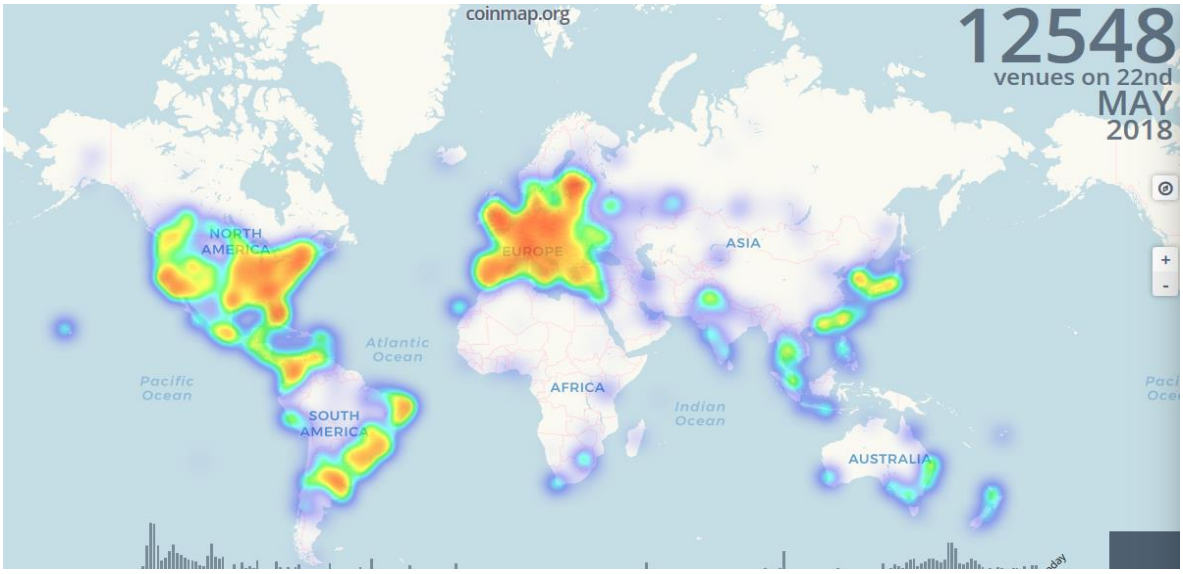


Figura 3.2 Rappresentazione grafica del numero degli esercenti che accettano BTC nel 22 maggio 2018. Fonte Url: "www.coinmap.org".

Nella figura 3.2 viene mostrato il numero totale degli esercenti che accettano il BTC come metodo di pagamento. Attualmente sono 12,548 punti. Nella figura sottostante (3.3), invece, viene mostrato il numero totale nel 2014, dove erano poco più di 2,000.

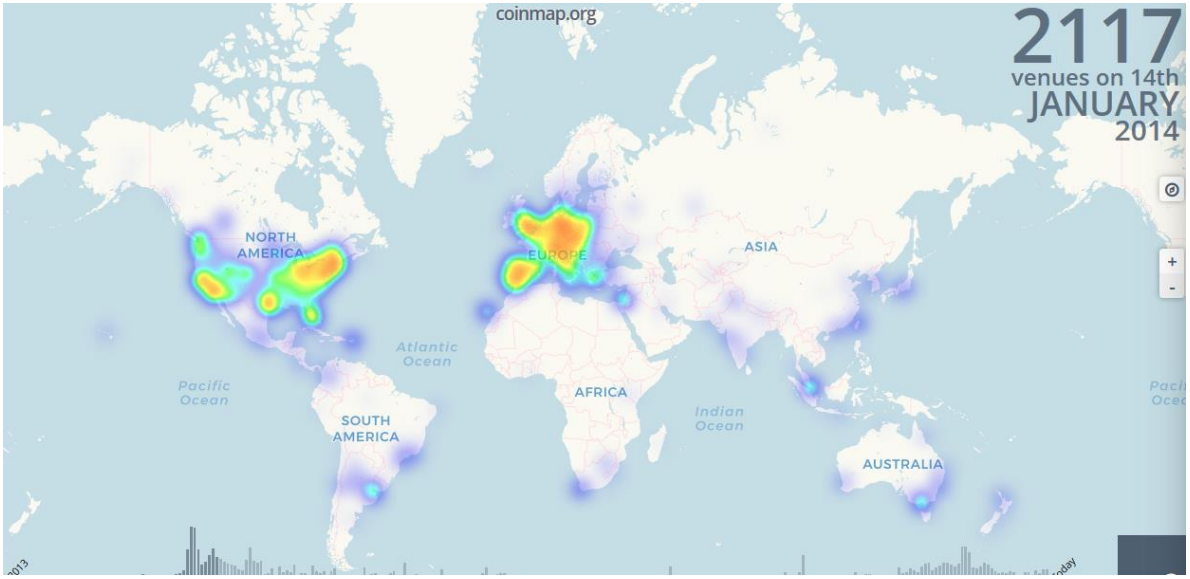


Figura 3.3 Rappresentazione grafica del numero degli esercenti che accettano BTC nel 14 gennaio 2014. Fonte Url: "www.coinmap.org".

Come si evince dalle figure soprastanti, l'accettazione della criptovaluta nel mondo reale è abbastanza rapida e, contando che il BTC ha solamente nove anni di vita, ha registrato una grande espansione, contro ogni prognostico. Basti rammentare, come si è detto già nel primo capitolo, che nel 2010 venne fatta una transazione di 10,000 BTC per effettuare l'acquisto di due pizze, a dimostrazione della praticità di tale metodo.

Le Criptovalute in termini economici

In questo sotto paragrafo verranno analizzate le criptovalute, in maniera dettagliata e puntuale, sotto il punto di vista prettamente economico. In particolare, questo paragrafo verrà suddiviso ulteriormente in altri 4 sotto paragrafi nei quali verranno studiate le componenti economiche di ognuna di esse.

L'andamento dei prezzi

In data 23 aprile 2018 alle 11:05, sono state analizzate le seguenti criptovalute registrandone i prezzi e la capitalizzazione di mercato:

Cryptocurrency	Market Cap	Price	Ranking per Market Cap
Bitcoin	$ 151,597,302,525	$ 8,920.44	1°
Ethereum	$ 63,154,974,805	$ 637.96	2°
Ripple	$ 34,381,307,832	$ 0.878805	3°
Stellar	$ 6,954,925,885	$ 0,374532	8°
Iota	$ 5,930,433,607	$ 2.13	9°

Tabella 3.1 Tabella riassuntiva della capital. di mercato e dei prezzi, delle diverse criptovalute prese in esame. Fonte Url: "https://coinmarketcap.com/".

Come si può evincere dai dati in tabella, ognuna delle monete digitali prese in considerazione sta cercando di ritagliarsi un proprio spazio all'interno del mercato. In generale, la somma delle capitalizzazioni di mercato di ognuna porta a un risultato pari a $ 262,018,944,657, ossia circa al 66% di tutto la capitalizzazione di mercato dell'intero criptomondo ($ 397,224,735,238). Per avere un termine di confronto, queste cifre possono essere paragonate al Pil lordo della Danimarca ($ 306.9 Mld nel 2016)[124], mentre l'intero cripto-mondo al Pil lordo della Norvegia ($ 371.075 Mld nel 2016)[125].

[124] Fonte Url: "https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DK".
[125] Fonte Url: "https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=NO".

La grandezza di questi numeri fa aumentare sempre più l'attenzione verso questo delicato tema. Si è voluto utilizzare "delicato" per via delle complicazioni che hanno sull'impatto economico mondiale. Di seguito verranno illustrate le serie storiche dei prezzi relativi a ognuna delle cinque criptovaluta analizzate. Quindi il discorso verrà ripreso tramite tabelle adibite per riportare, oltre all'andamento dei prezzi, anche la deviazione standard relative ad esse.

<u>Bitcoin (BTC)</u>:

Grafico 3.1 L'andamento del Prezzo e Market Cap di bitcoin. Fonte Url: "https://coinmarketcap.com/currencies/bitcoin/#charts".

Dal grafico 3.1 si possono osservare gli andamenti storici del prezzo, della capitalizzazione di mercato e del volume di transazioni avvenute nelle ultime 24 ore. In realtà, il grafico inizia dal 28 aprile 2013 e questo può essere spiegato sotto la *ratio* di *rilevanza*, ossia inizierebbe a rappresentare quando il prezzo per ogni singolo BTC aveva raggiunto la soglia di circa $ 100. Infatti, è dai primi aprile 2013 che il prezzo raggiunge la soglia dei $ 100 a token. Invece, la prima quotazione avviene il 18 agosto 2010 per la cifra di soli $ 0.074. Ovviamente questi importi sono la media dei maggiori exchanges di bitcoin. Solamente nel 2017 si è registrata un'esplosione per questo token e più in generale di tutto il criptomondo, raggiungendo il picco massimo dei $ 19,290 a token il 17 dicembre 2017. Difficile spiegare la ratio dietro a questi movimenti *schizofrenici*, sicuramente come hanno affermato alcuni economisti, a dicembre si era registrata una bolla speculativa di

dimensioni bibliche. Sicuramente questo ha tagliato fuori le stesse persone che puntavano ad un alto rendimento, attraverso la realizzazione di una plusvalenza.
Il prezzo è dettato dal mercato, vale a dire dalla legge di domanda e offerta, dove in particolare si ha una correlazione positiva della domanda e del prezzo. Ovvero, quando ci sarà un aumento della domanda del token ci sarà anche un aumento del prezzo, e viceversa. Mentre l'offerta del bitcoin, ovvero la creazione del token, avviene tramite il processo di mining, in cui viene estratto dai miners. Ricordando che questo processo decrescita progressivamente fino ad azzerarsi, per questo motivo l'offerta è rigida e priva di correlazione con la variazione della domanda. Questo procedimento differisce sensibilmente con le valute legali, nelle quali si trova un ente centrale, dove viene gestita la coniazione di nuova moneta, in caso di necessità.
In realtà pur avendo ormai nove anni di vita, è solo negli ultimi anni che questa moneta digitale (e più in generale di tutto il criptomondo) è stata presa in considerazione. Questo perché essenzialmente la gente comune non sapeva e solo tuttora sta iniziando a comprendere realmente la sua potenzialità. In aggiunta, si deve riportare anche il tema della speculazione che ha portato il prezzo del token intorno ai $ 20,000 lo scorso dicembre 2017. Inoltre, a riportar il prezzo in discesa sono anche complici le informazioni nefaste che arrivano sia dall'interno del criptomondo sia dall'esterno. In particolare, dall'interno quando ad esempio si verificano dei furti negli exchanges, dall'esterno quando per esempio ci sono delle dichiarazioni ufficiali da parte dei soggetti regolatori o dall'alta finanza. Proprio per questi motivi speculativi il prezzo della criptovaluta registra una fortissima volatilità, in cui nei momenti di crescita (soprattutto quella esponenziale) sembra quasi inarrestabile per via del fascino che attrae nuovi investitori all'acquisto dei token, portando il prezzo a cifre inimmaginabili rispetto a poche ore prima. Successivamente, questo subirà una correzione verso il basso proporzionale o più che proporzionale a quella che l'ha fatta ascendere, per via del comportamento degli investitori che vogliono disfarsi dei token per realizzare immediatamente una corposa plusvalenza (per ora ancora esentasse). Questo procedimento è similare a quello dello scoppio di una bolla finanziaria, ed è proprio per questo motivo che molti economisti l'avevano paragonata allo scoppio del bulbo di tulipano del 1600.

Ethereum (ETH):

Grafico 3.2 L'andamento del Prezzo e Market Cap di Ethereum. Fonte Url: "https://coinmarketcap.com/currencies/ethereum/#charts".

Nel grafico 3.2 viene mostrato l'andamento dei prezzi e la capitalizzazione di mercato di Ethereum, e in più in particolare del token Ether. Inoltre, qui Ether viene comparato al corrispettivo prezzo in BTC. Questa moneta digitale ha una vita più breve rispetto al bitcoin, ma dal grafico si può derivare un andamento simile all'altra. In effetti, questa particolarità la si trova anche negli altri token, ossia il similare ciclo di vita delle criptovalute. Questo tema verrà ripreso più avanti.

In ultima analisi, si può evidenziare un aumento del prezzo che, dopo il crollo di inizio anno, sta registrando un andamento positivo.

Ripple (XRP):

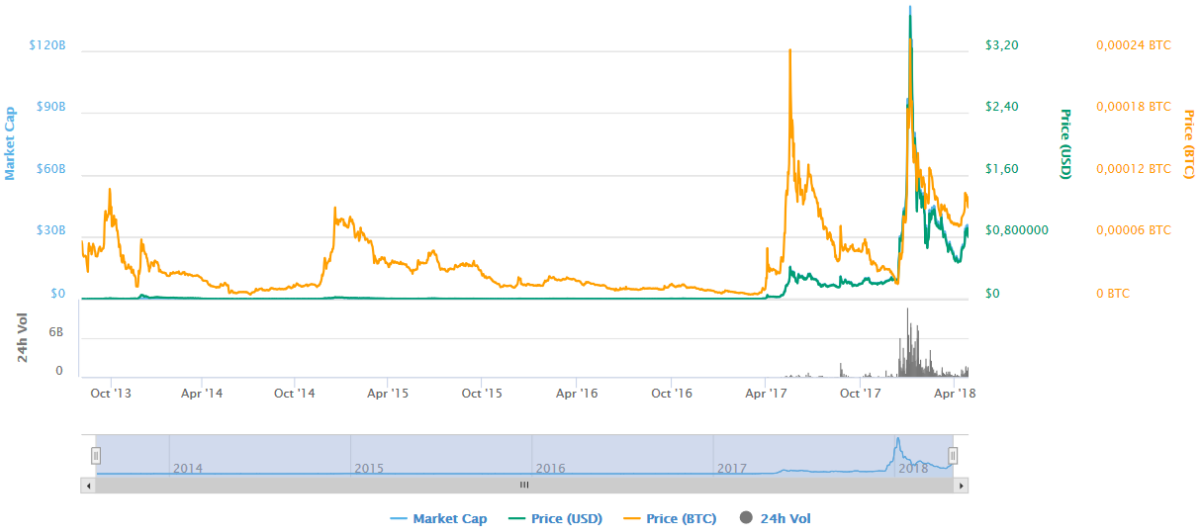


Grafico 3.3 L'andamento del Prezzo e Market Cap di Ripple. Fonte Url: "https://coinmarketcap.com/currencies/ripple /#charts".

Nel grafico 3.3 si può notare l'andamento del prezzo e la capitalizzazione di mercato di Ripple, o meglio del relativo token: XRP. Anche qui si il token viene comparato con il prezzo di bitcoin.

Stellar (XLM):

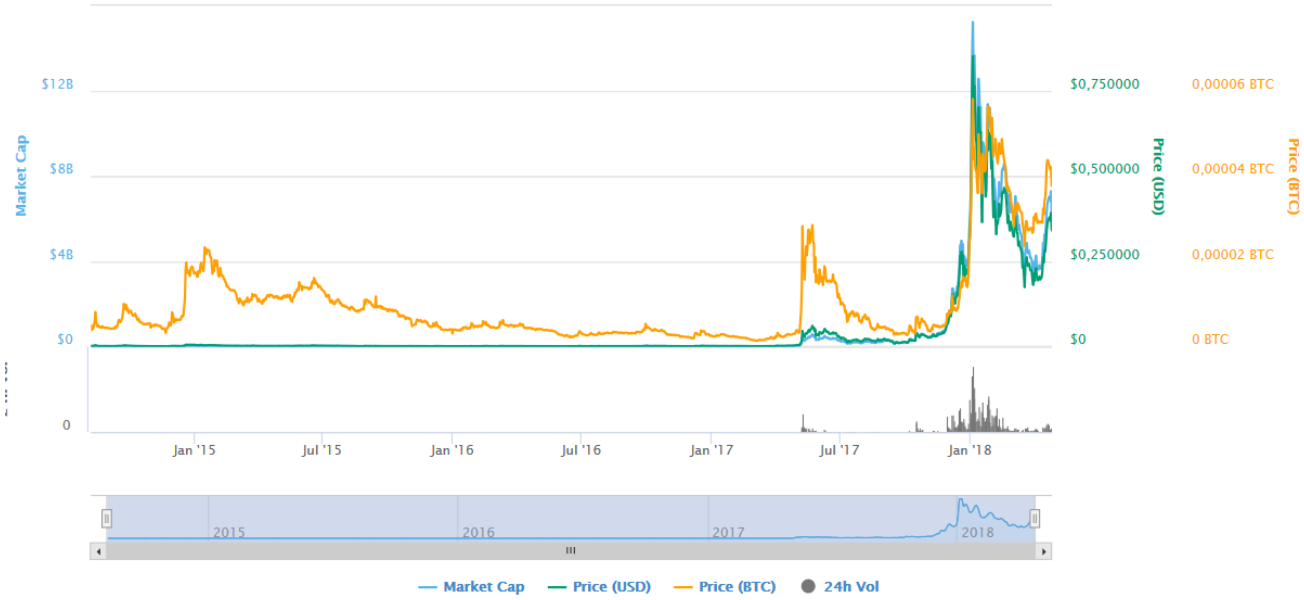


Grafico 3.4 L'andamento del Prezzo e Market Cap di bitcoin. Fonte Url: "https://coinmarketcap.com/currencies/stellar/#charts".

Nel Grafico 3.4 vengono illustrati l'andamento del prezzo e la relativa capitalizzazione di mercato di Stellar che dopo la vertiginosa impennata di fine 2017 ha registrato un crollo nei premi mesi del 2018, anche se attualmente sta avendo un andamento positivo.

IOTA (MIOTA):

Grafico 3.5 L'andamento del Prezzo e Market Cap di IOTA. Fonte Url: "https://coinmarketcap.com/currencies/iota /#charts".

Nel 3.5 viene evidenziato l'andamento del prezzo e la relativa capitalizzazione di IOTA. Questo token rispetto alle altre quattro monete digitali è la più giovane in termini anagrafici, ma rispetto alle altre si può notare come l'andamento del prezzo abbia subito un'accelerazione dovuta al fatto che il criptomondo è stato "accettato" a livello globale. Esattamente come per le altre monete, anche qui c'è stata un'impennata vertiginosa a fine 2017 per poi riportare il token al suo prezzo sgonfiato dalla speculazione.
Da notare, probabilmente per via della giovane età, come il prezzo di MIOTA non è più ritornato al periodo pre-bolla e, anche se questa ha seguito l'andamento delle altre, attualmente sta registrando un andamento positivo.

In conclusione, i token analizzati evidenziano il ciclo di vita delle criptovalute. Più precisamente, quando vengono prese in esame le valute digitali più anziane, quali: BTC, ETH e XRP, si può notare come la nascita di queste avvenga molto lentamente. In particolare, si registrano dei prezzi sotto il dollaro proprio ad indicare l'inizio dell'accettazione del token sul mercato. Questo fenomeno è diverso se si prende in esame l'ultima criptovaluta: IOTA che è stata legittimata dal mercato in tempi assai più rapidi rispetto alle cugine. Come si era detto precedentemente, questo può esser ricondotto sia all'accettazione del criptomondo dal pubblico sia dalla tecnologia che rappresenta questo token.

Il prezzo dei token aumenta, così come la loro quota di mercato, solo dopo che il pubblico inizia ad apprezzarli e a utilizzarli in maniera massiccia. Da notare che per Ripple, come per altre monete digitali, il prezzo è basso rispetto al bitcoin ed Ether pur essendo un grande player nel criptomondo. Questo può esser spiegato dall'assenza della procedura del Mining, quindi non vengono estratti nuovi token da quel processo; infatti, qui è proprio l'ente privato che ne rilascia il giusto quantitativo in base all'andamento del prezzo e dal tasso di inflazione. Per questo motivo, a differenza di bitcoin e di Ether (questo probabilmente potrà cambiare quando si attuerà il passaggio dal PoW al PoS) qui l'offerta di domanda non è rigida ma il prezzo dei token di Ripple, Stellar e Iota viene determinato anche dall'offerta. Come per bitcoin, anche tutto il cripto-mondo ha conosciuto l'esplosione speculativa di fine 2017 che ha portato a prezzi astronomici, per poi trovare un prezzo sgonfiato, così depurando il prezzo dagli speculatori. In effetti, l'andamento di una valuta digitale influisce positivamente su tutto il settore delle criptovalute soprattutto quando ci sono notizie negative che ruotano intorno ad esse. In generale, il mondo sta iniziando veramente a capire il loro funzionamento e le loro potenzialità; probabilmente si assisterà a dei prezzi meno volatili quindi questa economia potrà diventare più stabile e sicura.

Volatilità storica

La misura del rischio nel possedere degli asset finanziari, e in questo caso dei token, viene espressa dalla sua volatilità storica[126] che si riferisce alle oscillazioni storiche del prezzo, ossia una sorta di *timeline* dell'andamento dei prezzi.

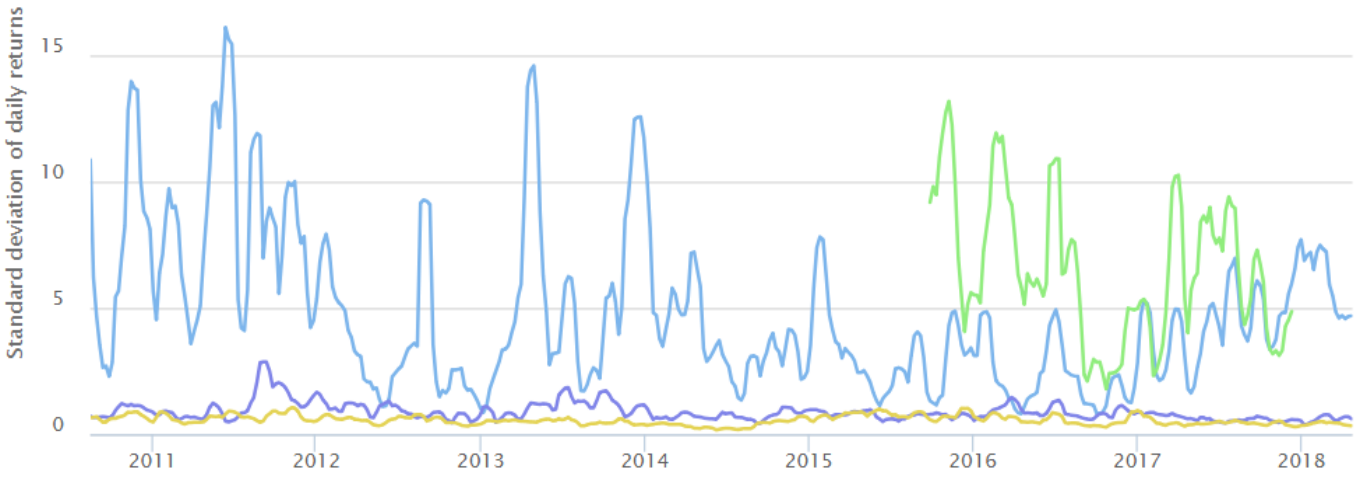


Grafico 3.6 Rappresentazione della volatilità dei prezzi di: BTC, ETH, Dollaro e Oro.
Fonte Url: "https://www.buybitcoinworldwide.com/it/indice-di-volatilita/".

Dalla figura 3.6 viene mostrata la deviazione standard su base mensile, relazionata alla *timeline* (da agosto 2010 ad aprile 2018), dove da una parte si trovano i token: BTC e ETH, e dall'altra il Dollaro e l'Oro. Queste monete digitali vengono comparate alle valute legali, quali il Dollaro, perché il criptomondo vorrebbe imporsi come metodo alternativo nelle transazioni. Inoltre, nel grafico si trova anche la comparazione con l'Oro, questo perché i token vengono impiegati anche come riserve di valore.

Da questa analisi emerge il rischio nel detenere queste valute digitali, e lo si capisce maggiormente dalla comparazione con il Dollaro e l'Oro.

Nel prossimo grafico verranno riprese anche le altre tre criptovalute che verranno comparate ulteriormente con l'Oro.

[126] Definizione: la volatilità è una misura della variazione percentuale del prezzo di uno strumento finanziario nel corso del tempo. La volatilità storica deriva dalla effettiva serie storica dei prezzi misurabile nel passato. La volatilità implicita deriva dal prezzo di mercato delle opzioni dello strumento finanziario analizzato, per scadenze future attualmente scambiate. Il simbolo σ viene utilizzato per la volatilità, e corrisponde alla Deviazione standard.
Fonte Url: "https://it.wikipedia.org/wiki/Volatilit%C3%A0_(economia)".

Dal grafico 3.7 emerge maggiormente come siano volatili i prezzi delle criptovalute e di conseguenza quanto siano rischiosi.

Da sinistra verso destra viene illustrato: l'oro (13.8837%), BTC (407.6872%), ETH (161.0406%), XRP (276.6944%), XLM (271.9726%) e MIOTA (85.3159%).

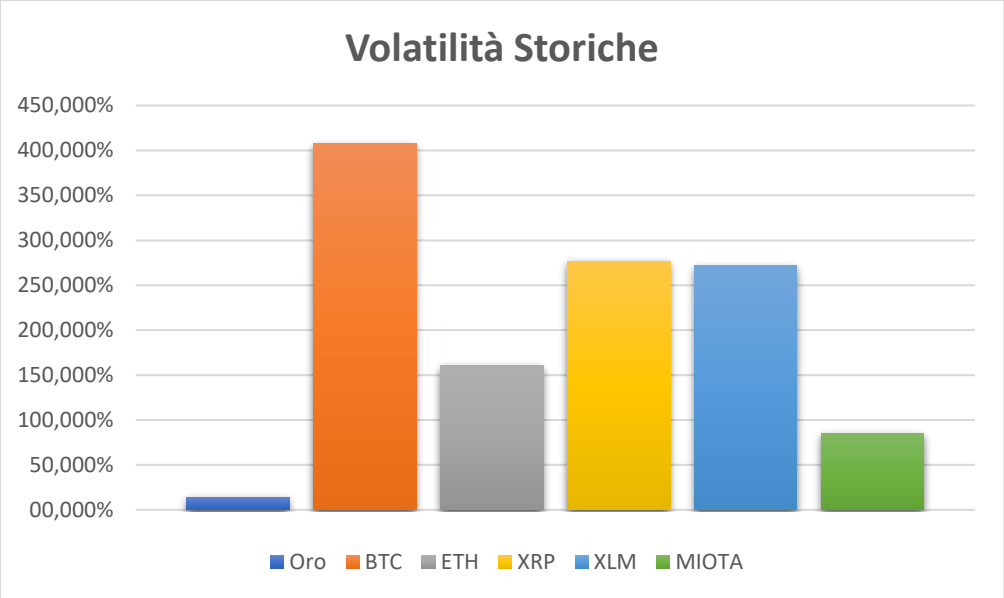


Grafico 3.7 Rappresentazione della volatilità storiche dei prezzi di: BTC, ETH, XRP, MIOTA e dell'Oro. Dal 18 agosto 2010 al 25 aprile 2018. I dati delle criptovalute sono state prese da: "https://coinmarketcap.com/"; mentre i prezzi dell'oro da: "https://www.gold.org/".

Nuovamente dal grafico 3.8 viene rappresentata graficamente la comparazione dei prezzi delle quattro valute digitali con l'Oro e l'indice di S&P.

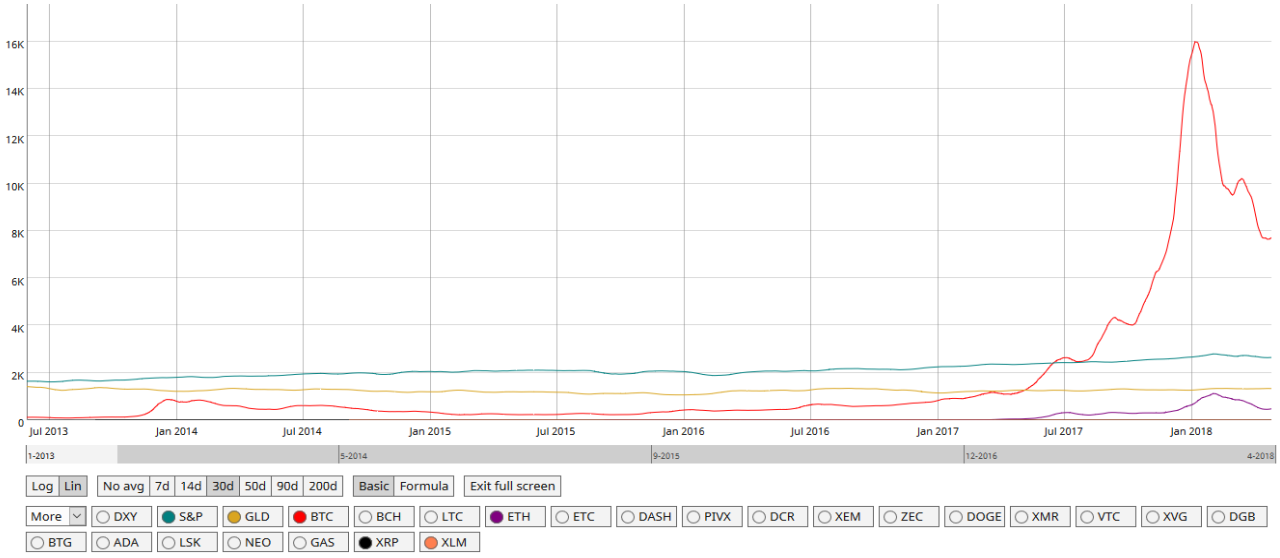


Grafico 3.8 Rappresentazione grafica della comparazione dei prezzi, dove da una parte ci sono le criptovalute: BTC, ETH, XRP, XLM, e dall'altra: l'Oro e S&P. Fonte Url: "https://coinmetrics.io/charts/#assets=btc".

Come si è già detto precedentemente, tutto il criptomondo è stato affetto dalla speculazione dei mercati soprattutto il bitcoin. Il token che si distingue è Miota (IOTA), perché ha avuto un'oscillazione dei prezzi inferiori agli altri token, così registrando una volatilità più bassa. A riguardo possono essere influiti due fattori principali: la giovane età della moneta digitale (il criptomondo era più aperto a nuovi token) e la tecnologia (ovvero Tangle) che rappresenta intrinsecamente. Infatti, come si era detto poc'anzi, quest'ultima ha registrato un iniziale ciclo di vita differente rispetto alle altre criptomonete.

I fattori determinanti del prezzo

Il prezzo delle criptovalute può essere determinato da diversi fattori, e in aggiunta ognuna è influenzata differentemente in base alle proprie caratteristiche. A tal proposito, è utile ricordare che il bitcoin e l'Ether vengono generati dal processo del Mining e, come più volte detto, il prezzo viene influenzato solamente dalla domanda poiché l'offerta è anelastica.

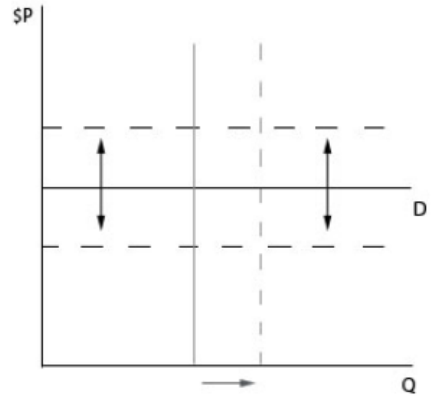


Figura 3.4 Rappresentazione grafica della determinazione del prezzo per il bitcoin.
Fonte Url: "Bits and Bets Information, Price Volatility, and Demand for Bitcoin" Buchholz, Delaney, and Warren.

Nella figura 3.4 si può distinguere la retta verticale (offerta) completamente rigida, mentre l'unica retta che può spostarsi è quella orizzontale (domanda), ed è questa che può alzare o diminuire il prezzo. Questo avviene perché appunto l'immissione di nuovi token nel sistema avviene indipendentemente dal prezzo.

Dunque, la diffusione di questa moneta digitale avviene perché viene accettata dal pubblico, e lo fa perché ne riconosce del valore intrinseco del token stesso. Secondo un'indagine di mercato condotta dal forum di Bitcoin, gli utenti che utilizzano la moneta digitale lo fanno per i seguenti principali motivi:

- scientifici e tecnologici (dal carattere disruptive),
- sociali (dal carattere "anarchico" e contro i sistemi centralizzati),
- tecnici della funzionalità (praticità nell'utilizzarla nella vita quotidiana).

Mentre i fattori che possono influire sulla determinazione del prezzo, sono:

- La regolamentazione dei governi,
- La diffusione di notizie positive/negative,
- L'ampia accettazione dei token nelle transazioni nell'economia reale,
- Il costo del mining,
- Numero delle transazioni,

- ❖ Scopi speculativi (caratteristica principale che comporta maggiore instabilità nel breve periodo).

A quanto si è detto finora, non lo si può traslare anche per le altre criptovalute, perché sono profondamente differenti. Come si era già descritto nel primo capitolo, ogni criptovaluta presa in analisi ha le sue particolarità sia dal punto di vista strutturale che dall'accettazione sul mercato. Senza tralasciare le valute digitali che non utilizzano il PoW come metodo di conferma delle transazioni, e che quindi non vi è l'estrazione di nuovi token lasciati come premi per i miners. Infatti, l'immissione delle nuove monete avviene Step-by-Step, in modo da tenere sotto controllo l'inflazione.

Numero delle transazioni e volumi scambiati

BITCOIN:

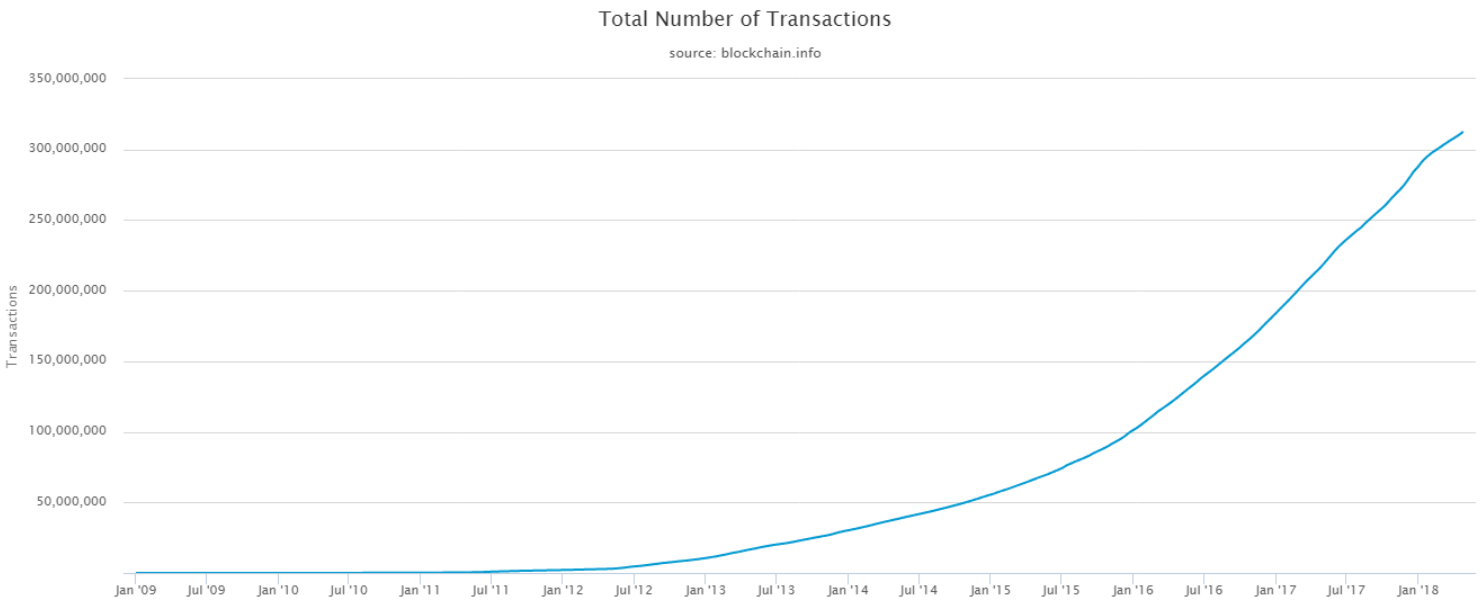


Grafico 3.9 Rappresentazione grafica del numero totale delle transazioni di bitcoin. Fonte Url: "https://blockchain.info/it/charts/n-transactions total?timespan=all".

Dal grafico 3.9 si evince l'aggregato totale del numero delle transazioni avvenute all'interno della Blockchain di Bitcoin. Questo grafico inizia dal 2009 e arriva al 20 aprile 2018 con un volume pari a 312,252,902 di transazioni.

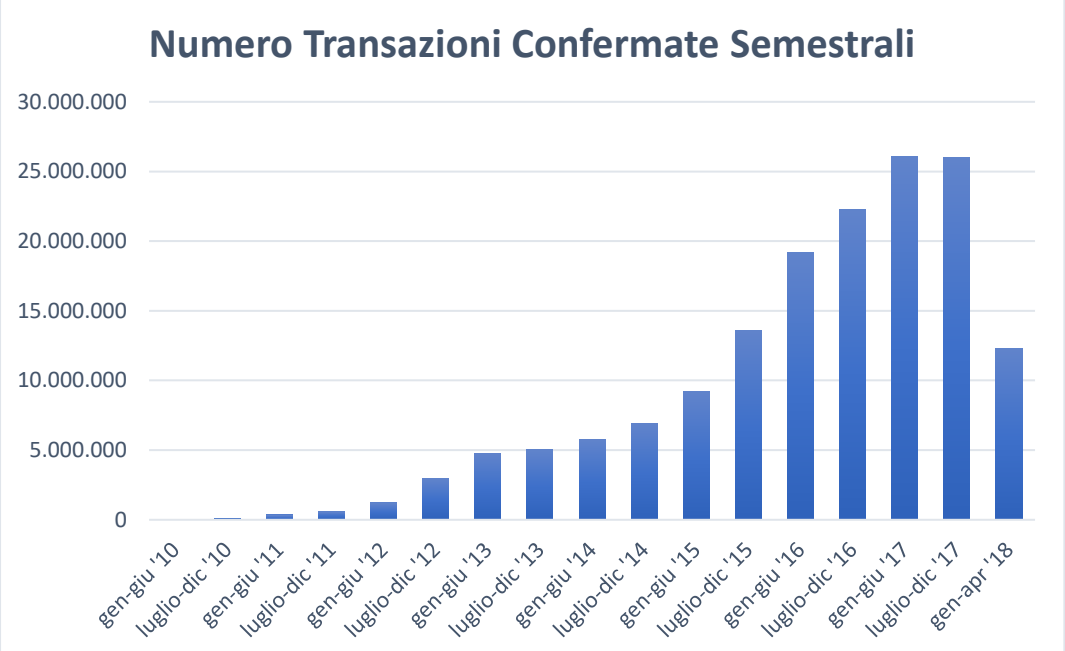


Grafico 3.10 Rappresentazione grafica del Volume di transazioni confermate semestrali, dal periodo: 1° gennaio 2010 al 24 aprile 2018. Fonte Url: "https://blockchain.info/it/charts/n-transactions?timespan=all".

Dal grafico 3.10 viene mostrato il numero delle transazioni confermate a livello semestrale. Comparando sia il grafico 3.9 e 3.10, si può evincere la graduale e continua espansione del bitcoin nel tempo. In particolare, dal periodo che inizia ad apprezzarsi, superando per la prima volta la parità con il dollaro (2011), da quel momento in poi in cui questa moneta digitale viene presa seriamente in considerazione dal mondo.
Da evidenziare le differenze dei due grafici soprastanti, nel primo viene raffigurato il volume aggregato di tutte le transazioni che si sono svolte, invece nel secondo viene mostrato quella parte di transazioni del primo grafico, che sono state confermate dai miners. Infatti, la restante parte di transazioni, sono ancora in attesa di essere autenticate. Ad ogni modo, a parte certi periodo di stallo o decrescita del volume registrato nei primi anni dell'utilizzo della valuta digitale, dal secondo semestre del 2013 si è registrata una crescita continua. Fino ad arrivare all'anno 2017, dove c'è stato il boom di tutto il criptomondo, soprattutto per bitcoin, si sono registrati volumi enormi. Infine, per assistere al momento dell'esplosione della bolla, con il consecutivo crollo nei primi mesi del 2018. Da ricordare però che l'ultimo periodo non è riferito ad un intero semestre, e che quindi non è propriamente opportuno compararlo agli altri.
In data 26 aprile 2018 viene registrata un volume di transazione giornaliero pari a $ 8,970,560,000. Una cifra incredibile se paragonata a pochi anni fa. Invero, come si può notare dal grafico 3.11, i volumi delle transazioni a livello semestrale hanno avuto una vera esplosione dal secondo semestre 2017, superano la soglia dei 200 miliardi di dollari americani. Questa esplosione è avvenuta proprio in coincidenza con il boom del criptomondo, registrando prezzi ai massimi storici.

Di seguito verranno mostrate quattro rappresentazioni grafiche degli andamenti dei volumi del bitcoin. In primis, si vedrà la timeline del volume totale delle transazioni in termini di dollari americani. Successivamente, verrà analizzata la quantità di token scambiata all'interno della blockchain. Infine, attraverso queste analisi si potranno mettere in luce importanti considerazioni, utili per fare delle congetture future.

Il grafico 3.11 evidenzia il volume delle transazioni a livello semestrale dal 1° gennaio 2014 al 26 aprile 2018. Il dato lampante è l'esplosione delle transazioni dal 2017 fino ad oggi, soprattutto dal secondo semestre del 2017, ricordando quel periodo come l'avvento della bolla speculativa, dove si è registrato il picco di prezzo.

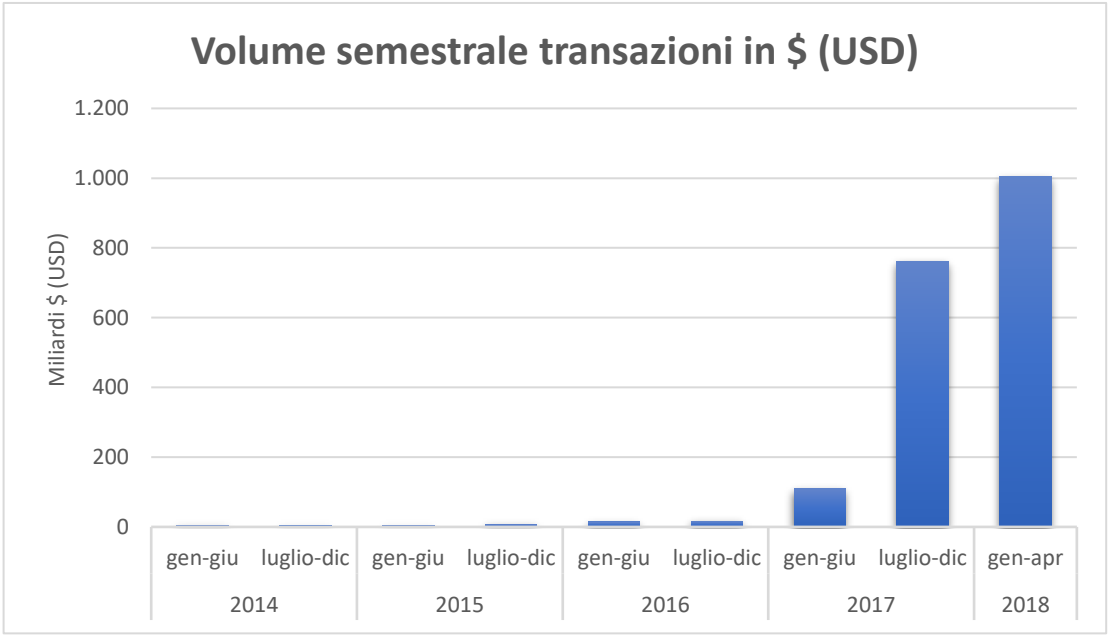


Grafico 3.11 Rappresentazione grafica dei volumi transazioni semestrali, espressi in Mld $ (USD).
Fonte dei dati reperiti Url: "https://coinmetrics.io/".

Invece, dal grafico sottostante (3.12) viene mostrato il valore totale stimato delle transazioni sulla Blockchain di Bitcoin. Ovvero, la quantità di BTC scambiata per le transazioni all'interno del sistema. In questa analisi non vengono contati i bitcoin che ritornato al venditore sotto forma di resto della transazione.

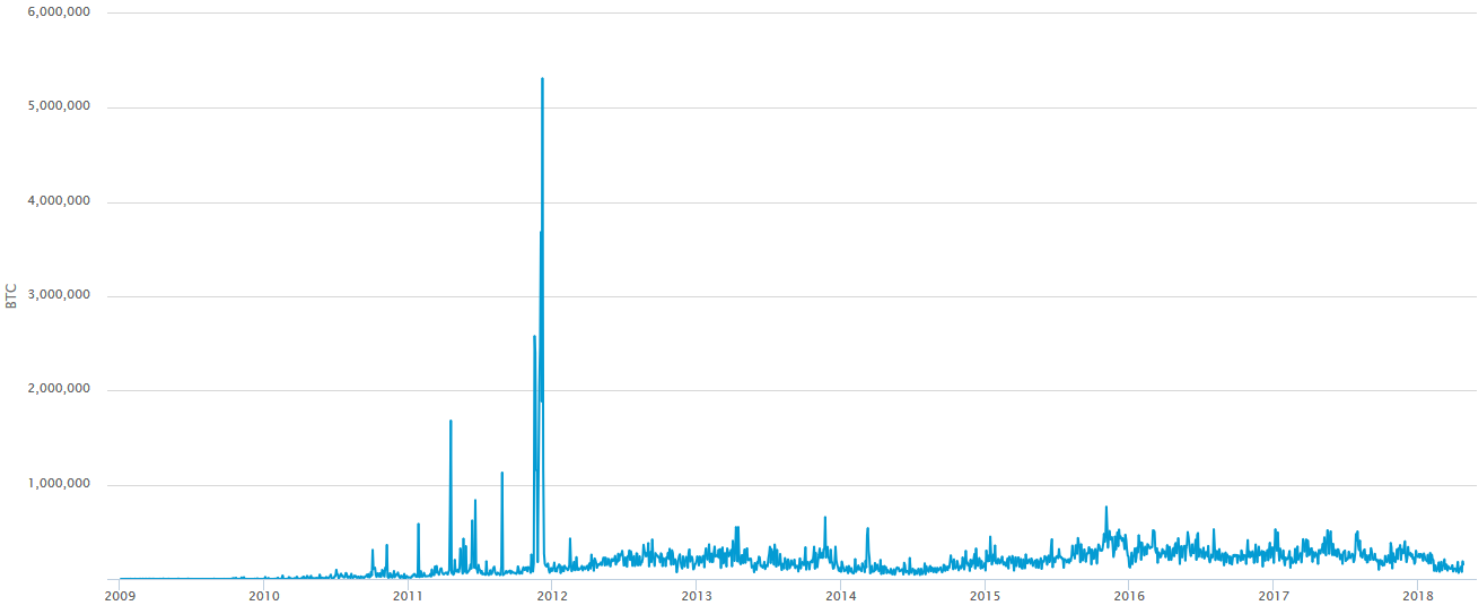


Grafico 3.12 Rappresentazione grafica del totale valore stimato delle transazioni di bitcoin sulla Blockchain.
Fonte Url: "https://blockchain.info/it/charts/estimated-transaction-volume?timespan=all".

Dalla comparazione dei grafici 3.11 e 3.12 si può evidenziare un fattore importante differenziale, ovvero l'oscillazione delle curve. In particolare, per sottolineare meglio i diversi andamenti, dal grafico 3.13 vengono analizzate le transazioni dal periodo 2014 al 2016, ovvero prima dell'anno dell'avvento speculativo.

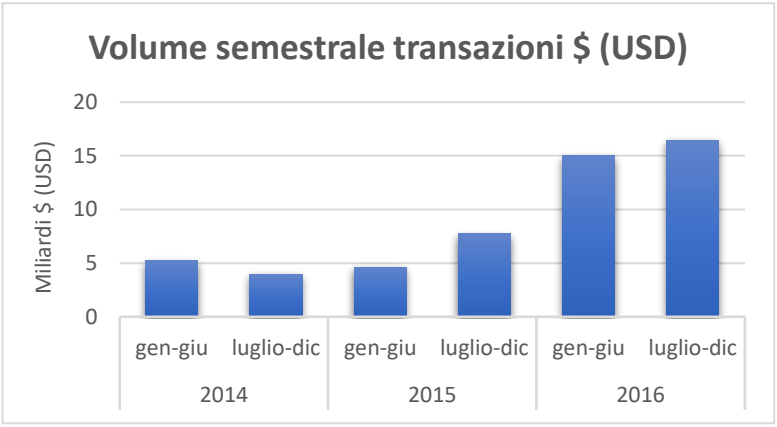


Grafico 3.13 Rappresentazione grafica dei volumi transazioni semestrali, espressi in Mld $ (USD). Fonte dati reperiti Url: "https://coinmetrics.io/".

In dettaglio, come si può evincere da questi tre grafici sopra stanti, che l'andamento oscillante del prezzo registrato in questi anni, abbia influito sui grafici 3.11 e 3.13, soprattutto nel 2017 quando si è registrata la massima speculazione (fino ad 'ora) del bitcoin. Da questa analisi risulta che l'andamento alla *random walk* dei prezzi del token non influisce anche sul grafico 3.12, ossia quello che rappresenta il numero delle transazioni e il numero dei BTC scambiati sulla blockchain, lo si può interpretare come un diverso comportamento degli attori nell'ecosistema del bitcoin.

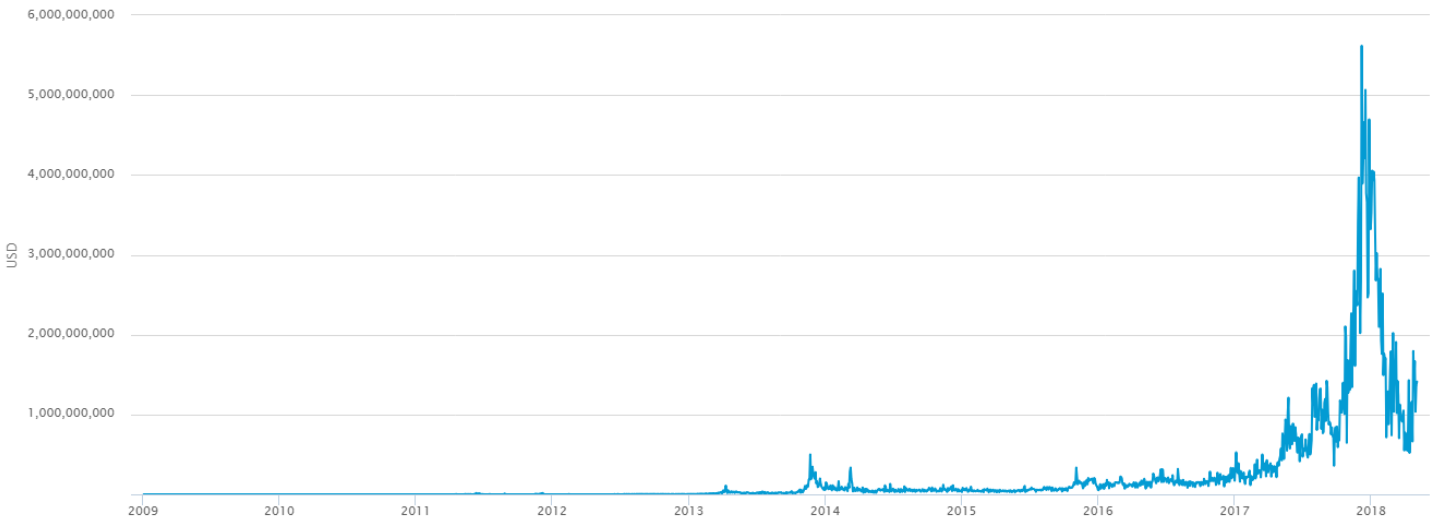


Grafico 3.14 Rappresentazione del volume stimato delle transazioni di bitcoin sulla Blockchain in $ USD. Fonte Url:" https://blockchain.info/it/charts/estimated-transaction-volume-usd?timespan=all".

Ovvero, il comportamento speculativo avviene all'interno degli Exchanges in cui un attore può trasferire la moneta digitale per effettuare una transazione effettiva, la quale sarà poi registrata sulla blockchain. In questa fase l'utente, che possiede un account digitale sull'exchange, potrà effettuare operazioni di compravendita del token attraverso accrediti o addebiti digitali di bitcoin o di valuta legale, questi movimenti verranno registrati dalla società che si occupa del exchange. Quindi l'operazione di compravendita di token, che avviene sulla piattaforma degli Exchanges non coinvolge la blockchain, ma lo farà soltanto quando qualcuno vorrà incassare i BTC dal proprio conto digitale.

Questo trova rappresentazione anche dal grafico 3.14, in cui viene rappresentato l'ammontare del volume delle transazioni in $ USD all'interno della Blockchain. Per far chiarezza, si può prendere il numero dei BTC scambiati sul network (grafico 3.12) e moltiplicarlo per il prezzo giornaliero del bitcoin (9,711)[127], si ottiene un importo di $ 1,411,348,185, ed è lo stesso del grafico 3.14.

Per maggiori chiarimenti, nei grafici sottostanti vengono mostrate le diverse oscillazioni, dove da una parte si trova il volume delle transazioni in termini di dollari americani, e dall'altra il volume delle transazioni in termini di BTC scambiati sulla blockchain.

[127] Fonte Url: "https://coinmarketcap.com", data 4 maggio 2018, ore 02:00.

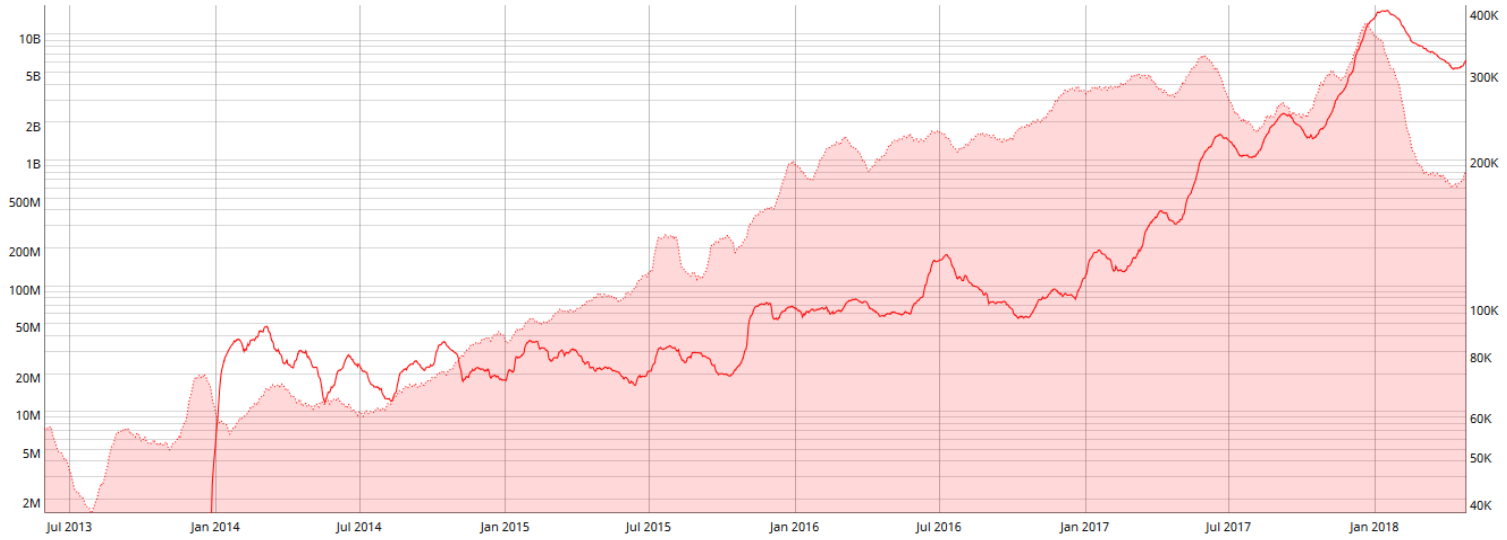


Grafico 3.15 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base mensile (30gg). Fonte Url: "https://coinmetrics.io".

Nei grafici 3.15 e 3.16 vengono comparati il volume delle transazioni negli Exchanges in $ USD (Linea Rossa) e il numero delle transazioni in BTC sulla Blockchain (Area rosa). Per maggiore coerenza con i precedenti grafici, il 3.16 è realizzato su base semestrale

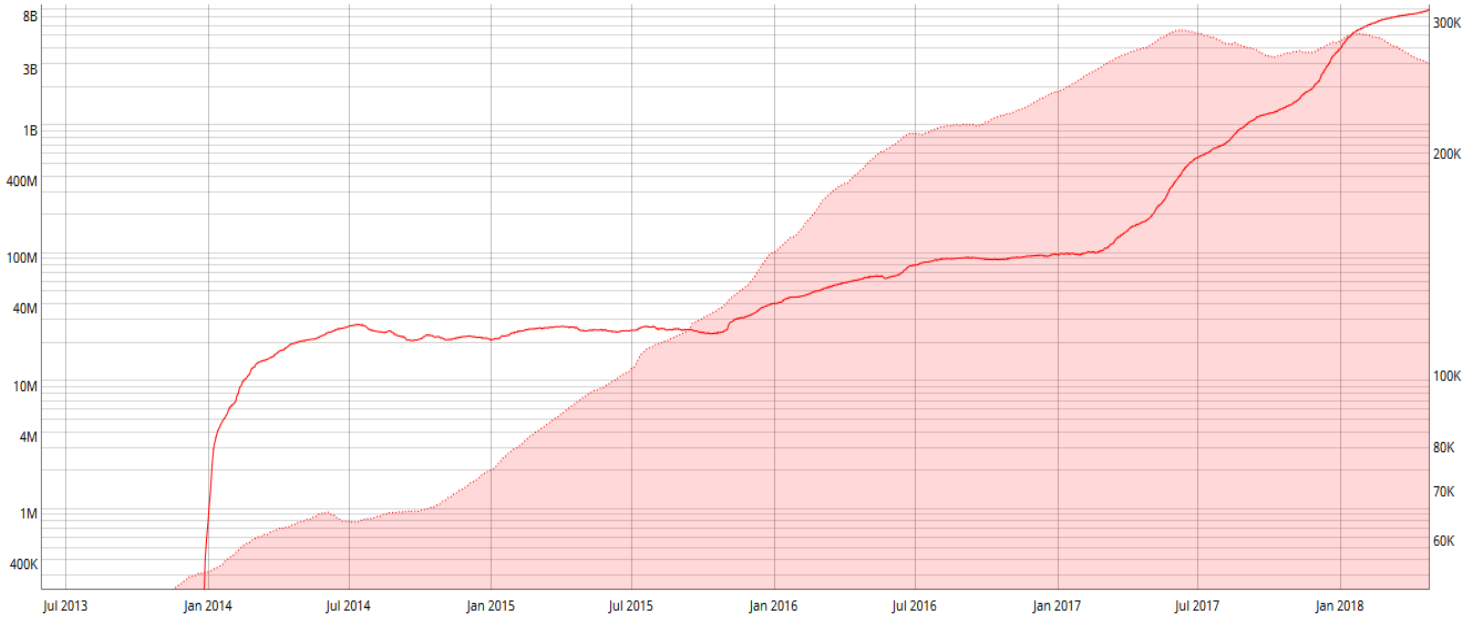


Grafico 3.16 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base semestrale (200gg). Fonte Url: "https://coinmetrics.io".

Come è stato già evidenziato precedentemente, i volumi registrati sugli exchanges (e quindi sui prezzi) hanno subito un andamento differente rispetto all'utilizzazione dei BTC per transazioni registrate sulla Blockchain.

Dal grafico 3.15, si può derivare la timeline del BTC e suddividerla in tre periodi distinti:

-Fase iniziale (dal 2013 al primo semestre 2015): il volume delle transazioni in $ (USD) è superiore al volume dei BTC scambiati, questo può rappresentare un comportamento più speculativo in cui il mercato utilizza maggiormente il bitcoin come strumento di riserva valore, sperando di realizzare una plusvalenza futura;

-Fase intermedia (dal secondo semestre 2015 alla fine del 2017): il volume dei BTC scambiati supera notevolmente il volume delle transazioni in $ (USD), questo perché è iniziata l'era della utilizzazione del token per acquisti nell'economia reale, quindi utilizzare il token come strumento monetario;

-Fase attuale (da gennaio 2018): la tendenza della fase intermedia è terminata, per ritornare al trend della fase inziale. In questa fase si può interpretare in modi differenti, da una parte come un comportamento meramente speculativo, che probabilmente gli utenti si sono scottati dopo l'esplosione della bolla speculativa del dicembre 2017, e per tal motivo in molti hanno venduto rapidamente il token per realizzare una perdita minore. Dall'altra parte, invece, gli utenti hanno forse iniziato a diffidare del bitcoin come possibile alternativa della valuta legale, magari proprio per l'avvento di altri nuovi Altcoins che sia per motivi sociali sia tecnologici sono differenti dalla capostipite.

ETHEREUM:

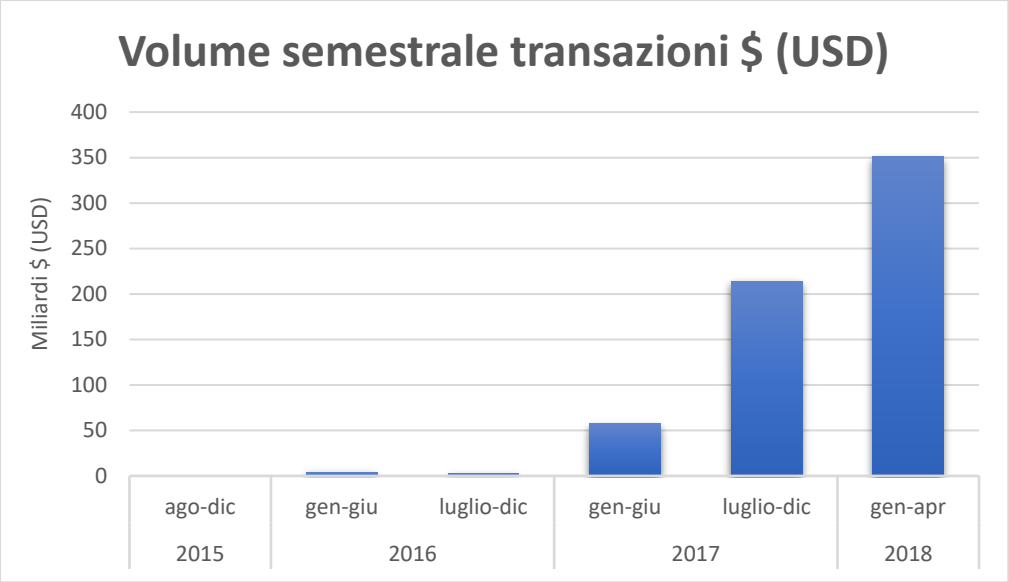


Grafico 3.17 Rappresentazione grafica dei volumi transazioni semestrali, espressi in Mld $ (USD). Fonte dati reperiti Url: "https://coinmetrics.io/".

Il grafico 3.17 mostra l'oscillazione dei volumi semestrali delle transazioni in $ americani di Ethereum, anzi precisando di Ether. Come si può notare l'esplosione del 2017 è stata rapida, proprio come è successo a bitcoin. Se pur con numeri inferiori, questa seconda criptovaluta ha registrato cifre esorbitanti, se paragonate al 2016. In data 26 aprile 2018 è stata registrato un volume di transazione giornaliera pari a $ 2,984,010,000.

Proprio come per Bitcoin, anche per Ethereum si studia la comparazione tra il volume delle transazioni degli Exchanges in $ americani (linea viola) e il volume delle transazioni sulla Blockchain in ETH scambiati (area viola). Nel grafico 3.18 viene mostrato questo a livello mensile (30gg) e nel grafico 3.19 viene mostrato su base semestrale (200gg).

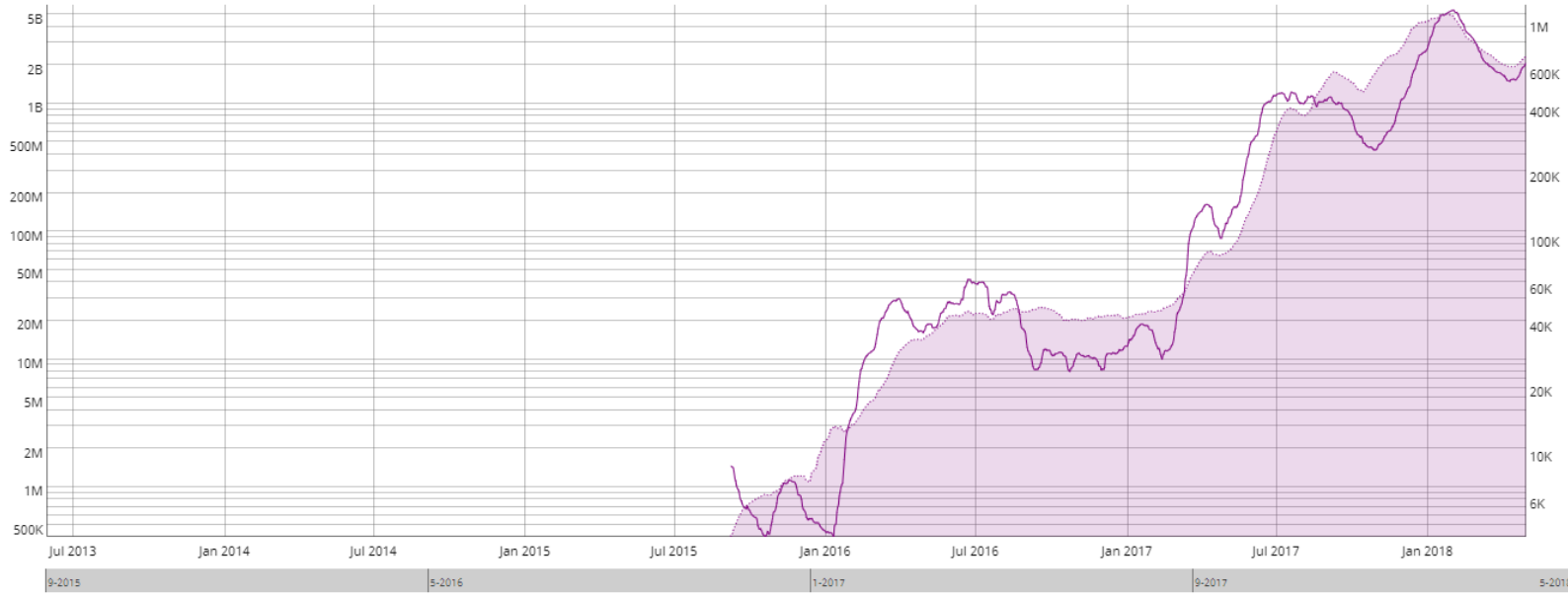


Grafico 3.18 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base mensile (30gg). Fonte Url: "https://coinmetrics.io".

Come si può notare dagli andamenti sfasati delle due curve si può dedurre lo stesso ragionamento fatto su BTC, ovvero cercare di interpretare se ci siano stati o meno dei comportamenti speculativi o meno. Rispetto al Bitcoin, nell'ultimo periodo preso in considerazione, le due curve collidono insieme, segno che questa criptovaluta è utilizzata sia negli Exchange che nelle transazioni all'interno della Blockchain, quindi si può ipotizzare che il prezzo di mercato sia più attendibile di Bitcoin. Nel grafico sottostante, invece, viene rappresentato quanto detto in ottica semestrale.

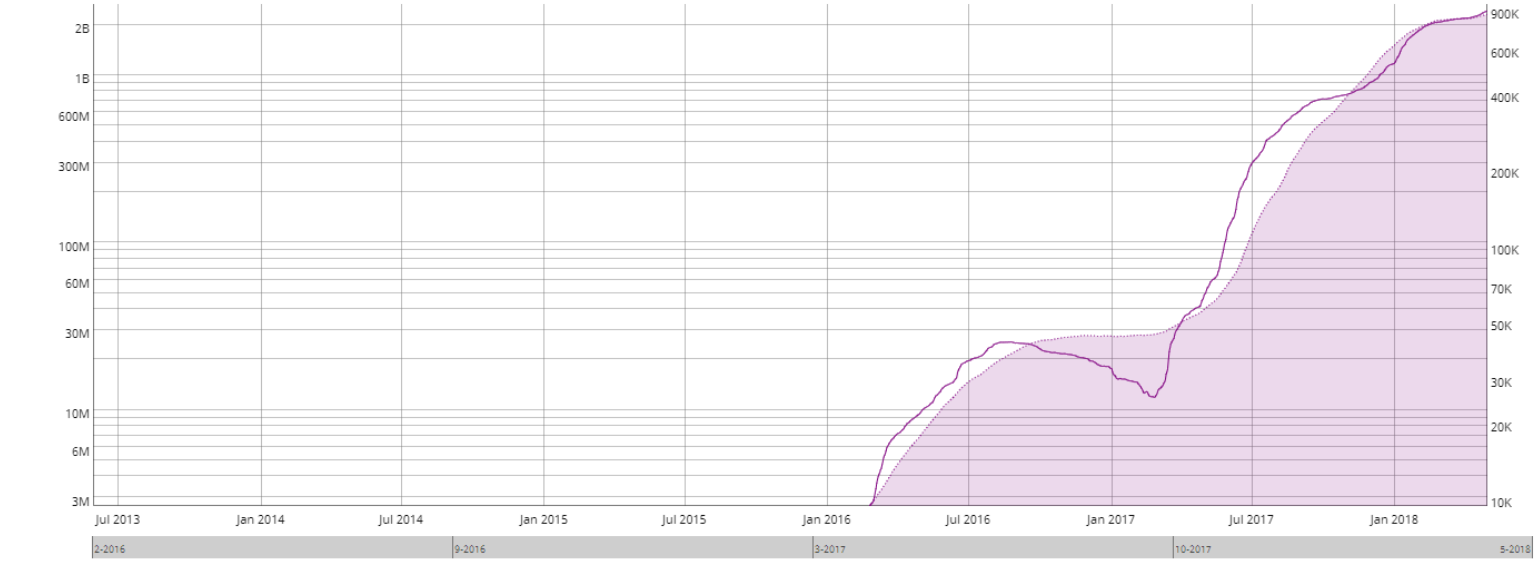


Grafico 3.19 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base semestrale (200gg). Fonte Url: "https://coinmetrics.io".

RIPPLE:

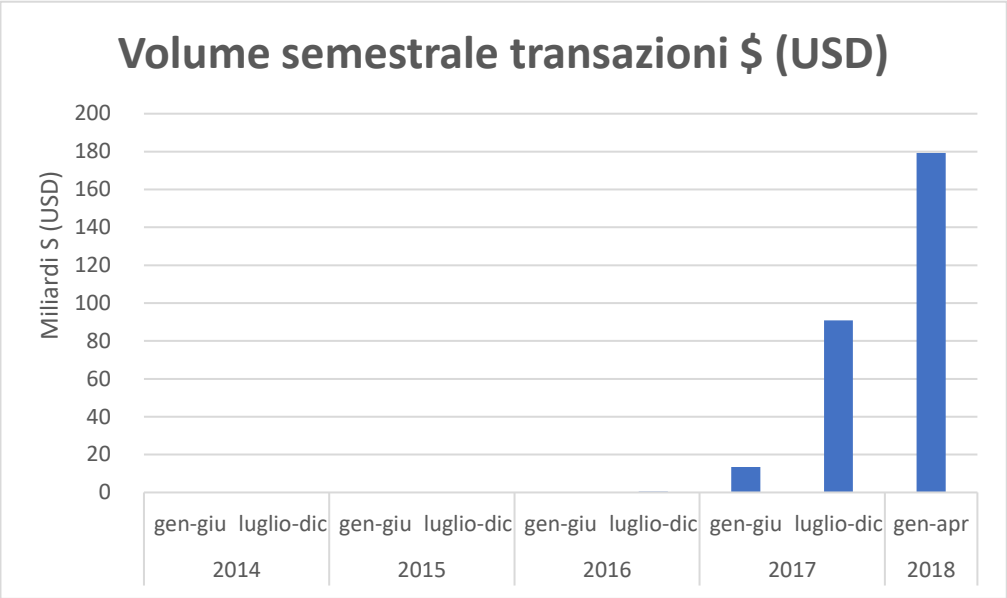


Grafico 3.20 Rappresentazione grafica dei volumi transazioni semestrali, espressi in Mld $ (USD). Fonte dati reperiti Url: "https://coinmetrics.io/".

Il grafico 3.20 mostra l'oscillazione dei volumi semestrali delle transazioni in $ americani di Ripple, anzi precisando di XRP. Come si può notare l'esplosione è stata rapida nel 2017, proprio come è successo a bitcoin. Se pur con numeri inferiori, questa seconda criptovaluta ha registrato cifre esorbitanti, se paragonate al 2016. In data 26 aprile 2018 è stata registrato un volume di transazione giornaliera pari a $ $1,028,590,000.

Proprio come per le altre criptovalute, anche per Ripple si studia la comparazione tra il volume delle transazioni degli Exchanges in $ americani (linea grigie) e il volume delle transazioni sulla Blockchain in XRP scambiati (area grigia). Dal grafico 3.21 viene mostrato questo a livello mensile (30gg) e dal grafico 3.22 viene mostrato su base semestrale (200gg).

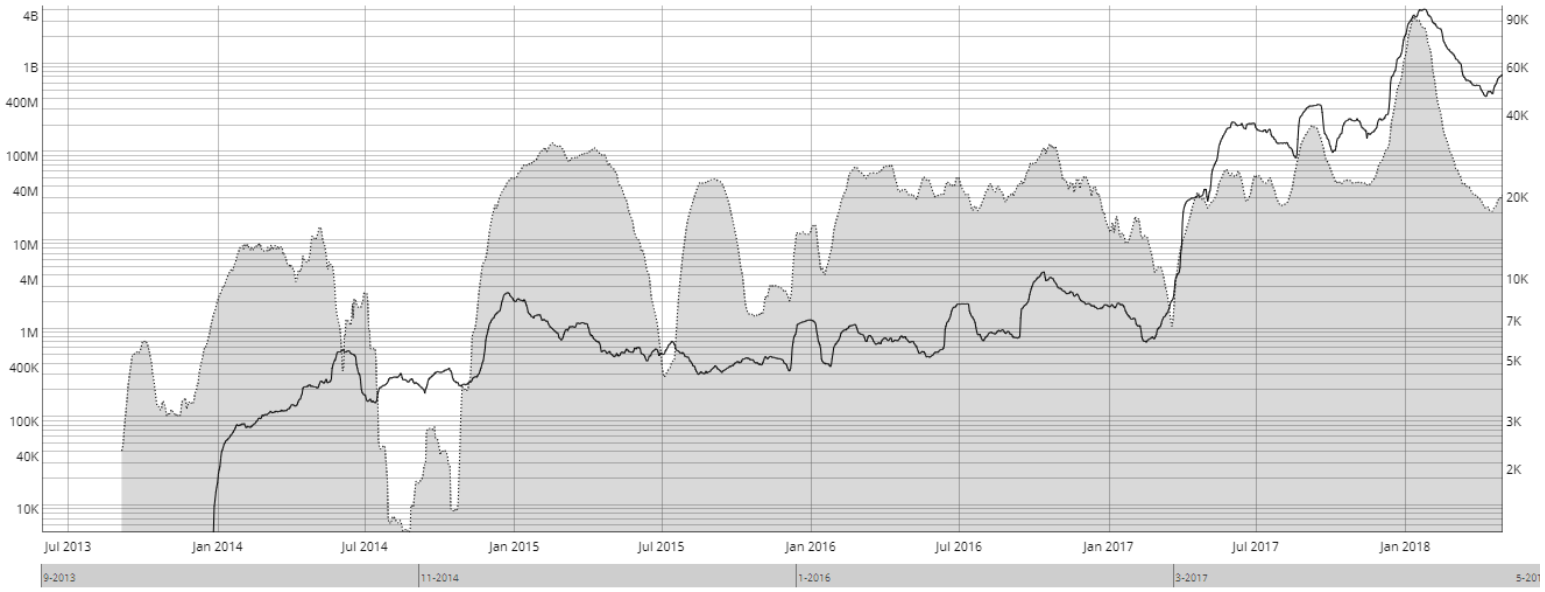


Grafico 3.21 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base mensile (30gg). Fonte Url: "https://coinmetrics.io".

Come si nota dagli andamenti sfasati delle due curve si può fare stesso ragionamento operato su BTC, ovvero cercare di interpretare se ci siano stati o meno dei comportamenti speculativi o meno. Ripple ha registrato un andamento simile al Bitcoin, ossia nell'ultimo periodo preso in considerazione le due curve segnano un gap importante e più precisamente la curva dei volumi scambiati sugli Exchanges è maggiore di quelli scambiati sulla Blockchain. Questo può essere segno che questa criptovaluta sia utilizzata più per scopi speculativi. Nel grafico sottostante, invece, viene rappresentato quanto detto in ottica semestrale.

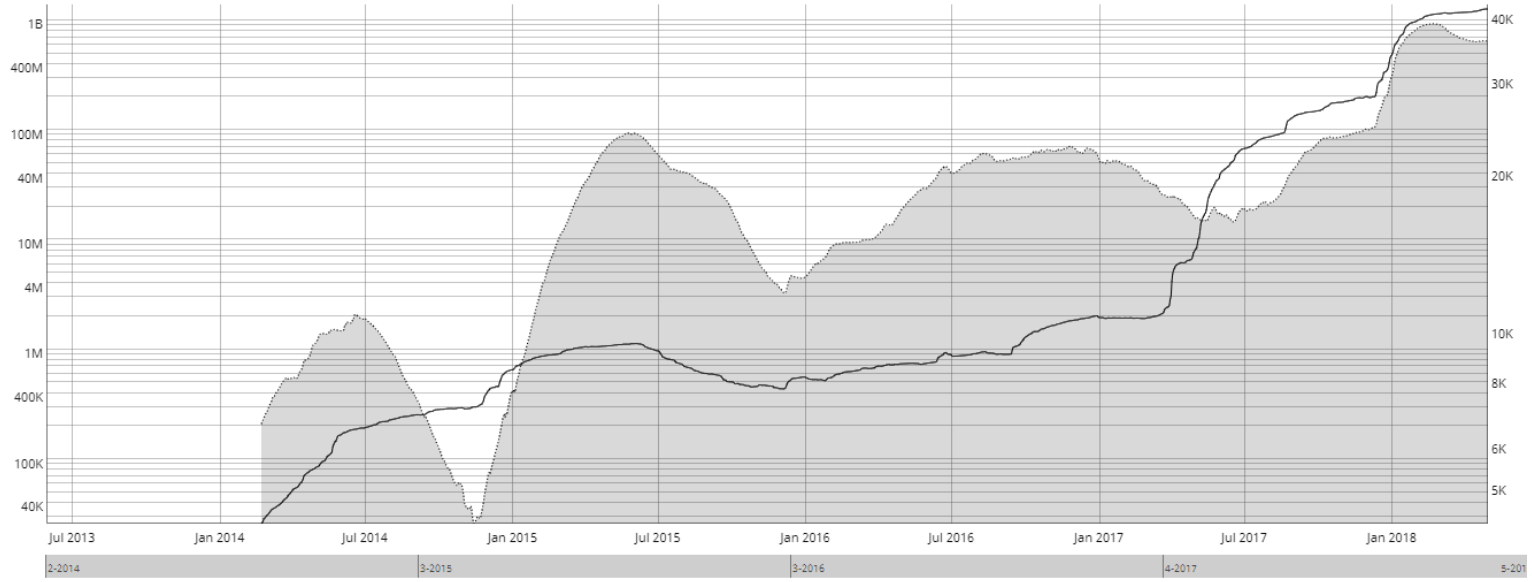


Grafico 3.22 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base semestrale (200gg). Fonte Url: "https://coinmetrics.io".

STELLAR:

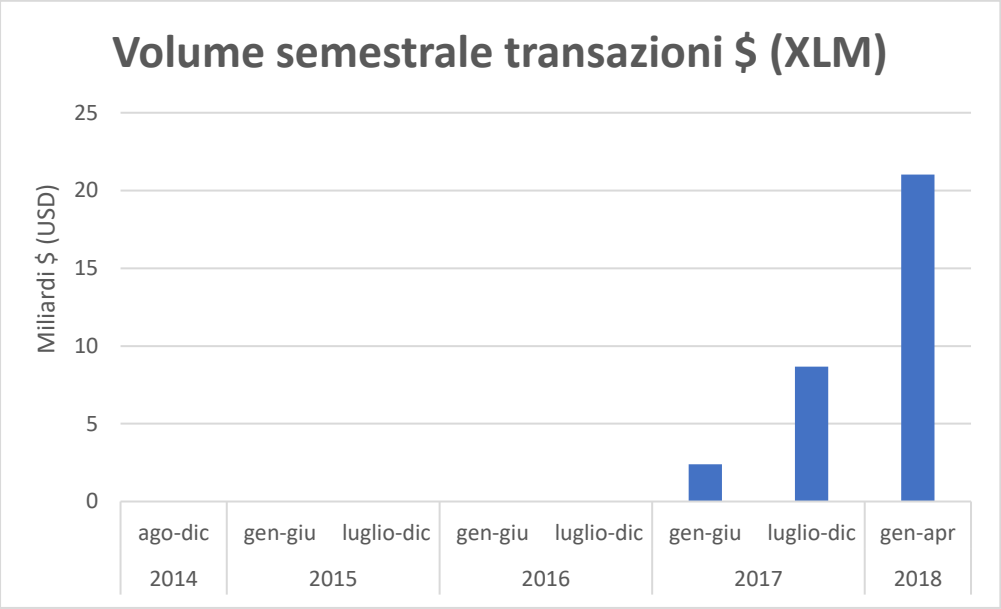


Grafico 3.23 Rappresentazione grafica dei volumi transazioni semestrali, espressi in Mld $ (USD). Fonte dati reperiti Url: "https://coinmetrics.io/".

Il grafico 3.23 mostra l'oscillazione dei volumi semestrali delle transazioni in $ americani di Stellar, anzi precisando di XLM. Come si può notare l'esplosione del 2017 è stata rapida, proprio come è successo a bitcoin. Se pur con numeri inferiori, questa seconda criptovaluta ha registrato cifre esorbitanti, se paragonate al 2016. In data 26 aprile 2018 è stata registrato un volume di transazione giornaliera pari a $ 152,903,000.

Proprio come per le altre criptovalute, anche per Stellar si studia la comparazione tra il volume delle transazioni degli Exchanges in $ americani (linea arancione) e il volume delle transazioni sulla Blockchain in XLM scambiati (area arancione). Nel grafico 3.24 viene mostrato questo a livello mensile (30gg) e dal grafico 3.25 viene mostrato su base semestrale (200gg).

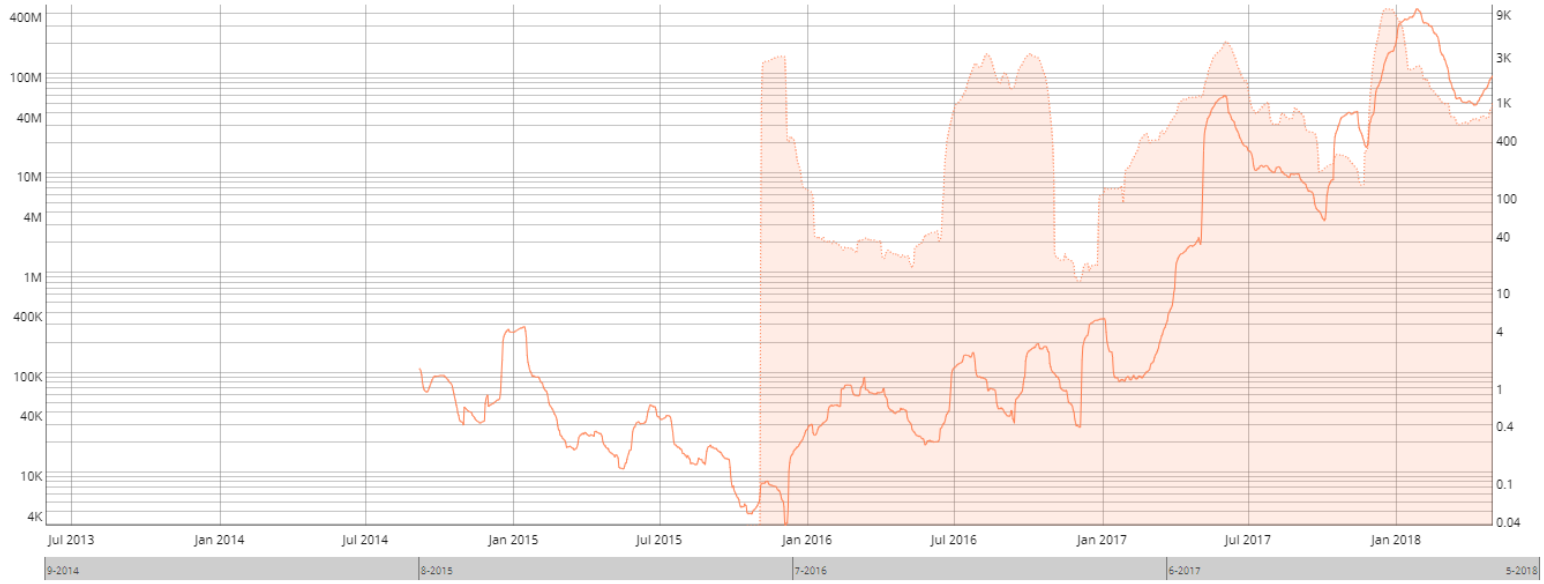


Grafico 3.24 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base mensile (30gg). Fonte Url: "https://coinmetrics.io".

Come si può notare dagli andamenti sfasati delle due curve si può fare lo stesso che quanto fatto per il BTC, ovvero capire se ci siano stati o meno dei comportamenti speculativi o meno. Stellar ha registrato un andamento molto meno speculativo rispetto alle altre criptovalute, in cui solamente l'ultimo periodo preso in considerazione le curve segnano un lieve gap, più precisamente la curva dei volumi scambiati sugli Exchanges è maggiore di quelli scambiati sulla Blockchain. Ad ogni modo, se questo viene valutato su base semestrale, si può notare come questo comportamento sia lieve. Necessaria è la valutazione di questo comportamento in futuro, se questo trend viene mantenuto o meno. Nel grafico sottostante, invece, viene rappresentato quanto detto in ottica semestrale.

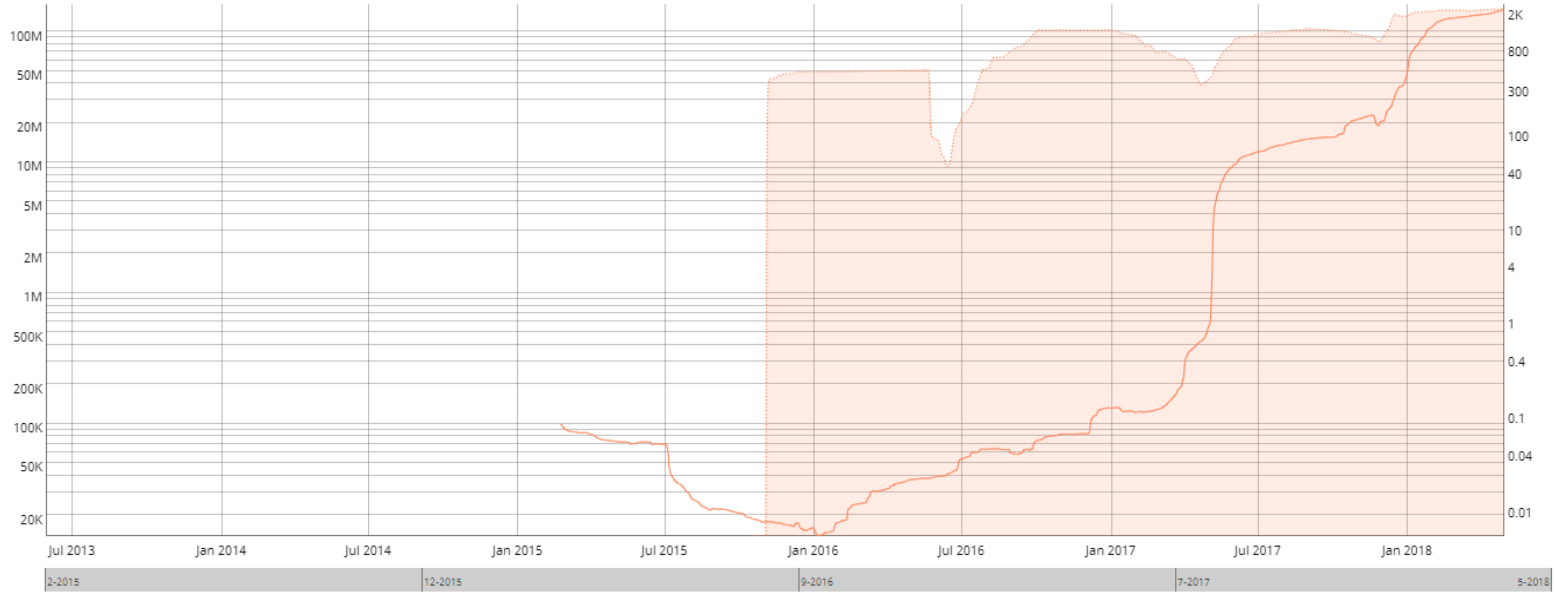


Grafico 3.25 Comparazione tra il volume delle transazioni negli Exchanges in $ USD, e il numero delle transazioni (escluse quelle in Coinbase). Il confronto viene fatto su base semestrale (200gg). Fonte Url: "https://coinmetrics.io".

Purtroppo, non ci sono tutti i dati storici per IOTA ma nel grafico 3.26 si è riusciti a prendere quelli che vanno dal periodo dal primo gennaio 2018 al 26 aprile 2018. Inoltre, sempre nello stesso grafico, vengono comparate le cinque criptovalute prese in esame per i volumi delle transazioni espressi in $ USD, per il periodo dal primo gennaio 2018 al 26 aprile 2018.

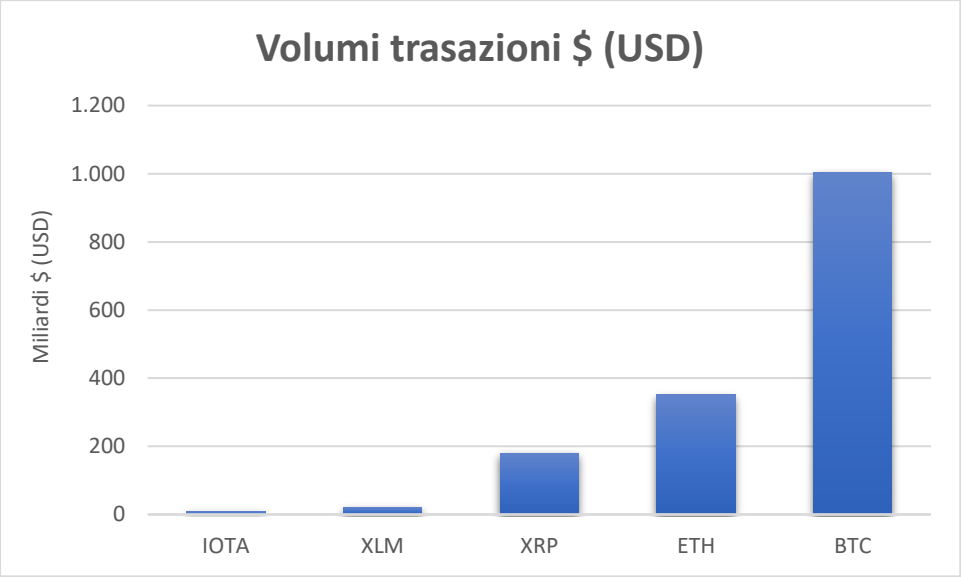


Grafico 3.26 Rappresentazione grafica dei volumi delle transazioni espresse in Mld $ (USD), delle cinque criptovalute, dal 1° gennaio 2018 al 26 aprile 2018. Fonte dati reperiti Url: "https://coinmetrics.io/" e "https://coinmarketcap.com".

Come si può evincere dal grafico sopra stante, è Bitcoin a registrare numeri esorbitanti raggiungendo e superando la soglia dei 1,000 miliardi di dollari. Ciononostante, anche per le altre si registrano cifre importanti.

Per fornire una visione più amplia del fenomeno preso in considerazione, nel grafico 3.27 queste criptovalute sono confrontate con altri sistemi di pagamento, utilizzati dalla finanza tradizionale.

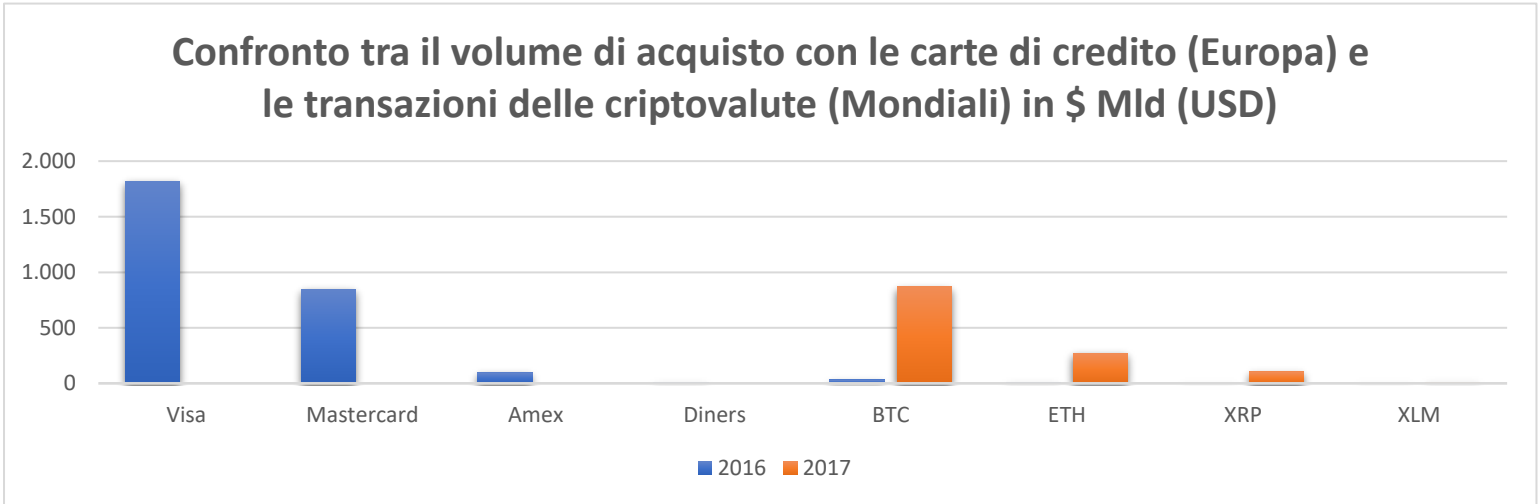


Grafico 3.27 Comparazione tra il Volume di acquisto con le carte di credito in Europa nel 2016 e il volume delle transazioni delle quattro criptovalute a livello Mondiale nel 2016 e 2017. Fonte dati reperiti Url: "https://nilsonreport.com/index.php"; "https://coinmetrics.io/".

Nel Grafico 3.27 vengono confrontati da una parte i sistemi elettronici tradizionali di pagamento, quali le carte di credito e di debito e dall'altra le quattro criptovalute prese in analisi (purtroppo IOTA non c'è per mancanza di dati). Non è una vera e propria comparazione pura, nel senso che per i sistemi elettronici tradizionali si è preso il dato europeo, mentre per le criptovalute si è preso il dato mondiale. Questa comparazione è utile per evidenziare maggiormente, con un termine di paragone adeguato, il fenomeno del criptomondo. In particolare, si può notare come l'anno 2017 sia stato un periodo fenomenale per le monete digitali, purtroppo non si hanno i dati dello stesso anno per le carte di credito più famose. Risulta eloquente l'esito di questa analisi infatti sempre più il criptomondo sta prendendo piede fra i sistemi di pagamento.

Per evidenziare maggiormente questo successo del criptomondo, nella figura sotto stante 3.5 si può evincere i dati di questa simile comparazione eseguita da uno studio sul Bitcoin della BCE nel 2015. In soli tre anni, il fenomeno del criptomondo è ancora a livelli inferiori dai sistemi tradizionali, ma non è più marginale rispetto ai suoi inizi.

Inoltre, è utile mostrare alcune cifre: nel 2016 il totale dei sistemi tradizionali ammontava a $ 2,765.17 Mld (USD), mentre queste quattro valute digitali erano a $ 39 Mld (USD). Nel 2017 il totale delle criptovalute ammontava a $ 1,256 Mld (USD), registrando una variazione percentuale pari a 3,158.78%.

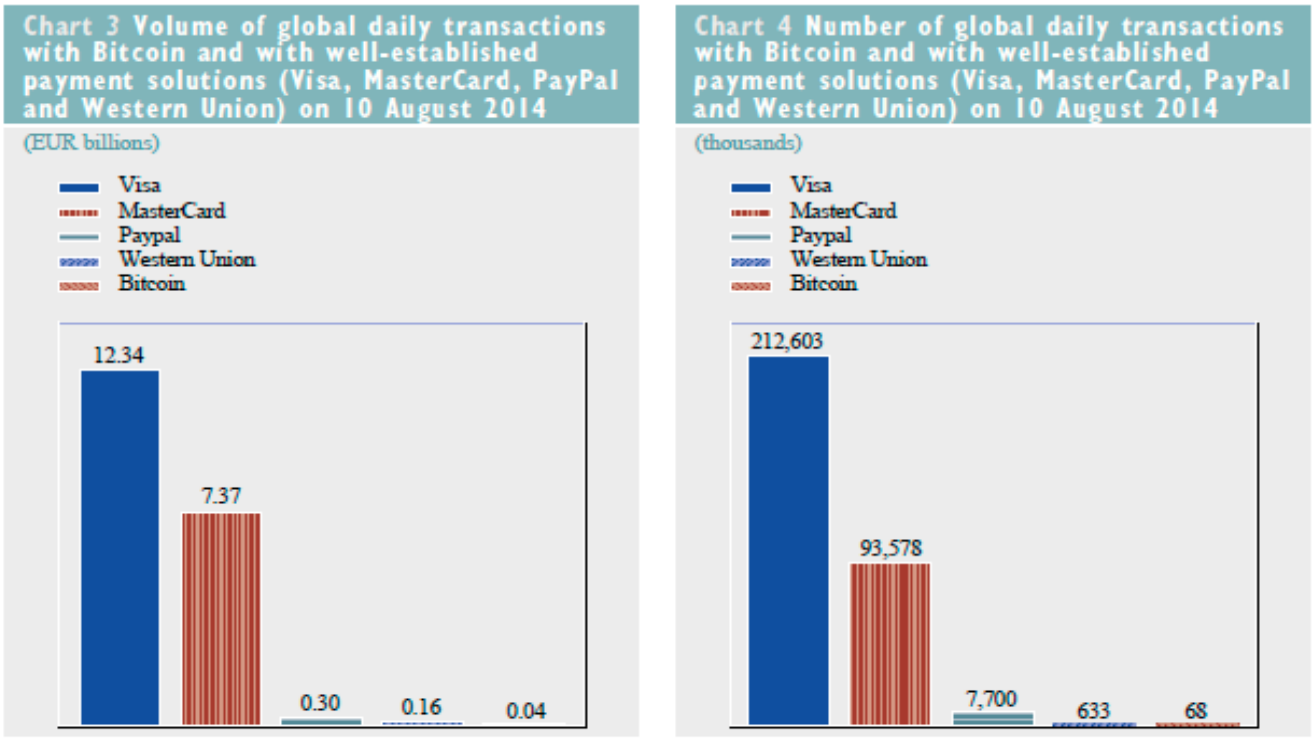


Figura 3.5 Fonte: "Virtual currency schemes – a further analysis", Febbraio 2015, BCE.

Il Mining dal punto di vista economico

Il processo di Mining è fondamentale per due motivi: innanzitutto per confermare ed autenticare le transazioni e quindi, attraverso questo, si riesce a immettere nel sistema nuovi token (*coinbase transaction*). Ovviamente questo processo lo troviamo per le criptovalute che utilizzano il PoW come sistema di convalida delle transazioni. In particolare, in questa analisi risultano essere: il Bitcoin ed Ethereum. Di seguito verrà analizzato questo processo per Bitcoin, successivamente verrà illustrato brevemente su Ethereum con i cambiamenti previsti in futuro.

Bitcoin:

Per rendere profittevole questo processo, entrano in gioco diversi fattori: l'Hashrate, la difficoltà, le componenti hardware degli elaboratori e il costo dell'energia elettrica.

Come si era illustrato nel secondo capitolo, per convalidare nuovi blocchi contenenti le nuove transazioni, è indispensabile una potenza di calcolo (Hashrate) proporzionata alla difficoltà che di volta in volta il sistema gestisce al fine di garantire la creazione del blocco nell'intervallo dei 10 minuti circa.

Nei due grafici sottostanti si possono dedurre questi aspetti:

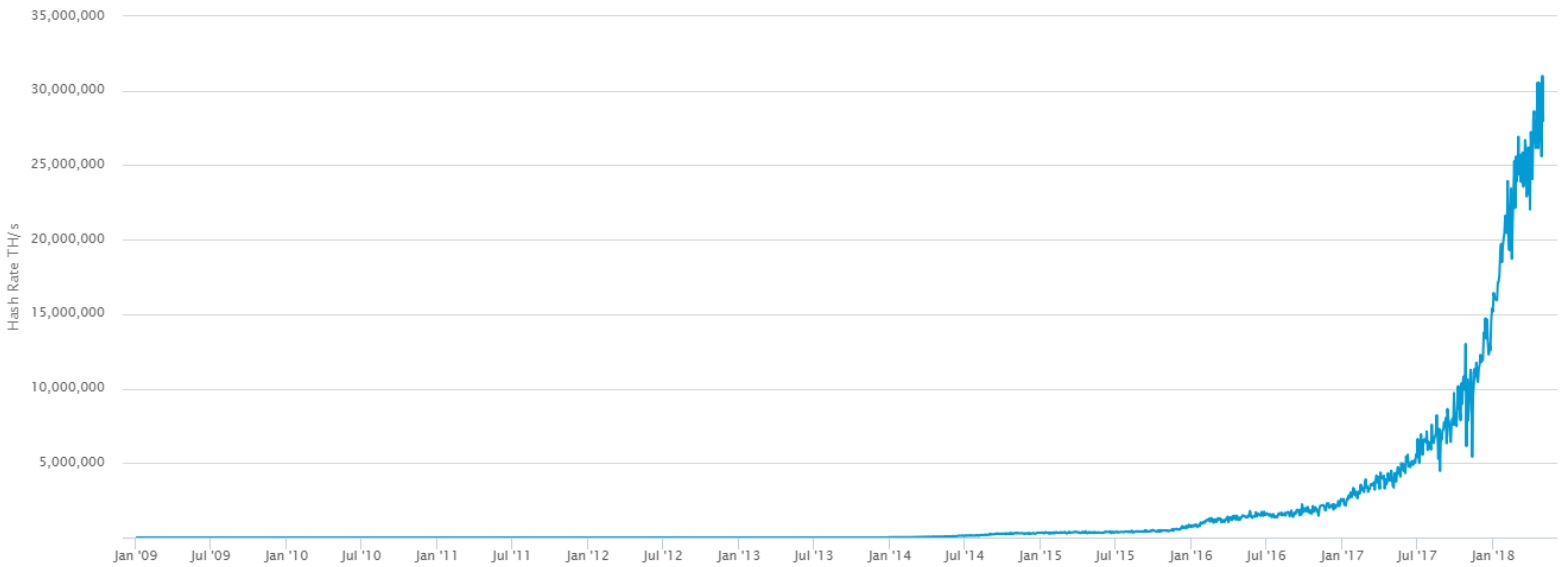


Grafico 3.28 Illustrazione dell'Hashrate totale. Fonte Url: "https://blockchain.info/it/charts/hash-rate?timespan=all".

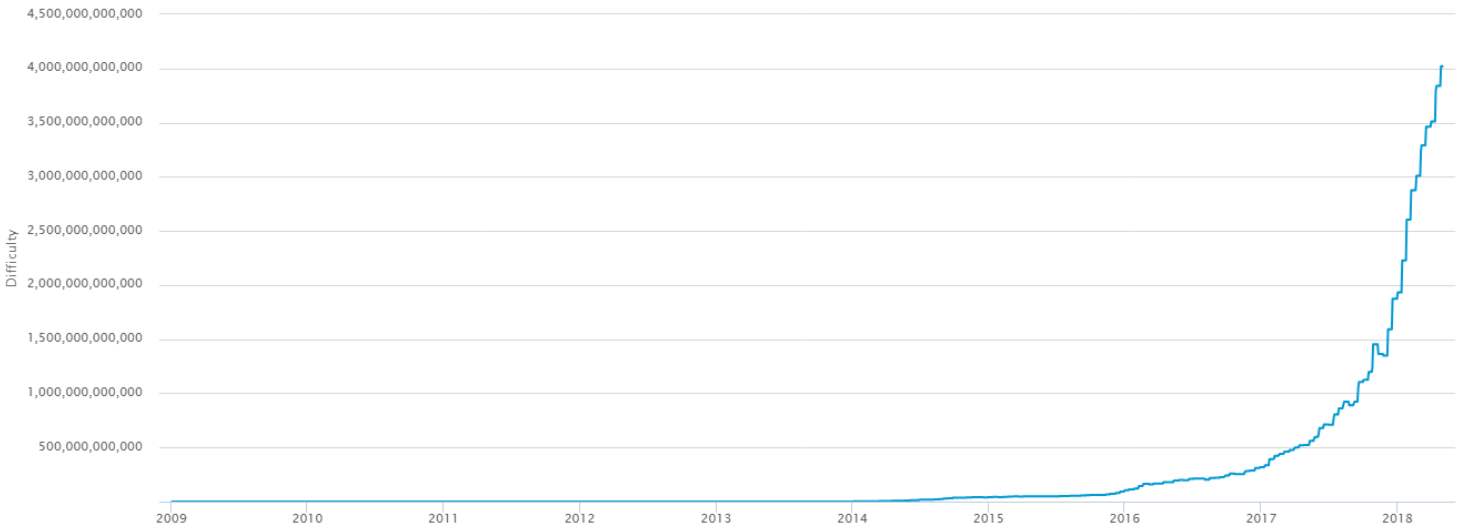


Grafico 3.29 Illustrazione della Difficoltà totale. Fonte Url: "https://blockchain.info/it/charts/difficulty?timespan=all".

Come si può argomentare dai grafici 3.28 e 3.29, l'aumento esponenziale della potenza di calcolo dell'intero network (Hashrate) è dovuta da una parte dalla diffusione del token, soprattutto per l'aumento del suo prezzo spingendo molti utenti ad investire nell'attività di mining, realizzando così enormi plusvalenze; mentre dall'altra il progresso tecnologico ha sopperito all'aumento della difficoltà del sistema adottando dapprima elaboratori di casa, per poi arrivare a sistemi ad-hoc adibiti solamente per minare i bitcoin. Partendo da questi motivi, si riesce ad interpretare adeguatamene le figure sopra stanti in cui entrambi sono correlati tra loro. Inoltre, questi si possono confrontare con il grafico 3.1, proprio perché sono riferiti all'aumento del prezzo del token. Infatti, la crescita sproporzionale agli andamenti precedenti è partita dal secondo semestre del 2016. Da quel momento in poi è aumentata esponenzialmente fino a raggiungere cifre spaventose nel 2017 e inizio 2018. Ad ogni modo, anche se non si riesce a leggere dal grafico per via delle sue dimensioni contenute, la prima vera crescita importante la si ha nel lontano 30 maggio 2013 alle ore 02:00. In quella data, ha superato per la prima volta il livello 100 di TH/s, fino ad arrivare quasi a quota 10,000 TH/s a fine dicembre 2013. Successivamente, dipendentemente dalle oscillazioni del prezzo, ci sono stati dei rallentamenti di tale crescita. Attualmente si parla di una cifra pari a: 27,991,271 TH/s[128].

[128] Fonte Url: "https://blockchain.info/it/charts/hash-rate?timespan=all", in data 2 maggio 2018 ora 02:00.

Solo Mining:

In questa analisi merita un accenno l'operazione Solo Mining dal lato economico, quindi si vuole studiare come questo lavoro sia profittevole o meno. A differenza degli altri due metodi di mining (Cloud Mining e Pool Mining), qui è il singolo operatore che lavora individualmente alla ricerca di risolvere, prima degli altri utenti presenti nel network, i problemi crittografici dei nuovi blocchi con la propria potenza hardware e software. Tramite dei calcolatori online, si possono fare delle stime per capire quanto sia profittevole il lavoro. Per tale ragione, chi vuole cimentarsi in questa attività dovrebbe ricorrere a specifici hardware: ASIC, come quello sottostante:

Figura 3.6 Hardware ASIC: Antiminer S9 della Bitmain.

Dalla figura 3.6 viene illustrato com'è fatto un estrattore di bitcoin. Questo in particolare viene realizzato dalla ditta Bitmain ed è in grado di processare 14 TH/s con un consumo sui 1,500w. Questo elaboratore è stato venduto nel 2017, in pieno boom delle criptovalute, a cifre astronomiche ($ 5,000) ora invece nel mese di aprile lo si può trovare a metà di quel prezzo[129] e in data 4 maggio 2015 lo si poteva trovare su Amazon a un prezzo pari a € 1,580[130]. Impressionante come questa azienda sia cresciuta così enormemente e così in poco tempo. Attualmente quest'impresa ha registrato profitti tra i 3 e i 4 miliardi di dollari nel 2017, più dell'Invidia (colosso delle GPU) che veniva scelta dagli operatori del mining per le sue schede video. Questa azienda cinese, ha optato per l'integrazione verticale, ovvero è egli stessa a produrre i processori, che saranno successivamente assemblati nelle macchine. Inoltre, oltre alla produzione e vendita delle suddette, gestisce anche l'Antipool, uno dei più grandi Pool Mining del mondo.

[129] Fonte Url: "http://www.lastampa.it/2018/03/04/tecnologia/questa-fabbrica-di-bitcoin-guadagna-pi-dei-colossi-tech-tOKIljDpmI4zlzpAXP1TJI/pagina.html".
[130] Fonte Url: "https://www.amazon.it/Bitmain-antminer-14TH-lestrazione-bitcoin/dp/B004GEJU84".

Tutt'ora quest'azienda si sta dirigendo verso l'intelligenza artificiale per diversificarsi e non restare solamente nel mercato del cripto-mondo (molto suscettibile sul mercato) e punta anche a specializzarsi nel mining di Ethereum.

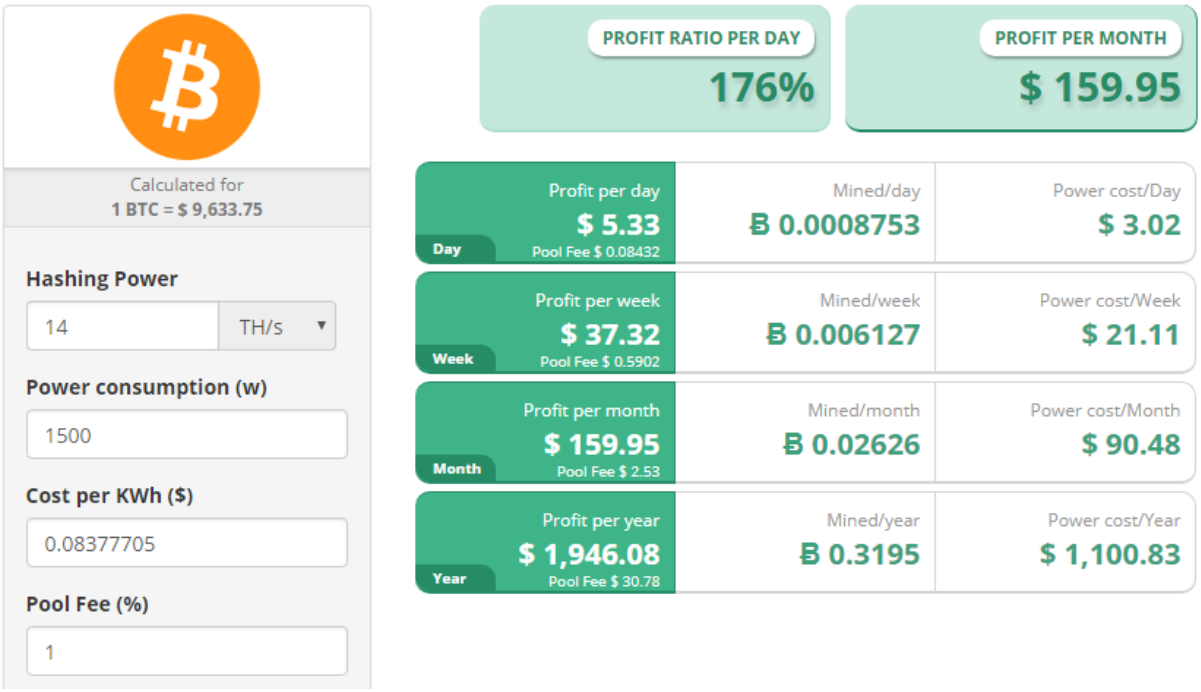


Figura 3.7 Illustrazione del funzionamento di un calcolatore online per la stima economica del processo di Mining di Bitcoin. Fonte Url: "https://www.cryptocompare.com/". Data 04 maggio 2018, ore 13:00.

Dalla figura 3.7 si può evincere un esempio empirico di quanto potrebbe essere profittevole un investimento con un elaboratore che sviluppi almeno 14 TH/s. Prendendo come prezzo medio per energia elettrica pari a 0.07 €/Kw e che al momento attuale il cambio €/$ è di 1.196815[131] si ottiene un prezzo medio pari a $ 0.08377705 Kw. Si riesce ad ottenere un profitto pari a $ 1,100.83 dopo un anno.

	1 DAY	1 WEEK	1 MONTH
Income	0.00089389 BTC 8.61 USD	0.00610007 BTC 58.78 USD	0.02761457 BTC 266.09 USD
El. costs	-0.00028266 BTC -2.72 USD	-0.00200253 BTC -19.30 USD	-0.00859732 BTC -82.84 USD
Profit	0.00061123 BTC 5.89 USD	0.00409754 BTC 39.48 USD	0.01901724 BTC 183.25 USD

Figura 3.8 Illustrazione del funzionamento di un calcolatore online per la stima economica del processo di Mining di Bitcoin. Fonte Url: "https://www.nicehash.com". Data 04 maggio 2018, ore 19:55.

Mentre dalla figura 3.8 si evince un altro risultato, ovvero un profitto pari a $ 183.25, utilizzando gli stessi input, tranne che il prezzo di bitcoin è pari a $ 8,636.00.

[131] Fonte Url: "http://finanza-mercati.ilsole24ore.com/quotazioni.php?QUOTE=!EURUS.FX". Data 4 maggio 2018, ore 13:20.

Pool Mining:

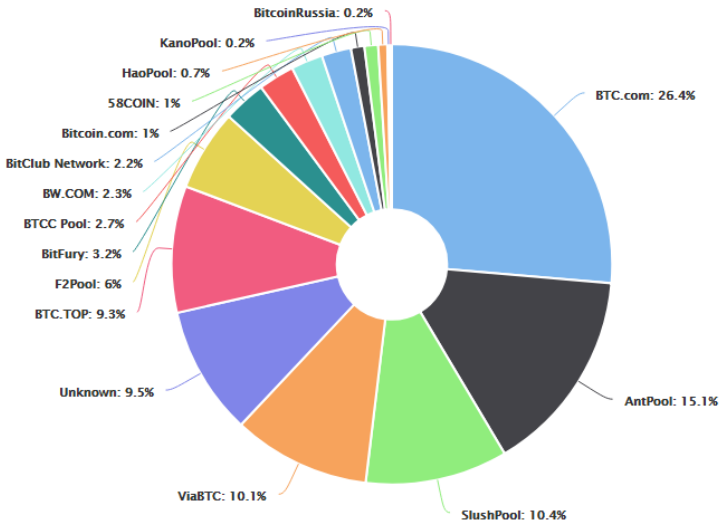


Figura 3.9 Distribuzione della percentuale di Hashrate tra i principali Pool Mining, all'interno del network. Fonte Url: "https://blockchain.info/it/pools".

Nella figura 3.6 viene illustrata la stima della distribuzione della percentuale di Hashrate trai principali gruppi di Pool mining sul mercato. Il sito precisa che quel 9.5% non rappresenta un tentativo di 51% attack del network, ma che non si ha un'origine ben precisa. Da notare come la società Antpool, controllata da Bitmain, abbia una quota più che rilevante, essendo la seconda in termini percentuali di Hashrate.

Ricavi dei Miners:

Grafico 3.30 Illustrazione dei ricavi totali dei miners, calcolando sia le transazioni di coinbase per i primi dei blocchi aggiunti sul network che delle commissioni. Fonte Url: "https://blockchain.info".

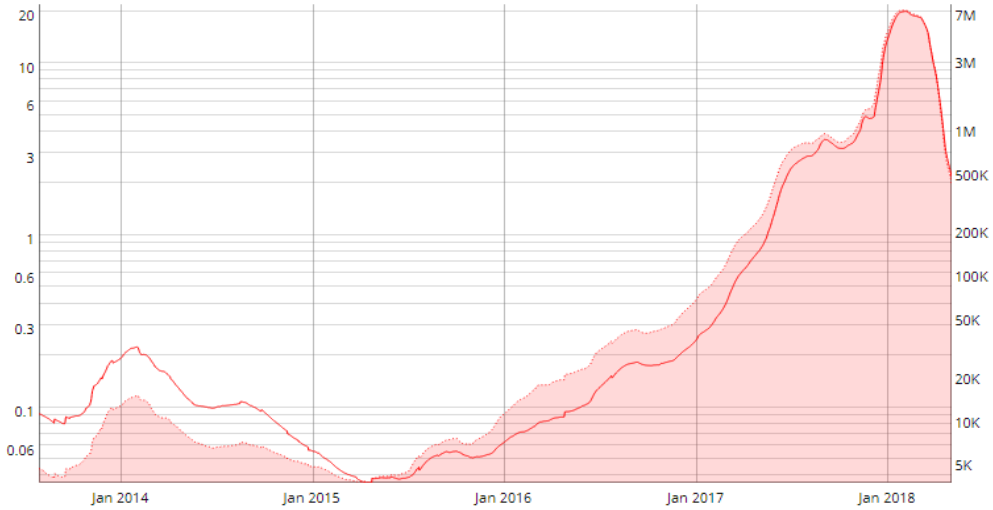


Grafico 3.31 Confronto tra la media delle commissioni per transazioni in $ USD (linea rossa) e del volume delle commissioni in $ USD (area rossa), queste analisi sono su base trimestrale. Fonte Url: "https://coinmetrics.io".

Dai grafici soprastanti (3.30 e 3.31) si può evincere l'andamento dei profitti per i miners, nella gestione del processo di mining. In particolare, dal grafico 3.29 viene illustrato l'andamento dei ricavi totali (sommatoria tra le transazioni di coinbase e le commissioni per le transazioni). Nel grafico 3.31, invece, viene raffigurato l'andamento della media delle commissioni espresso in $ americani. Attualmente, il volume totale delle transazioni giornaliero è pari a $ 409.56572 migliaia, mentre la media per le commissioni giornaliere è pari a $ 2.1606 in data al 3 maggio 2018.

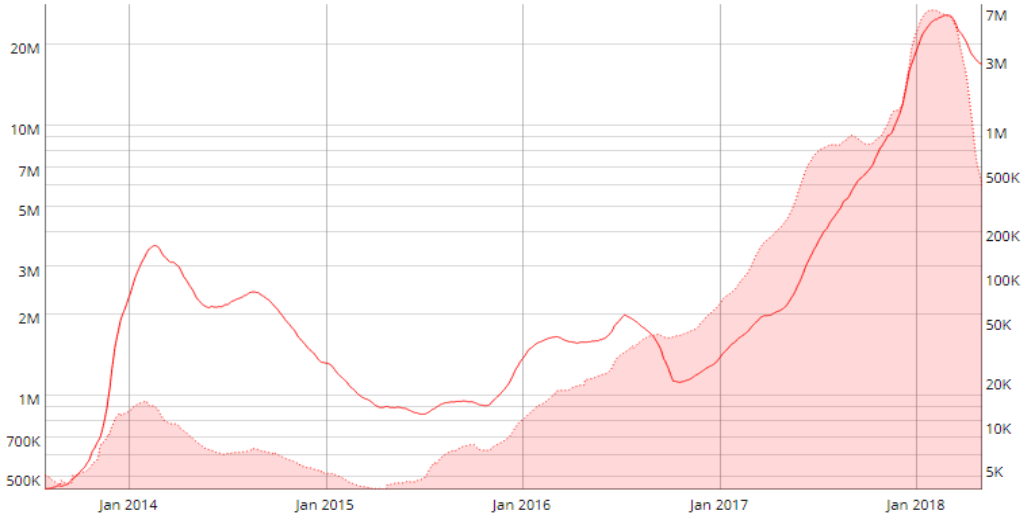


Grafico 3.32 Comparazione tra il valore delle transazioni di coinbase in $ USD (Linea Rossa) e il volume delle commissioni in $ USD (area rossa), su base trimestrale. Fonte Url: "https://coinmetrics.io/".

Il grafico 3.32, scorpora i volari del grafico 3.30, infatti qui i ricavi dei miners viene scomposto dal valore delle transazioni di coinbase, ossia il valore della creazione dei nuovi BTC, e il volume delle commissioni delle transazioni, il tutto espresso in $ americani e su base trimestrale.

Da questi grafici si evidenzia i ricavi dei miners, questo valore rappresenta la sommatoria tra le ricompense attribuite a chi risolve per prima il blocco (transazioni di coinbase) e tutte le commissioni delle transazioni incluse nel blocco.

Attualmente il valore della ricompensa è pari a 12 BTC per ogni blocco risolto (inizialmente era di 50 BTC), come descritto nel secondo capitolo, questo valore è destinato a dimezzarsi ogni quattro anni fino ad annullarsi, e i minatori verranno remunerati solamente dalle commissioni e dalle transazioni. Con i dati relativi fino a maggio 2018, possiamo quantificare il numero massimo delle transazioni di coinbase, facendo un calcolo molto semplice: 144 blocchi al giorno (10 minuti per ogni blocco) moltiplicato per 12.5 (quantità di BTC rilasciata ad ogni blocco risolto), per arrivare alla cifra di 1800 BTC creati al giorno. Attualmente, il prezzo per un BTC è pari a $ 9,886.27[132], quindi in definitiva il ricavo complessivo giornaliero per le transazioni di coinbase è pari a $ 17,795,286. Oltre a questo risultato bisogna aggiungere le commissioni, che mediamente sono di 0.0001 BTC a transazione.

Le commissioni in Bitcoin vengono richieste a chi effettua la transazione. In realtà non è una cifra fissa, ma il loro importo dipende da tre aspetti fondamentali:

- spazio occupato dalla transazione nel blocco, che mediamente occupata 225 byte;
- il numero delle transazioni sul network: proprio perché lo spazio nel network è limitato, più il numero delle transazioni aumenta più utenti alzeranno il costo della commissione per far sì che la propria venga processata il più presto possibile. In definitiva, questo processo viene lasciato alla legge di mercato, ossia il principio della domanda e dell'offerta. Proprio per questo che molti wallet hanno l'opzione di lasciare varabile il costo della transazione, proprio per far sì che vada a buon fine. Il costo di esse è correlato al numero delle transazioni effettuate in quel preciso momento. I miners saranno più disposti a scegliere le transazioni con più alto valore di commissione.
- Il valore del bitcoin, ossia il prezzo di mercato del token, infatti le commissioni vengono pagate in BTC, per cui il costo delle commissioni oscillerà in base all'andamento del prezzo del bitcoin.

[132] Fonte Url: "https://coinmarketcap.com/", in data: 5 maggio 2018, ore 12:24.

Proprio per i motivi sopra elencati, i grafici sopra descritti risentono dell'oscillazione *random walk* del prezzo del BTC, come per il resto del criptomondo è sicuramente la variabile più rischiosa per chi decidesse di investire sul mining.

ETH:

Da una notizia del 1° aprile 2018, sembrerebbe che il fondatore di Ethereum, Buterin e il team degli sviluppatori del network vogliano limitare Ether fino a 120 milioni di ETH. Questa limitazione è sempre stata discussa sia all'interno degli sviluppatori che tra i fans della moneta digitale. Ora più che mai, visto con quale velocità vengono creati i nuovi token, il fondatore è preoccupato se l'offerta sia sproporzionale alla domanda. Quindi probabilmente stanno cercando di evitare che il proprio token si inflazioni, proprio come per Bitcoin. Inoltre, l'anno 2018 è il momento in cui entrerà in funzione il PoS in Ethereum e tutto il mono dei minatori di questa piattaforma sa che il suo lavoro sarà destinato a concludersi a breve, questa è una variabile che ha influito negativamente sugli investimenti in questa attività.

Le applicazioni della Blockchain

Inizialmente la tecnologia della Blockchain è stata sviluppata per consentire transazioni trasparenti, sicure, immutabili ed efficienti, quale ad esempio per il corretto funzionamento di Bitcoin. Tuttavia, come si è detto più volte, questa tecnologia dal carattere *disruptive* ha un altissimo potenziale in grado di far evolvere il modo di operare sia dell'imprese che dei governi. Ci sono quattro caratteristiche comuni che ogni Blockchain deve avere per esser messa in atto:

1- natura transazionale,
2- l'esistenza degli intermediari,
3- bisogno di fiducia,
4- bisogno di verifica.

L'applicazione più famosa dell'attuazione di questa tecnologia è sicuramente nei servizi finanziari, essendo quelli più predisposti per ricevere l'alto potenziale innovativo dall'applicazione blockchain. Tuttavia, questo potenziale lo si vede anche nei settori dell'assistenza sanitaria, dei trasposti, dell'industria di produzione di beni e di servizi, e anche del settore pubblico. Benché non ci sia ancora l'adozione di massa che probabilmente ci sarà in futuro, le aziende stanno investendo tempo e sforzi per comprendere tutte le potenzialità insite di questa tecnologia.

Attualmente sono le istituzioni finanziarie a essere le principali investitrici, visto che questa tecnologia dovrebbe esprimere il suo massimo potenziale sui servizi finanziari. Ad ogni modo, come si può vedere dalla figura sottostante, i vari prototipi di Blockchain possono trovarsi in diversi settori.

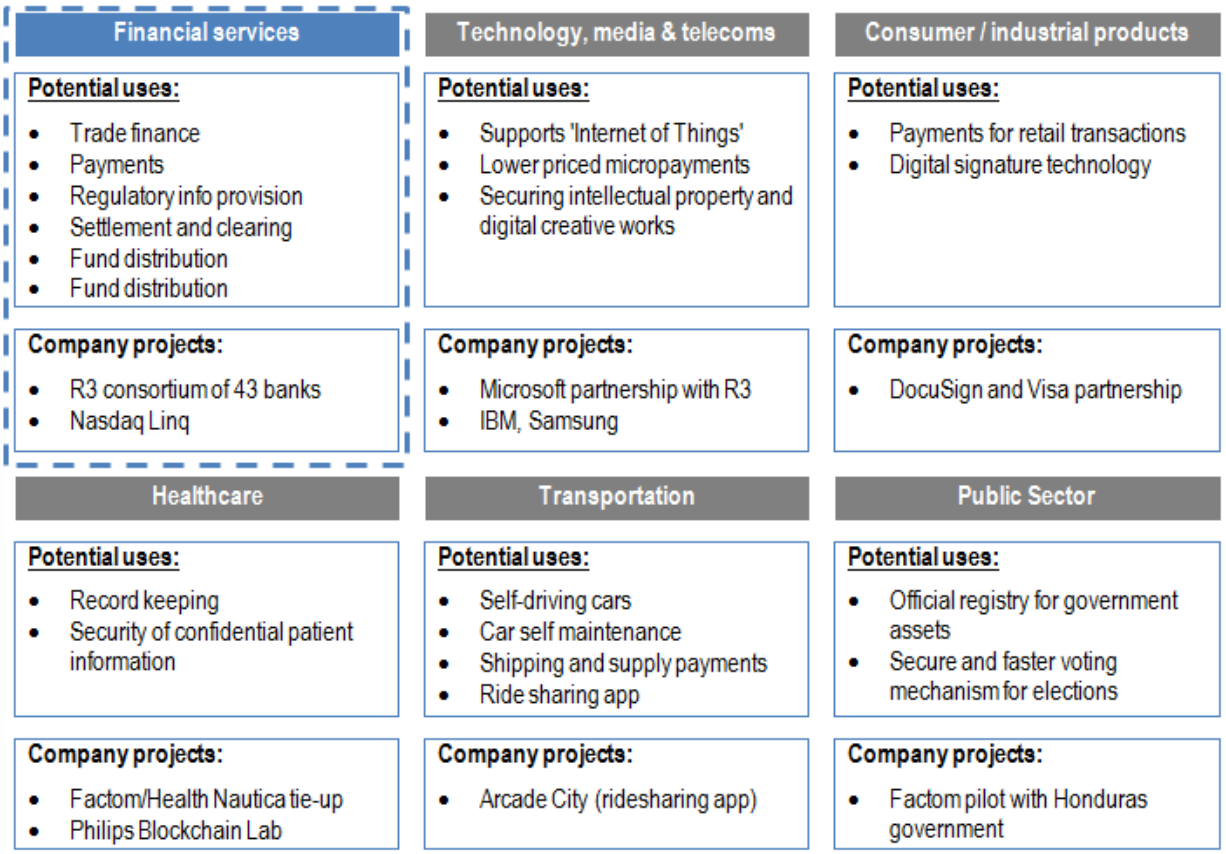


Figura 3.10 Le applicazioni della tecnologia Blockchain nei diversi settori. Fonte "J.P. Morgan Perspecives – Decrypting Cryptocurrencies", J.P. Morgan, pag. 13.

Dalla figura 3.10 si evincono sei settori differenti, dove all'interno viene evidenziato il potenziale della tecnologia Blockchain come strumento innovativo e dal carattere disruptive. Da precisare che sono ancora tutti prototipi ma è interessante notare quale società ci sia dietro a questi.

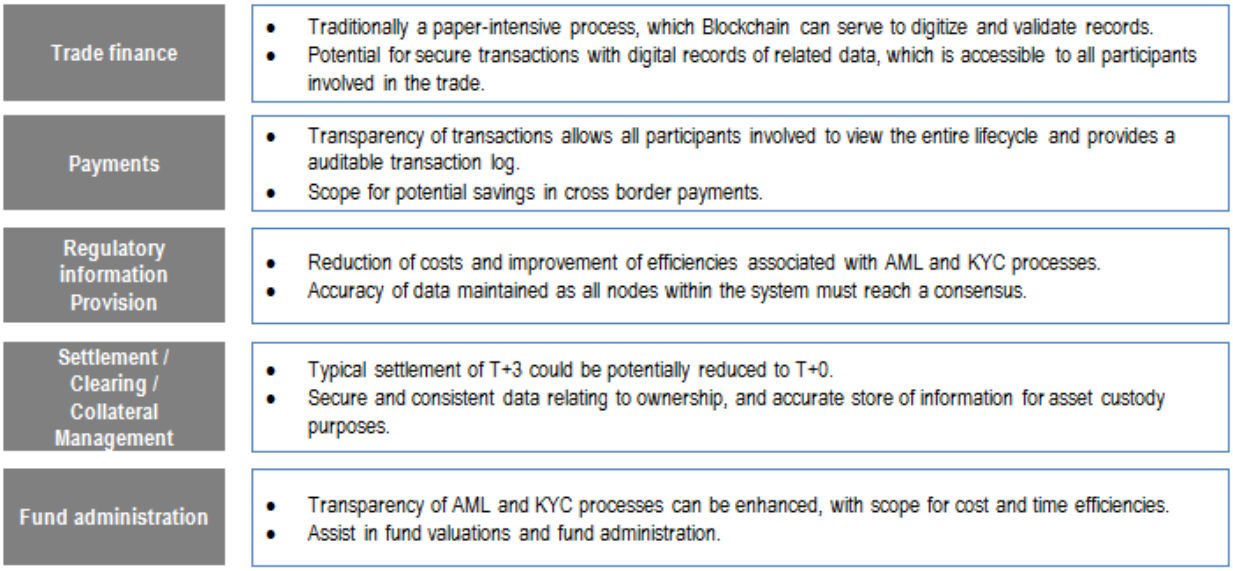


Figura 3.11 Le potenzialità della tecnologia Blockchain adibita nel settore dei servizi finanziari. Fonte "J.P. Morgan Perspecives – Decrypting Cryptocurrencies", J.P. Morgan, pag. 14.

Nella figura 3.11 vengono illustrati le principali applicazioni di questa tecnologia all'interno del settore dei servizi finanziari. In particolare, a sinistra vengono elencate i vari servizi finanziari, mentre a destra vengono riassunte le applicazioni della Blockchain per ogni servizio.

Tuttavia, questa tecnologia non ha solo aspetti positivi anzi può nascondere insidie proprio per l'implementazione all'interno del sistema.

Figura 3.12 Illustrazione dei benefici e degli ostacoli, nell'implementazione della tecnologia Blockchain. Tratto da J.P. Morgan.

Come per ogni scelta bisogna valutare precedentemente i benefici e gli ostacoli di questa tecnologia che, proprio per il suo carattere disruptive, non è facile prevedere in quanto non esistono eventi passati a cui far riferimento.

Nella figura 3.12 viene illustrata la Blockchain tra i suoi benefici ed ostacoli, quale questa tecnologia possa rappresentare.

Il Crowdfunding nel criptomondo: le ICO

Il crowdfunding è un tipo finanziamento alternativo a quello finanziario classico (banche e borse), ed è una sorta di micro-finanziamento che proviene dal basso, mobilita un gruppo di più persone con lo scopo di raccogliere capitali comuni per sostenere organizzazioni e società. Ci sono vari tipi di crowdfunding, da quello meramente filantropico a quello sotto forma di capitale di rischio. Nel criptomondo, invece, il crowdfunding ha assunto le sembianze di una *initial coin offering* (ICO). Così come le criptovalute hanno l'obiettivo di esser l'alternativa alle valute fiat, allo stesso modo le ICO si prefiggono di esserlo con i canali tradizionali della Borsa, delle Banche e dei Fondi di Venture Capital. Questo canale di finanziamento ovviamente è reso possibile dalla tecnologia della Blockchain, talvolta viene anche denominato *crowdsale* e coincide con il rilascio da parte di una cripto-azienda di propri crypto-tokens a scopo di finanziamento. Normalmente, questa prima crea tokens e poi li vende al pubblico in cambio di Bitcoins o denaro. Così facendo la società raccoglie capitale per finanziare i progetti di ricerca e sviluppo e il pubblico riceve in cambio azioni di cripto, diventandone proprietari. Ovviamente, il pubblico compra questi tokens ad un prezzo scontato, con la speranza che il progetto si completi in un tempo relativamente breve per poi vedere il prezzo di questi titoli incrementarsi nel futuro. Prima del 2017 le ICO erano praticamente sconosciute, poi in quell'anno hanno registrato un'esplosione senza precedenti: l'offerta di nuove valute ha raccolto oltre $ 6 miliardi, questo proprio di pari passo con il crescente interesse del criptomondo che da nicchia di mercato è passato a mercato di massa. Questo ovviamente ha implicato comportamenti del tutto irrazionali, perché ci sono state anche episodi di truffe, questo perché non tutte le offerte di nuove valute erano destinate a scopi di finanziamento. Per dar un termine di paragone, nel 2016 ci sono state solamente trenta ICO, per un valore di $ 94 milioni, mentre per l'appunto nel 2017 si è superata la soglia di $ 6 miliardi di fondi per un totale di 885 nuove valute.

Il primo progetto per il lancio di una ICO è stato nel 2013 da parte di Mastercoin che ha raccolto $ 5 milioni di Bitcoins vendendo i propri tokens. Molte altre hanno seguito lo stesso metodo, per esempio: Ethereum nel 2014 ($ 18 milioni) e Waves nel 2016 ($ 16 milioni).

Attraverso questo metodo vengono finanziati i cripto-progetti, salvo che il prodotto presentato sia voluto dal mercato e che esista un team competente dietro.

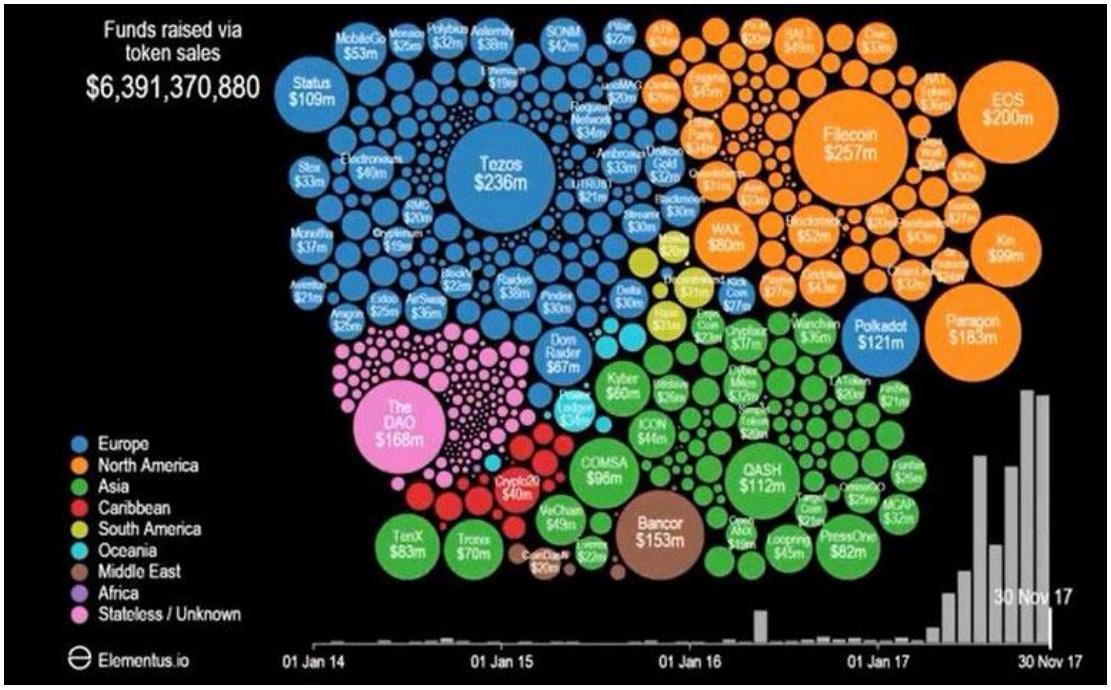


Figura 3.12 L'esplosione delle ICO per finanziare progetti di Blockchain nel 2017, per distinzione geografica. Fonte: "Bitcoin Generation" Nòva, Sole 24h.

A differenza delle IPO (initial public offering) in cui l'azienda cede quote del proprio capitale per ottenere denaro, nelle ICO (offerte iniziali di valute) i firmatari non ricevono quote di capitale (azioni) ma *token*: ossia semplicemente un gettone digitale equivalente ad una nuova emissione di criptovaluta. Qui il token diventa un nuovo *assett digitale* creato grazie alla tecnologia della Blockchain, dove verrà scambiato su piattaforme online dedicate. Proprio per come sono strutturare, le ICO vengono facilmente associate al Crowdfunding, ossia a quel metodo di finanziamento che utilizza il web come tramite comunicativo per aziende ed individui nella raccolta di finanziamenti anche di piccole entità, attraverso piattaforme online predisposte. Ci sono due differenze tra l'una e l'altra: la prima è l'assenza di un intermediario nelle ICO e la seconda è che nel crowdfunding si utilizzano le valute fiat e non le valute digitali come nelle ICO. Il mercato delle ICO è rimasto per anni fuori da ogni tipo di regolamentazione perché è un mercato nato da poco. Come si vedrà nel prossimo capitolo, alcuni Stati hanno preso posizione, per esempio Cina e Corea del Sud le hanno vietate mentre altri stanno cercando di capire che prassi seguire, ed è proprio per questo che il mercato delle ICO è come il *Far West*.

Nel 2017 c'è stata l'esplosione del criptomondo e in aggiunta anche le aziende hanno manifestato grande interesse per questo metodo alternativo di finanziamento, forse proprio per la sua praticità e convenienza.

Proprio come per ogni scelta di investimento, il mercato ha scommesso su queste forme alternative, perché gli è stato garantito grandi ritorni economici, ma ad ogni modo non sono mancate episodi di truffe, perché il mercato non è del tutto trasparente e chiaro. Infatti, si sono verificati episodi in cui le cripto-aziende, dopo aver raccolto centinaia di migliaia di dollari con un'ICO, si sono dileguate rapidamente. Non sono mancati anche casi di attacchi di hacker. Infine, non si deve dimenticare lo scopo ultimo dei token, ossia la loro utilizzazione come moneta e nel mercato secondario, in cui vengono scambiate, il loro prezzo resta estremamente volatile ed illiquido, quindi questo è un ulteriore rischio che si accolla l'investitore.

Funzionamento:

In una IPO classica, una società che vuole quotarsi in Borsa deve inizialmente dirigersi in una o più banche sottoscrittrici per pianificare dettagliatamente il numero di azioni da collare sul mercato, il prezzo e i relativi tempi, nonché tutti le peculiarità dell'operazione. Inoltre, si dovrà redigere un prospetto informativo specifico ed attendere che l'autorità di controllo dei mercati finanziari (in Italia c'è la Consob), controlli e verifichi in dettaglio il documento presentato, e se questo è legittimo in termini di legge. Solo successivamente, con l'approvazione dell'autorità preposta al controllo, si potrà rivolgere al mercato. In definitiva è un iter abbastanza complesso sia termini burocratici che economici.
Mentre se una società sceglie l'alternativa ICO, questa complessità si riduce notevolmente. Nella ICO, in linea teorica occorre presentare:

- un sito web per presentare al pubblico l'offerta;
- una network Blockchain su cui fare riferimento (per ora la più richiesta è quella di Ethereum, perché è in grado di regolare gli smart contracts);
- un documento denominato *white paper*, adibito per comunicare i dettagli dell'offerta;
- un'efficace campagna marketing online per farsi conoscere agli investitori.

Ovviamente se l'offerta raccoglierà consenso tra il pubblico, questo dipenderà anche come verranno eseguite le fasi. Normalmente le ICO prevedono una fase di prevendita dei tokens a prezzi ridotti, e questo processo può durare dai diversi giorni a pochi minuti, perché questo è ulteriormente influenzato anche dall'entusiasmo del mercato per il criptomondo (com'è accaduto nel 2017). Di base c'è un obiettivo da raggiungere, e se questo non viene pervenuto, verranno rimborsati i sottoscrittori.

Invece, se l'obiettivo viene raggiunto, i tokens prescritti inizieranno a circolare sui mercati secondari, ossia dove vengono scambiate le valute digitali. Trovare i tokens sulle piattaforme più utilizzate di trading di solito è un fattore che premia sul mercato.
In particolare, un'azienda può emettere due tipi di ICO, quindi oltre all'*equity token* (di cui si è già parlato precedentemente) si possono effettuare delle *utility token* ovvero dei buoni sconto per l'utilizzo dei servizi che l'azienda erogherà in futuro. Questo servizio le accomuna maggiormente al crowdfunding. Non tutti i tokens hanno le stesse caratteristiche perché ogni azienda ha la sua politica decisionale. Infatti, un'ICO può avere: dei diritti di voto, può essergli assegnata una quota degli utili futuri, ma può anche prevedere niente di tutto questo.
Proprio come per il criptomondo, anche nelle ICO c'è stata un'esuberanza irrazionale tra il pubblico. Infatti, per molti osservatori c'è stato lo stesso clima di quello della bolla delle dotcom dei primi anni del ventunesimo secolo. Questa esuberanza è dovuta dalla tecnologia Blockchain e per questo molti aspirano a puntare su una possibile prossima *Google*. Tuttavia, bisogna prestare molta attenzione perché non tutti i progetti sono destinati a sopravvivere. Nel corso di questi anni si sono verificate episodi sbalorditivi, caratterizzati da un successo incredibile, come per Ethereum i cui tokens hanno registrato un rialzo oltre il 300,000 % dal giorno dell'ICO. Nonostante ciò, si sono verificate anche truffe eclatanti, come per Confido che aveva raccolto $ 375,000 ma il progetto è svanito nel nulla. Oppure l'attacco di hacker subito dal The Dao, dove si è sottratto Ethereum per un valore di $ 50 milioni appena un mese dopo l'ICO da $ 150 milioni.
Senza dimenticare il tema della trasparenza che, a differenza delle IPO e quindi di chi si quota in Borsa, nelle ICO non è minimamente richiesta. Infatti, nelle IPO c'è una serie di documenti da presentare come garanzia per gli investitori, i quali attraverso i bilanci possono farsi un'idea del business della società e quindi comprendere l'effettivo valore offerto dalle quotazioni in Borsa. Tutto questo non è presente in un'ICO e per cui non si riesce a sapere se i valori offerti siano giustificati.
A riguardo si può citare l'ICO della Eos.io che ha messo insieme una capitalizzazione di oltre i $ 6 miliardi, ma a parte le informazioni che si possono trovare sul sito internet e delle comunicazioni che ha fatto il fondatore Blumer non si ha nessun dato di bilancio, neppure un business plan che possa spiegare il business model utilizzato dall'azienda (che peraltro è americana ma con sede nelle isole Cayman).

Capitolo IV – La Regolamentazione del criptomondo

In questo capitolo verrà descritto normativamente il criptomondo, ovvero si andrà ad identificare se le criptovalute siano o meno regolamentate. Inizialmente, si cercherà di classificare questa tecnologia, quindi si andrà identificare la loro natura intrinseca, ossia dapprima riprendendo la tematica della moneta e poi successivamente si farà un breve inciso sull'asset d'investimento. Nella seconda parte del capitolo, si andrà ad analizzare come il mondo è orientato sulle criptovalute, quindi lo studio inizierà dai Paesi extra-Cee fino ad arrivare all'Italia. In particolare, come verrà esplicato successivamente, non esiste una vera e propria regolamentazione mondiale, ma ogni Stato agisce individualmente, per questo motivo si parla di regolamentazione "a macchia di leopardo".

Inoltre, quando verrà analizzato il criptomondo sotto la lente legislativa italiana, si riporteranno tutte le problematiche annesse ad esso, quale per esempio il monitoraggio fiscale.

Infine, si cercherà di trarre delle conclusioni riassuntive, al fine di cercare di individuare le possibili normative future.

Determinazione della "*natura*" della Cryptocurrency

In questi anni si è discusso sulla natura di Bitcoin e più in generale delle criptovalute chiedendosi se si tratti di vere e proprie monete. Esistono diversi filoni di studi a riguardo: come verrà esplicato nei paragrafi successivi del capitolo, in Italia l'Agenzia delle Entrate ha qualificato le criptovalute alla stregua delle valute estere aventi corso legale, trattando il Bitcoin come una moneta a tutti gli effetti. Questa operazione era atta però a individuare una normativa fiscale applicabile.

Di seguito vengono elencate le possibili nature delle criptovalute:

- Moneta;
- Valuta estera;
- Beni Immateriali;
- Commodity;
- Security (titolo);
- Diritti di Baratto (Barter Rights);
- Sistema di pagamento.

In questa analisi, verrà trattata la natura della moneta, perché per l'appunto le valute digitali sono nate per assolvere questo scopo.

Un modo per verificare la correttezza nel definirle monete è un'analisi comparativa tra le monete tradizionali e quelle digitali. L'analisi consiste in due parti: in una si evidenzieranno le caratteristiche a ciò che viene considerato moneta, e poi successivamente si analizzeranno queste caratteristiche all'interno delle criptovaluta, per verificare se sono riscontrabili anche nel criptomondo. Successivamente, cercheremo di capire se le valute digitali rientrino nella categoria degli Asset d'investimento.

Da non dimenticare che quanto verrà analizzato nei prossimi paragrafi è il frutto di considerazioni tratte nel momento della scrittura dell'elaborato, cioè inizio giugno 2018; per cui, visto che si tratta di una tecnologia innovativa e che il suo inquadramento giuridico ed economico è in divenire, in futuro potrebbero sorgere disposizioni diverse.

Cryptocurrency come Moneta?

La moneta tradizionale assolve tre funzioni:

- Unità di Conto: secondo gli storici è la funzione più antica, ed è considerata come oggetto-moneta è viene usata come unità per misurare il valore.
- Mezzo di Scambio: consente la possibilità di accettare uno scambio di un oggetto in cambio di un altro. Alla base di questo c'è il rapporto fiduciario, ossia che l'oggetto scambiato si possa adibire per altri scambi. Per far si che sia accettata dalla collettività è essenziale che vi sia l'aspettativa/fiducia e che la moneta si possa utilizzare come mezzo di scambio. Come è stato esplicato nel primo capitolo, ci sono vari fattori che influiscono sulla fiducia tra gli utilizzatori, dalle proprietà intrinseche della moneta (oro e altri metalli preziosi), dalla sua fungibilità, omogeneità ed incorruttibilità. Un chiaro esempio di questo lo troviamo in passato, quando veniva coniata la moneta-merce.
- Riserva di Valore: è la capacità dell'oggetto di conservare il suo valore nel tempo, quindi di detenere moneta per un uso futuro, senza la preoccupazione che si possa deteriorare (svalutare).

In Aggiunta:

- Mezzo di Pagamento: in realtà, esiste questa funzione che si contrappone al mezzo di pagamento, per una caratteristica fondamentale: la dimensione temporale. In particolare, il mezzo di pagamento non ha una dimensione temporale, perché consiste nell'utilizzazione della moneta nello scambio immediato e questo che rende possibile l'interscambio degli oggetti. Mentre la funzione di mezzo di pagamento consiste nella possibilità di estinguere i debiti che sono stati contratti. Questa funzione riesce ad assolvere al bisogno del potere liberatorio, ossia consente al debitore di sgravarsi dall'onere debitorio. Quindi qui si trova sia la dimensione temporale da una parte sia la presenza di un organo socio-giuridico-economico che autorizza questo potere liberatorio alla valuta stessa.

Rapido confronto con le Criptovalute:

Fatto un breve inciso sulle quattro funzioni delle criptovalute, si può fare un confronto con queste caratteristiche all'interno delle valute digitali:

- Funzione di unità di conto: questa proprietà non viene soddisfatta secondo diversi esperti. In realtà, questa proprietà è negativa nei Bitcoin e nelle valute digitali dove l'offerta dei tokens è limitata. Questo perché quando esiste un limite massimo nella coniazione di nuovi token, questo lo rende variabile al mutamento della domanda. Quindi proprio come un metro, con il trascorrere del tempo si potrebbe allungare o accorciare e non è utile nella contabilizzazione.
- Funzione mezzo di scambio: in questo senso le valute digitali, secondo gli esperti, l'assolvono pienamente. Sebbene ci siano fortissime oscillazioni di prezzo e della variazione del suo valore, non ci si deve soffermare a questo, anzi bisogna guardare attentamente al suo funzionamento, infatti questa funzione è per definizione a-temporale. Se si decidesse di scambiare un bene materiale per un certo numero di moneta in un determinato momento, le valute digitali lo consentirebbero pienamente. Al contrario, invece, non si potrà fissare ex-ante un prezzo del bene materiale perché le valute digitali non sono un'unità di conto.
- Funzione mezzo di pagamento: le criptovalute non possono assolvere a questa funzione. O meglio, potrebbero assolverla, ma vista l'impossibilità di inserire la temporalità delle transazioni all'interno delle valute digitali, risulterebbe un problema di efficienza. Idealmente si potrebbe anche fare, ma si è in presenza di una forte volatilità, quindi risulterebbe assai problematico perché bisognerebbe preoccuparsi di verificare continuamente la variazione del valore del token, per usarlo come mezzo di pagamento nelle transazioni reali. Uno degli obiettivi cardini di una moneta è l'efficienza, ossia nelle transazioni commerciali non può esserci l'ulteriore problema nella determinazione continua del valore di una valuta, ciò comporterebbe un rischio aggiunto.

Cryptocurrency come Asset d'investimento?

In questa analisi si cerca di analizzare il criptomondo sotto un'altra prospettiva, ossia verificare se le valute digitali possono essere considerati alla stregua di asset d'investimento. Diversi esperti parlano di criptovalute come se fossero asset d'investimento e lo fanno usando la similitudine dell'oro digitale. Le criptovalute vengono paragonate a questo materiale prezioso per queste caratteristiche: scarsità, fungibilità, incorruttibilità ed omogeneità. Tutte queste proprietà vengono garantite dalla tecnologia Blockchain e dalla crittografia.
In definitiva, esiste una somiglianza con questa categoria, questo perché è fattibile acquistare le valute digitali per poi liquidarle cercando di realizzare nell'operazione importanti plusvalenze. Certamente non si può affermare che questa operazione sia un'opportunità per i risparmiatori, vista l'altissima volatilità dell'operazione.

La regolamentazione delle Criptovalute "*a macchia di leopardo*"

Se l'anno 2017 è stato l'anno dell'esplosione del criptomondo, sicuramente il 2018 è visto come l'anno della sua regolamentazione a livello mondiale. Ma è davvero così?
Ci sono state altissime aspettative a riguardo, ma effettivamente fino a maggio 2017, si è assistito a comportamenti lievi su questo fronte. Complici svariati fattori, come i Paesi che strizzano l'occhio a questo nuovo mondo e che si trovano in contrasto con altri che vogliono addirittura vietarlo (o già lo hanno fanno). Nel mezzo vi si trovano altri Stati che invece vogliono regolamentare tutto il criptomondo, ai fini di aumentarne la sicurezza.
Questo paragrafo sarà suddiviso in tre parti: la prima è riferita alla regolamentazione a livello mondiale, e quindi vedere come si stanno comportando le varie istituzioni internazionali; nella seconda invece si farà un focus sull'Europa e sulle decisioni della BCE, che più volte si sono espresse a riguardo; e infine si vedrà in maniera dettagliata come questo settore è inquadrato nell'ordinamento giuridico italiano.

Nel Mondo

La regolamentazione internazionale è divisa e ha prodotto leggi in contrasto riguardo la regolamentazione del criptomondo. Molti Paesi ne vorrebbero una uniforme, per contrastare fenomeni dannosi per tutta l'economia reale.
Di seguito verrà esposto come le grandi istituzioni finanziarie si sono espresse in questi anni. Attualmente, l'ecosistema del criptomondo si presenta sotto una veste grigia una sorta di *new wild west*, in cui l'oro attira truffatori, prestigiatori e furfanti e non ci sono né mappe né tantomeno sceriffo. Proprio come l'oro, le valute digitali stanno attirando tutto il mondo che tenta di imporre loro dei vincoli ma ciò tecnicamente impraticabile. Senza dimenticare che le transazioni di molte fra queste lasciano delle tracce elettroniche (seppur non veritiere), facilitando le investigazioni rispetto alle transazioni in contante e in metalli preziosi.

G20:

Da tempo che si vuole mettere in agenda del G20 il tema delle criptovalute, infatti già a dicembre 2017 il ministro delle Finanze francese Le Maire affermò:
"risorsa speculativa che può dissimulare ogni tipo di attività illegale; è necessario esaminarlo e vedere come, insieme a tutti i Paesi del G20, possiamo regolarlo"[133].
Le più grandi preoccupazioni che suscita il criptomondo sono la tutela dei risparmiatori, il finanziamento del terrorismo, nonché il riciclaggio di denaro sporco.
A febbraio 2018 si è espresso Mario Draghi, il governatore della BCE, affermando che non spetta alla Banca Centrale Europea il pronunciamento, ma lo sono i Paesi sovrani.
A spingere fortemente su una normativa comune per regolare il mercato delle criptovalute sono Francia e Germania. A marzo 2018 si è riunito il G20 a Buenos Aires, ma purtroppo non si è trovato un unico apparato normativo comune. I 20 ministri delle Finanze hanno fatto fatica a normare tutta la complessità del criptomondo, e quindi riuscire a regolamentare il cripto-settore. Ad ogni modo, i Ministri delle Finanze non hanno classificato il bitcoin e le altre criptovalute alla stregua delle monete sovrane nazionali (fiat), e in aggiunta si sono dimostrati preoccupati sulla possibilità che vengano adibite per finanziare il terrorismo. Secondo il presidente della banca centrale

[133] Tratto da: "http://www.ilsole24ore.com/art/mondo/2017-12-27/i-bitcoin-nell-agenda-prossimo-g20--170020.shtml?uuid=AEQnjnXD".

dell'Argentina Sturzenegger, verranno date delle raccomandazioni specifiche entro luglio 2018.

Tuttavia, rimane la difficoltà di trovare una posizione comune tra chi vuole una maggiore regolamentazione a chi invece non la vuole. Secondo Gossens, lo specialista di diritto bancario della BianchiSchwald, si potrà trovare dei compromessi come è stato fatto nei Cantoni Svizzeri. Ancora, egli stesso afferma che combattere l'anonimato è fondamentale in modo tale da ridurre comportamenti illegali, quali truffe e riciclaggio di denaro.

Inoltre, viene riconosciuta l'innovazione tecnologica sottesa alle valute digitali, ossia la blockchain, con la speranza che possa effettivamente migliorare il sistema finanziario e dell'economia in generale. Alla fine del comunicato, è stato chiesto al FSB (*Financial Stability Bard*), in concomitanza con altri SSB (tra cui CPMI, IOSCO e FATF) di riferire dell'operato dei loro cripto-consulenti entro luglio 2018.

Rispetto a quanti pensavano a forti restrizioni del criptomondo, l'ultimo G20 ha dato un primo riconoscimento ufficiale delle criptovalute riconoscendone un ruolo positivo per l'economia (stante il fatto dei possibili eventi negativi che possono generare: comportamenti illeciti e bolle finanziarie) e nei documenti ufficiali vengono denominate: *criptoasset*.

Financial Stability Board (FSB):

L'organismo internazionale, che controlla i potenziali rischi per la stabilità finanziaria mondiale, ha espresso al G20 che non vede un reale pericolo per il criptomondo nell'economia mondiale. Il presidente Carney, nonché governatore della Bank of England, ha confrontato l'intera capitalizzazione del criptomondo che a marzo 2018 era inferiore all'1% del Pil mondiale, con il valore nozionale del credit default swap (della crisi finanziaria 2008), il quale era al 100% del Pil mondiale.

Stati Uniti d'America:

Negli U.S.A. non esiste un regolamento specifico sulla criptovaluta, anche se il Paese ci sta lavorando. Tuttora, il Governo centrale ha lasciato libera scelta ad ogni stato federale, se regolamentare o meno l'utilizzo delle valute digitali. Si può citare lo Stato di New York, il quale già dal 2015 ha iniziato a regolare le società impegnate nel settore del criptomondo attraverso un'agenzia statale. Sempre in quell'anno il Paese le aveva classificate come *commodity*. La Securities and Exchange Commission (SEC) ha lanciato avvertimenti sui

reali rischi legati al criptomondo, ha messo fine ad alcune ICO e inoltre ha comunicato che vorrebbe una vera regolamentazione a riguardo di essa. Oltre alla SEC; anche il segretario al Tesoro (Steve Munchin) ha comunicato preoccupazioni simili. Inoltre, il Financial Stability Oversight Council (FSOC) ha ideato un comitato per investigare sul mercato della crittografia che pone l'attenzione principalmente sull'aumento di attività illegali.
A giugno 2017, l'FBI ha comunicato pubblicamente di aver bisogno di 80 nuove posizioni lavorative, con un budget pari a $ 21.6 milioni per migliorare la capacità investigative sulle attività illegali legate al dark web e alle valute digitali.
In uno studio recente, pubblicato dal Sole 24 ORE, si evidenziava come un quinto dei giovani universitari utilizzano le risorse monetarie adibite per l'istruzione per acquistare criptovalute.
A gennaio 2018, il bitcoin provò ad entrare nel tempio della finanza: *Wall Street*, ma la SEC (la Consob americana) si impose e bloccò questo tentativo. Infatti, due società volevano quotare degli Etf (strumenti derivati che offrono la possibilità di scommettere su un bene), ma la SEC bloccò questo tentativo per tutelare gli investitori, per via dell'inspiegabilità della sua volatilità.

Australia:
Il governo australiano ha optato per un approccio *hands-off* nei confronti del criptomondo. Tuttavia, nel 2017 si sono rivelate delle problematiche. Cosicché alla fine del 2017, il governo ha provato a seguire la prassi del Giappone, cercando di regolamentare le criptovalute.

Giappone:
Il Giappone è stato il primo Paese al mondo ad accettare bitcoin e le criptovalute, in particolare è stato definitamente regolamentato, ed è stato legalmente riconosciuto come moneta a corso legale. Nello specifico, i legislatori hanno esaminato le piattaforme sotto l'antiriciclaggio e hanno categorizzato il bitcoin alla stregua di un metodo di pagamento prepagato. Questa posizione forte ed aperta verso il criptomondo ha fatto ben separare agli investitori. Successivamente, è accaduto il furto più grande della storia del criptomondo. Infatti, è stato hackerato un exchanger il 26 gennaio 2018, dopo quel evento l'entusiasmo è stato frenato per tutto il cripto-settore. Questo evento ha registrato una

perdita del token NEM, per un valore pari a $ 530 milioni. Questo ha fatto ricredere il Sol Ponente restringendo la piattaforma del criptomondo.
Ad aprile 2018, il governo nipponico sta cercando nuove regole per le ICO, cercando così di trovare delle linee guida al fine di prevenire il riciclaggio di denaro sporco, restringere la pratica di insider trading ed aumentare gli sforzi di cybersecurity.
Nel frattempo, le criptovalute conquistano la fascia tra i 20 e i 30 anni della popolazione, infatti il 14% dei giovani lavorati possiede valuta digitali. Inoltre, il numero di aziende del settore crittografico è aumentato esponenzialmente, creando problemi in termini di carenza di ingegneri e programmatori, cosicché ha portato ad aumentare gli stipendi fino al 30% del settore.

Cina:
La Repubblica Popolare Cinese è l'esempio perfetto di un Paese che è ostile al bitcoin e più in generale di tutto il criptomondo. Non ha avuto sempre questa politica, anzi una volta proprio in questo Paese c'era il numero più di trading delle criptovalute. Le prime restrizioni arrivarono per le ICO, le quale diventarono illegali, per poi vietare tutti i conti bancari legati ai cambi. Inoltre, la Cina ha vietato qualsiasi accesso a Internet o al telefono cellulare legato alla crittografia. L'obiettivo della Cina è quella di diminuire la fuga dei capitali, ed eliminare la corruzione.
Le ICO sono diventate illegali nell'agosto 2017. Questo però ha favorito il Bitcoin perché le criptovalute che utilizzavano le ICO come raccolta di fondi, la maggior parte utilizzava la blockchain di Ethereum. In questo modo la Cina ha voluto privilegiare il Bitcoin (in cui il Paese ne è leader) rispetto ad Ethereum, senza dimenticare che i più grandi mining pool si trovano proprio in questo Paese. Giusto per dare due numeri di riferimento, secondo un report di Bloomberg di dicembre 2017, veniva dichiarato che circa il 58% del mondo di Mining Pools erano situati in Cina, seguita al 16% dagli U.S.A.
Da ultimo, è fondamentale evidenziare come il governatore della Banca Centrale Cinese (PBOC) Zhou Xiaochuan abbia comunicato l'intenzione di creare una possibile criptovaluta ufficiale cinese. Secondo il governatore cinese le valute digitali sostituiranno quelle tradizionali, quindi è essenziale sviluppare delle monete fiat digitali. È utile ipotizzare che la Cina stia testando una sua possibile criptovaluta di Stato.

Venezuela:

Il 20 febbraio 2018, Il Venezuela è il primo Paese al mondo ad aver lanciato una valuta digitale ufficiale: la *petro-token*. Nicolàs Maduro lancia questa valuta digitale, cercando di salvare il proprio Paese che è nel mezzo di una crisi umanitaria ed economica senza precedenti. La criptovaluta venezuelana sarà garantita dal petrolio e l'obiettivo è quello di aggirare le sanzioni occidentali. L'operazione consisterà di lanciare 100 milioni di *petro-token*, dove ciascun token sarà garantito da un barile di greggio, per un valore stimato sui $ 6 miliardi. Ad ogni modo, sorgono forti dubbi su tale riuscita perché da una parte risulta difficile stimare l'estrazione di petrolio dal pozzo Ayacucho 1 nell'Orinoco, e in più questo sarà estratto da una joint venture. L'opposizione al governo è fortemente contraria a questa politica, ossia di coprire il debito del Venezuela con l'estrazione del greggio. Cionondimeno, il presidente Trump e il tesoro americano hanno ben specificato che chi acquisterà il *petro-token* sarà considerato in violazione delle sanzioni imposte da U.S.A. ed Europa.

Questa mossa, di aggirare le sanzioni occidentali, ha fatto muovere persino il **Cremlino**. Infatti, il presidente Putin è interessato ad una possibile creazione di una **criptovaluta russa**, la *cripto-rublo*.

Ghana:

Il Ghana è uno dei 6 Paesi che hanno vietato il bitcoin. In particolare, il governatore della Banca del Ghana ha affermato che le criptovalute non hanno corso legale nel Paese.

Sudafrica:

A differenza della maggior parte degli Stati africani, il Sudafrica è abbastanza aperto per le criptovalute. In particolare, nel 2017 il Paese era favorevole ad una regolamentazione per il bitcoin. Certo che rimane la curiosità di vedere come si evolverà nel futuro, visto che il rand sudafricano dipende dallo yuan cinese, bisognerebbe vedere se questa dipendenza si rifletterà anche su una possibile regolamentazione in materia di valute digitali.

BRI:

La Banca dei regolamenti internazionali (*Bri*) ha raccolto le opinioni delle varie Banche Centrali e di queste ne ha pubblicato un'analisi, sottoscritta dall'analista della BCE Löber e da Houben della Banca Centrale Olandese. In questa analisi emerge un parere negativo verso l'emissione delle valute digitali, perché potrebbero minacciare la stabilità di tutto il sistema finanziario internazionale. La minaccia è abbastanza reale, perché è molto probabile che le valute digitali diventerebbero rivali rispetto alle valute fiat tradizionali.

In definitiva, Le principali autorità mondiali stanno studiando i possibili eventi, sicuramente vogliono tenere sotto controllo il criptomondo, anche se questo risulta ben difficile, proprio perché ci sono vari opinioni contrastanti a riguardo.

In Europa

"Le valute virtuali sono come 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"[134].

Questa è la definizione data dall'Autorità bancaria europea (*Eba*) che ha dato nell'aprile 2018. Come verrà descritto, ogni Stato europeo si sta muovendo per conto proprio, e la Bce ha preso le distanze su una probabile regolamentazione sostenendo che spetta direttamente agli Stati e non alla Banca Centrale.

A febbraio 2018, Mario Draghi, il Governatore della Bce ha affermato:

"Un euro oggi, è un euro domani. Il suo valore è stabile. Il valore del Bitcoin oscilla enormemente. Per questo motivo la Bce non considera la criptovaluta una moneta. Ma anche per una seconda ragione: l'euro è supportato dalla Banca centrale europea, il dollaro dalla Federal Reserve, le monete sono sostenute dalle banche centrali. Nessuno sostiene il Bitcoin"[135]. Questo pensiero si accosta perfettamente all'azione intrapresa il 7 settembre 2017 da Draghi nei confronti della Banca Centrale dell'Estonia, dove in particolare il Paese volle lanciare una propria valuta digitale statale: l'*estcoin*.

[134] Tratto da: "http://argomenti.ilsole24ore.com/parolechiave/criptovaluta.php".
[135] Tratto da: "http://www.repubblica.it/economia/2018/02/13/news/bce_askdraghi_bitcoin_crisi-188765722/".

In quel frangente il Governatore ha affermato che la Bce non avrebbe mai consentito a nessun Paese dell'Unione europea ad introdurre una propria valuta digitale.
La Bce dopo aver illustrato dettagliatamente nel 2015 il criptomondo, ha preso le distanze perché vede le criptovalute alla stregua di asset anziché di monete vere e proprie. Inoltre, secondo il Presidente del Consiglio di Vigilanza Daniele Nouy non c'è per ora un sostanziale coinvolgimento delle banche regolate dalla Bce delle criptovalute. Aggiunge ulteriormente che non esiste per il momento una regolamentazione della Bce, perché non è attualmente una priorità.

Svizzera:
L'unico Paese europeo che ha accettato il mondo delle criptovalute e la loro tecnologia è stata proprio l'autorità elvetica, infatti è diventata uno fra i primi hub europei per lo studio e lo sviluppo della Blockchain e del criptomondo. Inoltre, è stato pubblicato un primo regolamento sulle ICO e questo potrebbe esser traslato anche negli altri stati europei.
Secondo Gossens, il vero problema del criptomondo è legato all'anonimità e questa dovrebbe essere combattuta all'unisono da tutti i governi perché il rischio di comportamenti illegali, come frodi e riciclaggio di denaro sporco, rimane sempre molto alto. Nel cantone di Zug, è diventata la capitale della *crypto-valley*, anche grazie alle vantaggiose condizioni fiscali. Inoltre, è stata fondata la *Crypto Valley Association*, un'associazione no-profit che ha l'obiettivo di visionare e garantire il lancio delle ICO.
In questa zona si trovano molte start-up pronte a lanciare le ICO e progetti Blockchain. La Svizzera è orientata in questo settore e a settembre 2017 la città di Zoug ha comunicato che nascerà un app che consentirà agli abitanti di crearsi un'identità digitale (anche in abbinamento di una carta d'identità), e questa si baserà sulla tecnologia della Blockchain di Ethereum.

Francia e Germania:
Sia Francia che Germania hanno alzato le barriere contro tutto il criptomondo, nella speranza di bloccarne l'utilizzo in attività illecite, quali ad esempio: l'elusione fiscale e il riciclaggio di denaro sporco allo scopo di finanziare il terrorismo. Secondo questi Stati, l'unico modo per arginare questi fenomeni illegali è quello di agire globalmente all'unisono.

Attualmente per la legge tedesca, le valute digitali sono meri strumenti finanziari, ovvero rientrano sotto forma di denaro privato e per questo vengono tassati come capitale. Ma per utilizzarli sono richieste delle licenze.

Spagna:

In Spagna si evita il problema del pagamento delle tasse. Qui vengono tassate come sistemi di pagamento elettronico alla stregua delle scommesse. Mentre devono essere ancora regolamentate per quanto riguarda le altre aree.

Austria:

L'Austria regola i servizi finanziari che coinvolgono le valute virtuali.

Belgio:

La Banca Nazionale del Belgio ha comunicato i rischi connessi alle valute digitali agli investitori e risparmiatori, in più dichiarandole proprietà illegali, mentre al contrario, al Ministero della Giustizia si intende regolamentarle.

In Italia

L'Italia è stato il primo paese al mondo a dare una definizione giuridica delle criptovalute, anche se limitata alla visuale delle regole di prevenzione del riciclaggio.
In aggiunta, è stato il primo Stato europeo a introdurre regole sugli exchangers così creando una figura innovativa: il cambiavalute virtuale. Ma è meglio vedere le cose per ordine. A seguito dell'emanazione della prima avvertenza dell'Autorità Bancaria Europea (EBA) nel 2014, si è espressa subito dopo la Banca d'Italia nel gennaio 2015. In quella occasione è stato emesso uno specifico documento in cui venivano descritte le caratteristiche di queste monete virtuali, richiamando da una parte la rischiosità del criptomondo e dall'altra spostando l'attenzione sui nuovi operatori che si lanciavano su questo mercato, i quali violavano le disposizioni normative.
Nel 2016 l'Agenzia delle entrate, in risposta ad un interpello di un operatore intermediario di valute digitali, si associa al pensiero della Corte di Giustizia dell'Unione Europea, e quindi associa l'attività di intermediazione in criptovalute alle tradizionali operative relative a diverse, banconote e monete di cui all'art. 135, paragrafo1, lett. e), della Direttiva 2006/112/CE.
Ad ogni modo, le criptovalute non ricevano una chiara natura giuridica. Questo ha comportato e comporta tutt'ora problematiche sull'inquadramento di ogni singola operazione, per le istituzioni e per il Fisco.
Per quanto affermato nella risoluzione n. 72/E/2016 delle Agenzia delle entrate, assimilerebbe le criptovalute nella sfera della moneta, dove viene intesa: come un'unità di conto, mezzo di scambio e funzione da riserva di valore. Invece, al contrario per l'EBA e per la Banca d'Italia, affermano che non si può trattare di una moneta, ma piuttosto di strumenti finanziari.
Sempre la Banca d'Italia interviene e afferma che potrebbe trattarsi di una forma di baratto, anche se questo va in contrasto con il D. Lgs. n.90/2017 (che va a modificare il D. Lgs. n. 231/2007), il quale espone gli operatori di valute elettroniche tra gli operatori finanziari paragonabili ai cambiavalute, ma specificando che le criptovalute non hanno uno status giuridico di moneta, ma comunque vengono accettate dalle persone fisiche e giuridiche come mezzo di scambio. In tema di rintracciabilità e controllabilità delle operazioni e degli operatori, interviene da ultimo un progetto di Decreto ministeriale, in cui verranno specificate le modalità e le tempistiche per i prestatori di servizi di valute

digitali, che saranno tenuti a comunicare al Ministero dell'Economia e delle Finanze la propria attività sul territorio italiano.

Effetti fiscali e dichiarativi

Innanzitutto, è necessario definire le criptovalute perché è da questo che dipenderanno le disposizioni giuridiche. Le criptovalute rappresentano una forma anomala, rispetto alle tradizionali valute fiat, di riserva di valore, unità di conto e mezzo di pagamento. Volendole considerate come una valuta, dove sono caratterizzare da un proprio corso, il che prevede l'esistenza di un tasso di cambio. Questo rende necessario riferirle alla disciplina richiesta per le operazioni in valuta, in particolare per la determinazione di eventuali fattispecie fiscalmente rilevanti. In particolare, possono essere definite come *panvalute*, ossia delle valute accettate da chiunque che decide di aderire a tale protocollo, una valuta creata e utilizzata sul web e che non conosce confini geografici.
La criptovaluta può essere trattata normativamente in modi differenti, dipendentemente dal tipo di inquadramento che si vuole dare, proprio perché non esiste una vera e propria normativa di riferimento. In particolare, possono essere riferite a:

Contante virtuale

Al fine di considerarle come denaro contante bisogna tenere in conto la normativa di antiriciclaggio per non violarla. In particolare, non si potranno effettuare operazioni singole, o tra loro collegate, per importi superiori a € 3,000 alla data dell'operazione. Inoltre, se si vorranno effettuare transazioni transnazionali sarà necessario comunicarlo all'Agenzia delle dogane, proprio come avviene per l'invio o la ricezione tramite plico postale, quando il valore eccede la cifra di € 10,000. In questo caso, se trattate alla stregua di denaro contante queste non rientreranno tra i valori oggetto di monitoraggio (nel quadro RW).
Per quanto riguarda il tema fiscale interviene il T.U.I.R. che stabilisce per i redditi diversi, disciplinati dall'art. 67, la tassazione delle plusvalenze generate dalle operazioni in valuta. È sorprendente notare che in questo particolare contesto, le criptovalute, pur avendo generato nell'ultimo periodo delle enormi plusvalenze, non determino la nascita di un momento impositivo. Questo perché, quando la valuta digitale viene considerata alla stregua di denaro contate, ciò non può rappresentare per il Fisco una materia tassabile in

quanto non è assimilabile a un deposito in conto corrente e l'uso per operazioni di acquisto, non può essere considerato operazioni di investimento.

Deposito di valuta o titoli finanziari

A seconda se consideriamo le criptovalute come valori di tipo finanziario, paragonabili alle transazioni elettroniche e a portafogli di depositi (wallet o depositi su portali di trading) e quindi assimilabili a conti correnti o di deposito di valuta (ricordando che valutare le valute digitali come moneta estera è un errore), il tema fiscale cambia notevolmente.

Esistono obblighi di identificazione e segnalazione degli investitori e delle operazioni di trasferimento (previsione inserita nel D. Lgs. n. 231/2007 a seguito delle modifiche dal D. Lgs. n. 90/2017) per chiunque offra servizi di cambio, acquisto, vendita e deposito di valori in moneta digitale.

L'art. 67 comma 1, lett- c-ter, del T.U.I.R., prevede l'imponibilità fiscale dei redditi diversi, i quali sono composti dalle plusvalenze realizzate attraverso la cessione a titolo oneroso, o il prelievo da depositi e conti correnti di valute estere o nella fattispecie di valute virtuali. In questo caso, la cessione onerosa rileva anche nell'operazione del cambio valuta (per esempio: da BTC a €) come anche nell'utilizzo della moneta digitale per operazioni di acquisto di beni o servizi configura come una forma di prelievo di tale valuta, e quindi si concretizzano momenti impositivi di un'eventuale plusvalenza. Nel dettaglio, qui bisogna prestare particolare attenzione, perché questo si verifica solo e solamente quando il valore complessivo dei depositi e dei conti correnti in valuta abbia complessivamente superato consecutivamente, per sette giorni lavorativi, un valore corrispondente ad € 51,645.69 valutati al tasso di cambio vigente al 1° gennaio dell'anno di riferimento.

Questo criterio di valutazione è un elemento da prendere in considerazione per chi abbia acquistato e venduto o comunque utilizzato criptovalute nel corso dell'anno.

Attraverso un esempio numerico si può dimostrare come questo metodo di valutazione abbia dal principio degli enormi errori. Se si prende in considerazione l'anno 2017, anno in cui tutto il criptomondo ha registrato un enorme interesse sia come tecnologia che di investimento, il valore da prendere come riferimento per calcolare il livello di interesse per l'imponibilità è un tasso di cambio pari a € 905 per Bitcoin, facendo corrispondere a tale data il limite imposto dalla normativa di € 51,645.49, e quindi di conseguenza per

l'anno intero, a circa 57 token. Tenendo presente che nel 2017 si è registrato il picco massimo di prezzo pari a € 15,867 al 18 dicembre, e quindi diventa rilevante per un potenziale capital gain.

Questo rende necessario assolutamente la creazione di una norma ad hoc per evitare, perché qualora si pendesse per assimilare le criptovalute ai depositi in conti corrente, gli speculatori potranno generare enormi profitti senza contribuire in alcun modo alla finanza pubblica. La norma che disciplina un'eventuale plusvalenza imponibile è l'art. 68, comma 6, del T.U.I.R., in cui vengono quantificate come differenza tra prezzo di vendita (tasso di cambio) al giorno del prelievo ed il relativo costo di acquisto, infine deve essere specificato che il costo della valuta estera (nella fattispecie la criptomoneta) deve essere documentata dal contribuente. Questo meccanismo è fattibile quando il contribuente voglia liquidare in un'unica volta la propria posizione. Quindi se ci fossero più liquidazioni e di conseguenza la determinazione del costo della singola operazione utilizzata risulta infattibile, il T.U.I.R. da un'altra strada utilizza, ovvero il minore tra i tassi di cambio mensili accertati con provvedimento dell'Agenzia delle entrate nel corso dell'esercizio in cui si è generata la plusvalenza.

Ad ogni modo, attualmente risultano inapplicabili questi metodi perché da una parte non esiste una chiara definizione di cosa siano le monete virtuali e dall'altra non esiste la registrazione tra i tassi accertati dall'Agenzia delle entrate del tasso di cambio tra l'euro ed alcuna criptomoneta esistente. Data la mancanza di strumenti ufficiali con cui si possa determinare un'eventuale plusvalenza generata, l'unica soluzione coerente è quella di adottare il criterio indicato per la determinazione delle plusvalenze su valute, ossia dalla redazione del quadro RW nelle quali viene adibito il LIFO come criterio di valutazione.

Invece, quando le valute digitali sono depositate presso i wallet e le piattaforme estere, il contribuente dovrebbe dichiararle utilizzando il quadro RW della dichiarazione dei redditi però usando diverse condizioni, come il superamento nel corso dell'anno della soglia di € 15,000 valorizzato al tasso di cambio al 31 dicembre dell'anno d'imposta.

Rimane l'assoggettabilità all'imposta di € 34.20 (IVAFE), presente nel quadro RW, quando nel corso dell'anno il controvalore medio delle valute possedute all'estero eccede l'importo di € 5,000.

Il tema rimane centrale, perché la determinazione del valore delle valute digitali è rilevante ma proprio per l'estrema volatilità delle quotazioni, i metodi ad oggi indicati sembrano inadeguati ed inefficaci per una determinazione precisa ai fini fiscali.

Dovrebbe essere coerente valutare le valute digitali attraverso la redazione del quadro RW della dichiarazione dei redditi, quando esse siano depositate presso un wallet situato all'estero, per l'applicazione delle imposte sulle attività finanziarie detenute.

Beni Immateriali:

Proprio per la mancanza di un preciso inquadramento da parte delle autorità finanziarie, amministrative e bancarie nazionali è legittimo classificare le criptovalute come una sorta di bene immateriale. In questo senso, l'uso delle valute digitali nell'effettuare le transazioni nel mondo reale appare sotto forma di baratto, proprio come è stato indicato dalla Banca d'Italia: "Avvertenze sull'utilizzo delle c.d. *valute virtuali*" del 2015.

Ai fini fiscali, anche l'attività di baratto è assoggettata nella base imponibile quando viene generata una plusvalenza. Come disciplinato dall'art. 67 comma 1, lett. i, del T.U.I.R., si determina un reddito diverso legato ad una vendita occasionale. Mentre ai sensi dell'art. 71, comma 2, viene esplicato il calcolo della plusvalenza come differenza tra valore di cessione e spese sostenute per l'acquisto o la produzione di tale bene, cioè dal costo di acquisto della valuta stessa. Attribuendo come costo di acquisto della valuta la valorizzazione al tasso di cambio alla data di acquisto, attraverso l'utilizzazione del LIFO. Considerare le valute digitali alla stregua di beni immateriali, agevola il loro inquadramento perché non vi è più l'obbligo del monitoraggio fiscale visti precedentemente.

Le Direttive Europee e la legge 231 del 2007 / D. lgs. 25 maggio 2017 n. 90

A quanto si è descritto, occorre enunciare le varie riforme fatte dal Paese in tema di antiriciclaggio. Dagli anni Novanta si susseguono diverse direttive europee su questo tema. Bisogna attendere fino alla quarta direttiva europea antiriciclaggio per arrivare a determinare in qualche modo la criptovaluta, (Direttiva UE 2015/859) recepita in Italia con il recente il D.lgs. 25 maggio 2017 n. 90, la quale ha riscritto totalmente il D.lgs. 231/2007 per l'individuazione anche del settore delle criptomonete.

Con questa riforma, l'Italia ha preso l'occasione di inserire gli Exchanger come nuovi soggetti destinatari o della normativa antiriciclaggio. Prevede l'obbligo di iscrizione in un apposito registro da parte dei cambiavalute virtuali (sono destinati a iscriversi nella sezione speciale del registro dei cambiavalute, dal 2015 tenuto dall'Organismo per la

gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi – OAM, istituito dall'art. 128-undecies del TUB).

"Prestatori di servizi relativi all'utilizzo di valuta virtuale ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale"[136].

Inoltre, oltre all'inquadramento giuridico di questi soggetti, la legge dà una prima definizione di valuta virtuale:

"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"[137].

Con la nuova normativa i soggetti destinatari di obblighi in materia di antiriciclaggio vengono suddivisi in 5 categorie, in cui una viene riferita agli operatori non finanziari i quali vengono assimilati ai cambiavalute tradizionali.

Risoluzione n. 72/E/2016 dell'Agenzia delle Entrate

L'Agenzia delle entrate è intervenuta su questo tema fornendo interessanti considerazioni. In particolare, a seguito di un quesito di un Exchanger che chiedeva chiarimenti sul trattamento ai fini IVA, l'Agenzia ha espresso delle delucidazioni su questo tema. Avvalendosi della Direttiva 2006/112/CE, e quindi annoverando gli Exchange sotto la sfera dei prestatori di servizi di operazioni relative a divise, banconote e monete con valore liberatorio, è prevista per queste figure l'esenzione ai fini IVA, prevista dall'art. 10, comma 1, n.3), del D.P.R. n. 633/1972.

Per il solito problema della mancanza di normativa di riferimento, l'Agenzia afferma che la sentenza della Corte di Giustizia dell'Unione Europea, che ha classificato gli exchanger, possa costruire il fondamento per la quale deriva ai fini di imposte dirette, calcolato sul

[136] Fonte normativa: "d.lgs. n. 231/07, art. 1, comma 2, lett. ff; come riscritto dal d.lgs. n. 90/17".
[137] Fonte normativa: "d.lgs. n. 231/07, art. 1, comma 2, lett qq; come riscritto dal d.lgs. n. 90/17".

margine di intermediazione. Inoltre, vanno valorizzati (utilizzando il Valore normale) le valute digitali che rimangono come rimanenze a disponibilità delle società.
Queste conclusioni, a cui arriva L'Agenzia delle entrate, sono più che condivisibili perché questa è tutto gli effetti attività di impresa.
Mentre per chi detiene criptovalute al di fuori di attività di impresa, sia persone giuridiche che fisiche, l'Agenzia precisa che le operazioni a pronti (acquisti e vendite) di valuta non genera redditi imponibili, perché non vi è la finalità speculativa.
Qui a motivare questa riflessione dell'Agenzia, interviene l'art. 67 del T.U.I.R.:
"-Le plusvalenze realizzate mediante cessione a titolo oneroso di valute estere, oggetto di cessione a termine o riveniente da depositi o conti correnti (comma 1, lett. c-ter);
- i redditi, diversi da quelli precedentemente indicati, comunque realizzati mediante rapporti da cui deriva il diritto o l'obbligo di cedere od acquistare a termine valute ovvero di ricevere o effettuare a termine uno o più pagamenti collegati a tassi di interesse, a quotazioni o valori di valute estere (comma 1, lett. c-quater), con l'ulteriore condizione che le plusvalenze rilevano se la giacenza media del conto corrente da cui provengono le valute estere cedute superi per almeno sette giorni lavorativi continui l'importo di 51,645,70 euro (comma 1-ter)"[138].
Da questi riferimenti normativi, viene da sé che le normali transazioni di acquisto e vendita non a pronti di criptovalute, fatte da privati non sono idonee alla creazione di reddito imponibile e in più i wallet non possono rientrare tra i conti correnti o depositi definiti dall'art. 67.

Monitoraggio Fiscale

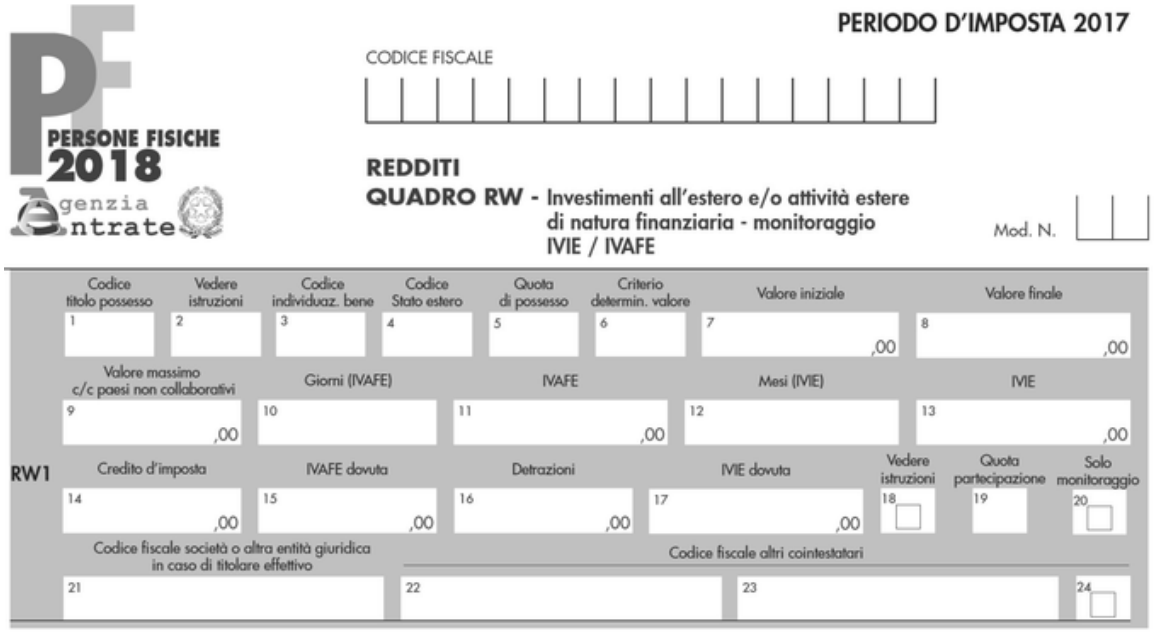
Il monitoraggio fiscale è disciplinato sia per le persone fisiche sia per le persone giuridiche, dall'art. 4 del D.L. n. 167/1990., ed il relativo adempimento da eseguire che risulta nella compilazione del quadro RW della dichiarazione dei redditi. Il presupposto della compilazione del quadro RW, consiste nella produzione di reddito imponibile in Italia delle attività o investimenti detenuti all'estero.
Nella fattispecie, l'Agenzia delle entrate, nella risoluzione afferma che per le operazioni a pronti (acquisti/vendite) di criptovaluta detenuta da persone fisiche al di fuori

[138] Fonte normativa: "l'art. 67 del T.U.I.R.".

dell'attività d'impresa non generano redditi imponibili, non sussisterebbe l'obbligo della compilazione del quadro normativo RW.

Tuttavia, è da tenere presente che c'è l'obbligo (della compilazione) per il semplice fatto della potenzialità dell'investimento, quindi se al momento non vi è reddito imponibile, questo non esclude la compilazione del quadro RW.

Proprio perché il criptomondo non è regolamentato, si apre un'universalità di ipotesi circa la sua detenzione che possa produrre una forma di remunerazione oppure nell'esecuzione di transazione che producono redditi imponibili. Ma ad ogni modo, sorge comunque l'obbligo di compilazione, con la particolarità dell'investimento possa originare alcune incertezze.


PERSONE FISICHE 2018
Agenzia Entrate

PERIODO D'IMPOSTA 2017

CODICE FISCALE

REDDITI

QUADRO RW - Investimenti all'estero e/o attività estere di natura finanziaria - monitoraggio IVIE / IVAFE

Mod. N.

Codice titolo possesso	Vedere istruzioni	Codice individuaz. bene	Codice Stato estero	Quota di possesso	Criterio determin. valore	Valore iniziale	Valore finale
1	2	3	4	5	6	7 ,00	8 ,00

Valore massimo c/c paesi non collaborativi	Giorni (IVAFE)	IVAFE	Mesi (IVIE)	IVIE
9 ,00	10	11 ,00	12	13 ,00

RW1	Credito d'imposta	IVAFE dovuta	Detrazioni	IVIE dovuta	Vedere istruzioni	Quota partecipazione	Solo monitoraggio
	14 ,00	15 ,00	16 ,00	17 ,00	18	19	20

Codice fiscale società o altra entità giuridica in caso di titolare effettivo	Codice fiscale altri cointestatari		
21	22	23	24

Figura 4.1 Rappresentazione del Quadro RW. Fonte Url:" www.bigsuite.ipsoa.it". Potrebbe essere compilato nel modo seguente:
*-**Cod. individuazione bene (campo 3)**: potrebbe essere utilizzato il codice 14: Altre attività estere di natura finanziaria;*
*-**Cod. Stato estero (campo 4)**: cod. corrispondente allo Stato estero è reperibile nella tabella delle istruzioni del fascicolo 1 del Mod. Redditi P.F. 2018. La vera difficoltà è trovare lo stato in cui sono collocate le valute digitali. Trovandosi nelle piattaforme online e wallet, quindi è difficile trovare la localizzazione del software .Per approssimazione si può quindi assegnare il codice dello Stato, facendo riferimento alla collocazione del gestore dell'applicazione (sempre che sia identificabile), altrimenti si farà una congettura.*
*-**Valore dell'attività (campi 7 ed 8)**: nelle istruzioni per la compilazione, precisano che il valore per queste attività è quello di indicare quello di mercato, data la quotazione rilevata al 31 dicembre. Invece per le attività non quotate, si fa rifermento al valore nominale (anche se questo manca al valore di rimborso). Tuttavia, per le Criptovalute, non ci sono i parametri richiamati, non avendo infatti corso legale e non c'è neppure il valore nominale. Quindi si utilizza il criterio del costo di acquisto, ossia il costo pagato in valuta "tradizionale" per acquistare la criptovaluta.*

Recente risposta ad un interpello regionale dalla Direzione Regionale dell'A.G. Lombardia

La Direzione Regionale della Lombardia si è espressa con l'interpello n. 956-39/2018, nel quale ha confermato indirettamente quanto descritto dalla risoluzione n. 72/E, sulla natura delle valute digitali, e dal D. Lgs n. 231/2007 visto in precedenza.
Nel dettaglio la Direzione Regionale della Lombardia afferma che l'utilizzo della valute digitali possa avvenire in due modalità: come mezzo di pagamento per acuisti di beni e servizi nel mondo reale ma anche per fini speculativi, utilizzando lo scambio on line con altre valute utilizzando il tasso di cambio. Viene confermato che quando una persona fisica, al di fuori dell'attività di impresa, ceda valuta digitale a pronti, non produce reddito, a meno che:

- il periodo di giacenza media del deposito (wallet) non superi un controvalore di € 51,645.49
- per un tempo di almeno 7 giorni lavorativi continui nel periodo d'imposta.

Viceversa, se la cessione viene a termine, ad esempio con un contratto finanziario specifico, non sussisterebbero questi vincoline quindi si potrebbe generare un reddito imponibile (data da un'eventuale plusvalenza tra il costo di cessione e quello di acquisto).
Inoltre, viene ricordato che la tassazione dei redditi conseguiti dalla persona fisica al di fuori dell'attività d'impresa, viene calcolata con l'imposta sostitutiva del 26%, con l'indicazione specifica nel quadro RT: "*redditi diversi di natura finanziaria*".
La Direzione Regionale interviene anche sulla questione del monitoraggio fiscale con il richiamo del principio generale per l'obbligo di compilazione del quadro RW, ossia va indicata l'attività detenuta all'estero dalla quale si potrebbe generare reddito imponibile in Italia.
Visto che le valute digitali non sono collate attraverso gli intermediari finanziari, le criptovalute vanno indicate nel quadro RW (come se fossero altre valute estere), utilizzando il codice 14, che corrisponde a: "a*ltre attività finanziarie*". Mentre il loro controvalore si deriverà dal cambio alla data di acquisto.
Questi ragionamenti vanno a prescindere dal conseguimento di un reddito, anzi di fatto c'è l'obbligo della compilazione del quadro RW in ogni caso di detenzione di valuta digitale.
Per ultimo, la Direzione Regionale afferma che in tema di IVAFE ritiene che l'imposta non sarebbe applicabile perché non si tratta di depositi bancari; tuttavia, attraverso una

circolare delle Agenzia delle entrate, in questa imposta vanno anche fatti rientrare anche le valute estere in genere, senza far riferimento ai rapporti bancari.

Conclusioni Finali

La mancanza di un qualsiasi tipo di regolamentazione delle criptovalute in generale, sta generando incertezza sulla prassi da seguire in vista della dichiarazione dei redditi.
In questa analisi è giusto fare un distinguo tra:

- Persona giuridica, se si è nel caso di un'attività d'azienda, l'incasso delle valute digitali riceve lo stesso trattamento fiscale delle valute estere, quindi dollari o sterline. Se l'azienda dovesse poi ricavare una plusvalenza dalla loro vendita, dovrebbe pagare l'erario come un normale reddito di impresa. Invece, se non li avesse ceduti, si effettuerà una valutazione dei movimenti a fine esercizio.
- Persona fisica, se si è nel caso di un privato che non sarà tenuto ad alcun pagamento impositivo a meno che: nel corso di un anno e per almeno sette giorni consecutivi, le valute digitali possedute non abbiano superato un controvalore pari a € 51,645.69, utilizzando il tasso di cambio di inizio periodo. Quindi solo in quel caso, l'Agenzia delle Entrate riconoscerà l'attività speculativa e si dovrà versare un'imposta calcato con l'aliquota sui proventi finanziari: 26%. Ad ogni modo, l'ammontare delle criptovalute andrebbe inserito nel quadro RT della dichiarazione dei redditi delle persone fisiche.

Tutto questo è quello che per appunto è emerso dalla Direzione regionale dell'Agenzia dell'entrate della Lombardia. Tuttavia, questo secondo gli esperti non potrà essere la normativa definitiva. Questo perché in Italia le tasse sul reddito vengono imposte al contribuente quando vi è la creazione di nuova ricchezza o comunque è espressa dalla legge. Quindi le valute digitali sono soggette a tassazione solo quando viene generato un capital gain dall'operazione. Dall'Agenzia delle Entrate viene suggerito di applicare la medesima normativa fiscale delle valute estere. Secondo un esperto in materia: Paolo Luigi Burlone (commercialista e fondatore di Coinlex, blog specializzato in temi fiscali e legali del criptomondo), questo è sia concettualmente erroneo che in contrasto con la sentenza della Corte di giustizia europea, con pronunce della Bce e con l'appena promulgata Diretta Aml V. Quindi l'Agenzia delle Entrate fa considerazioni senza l'esistenza di una vera e propria legge e in più potrebbe entrare in conflitto con la quinta

(V) direttiva europea di antiriciclaggio. Ancora, porre l'obbligo dell'iscrizione delle criptovalute ai fini del monitoraggio fiscale sempre e comunque anche se non vi è l'esistenza di un rapporto giuridico con un soggetto ubicato in un paese estero, sarebbe una forzatura ad una nuova tecnologia e non vi è ragione perché un residente dovrebbe indicare le proprie criptomonete nella dichiarazione dei redditi, cosa che per altro non si fa per i metalli preziosi ed opere d'arte. In più, come si è descritto in precedenza, applicare l'art. 67 comma1-ter del T.U.I.R. (la valutazione al cambio di inizio periodo) non sempre porterebbe a far tassare chi ha effettivamente realizza un capital gain.

Inoltre, è utile citare due esempi contrapposti per far evidenziare maggiormente le lacune dell'applicazione di questa normativa fiscale:

- il signor Rossi è un detentore di un'unica valuta digitale nel proprio wallet, ad esempio 5000 ether: poniamo che li abbia acquistati negli anni precedenti al costo unitario di € 1, e che li avesse venduti al loro prezzo di picco a dicembre 2017 al prezzo unitario di circa € 700, così relazionando un'operazione di cessione a pronti pari a € 3,5 milioni. Il capital gain realizzato, secondo l'applicazione dell'art. 67 del T.U.I.R., utilizzando il cambio di inizio periodo, di circa € 7 cadauno, sarebbe inferiore alla fatidica soglia di € 51,645.69 per i sette giorni continuativi, cosicché non rientrerebbe nella casistica di creazione reddituale per la cessione di valute estere;
- il signor Bianchi è un detentore di un unico wallet di 5 bitcoin, i quali ad inizio periodo avevano un valore poco superiore a € 800 cadauno e decide di scambiarli con un la valuta digitale: *tether*, cosicché incassa un controvalore di circa € 82,000, così facendo ha realizzato un capital gain, il quale rientrerebbe a piena imponibilità, perché dal 19 al 31 dicembre, ha superato abbondatamene la soglia dei sette giorni continuativi, e così superando il saldo dei € 51,645.69.

Questo esempio evidenzia come chi ha ottenuto maggior capital gain, non per forza dovrebbe pagare proporzionalmente di più di chi ne ha realizzata di meno. Infatti, il signor Rossi, pur diventando milionario in valuta fiat (€), non dovrebbe saldare nulla all'erario. D'altro canto, invece il signor Bianchi che avendo in portafoglio non euro ma tether con cui per definizione non si possono adempiere alle obbligazioni tributarie, dovrebbe

pagare il suo saldo d'imposta e come ha dichiarato l'esperto: "in un palese violazione del principio di parità di trattamento e di capacità contributiva"[139].

In conclusione, questo pronunciamento dell'Agenzia delle Entrate ha intrinsecamente troppe lacune: dalla erronea rendicontazione dell'effettivo valore delle valute digitali alla soglia prefissata dei € 51,645 e il periodo di sette giorni lavorativi, come elementi per l'imposizione tributaria o meno. Tuttavia, questo non può essere adattato al criptomondo, il quale è caratterizzato da un'elevatissima volatilità.

[139] Tratto da: "https://www.wired.it/economia/finanza/2018/05/04/bitcoin-criptovalute-agenzia-entrate/".

Capitolo V – Sintesi e Analisi prospettica

In questo ultimo capitolo dell'elaborato vengono descritti il criptomondo e le valute digitali: si propone una lente puntuale e prospettica attraverso cui sono ripresi i concetti analizzati nei capitoli precedenti, evidenziando i tratti conclusivi dell'elaborato.

In particolare, il capitolo è suddiviso in tre paragrafi: nei primi due vengono descritti da una parte i vantaggi e le opportunità che questa tecnologia, altamente innovativa, può portare, mentre dall'altra vengono esposti gli svantaggi e i rischi connessi. Tali temi sono trattati sotto tre macro-categorie:

1. le funzioni della moneta, quindi verrà analizzata la valuta digitale da due esperti, con opinioni opposte;
2. il funzionamento delle valute digitali, le enormi potenzialità e le criticità che possono emergere;
3. gli impatti economici che ha avuto e che sta avendo il criptomondo sull'economia reale.

Infine, nel terzo paragrafo si porteranno tutti questi argomenti in chiave prospettica, con l'obiettivo principale di cercar di determinare le prossime evoluzioni del criptomondo e della sua tecnologia.

Da ultimo, ci sarà un paragrafo riassuntivo nel quale si esporranno concisamente le conclusioni cardini dell'intero lavoro, mettendo in luce quello che è stato approfonditamente analizzato durante l'elaborato e i risultati ottenuti.

Vantaggi ed Opportunità

Crypto-moneta?

In un'ottica favorevole, da parte di un filone di studiosi, si sono posti la domanda se realmente la criptovaluta possa soddisfare o meno le funzioni della moneta, e quindi denominarla come tale.

In particolare, Ferdinando Ametrano[140] ha seguito questa corrente di pensiero. Infatti, secondo il professore di Milano, il bitcoin riesce straordinariamente a soddisfare la funzione mezzo di scambio perché trasferisce valore senza appoggiarsi agli intermediari, in tutta sicurezza e in più quasi istantaneamente. Ciononostante, egli ragguarda l'impossibilità di utilizzare le valute digitali come l'oro fisico, che per secoli è stato adibito a moneta. Questo proprio per la natura intrinseca del bitcoin e per la propria politica monetaria, caratterizzata dall'offerta completamente anelastica. Secondo la sua opinione, il bitcoin è una *crypto-commodity* più che una *crypto-currency* ovvero svolge meglio la funzione di riserva di valore che di moneta adibita allo scambio. Proprio per questo, egli cita l'esempio del famoso pagamento di due pizze per un valore di 10,000 BTC, evidenziando come sia irrealizzabile utilizzare il BTC alla stregua di una moneta tradizionale.

Tuttavia, secondo questo punto di vista, il bitcoin avrebbe aperto nuove possibilità di ingegneria monetaria. Infatti, questa innovazione renderà possibile la creazione di monete digitali fiduciarie da una parte e criptovalute decentralizzate con politica monetaria algoritmica elastica (differentemente dal bitcoin) dall'altra, ed entrambe saranno garantite dal bitcoin stesso proprio come *asset di riserva*. Per questo motivo Ametrano compie un'analogia con il *gold standard* di un tempo, ribattezzandolo: *bitcoin standard*. Insomma, secondo il suo parere si potrà realizzare quello che il premio Nobel dell'economia Friedrich von Hayek aveva ipotizzato nella seconda metà del Novecento, ovvero utilizzare contemporaneamente le monete a corso legale con le monete private. Mettendo in competizione le due valute, per superare il monopolio governativo della moneta, sarà solamente il libero mercato (la mano invisibile) a far emergere buone monete e buone prassi monetarie.

[140] Docente di Bitcoin e blockchain technology al Politecnico di Milano e all'Università Milano Bicocca.

Crypto-funzionamento

Blockchain:

Questa tecnologia è sicuramente la più grande scoperta dopo l'avvento del Web: senza richiamare tutti concetti affrontati nel secondo capitolo, bisogna ricordare che è stato il Bitcoin a portare con sé questa innovazione tecnologica, che è stata subito studiata ed analizzata dagli altri Altcoins e non solo. Infatti, come si vedrà nel proseguo di questo capitolo, la struttura Blockchain è stata ripresa anche dalle società finanziarie ed industriali. Questo perché si tratta per l'appunto di un registro elettronico a calcolo distribuito su un network P2P, in cui le informazioni sono progettate sotto dei sistemi crittografici, al fine di rendere impossibile ogni tipo di manomissione. Inoltre, dando rilievo importante agli utenti di tale network, ossia il ruolo di autenticatori del sistema, ovviando così ad un'autorità centrale come garanzia.

Inizialmente questa è stata adibita ad assolvere alla fruizione di una moneta digitale, quale Bitcoin, ma può essere utilizzata anche per altri scopi.

Senza dimenticare un fattore fondamentale: l'evoluzione di questa tecnologia, ossia dal "classico" registro a calcolo distribuito di Bitcoin, denominato Blockchain 1.0, si è passati ad un utilizzo più evoluto, in cui è consentita l'adibizione degli smart contracts, in particolare nella Blockchain 2.0. Fino ad arrivare al successivo step, quindi la connessione di tale tecnologia con l'IoT, ovvero Tangle la Blockchain 3.0.

Questi argomenti sono stati ben descritti nel secondo capitolo, qui li si vuole solo richiamare per arrivare ad un chiaro e cristallino risultato, ossia vale a dire: la continua evoluzione di tale tecnologia.

Si possono fare quattro rapide conclusioni a riguardo della Blockchain:

- La prima è che si tratta di una tecnologia che sorregge tutte le criptovalute, e quindi permette lo scambio di esse, realizzando il loro obiettivo primario: essere monete digitali decentralizzate;
- La seconda è che permette il corretto funzionamento delle ICO;
- La terza è l'utilizzazione nel mondo reale, quindi non solo riesce a soddisfare pienamente il criptomondo, ma riesce ad adattarsi in ogni diverso contesto;
- La quarta riguarda invece la sua continua evoluzione, adattandosi all'esigenze del mondo reale.

Trasparenza e pseudonimo:

Questi due concetti sembrano antitetici, ma in realtà le criptovalute riescono ad assolverli entrambi. Nello specifico bisogna ricordare che la maggior parte delle valute digitali, attraverso il loro libro mastro riescono a tenere traccia di tutte le singole transazioni, e quindi di tutti i titoli di proprietà che i token avranno nel corso della loro vita. Inoltre, anche se la Blockchain permette questo, non si deve dimenticare che gli utenti che effettuano le transazioni possono usare degli pseudonimi, e che alla fine risulterà molto arduo identificare il vero proprietario. Cionondimeno, come illustrato nel terzo capitolo, ci sono valute digitali che offrono la possibilità di tenere all'oscura la propria identità, assolvendo anche a questo tipo di bisogno.

Rigidità del protocollo:

Le criptovalute si basano su evoluti software applicativi, e che subiscono continui aggiornamenti dagli sviluppatori. Specialmente, nelle valute digitali che sono supportate da associazioni conosciute e da team solidi (quali: Ethereum, Ripple, Stellar e Iota), ma anche la stessa Bitcoin, che per antonomasia è la più diffusa criptomoneta del criptomondo, ed ha solamente un team di sviluppatori che vi stanno a monte, lavorano ininterrottamente per migliorare continuamente il protocollo che permette il perfetto funzionamento del sistema.

Crypto-economy

Costi di transazione

Tutto il criptomondo è diventato famoso proprio per questo motivo, ovvero la quasi totale assenza di costi di commissioni sulle transazioni. Tuttavia, è opportuno fare alcune considerazioni a riguardo. Prendendo in analisi bitcoin, in realtà dalla sua creazione fino al 2016, il prezzo di commissioni ovvero le cosiddette fee erano davvero molto contenute. In particolare, nel 2014 il costo medio era fissato al valore i 0,0001 bitcoin, che al cambio del 2014 (€ 755 cadauno) erano intorno ai € 7.5 cent di fee per transazione. Mentre se si va ancora più indietro si arriva alla modica cifra di € 1 cent.

Successivamente, con il maggior numero di transazioni presente in rete, il prezzo delle commissioni si è alzato sproporzionalmente fino ad arrivare a maggio del 2017 ad una fee di 88,140 satoshi per una transazione media di circa 226 byte, ovvero intorno ai € 2.
Per maggiori informazioni, si può utilizzare questo sito internet: "https://bitcoinfees.earn.com/", il quale mostra i possibili prezzi di fee per un'ipotetica transazione veloce (molto veritiera) di 225 byte.
Quindi, facendo i dovuti calcoli risulta che una transazione di 225 byte costerebbe 2,250 satoshi, ricordando che 1 satoshi è uguale a: 0,00000001 BTC.
Per agevolare il calcolo, questo importo viene convertito in milli bitcoin corrispondente a: 0.0225, e per un prezzo attuale pari a: $ 7,630.76[141] a BTC, e con un cambio di $/€ di 1.17[142], si ottiene un valore di € 6,522.02 per ogni singolo token.
Quindi una fee per una transazione veloce (225 byte) corrisponderebbe circa a: € 0.15 cent.
Ricordando alcuni concetti chiave per le fee di BTC:

- I miners sceglieranno di evadere le transazioni che offriranno un "giusto" valore, quindi quelle che offriranno un valore di fee mediamente più alto, saranno prese in considerazione più velocemente di altre;
- Le fee sono costi di commissioni presenti in tutte le transazioni, in aggiunta vengono pagate direttamente dal proprietario, ovvero l'emittente della transazione e il destinatario non deve versare nulla;
- Questa forma di pagamento va dall'emittente al miner come premio per il suo lavoro, inoltre questa sarà l'unica forma di guadagno dopo che sarà estratto l'ultimo bitcoin.

Facendo un breve raffronto con i metodi tradizionali (Visa, Mastercard e Paypal), dove sussisteranno altissimi costi di commissioni rispetto alle criptovalute, si può evidenziare come questi siano dispendiosi sia in termini economici che tempistici. In particolare, i costi di commissione di tali metodi, a differenza del bitcoin, vengono addebitati al destinatario, ovvero ad esempio un commerciante, il quale può prontamente rincarare la vendita del bene maggiorato dalla percentuale di commissione che gli viene imposto da questi metodi.

[141] Riferimento Url: "https://coinmarketcap.com/", in data 5 giugno 2018, ore: 21:25.
[142] Riferimento Url: "https://www.milanofinanza.it/valuta/cambio-euro-dollaro", in data 5 giugno 2018, ore: 21:26.

In aggiunta, PayPal chiede una commissione pari a 2.9% + € 0.30 cent, mentre per le carte di credito Visa e Mastercard vi è una fee che parte dal 2-3% a salire.
Invece, nel caso del bonifico bancario il costo è a carico dell'emittente, ovvero chi compie l'acquisto, ovviamente qui i costi sono diversi dipendentemente dalla banca scelta, ci potrà essere un costo di commissione per ogni singolo bonifico con l'aggiunta di un costo fisso per il mantenimento del conto corrente bancario.
Ovviamente, tutti questi costi sono assai inferiori in Bitcoin e maggiormente anche nelle altre criptovalute. In particolare, risulta evidente che nel caso delle valute digitali è permesso il micro-pagamento, è consentito effettuare delle micro-transazioni anche inferiori ad € 1.
Oltre a questo, si prenda in considerazione che molte altre valute digitali hanno costi di fee ancora inferiori al bitcoin (anche se nel 2018 le fee di BTC sono calate enormemente), ad esempio IOTA. Infatti, questa valuta digitale utilizza come la Blockchain *Tangle*, in cui non vi è più la presenza di nessuna commissione per la transazione. Infatti, come si era già illustrato nel secondo capitolo, la piattaforma Tangle migliora proporzionalmente all'utilizzazione da parte degli utenti, cioè più transazioni vengono effettuate e più il sistema diventa efficiente. La fee viene addebitata all'emittente ma solamente per i calcoli che viene richiesto di fare dalla propria CPU, quindi consumando solamente una piccola percentuale di batteria perché qui il mining non è richiesto, e le transazioni vengono aggiunte continuamente.

Tempi di attesa per le transazioni

I tempi di attesa vengono enormemente ridotti nelle criptovalute. Come si è evidenziato dai capitoli precedenti, Bitcoin impiega 10 minuti per minare un blocco contenente un paniere di transazioni. Si ha la certezza delle transazioni dopo 6 blocchi minati, per cui circa dopo un'ora si può avere la certezza dell'effettività delle transazioni, evitando così il problema del double-spending. Inoltre, i commercianti potrebbero accettare delle transazioni di piccola entità o comune meno rilevanti rispetto a transazioni consistenti, con minor numero di blocchi confermati, quindi anziché aspettare 6 blocchi (circa 1 ora), potrebbero accettare anche dal 2°. Intanto, si può verificare immediatamente, dalla Blockchain online, l'iscrizione di tale transazione che sta aspettando di essere minata.

Ricordando l'impiego del *escrow service* come metodo di garanzia per le trazioni, che potrebbe essere utilizzato da una parte per velocizzare le transazioni e dall'altra per garantire importi rilevanti.
Sta di fatto che ci sono ulteriori criptovalute che garantiscono minor tempi di transazioni, o pressoché nulla rispetto al BTC. Infatti, molte di esse sono nate per assolvere a questo problema, che ha messo in discussione più e più volte questa valuta digitale. Si può citare Ripple che impiega circa 4 secondi e anche IOTA. Cionondimeno, basti ricordare all'esempio presentato nel primo capitolo, quando si spiegava la creazione di Bitcoin Cash, la quale era una *hard fork* rispetto al BTC classico, ed era stata coniata proprio per velocizzare i tempi delle transazioni.
Ad ogni modo, giusto per dare dei termini di confronto con i metodi classici, mediamente per effettuare dei bonifici SEPA ci si impiega dai 3 ai 4 giorni lavorativi.

Facilità ed accessibilità

Creare un indirizzo nel quale ricevere somme in BTC non è affatto difficile, come è stato illustrato nel secondo capitolo. Chiunque può aprirsi sull'utilizzo di questa tecnologia, a differenza dei conti correnti bancari, dove vengono richieste tutele e garanzie. Senza dimenticare la totale separazione dalle politiche finanziarie delle banche e dei Governi. Nessuno può pretendere di ottenere in qualche maniera le somme possedute in valute digitali perché hanno un solo proprietario e rispondono solamente a lui. Inoltre, com'era avvenuto in passato, nessuno Stato potrà congelare i fondi o chiedere una somma come prelievo forzoso per contribuire alla spesa pubblica.

Disintermediazione e assenza di controlli sociopolitici

La disintermediazione dagli istituti finanziari è una delle principali caratteristiche intrinseche delle criptovalute ed è uno degli elementi che le hanno permesso di ricevere tanta notorietà. Inoltre, proprio grazie ad esso, si è portato nei dibattiti pubblici il tema della democraticità delle monete tradizionali. Infatti, le valute digitali sono nate proprio per ridare il potere monetario al popolo, svincolandolo così dalle politiche monetarie e logiche sociopolitiche.
Occorre non tralasciare un fattore che spesso rimane in sordina, ovvero l'*Unbancked*. Infatti, non tutti possiedono un conto corrente bancario, non contando i paesi del

secondo-terzo mondo, i quali sono ancor maggiormente penalizzati, per esempio in Kenya viene molto utilizzata M-PESA[143].

In Italia è considerato un paese avanzato e uno dei Paesi rientrante del G7, eppure questo ha il numero più alto di persone che non utilizzano i servizi bancari. Da uno studio dell'Ufficio studi della Cgia di Mestre, si evince che sono circa 15 milioni di italiani che non utilizzano i conti correnti bancari (il 29% degli italiani sul totale della popolazione con più di 15 anni). Questo studio risale al 2013, quindi si assume che ipoteticamente il numero possa essere variato (o in aggiunta o in diminuzione), ma comunque questo dato risulta un record rispetto a tutta l'Unione Europea. Questo primato ovviamente è riconducibile a più fattori, quali ad esempio ragioni storiche e culturali. Lo studio di Cgia prende in esame i dati della Commissione Ue, dove vengo considerati i cittadini europei di età superiore a 15 anni che non dispongono un conto corrente bancario. Per aver un confronto, si può rammentare che il Paese che segue è la Romania con circa 9.8 milioni di persone (55% sul totale della popolazione con più di 15 anni), mentre i Paesi a cui far più similitudine: Francia (1.5 milioni, il 3% sul totale della popolazione con più di 15 anni), U.K. (lo stesso della Francia) e Germania (1.4 milioni, il 2% sul totale della popolazione con più di 15 anni).

[143] M-Pesa: "è un servizio di trasferimento denaro tra utenti del servizio di telefonia cellulare nato nel 2007 sulla rete mobile di Safaricom, una società affiliata di Vodafone, per permettere alle istituzioni di microfinanza di inviare e ricevere denaro con facilità dai prestatori. Il servizio è nato in Kenya e si è poi diffuso in altri stati africani, europei ed asiatici. Il nome viene dall'unione tra il termine mobile e Pesa, che in swahili significa denaro. Sviluppato inizialmente da Sagentia, il progetto è stato sponsorizzato negli anni 2003–2007 dal Dipartimento per lo sviluppo internazionale (DFID) in Regno Unito".
Il funzionamento è relativamente semplice: i clienti si rivolgono a un agente M-Pesa per caricare il proprio account e a questo punto possono con il loro telefonino effettuare acquisti o inviare soldi a terzi che li possono prelevare da un agente M-Pesa.
Un sistema che alla vigilia del suo decimo compleanno, a dicembre 2016, ha registrato un record di operazioni pari a 614 milioni. Alla fine dello scorso anno i clienti attivi sfioravano i 29,5 milioni, mentre la rete degli agenti conta su 287.400 persone.
Fonte Url: "https://it.wikipedia.org/wiki/M-Pesa", "http://www.vita.it/it/article/2017/02/22/m-pesa-i-pagamenti-mobile-che-cambiano-la-vita-in-10-paesi/142559/".

Superare il Paradosso della moneta tradizionale

Com'era già stato evidenziato nel primo capitolo, la criptovaluta è riuscita finalmente a scardinare il paradosso delle monete tradizionali, riuscendo così ad unire i vantaggi della moneta elettronica e quelli del contante. Ovvero, la valuta digitale riesce ad effettuare pagamenti a distanza proprio come un bonifico bancario, ed è praticamente istantaneo e non implica costi esagerati (praticamente azzerati), sia per emittente che per destinatario, proprio come si trattasse di contanti. Senza dimenticare che alcune di esse possono offrire l'anonimità assoluta. A riguardo si può vedere questo sito: "www.bitpesa.co", attraverso cui è possibile trasferire i propri bitcoin in Africa, particolarmente indicato per i lavoratori extra-comunitari che vogliono trasferire i soldi alle proprie famiglie, nella loro patria.

Svantaggi e Rischi

Crypto-moneta?

Nell'accezione negativa del criptomondo da parte di un filone di studiosi, si sono posti la domanda se realmente la criptovaluta possa soddisfare o meno le funzioni della moneta.
A tale tesi è intervenuto Luca Fantacci[144], il quale ha espresso il suo pensiero a tal riguardo. Secondo questo professore della Bocconi, il Bitcoin riesce ad assolvere pienamente la funzione di mezzo di scambio, perché in effetti è nato per assolvere questo scopo, quindi può agevolare il commercio elettronico, consentendo transazioni online immediate ed irreversibili. Inoltre, il Bitcoin riesce a coniugare i vantaggi della moneta elettronica e del contante. Ad ogni modo, la valuta digitale viene adibita molto poco come mezzo di scambio, questo perché il suo valore è enormemente instabile. Questa instabilità si riflette nel comportamento degli utilizzatori, i quali difficilmente accetteranno questa moneta digitale in cambio di un bene, se poi quando si andrà a convertirlo probabilmente inferiore al momento della transazione.
Certo è anche pur vero il contrario, ovvero che nell'arco di quasi 10 anni della sua vita, il valore è aumentato sproporzionalmente, però questo cela anche un elemento negativo. Il fatto che una moneta possa tendenzialmente crescere nel tempo il suo valore, di conseguenza questa sarà conservata più che spesa, nella speranza di poter comprare più beni in futuro.
Per i ragionamenti fin qua si fatti, si nota che la criptovaluta risponde alla funzione di riserva di valore. Allorché il professore evidenzia come una moneta che non viene adibita allo scambio, e quindi circolare liberamente nell'economia, non può essere una moneta degna di nota. Per ultimo, si osserva che la proprietà di riserva di valore di bitcoin, non consente nemmeno di assolvere all'ultima funzione: ossia quella di unità di conto. Questo discorso vale anche quando il bitcoin viene accettato come mezzo di pagamento, perché non può essere adibito per denominare i prezzi, e specialmente nella determinazione dei crediti e dei debiti. Ovviamente, questo perché se qualcuno contraesse un debito in una moneta destinata ad apprezzarsi sempre di più con il passare del tempo, il tempo per estinguerlo crescerebbe enormemente.

[144] Docente di storia economica e finanziaria e di storia del pensiero economico all'Università Bocconi.

Vulnerabilità nei Servizi connessi

Com'è stato potuto verificare nel corso dell'elaborato, le vere problematiche nel criptomondo risalgono agli operatori Exchangers, i quali più volte nel tempo sono stati violati dagli cyber-criminali. La tematica sulla gestione e conservazione delle valute digitali rimane tuttora centrale, essendo che è l'unico modo per sottrarre le criptovalute ai legittimi proprietari. Si è visto come ci siano differenti tipi di wallet, i quali offrono diversi tipi di sicurezza. I *paper wallet* e i recenti *hardware wallet* offrono una sicurezza maggiore, specialmente i secondi, i quali sono stati concepiti proprio per assolvere a questa funzione.

Vulnerabilità nel Protocollo

In realtà, quello che si è detto nel punto precedente è solo in parte vero perché vi è la possibilità (anche se in percentuale bassissima) che qualcuno o gruppi di persone possano attuare il cosiddetto *51% Attack*. Questo lo si era esplicato nel secondo capitolo, dove veniva illustrato come l'unico modo per aggirare la Blockchain, e così aver la possibilità di compiere frodi attraverso più transazioni con la stessa valuta digitale, il cosiddetto *Double-spending*.

Volatilità

L'estrema volatilità dei prezzi e delle relative capitalizzazioni sul mercato, rende questa valuta e tutto il criptomondo molto difficili da prevedere, se non impossibile. Questo lo rende quasi ingestibile sia sul piano di investimento col fine speculativo sia sul piano di investimento col fine di poterla utilizzare in futuro.

Infatti, come è stato ampiamente descritto precedentemente, è difficile identificare le valute digitali come una vera e propria moneta perché non riescono ad assolvere alle tre classiche funzioni della stessa.

Irreversibilità nelle transazioni

È utile tenere a mente che le transazioni che vengono effettuate nel criptomondo sono irreversibili, una volta che viene effettuata una transazione non si può più chiedere l'annullamento. A differenza delle monete fiat, le quali riescono a tutelare i consumatori da possibili frodi, semplicemente consentendo l'annullamento delle transazioni e con la conseguenza la restituzione della somma di denaro (questa modalità ad esempio è prevista per il bonifico bancario, contattando la propria banca). Questa procedura si chiama *chargeback* e consiste proprio nell'annullamento della transazione e quindi della restituzione dei soldi al consumatore. Questo processo assolve allo scopo di dar allo stesso consumatore maggiori tutele in caso di frodi.

Invece, nel criptomondo ogni token che viene trasferito verrà registrato all'interno del blocco della catena, nella quale sarà contenuta la timeline di tutti gli scambi effettuati. Quindi, in questo processo una volta che i blocchi sono stati approvati diventeranno immodificabili. Questa è dettata dalla crittografia adibita alla creazione di chiavi e indirizzi, quindi diventerà impossibile risalire all'indirizzo della transazione registrata nel blocco. Per questo motivo nel criptomondo viene maggiormente garantito il venditore, il quale sarà ben lieto di ricevere il denaro senza aver cattive sorprese, cosicché egli possa permettersi il rischio di espandersi in nuovi mercati caratterizzati da un alta percentuale di frodi; mentre il consumatore si trova dalla parte opposta, prima era super tutelato ora invece non potrà annullare nessuna transazione, né nel caso in cui dovesse erroneamente immettere un indirizzo a posto di un altro (perché non vi è nessuna autorità che potrebbe gestire l'accaduto), né tantomeno se dovesse imbattersi in un caso di frode.

Prospettive per il Futuro

In questo paragrafo vengono tratte delle ipotesi personali a riguardo delle criptovalute e del criptomondo. Dopo aver analizzato Le opportunità e i rischi collegati ad essi, qui verranno ripresi alcuni concetti chiave di questa tecnologia e si cercherà di dare un taglio prettamente empirico e prospettico.

Monete Fiat Digitali

Come si è potuto vedere all'interno dell'elaborato, le criptovalute hanno scardinato molti preconcetti tra cui la legittimazione della moneta. Quanto è avvenuto nella crisi finanziaria del 2008 ha fatto emergere le problematicità dell'attuale sistema monetario, in cui le manovre monetarie e il salvataggio degli istituti di credito, non sono state percepite dal popolo come un reale aiuto per la popolazione stessa. Per esempio, si può citare come la tematica delle iniezioni di liquidità del QE non sia stata percepita dai cittadini come uno strumento di aiuto per contrastare l'emergenza economica-finanziaria. Questo perché è stata connessa al concetto del *Too Big To Fail*, quindi all'operazione di salvataggio degli istituti di credito. Per dipiù, questa grande iniezione di liquidità è andata solo in una parte nei portafogli dei cittadini perché si era creato un meccanismo perverso, in cui alcuni istituti di credito invece di rilasciare la nuova liquidità ricevuta dalla Banca Centrale a famiglie ed imprese, veniva o reinvestito in strumenti speculativi, oppure tenuto nelle casseforti per via dell'alta rischiosità dell'insolvenza dell'economia reale e dei tassi quasi negativi. Inizialmente si è assistita ad una crisi finanziaria, la quale poi si è traslata verso l'economia reale così costringendo gli Stati ad intervenire massicciamente per sostenere i propri cittadini, in questo modo si è scatenata una crisi del debito degli Stati Sovrani. Senza entrare troppo nel merito, quello che si vuole rimarcare qui è come sono stati trattati questi interventi da parte degli Stati perché questo ha avuto delle conseguenze a livello sociale. Infatti, intervenendo così massicciamente (d'altro canto l'Italia è intervenuta solo sotto forma di prestiti e ha concesso pochi finanziamenti, rispetto a tutti gli altri Paesi industrializzati), gli Stati si sono indebitati proprio per quegli istituti di credito (molti di questi avevano in portafoglio CDO e altri titoli sub-prime), che poi concedevano i prestiti in misura ridotta nell'economia reale.

Tutto questo è stato percepito dalla popolazione mondiale come un atto che disi legittimava il popolo stesso. Questo perché ha fatto riflettere sulla vera natura della moneta, e se realmente si è prosperati della moneta stessa. Visto che è sotto il controllo totale degli istituti di credito e degli Stati Sovrani.

Molti esperti sono d'accordo sull'impossibilità di utilizzare le criptovalute odierne in futuro, per svariate ragioni quale ad esempio la mancanza di un'autorità centrale che possa vigilare sul comportamento corretto di essa.

La vera domanda è se questa tecnologia verrà ripresa dalle Banche Centrali Mondiali, e che quindi possano nascere delle valute digitali fiat. Com'è stato descritto nel IV° capitolo, ci sono già stati episodi simili, si veda Venezuela (anche se rimane un caso particolare) o la Cina che sta studiando come realizzare una propria valuta digitale.

Quello che può succedere è la compresenza di valute digitali fiat e le tradizionali monete, magari adibite anche per svincolarsi dalle restrizioni commerciali, proprio come sta facendo il Venezuela, e la stessa Russia sta visionando la sua realizzabilità.

Attualmente, la BCE ha vietato alle Banche Centrali dell'Eurozona di coniare questa tipologia di valute, chissà se in futuro sarà proprio la stessa BCE a creare una valuta digitale tutta sua, ad esempio: l'*Euro-coin*.

A riguardo, si può citare il teorema sulla concorrenza monetaria vista nel primo capitolo, pertanto è lecito porsi la domanda se dovesse mai sorgere una concorrenza delle valute digitali con quelle tradizionali, quindi in definitiva quale realmente sarà quella più diffusa e utilizzata tra i popoli?

Implementazione della Blockchain nel proprio Business

Un libro mastro distribuito e replicato su tutti i nodi presenti sul network, in modo tale da evitare il *double-spending*, questa è la Blockchain. Questa tecnologia riesce a superare il bisogno degli intermediari, i quali normalmente sono adibiti alla verifica e alla conferma delle le singole transazioni. Nella Blockchain questo lavoro viene lasciato in capo ai miners.

Per questo motivo, la Blockchain è il primo registro contabile che non richiede la fiducia verso un intermediario, perché appunto in un qualsiasi momento si può verificare la correttezza delle transazioni, le quali sono registrate su questo registro contabile, in cui qualsiasi utente del network può visionare. In definitiva, si può affermare che la fiducia che si riponeva negli intermediari finanziari, si è spostata nelle regole informatiche di funzionamento, attraverso l'uso di software e degli algoritmi appositi.
Inoltre, non esisteranno diversi registri contabili, come succede nel caso degli intermediari i quali avranno per forza di cose diversi registri aziendali, invece la Blockchain viene replicata esattamente uguale a tutti gli utenti del network, e questa sarà continuamente aggiornata e sincronizzata dai miners.

Le caratteristiche della Blockchain sono:

- Unicità: il registro contabile è univoco per tutti i nodi;
- Indipendenza: è totalmente indipendente da un organo di controllo centrale, infatti viene gestito da leggi matematiche, e viene accettato e verificato dagli utenti, e rimarrà immodificabile;
- Irreversibilità: la timeline delle transazioni non potrà essere modificata;
- Programmabilità: si possono modificare certe condizioni, quale ad esempio il vincolo della moneta, attraverso la riprogrammazione del software;
- Rintracciabilità: ogni token è tracciabile e rintracciabile.

Si era visto come vi possono coesistere due tipi di Blockchain nel criptomondo:

- *Permissionless*: questo è il registro contabile effettivamente indipendente da autorità centrali, perché è il sistema pubblico che garantisce il suo funzionamento;
- *Permissioned*: questo è il registro contabile gestito da società o associazioni, nel quale viene adattato in relazione a problemi specifici, per questo che secondo i *puristi*, questa Blockchain risulta solo in parte decentralizzato.

Nella figura 5.1 viene mostrata la differenza dei due tipi differenti di Blockchain.

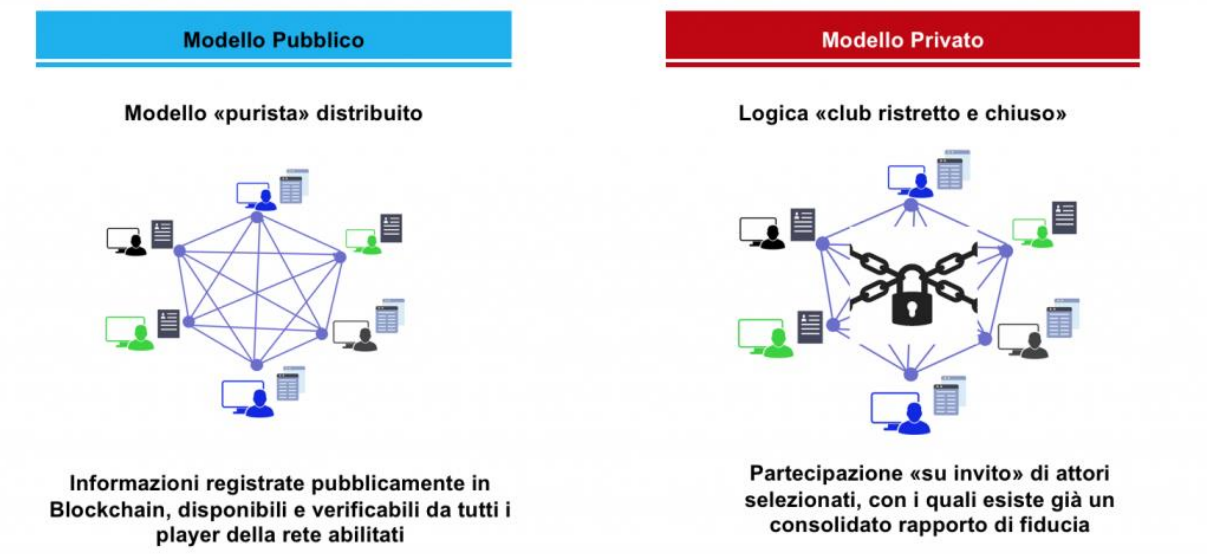


Figura 5.1 Rappresentazione dei due diversi tipi di Blockchain. Fonte Url: "https://www.blockchain4innovation.it/".

Si è voluto riprendere questo argomento, perché è sicuramente una tecnologia che già sta cambiando il mondo. Inizialmente, le criptovalute non erano state prese sul serio e tuttora rimangono ancora ignote le loro reali potenzialità, invece quello che riesce a permettere il loro funzionamento, ovvero la Blockchain, è stato subito preso in considerazione. Proprio per questo, ci sono e ci sono stati importanti investimenti di Venture Capital sulla Blockchain, ovvero circa $ 900 milioni nel 2017 e solamente nei mesi di gennaio e febbraio 2018 si contano quasi $ 375 milioni. Se qualche di questi progetti prenderà forma concretamente, per cui potrà permettere soluzioni innovative ed efficienti grazie all'utilizzo della Blockchain, questo potrebbe rivoluzionare radicalmente tutta l'economia mondiale perché tutti dovranno convertirsi ed adeguarsi a questa.

Nel frattempo, nel settore finanziario Barclays, Ubs e Credit Suisse hanno già avviato un progetto pilota che utilizza la Blockchain di Ethereum, proprio per utilizzare gli *smart contracts* nella fase di *compliance* della Mifid II. Come si era detto nel secondo capitolo, non solo la finanza sta puntando in quella direzione, ma per esempio è stato investito anche il settore alimentare. Infatti, anche importanti player italiani stanno studiando la catena dei blocchi per tracciare in piena sicurezza l'intera filiera dei prodotti. Anche oltreoceano, Wall-Mart ha già avviato degli sperimenti per controllare la filiera delle migliaia di prodotti che compongono i suoi scaffali. Nel settore farmaceutico, l'azienda Pfizer sta putando alla ricerca di sistemi sicuri per seguire i componenti delle pillole prodotte.

Nella sanità invece si studia per mettere in sicurezza il patrimonio dei dati sanitari delle persone, ovvero si parlerebbe di una mole di dati pari a 10 volte quello delle carte di credito, cosicché possa essere accessibile alle altre aziende del settore. Secondo IBM, questa tecnologia sarà utilizzata già entro il 2020, da più della metà delle aziende del settore.

Ancora, si vuole evidenziare come due aziende storiche Telegram e Kodak si stanno dirigendo su questa tecnologia. In particolare, Telegram sta lanciando una ICO da record, ovvero potrebbe superare i dati consuntivi, ovvero la soglia dei $ 1.5 miliardi, per creare un sistema di transazioni più efficienti, superando la stessa blockchain di Bitcoin.

Il Token lanciato è denominato: Gram. Nei mesi preliminari ha raccolto ben $ 850 milioni (al di sopra della soglia prefissata: $ 600 milioni). Questa fase pre-sale è avvenuta nei mesi di gennaio e febbraio 2018, in cui era riservata solo ai Venture capital e ai grandi investitori, mentre l'apertura della sottoscrizione al grande pubblico era prevista a marzo 2018. Questa grande raccolta di capitali, viene adibita allo sviluppo della Blockchain Telegram Open Network (Ton), per sviluppare Telegram Messenger e altri scopi. Secondo alcune stime, la raccolta prevista da marzo 2018 potrebbe raccogliere fino ad $ 1.1 miliardo, per un totale pari ai $ 2 miliardi, realizzando così una delle più grandi ICO di sempre. In particolare, lo scopo ultimo di Ton è quello di creare un sistema di finanziamento delle attività di R&S sulla blockchain che sia alternativo ad Ethereum (attualmente questa è quella più utilizzata per lanciare le ICO). Quindi creare una piattaforma, concorrenziale ad Ethereum, per supportare il trend delle sperimentazioni di servizi ed applicazioni decentralizzate, che potranno essere sviluppati sulla Blockchain.

Kodak, che nel 2013 stava sfiorando la bancarotta ed aver venduto la maggior parte dei suoi brevetti ad altre compagnie tra cui Apple e Microsoft, sta puntando il tutto per tutto sulla Blockchain, con il suo *KokakCoin*, che permetterà di partecipare ad un sistema di gestione e controllo del copyright delle fotografie, risolvendo così la problematica della vulnerabilità delle immagini sulla rete.

Inoltre, la Blockchain è arrivata anche nel mondo degli aiuti umanitari. Questo per supportare le organizzazioni umanitarie nell'identificazione virtuale dei profughi, così tracciando le persone nei loro spostamenti e riassicurare i donatori che i soldi lasciategli siano spesi realmente per lo scopo adibito. Tra i protagonisti si trovano anche degli italiani: Aidcoin, e Helperbit, che utilizzano la tecnologia per la tracciabilità e disintermediazione delle donazioni.

Per ultimo ma non per importanza, la Blockchain potrebbe sopraggiungere anche nel settore dei media. In particolare, potrebbe salvare il mondo dei giornali che sta passando un'era grigia, tra un market share che si sta riducendo continuamente e l'avvento della digitalizzazione degli articoli in rete. Secondo a Jarrod Dicker, un veterano del settore, che ricopriva la carica di vicepresidente del Innovation & Commercial del Washngton Post, si è dimesso per guidare la Po.et, cioè una piattaforma innovativa che utilizza la Blockchain per l'editoria in ambito digital. Questa startup *open-source* si è prefissata di tracciare i contenuti e pubblicità digitali all'interno del network. In questo modo i creatori dei contenuti media e i giornalisti potranno venire a conoscenza dove e come i loro articoli sono stati utilizzati su internet. Questo potrà essere fatto tramite una blockchain *Permissioned*, cioè privata e viene offerto il servizio di notarizzazione dei contenuti su internet. Secondo Dicker, questa piattaforma può diventare un *market place* digitale, in cui i giornalisti potranno verificare la popolarità dei loro articoli e nel pieno rispetto del copyright. In aggiunta, contestualmente coloro che lavorano nel marketing potranno visionare quali contenuti ed autori siano più influenti in rete.

Di seguito verranno mostrati i progetti Blockchain che attualmente sono stati avviati da numerosi player internazionali.

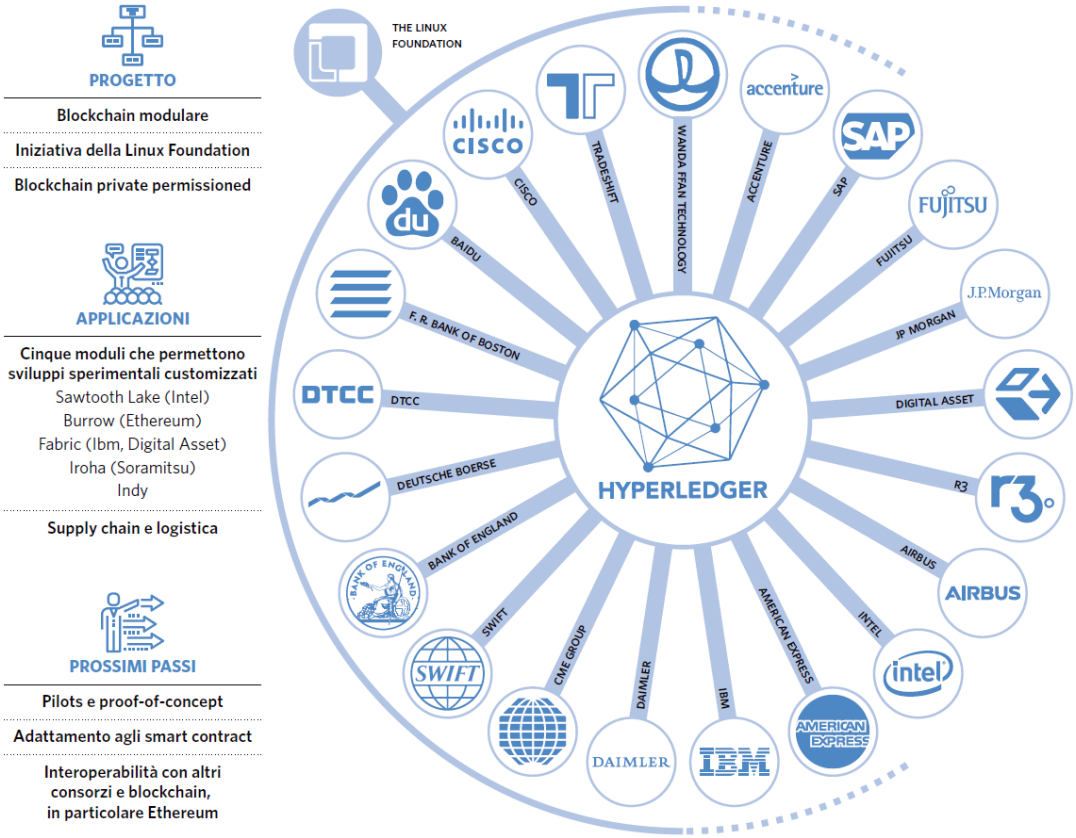


Figura 5.2 Rappresentazione dei progetti avviati dalle aziende che utilizzano la Blockchain di Hyperledger. Fonte Url: "Bitcoin Generation" Nòva, Sole 24 ORE.

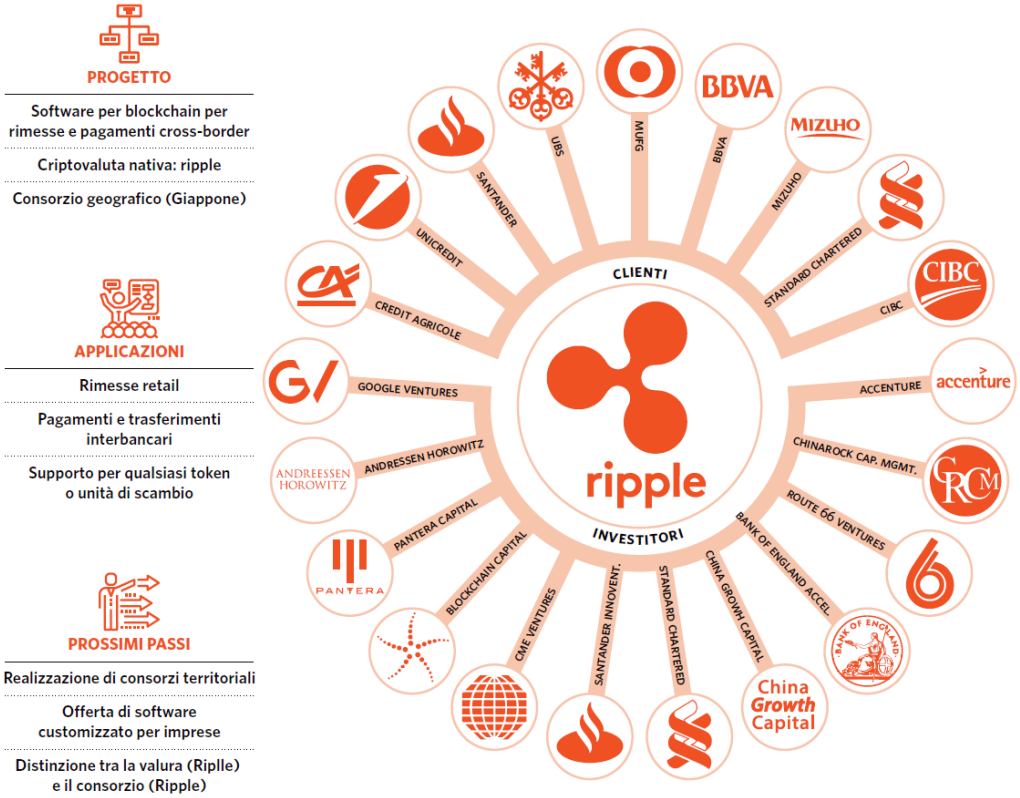


Figura 5.3 Rappresentazione dei progetti avviati dalle aziende che utilizzano la Blockchain di Ripple. Fonte Url: "Bitcoin Generation" Nòva, Sole 24 ORE.

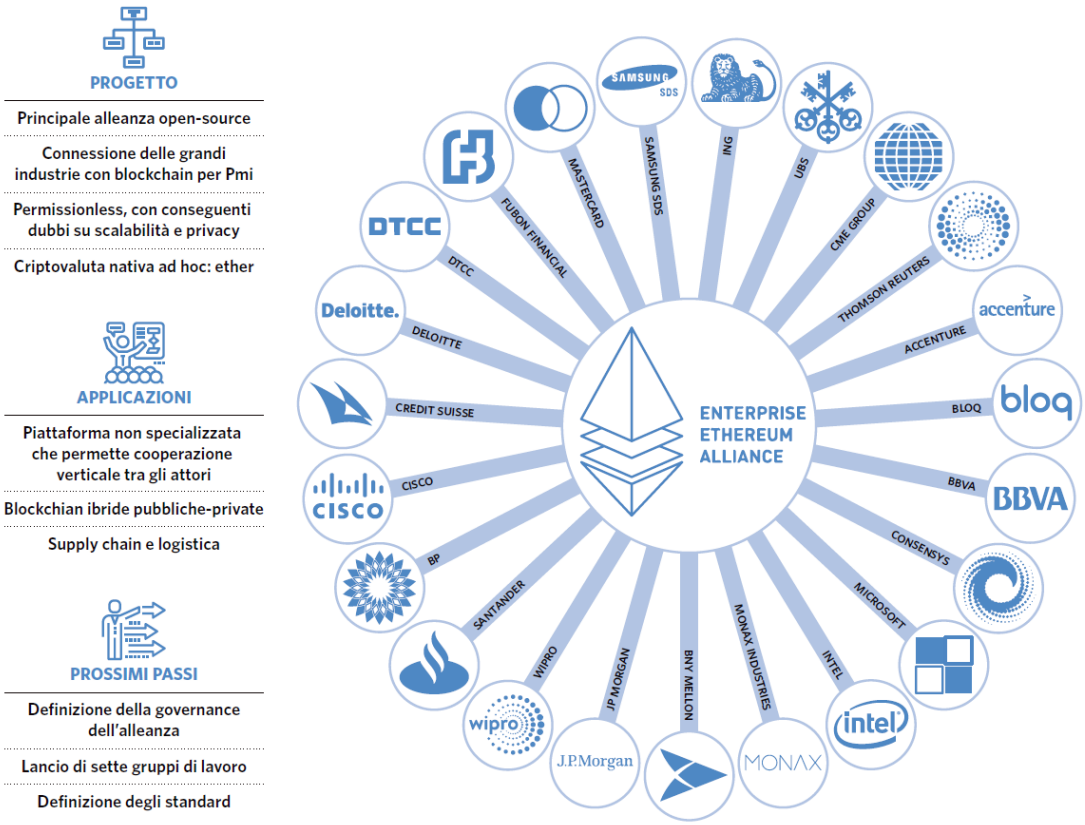


Figura 5.4 Rappresentazione dei progetti avviati dalle aziende che utilizzano la Blockchain di Ethereum. Fonte Url: "Bitcoin Generation" Nòva, Sole 24 ORE.

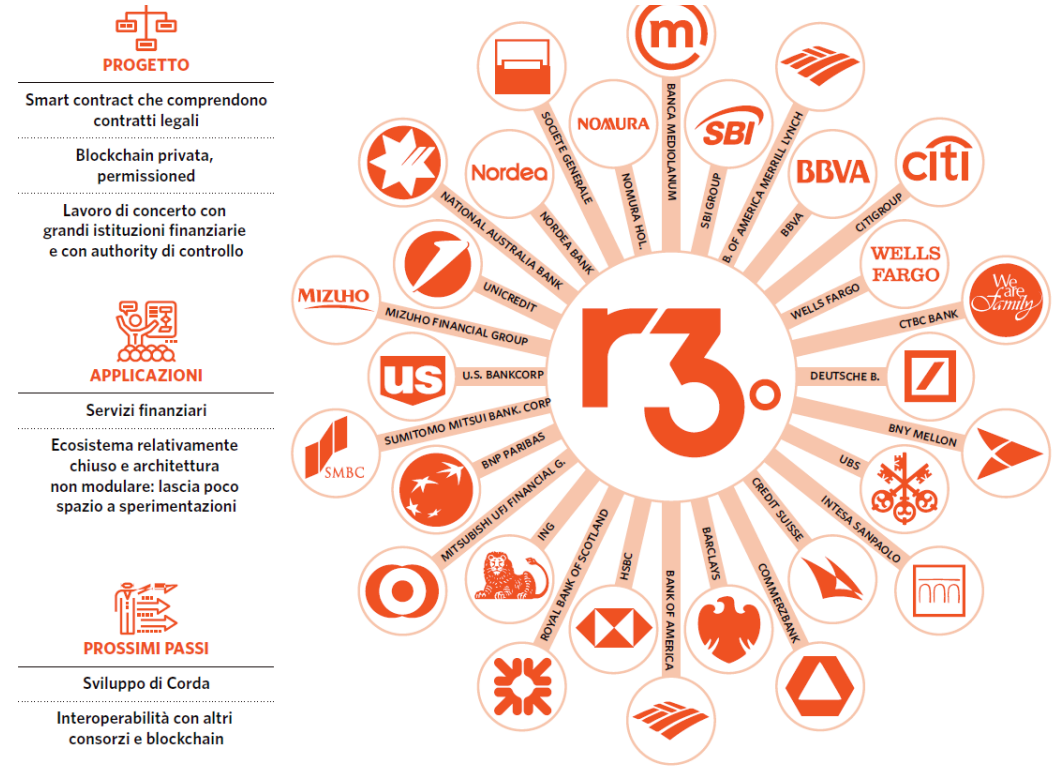


Figura 5.5 Rappresentazione dei progetti avviati dalle aziende che utilizzano la Blockchain di R3. Fonte Url: "Bitcoin Generation" Nòva, Sole 24 ORE.

Alla luce di quanto si è illustrato, si può affermare che la prima azienda che riuscirà a realizzare efficacemente questa tecnologia all'interno del proprio business, spingerà tutte le altre in questa direzione per non rimanere tagliata fuori dal mercato. Proprio come tutte le tecnologie disruptive, non si può sapere a priori se questo potrà andare a buon fine, certo è più opportuno studiare ex-ante piuttosto che arrivarci ex-post evitando così di rimanere indietro quando tutto il proprio settore si è già evoluto e ha implementato le nuove metodologie innovative all'interno del business.

Le ICO come metodo alternativo per finanziare le Imprese?

Si è illustrato come le ICO siano come il crowdfunding, ossia un metodo alternativo (rispetto a Banca, Borsa) per finanziare lo sviluppo di nuove criptovalute. Telegram ha lanciato la propria ICO per racimolare i fondi per finanziare i propri progetti. Inoltre, come è stato descritto nel terzo capitolo, il mondo delle ICO è del tutto deregolamentato e questo metodo di finanziamento è visto proprio come una scommessa, perché non c'è nessuna garanzia che non possa trattarsi di una truffa o che il progetto non possa vedere mai la luce. Detto questo, si potrebbe immaginare questo metodo non solo per le startup di criptovalute, ma anche per finanziare le imprese già esistenti e che operano in tutt'altri settori?
Telegram lo ha fatto, e ha raccolto un enorme successo sia per la presentazione dei propri progetti e sia specialmente per il brand che rappresenta. Probabilmente, se mai in un futuro intervenissero i legislatori per regolare questo metodo, può essere che potrebbe esser anche usato per finanziare i progetti delle aziende tradizionali. È anche vero che questo metodo abbia riscosso successo proprio perché non vi erano vincoli legislativi e normativi. L'investitore che aderisce ad una ICO lo fa principalmente per acquistare ad un prezzo assai ridotto dei token, per sperare poi di rivenderlo ad un prezzo superiore, realizzando così un capital gain.

Conclusioni

In questo elaborato si è voluto fornire una chiara e puntuale analisi delle diverse sfaccettature del criptomondo. Si è illustrato come dall'avvento del Bitcoin ad oggi questo settore sia completamente cambiato e ora esistono più di 1600 valute digitali. Nel corso di questi nove anni, molti esperti hanno dapprima ignorato o schernito questa tecnologia, per poi ricredersi poco tempo dopo. Tuttora, esistono molti dubbi a riguardo del futuro di questo settore: può realmente diventare il prossimo sistema monetario? Com'è stato illustrato lungo il proseguo dello scritto, quello che sembrerebbe certo è la tecnologia della Blockchain che può essere adattata ed implementata al più disparato settore economico esistente. Dapprima, è stata inventata per il criptomondo in modo da assolvere al problema del *double-spending*, successivamente in molti altri settori, non solo finanziari, ne stanno realmente testando le funzionalità.

Inoltre, analizzando e confrontando cinque diverse criptovalute, si è potuto dimostrare la diversità intrinseca di ciascuna, ognuna ha una propria filosofia che la contraddistingue dalle altre.

Ulteriormente, si è potuto constatare come il criptomondo sia improntato alla continua ricerca di sempre nuove criptovalute, partendo dalle debolezze ed inefficienze delle esistenti. Infatti, questo è stato anche uno dei motivi che ha portato il boom nel settore. A tal riguardo si può riprendere l'esempio della capostipite, che è stata più volte criticata anche se attualmente è quella più diffusa ed apprezzata, infatti ha un livello di capitalizzazione e numero di transazioni giornaliero più alto rispetto a tutte le altre. Probabilmente si potrà assistere a delle nuove valute digitali decentralizzate che potranno soppiantare quelle che attualmente sono presenti sul mercato.

L'atipicità che risiede in Bitcoin, e che è la sua caratteristica più importante, è il fatto che sia una valuta decentralizzata nella sua vera essenza, infatti non vi è nessuna organizzazione sopra ma solo un team di sviluppatori che continuano a monitorare ed aggiornare il software.

Ulteriormente, si è potuto dimostrare la natura delle criptomonete e se queste possano essere identificate come monete a tutti gli effetti. Nello specifico, si è visto come la struttura intrinseca delle valute digitali risulti ininfluente su tale decisione. Quindi, ad esempio che vi sia una predeterminazione sull'offerta monetaria o meno (come nel caso di Bitcoin, il quale è caratterizzato dalla sua inelasticità dell'offerta dei propri tokens).

Questo perché, come si è potuto descrivere abbondantemente, le valute digitali odierne soddisfano solamente una delle tre funzioni, vale a dire la funzione di mezzo di scambio; mentre per il loro valore altamente oscillante, ovvero caratterizzato da un'alta volatilità nel prezzo, non consentono di soddisfare alle altre funzioni tipiche della moneta.
Il criptomondo caratterizzato inizialmente per la sua volontà anarchica, contro il sistema monetario ufficiale il quale è stato incriminato più e più volte di essere controllato da un oligopolio, risultando così inefficiente ed ingiusto; si è poi adeguato e adattato ai diversi contesti della società, pur comunque rimanendo semi-decentralizzato rispetto al sistema tradizionale. Sotto questa lente, il Bitcoin non è riuscito nel suo intento, perché anziché ridare il potere monetario al popolo, la sua coniazione (o per meglio dire: l'estrazione) è stata affidata a privati fortemente concentrati (i *pools mining*), in aggiunta tale operazione ha portato costi insostenibili in termini economici ed ambientali (il consumo del mining è pari al fabbisogno energetico della Danimarca). In aggiunta, secondo alcune stime, i cento portafogli più ricchi al mondo detengono più di un sesto di tutti i bitcoin estratti, quindi c'è stata una fortissima disparità nella distribuzione della ricchezza. Invece di diventare il nuovo sistema monetario più meritocratico, ha fatto registrare *capital gain* del tutto iniqui ed immeritati.
Questo è potuto accadere per diversi fattori, quali ad esempio il fatto che non vi sia un'autorità centrale che vigili sulla corretta distribuzione dei tokens o anche dal fatto che principalmente questa valuta digitale viene più adibita come asset d'investimento ai fini speculativi che per altri utilizzi.
Questi discorsi li si possono traslare anche sugli Altcoins i quali, anche se profondamente differenti, sono caratterizzati da un forte utilizzo speculativo. Nel terzo capitolo, è stato illustrato come solo alcune di esse venivano utilizzate più sulla Blockchain che sugli Exchangers (nel caso di Bitcoin è riferibile al secondo caso).
Resta da capire come e quando verranno regolamentate seriamente queste valute da parte degli Stati; è molto difficile pensare che raggiungano un accordo per creare una legislazione internazionale comune che disciplini il criptomondo. Certamente, il mondo attuale ne sente la necessità, visto che le valute virtuali stanno lentamente diventando un fenomeno globale. In aggiunta, questo diventerebbe fondamentale per l'effettiva accettazione di tali valute nell'economia reale.

Attualmente, la regolamentazione influisce solo sul prezzo delle criptovalute, influenzandone positivamente o negativamente a seconda del tipo di normativa di riferimento. A tal riguardo, se gli Stati dovessero prendere in considerazione le valute digitali come monete a corso legale a tutti gli effetti, ciò si rifletterebbe poi sull'economia reale trovando tali valute sui banchi dei negozianti.

Cionondimeno, come è stato detto precedentemente, il criptomondo ha riportato finalmente il tema della natura intrinseca della moneta tradizionale all'attenzione pubblica. Inoltre, questo fenomeno è stato preso in esame anche dai Governi e dalle Banche Centrali, probabilmente nel prossimo futuro potremmo assistere all'avvento di nuove valute digitali aventi corso legale, che attraverso l'utilizzo della Blockchain potranno superare i limiti del sistema monetario tradizionale.

Quello che è dato per certo è che si sentirà parlare di criptovalute ancora nei prossimi anni e che, verosimilmente in un futuro prossimo, si assisterà all'avvento di un nuovo sistema monetario, il quale potrebbe mettere al centro nuovi pensieri e valori.

Bibliografia

Agenzia delle Entrate, Risoluzione n. 72/E/2016, ultima data consultazione 16 giugno 2018.

Amato, Fantacci M.L., (gennaio 2016), *Per un pugno di Bitcoin – Rischi e opportunità delle monete virtuali*, Università Bocconi Editore, ultima data consultazione 16 giugno 2018.

Ametrano, M. Ferdinando, (27 dicembre 2017), *I bitcoin nell'agenda del prossimo G20*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/mondo/2017-12-27/i-bitcoin-nell-agenda-prossimo-g20--170020_PRV.shtml?uuid=AEQnjnXD", ultima data consultazione 16 giugno 2018.

Aparo Von Flue, A., (17 novembre 2015), '*Dark web': l'Internet oscuro non è luogo dove andare a spasso*, Il Fatto Quotidiano, Url: "https://www.ilfattoquotidiano.it/2015/11/17/dark-web-linternet-oscuro-non-e-luogo-dove-andare-a-spasso/2227039/", ultima data consultazione 16 giugno 2018.

Aquini, F., (22 gennaio 2018), *Nvidia: chi vuole arricchirsi con le criptovalute fa salire il prezzo delle GPU*, DDAY.it, Url: "https://www.dday.it/redazione/25507/nvidia-chi-vuole-arricchirsi-coi-bitcoin-fa-salire-il-prezzo-delle-gpu", ultima data consultazione 16 giugno 2018.

Balestreri, G., (17 dicembre 2017), *Estrarre bitcoin è sempre più costoso: un esperto spiega fino a quando sarà redditizio*, Business Insider Italia, Url: "https://it.businessinsider.com/estrarre-bitcoin-e-sempre-piu-costoso-un-esperto-spiega-fino-a-quando-sara-redditizio/", ultima data consultazione 16 giugno 2018.

Balestreri, G., (17 dicembre 2017), Url: Estrarre bitcoin è sempre più costoso: un esperto spiega fino a quando sarà redditizio, Business Insider, Url: "https://it.businessinsider.com/estrarre-bitcoin-e-sempre-piu-costoso-un-esperto-spiega-fino-a-quando-sara-redditizio/", ultima data consultazione 16 giugno 2018.

Baran, P., (agosto 1964), *On Distributed Communications Networks*, The Rand Corporation, Santa Monica – California, ultima data consultazione 16 giugno 2018.

Bellini, M., (14 marzo 2017*), Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, Blockchain4innovation.it, Url: "https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/", ultima data consultazione 16 giugno 2018.

Bellini, M., (27 febbraio 2018), *Austria: una proposta per la regolamentazione delle criptovalute e dell'ICO*, Blockchain4innovation, Url: "https://www.blockchain4innovation.it/istituzioni-e-associazioni/austria-una-proposta-per-la-regolamentazione-delle-criptovalute-e-dellico/", ultima data consultazione 16 giugno 2018.

Bheemaiah, K., (gennaio 2015), *Block Chain 2.0: The Renaissance of Money*, Wired, Url: "https://www.wired.com/insights/2015/01/block-chain-2-0/", ultima data consultazione 16 giugno 2018.

Buchholz, Delaney Warren Parker, M. J. J. J., (2012), *Bits and Bets - Information, Price Volatility, and Demand for Bitcoin*, ultima data consultazione 16 giugno 2018.

Burke, N., (22 febbraio 2018), *Bitcoin: il valore è negli occhi di chi se lo tiene stretto*, Investing.com, Url: "https://it.investing.com/analysis/bitcoin-il-valore-e-negli-occhi-di-chi-se-lo-tiene-stretto-200219949", ultima data consultazione 16 giugno 2018.

Carboni, D., (2018), *Dagli smart contract alle ICO*, Amazon Kindle Edition, ultima data consultazione 16 giugno 2018.

Carlini, V., (17 gennaio 2018), *Bitcoin, ecco perché non è una moneta. Il vero valore? La blockchain*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/finanza-e-mercati/2018-01-15/bitcoin-perche-non-e-moneta-vero-valore-blockchain-155334_PRV.shtml?uuid=AEYilviD", ultima data consultazione 16 giugno 2018.

Carlini, V., (17 gennaio 2018), *Bitcoin, ecco perché non è una moneta. Il vero valore? La blockchain*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/finanza-e-mercati/2018-01-15/bitcoin-perche-non-e-moneta-vero-valore-blockchain-155334.shtml?uuid=AEYilviD", ultima data consultazione 16 giugno 2018.

Castelmur, F., (7 gennaio 2018), *Criptovalute, le alternative al bitcoin*, Il Fatto Quotidiano, Url: "https://www.ilfattoquotidiano.it/2018/01/07/criptovalute-le-alternative-al-bitcoin/4078579/", ultima data consultazione 16 giugno 2018.

Catena, N., (19 maggio 2017), *Che cosa stanno insegnando le criptomonete alle banche centrali (BCE, FED, etc.)?*, Quora, Url: "https://it.quora.com/Che-cosa-stanno-insegnando-le-criptomonete-alle-banche-centrali-BCE-FED-etc", ultima data consultazione 16 giugno 2018.

Chiaritti, M., (8 gennaio 2018), *Iota fa a meno della blockchain*, Il Sole 24 ORE – Nòva, Url: "http://nova.ilsole24ore.com/progetti/iota-fa-a-meno-della-blockchain/", ultima data consultazione 16 giugno 2018.

Chuen, D. L. K., (2015), *Handbook of Digital Currency – Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier - Academic Press, ultima data consultazione 16 giugno 2018.

Cinieri, S., *Bitcoin e criptovalute, inquadramento fiscale: problemi aperti*, in Riv. Ipsoa (26 marzo 2018), Url: "http://www.ipsoa.it/documents/fisco/imposte-dirette/quotidiano/2018/03/26/bitcoin-criptovalute-inquadramento-fiscale-problemi-aperti#", ultima data consultazione 16 giugno 2018.

Clark, Chris, (luglio 2013), *Bitcoin Internals: A technical guide to Bitcoin*, Amazon Kindle Edition, ultima data consultazione 16 giugno 2018.

Cohen, J., (21 febbraio 2018), *Le 5 criptovalute con la performance migliore nel 2018 (finora)*, Investing.com, Url: "https://it.investing.com/analysis/le-5-criptovalute-con-la-performance-migliore-nel-2018-finora-200219919", ultima data consultazione 16 giugno 2018.

Cosimi, S., (26 febbraio 2018), *Criptovalute, il 46% di quelle lanciate nel 2017 è già fallito*, La Repubblica, Url: "http://www.repubblica.it/tecnologia/sicurezza/2018/02/26/news/criptovalute_il_46_di_quelle_lanciate_nel_2017_e_gia_fallito-189821972/", ultima data consultazione 16 giugno 2018.

D.lgs. n. 231/07 (2007), ultima data consultazione 16 giugno 2018.

D.lgs. n. 90/17 (maggio 2017), ultima data consultazione 16 giugno 2018.

D.P.R. 22 dicembre 1986 n.917, Art. 67 del T.U.I.R., ultima data consultazione 16 giugno 2018.

Davies, G., (2002), *A history of money from ancient times to the present day*, 3rd ed.

De Masi, M., *Le criptovalute entrano nel quadro RW*, in Riv. Ipsoa, (2018), Url: "http://www.bigsuite.ipsoa.it", ultima data consultazione 16 giugno 2018.

Dello Iacovo, L., (12 Aprile 2013), *Ecco i Ripple, la moneta digitale che lancia la sfida ai Bitcoin*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/tecnologie/2013-04-12/ecco-ripple-sfida-bitcoin-112503.shtml?uuid=AbhBMXmH", ultima data consultazione 16 giugno 2018.

Dopsch, A., (1930), *Economia naturale ed economia monetaria nella storia universale*, Sansoni, ultima data consultazione 16 giugno 2018.

European Central Bank (ECB), (febbraio 2015), *Virtual currency schemes – a further analysis*, ultima data consultazione 16 giugno 2018.

Ferraresso, A., (7 maggio 2016), *La crittografia dietro a Bitcoin*, Medium Corporation, Url: "https://medium.com/@AndreaFerraresso/la-crittografia-dietro-a-bitcoin-72cc6ad3fa41", ultima data consultazione 16 giugno 2018.

Ferrari, E., *Bitcoin e Criptovalute: la moneta virtuale tra fisco e antiriciclaggio*, in Riv. Ipsoa, (2018), Url: "http://www.bigsuite.ipsoa.it", ultima data consultazione 16 giugno 2018.

Fior, P., (16 gennaio 2018), *Bitcoin, escalation di truffe nel silenzio della vigilanza. La Consob lascia campo libero a chi tosa il parco buoi*, Il Fatto Quotidiano, Url: "https://www.ilfattoquotidiano.it/2018/01/16/bitcoin-escalation-di-truffe-nel-silenzio-della-vigilanza-la-consob-lascia-campo-libero-a-chi-tosa-il-parco-buoi/4093706/", ultima data consultazione 16 giugno 2018.

Florindi, E., (2018), *Criptovalute: Manuale di Sopravvivenza*, Imprimatur, ultima data consultazione 16 giugno 2018.

Foti, L., (novembre 2017), *Capire Blockchain*, Amazon Kindle Edition, ultima data consultazione 16 giugno 2018.

Gentili, G. (9 marzo 2018), *Bitcoin Generation – la rivoluzione delle criptovalute*, Il Sole 24 ORE S.p.A., Milano, ultima data consultazione 16 giugno 2018.

Guttman B., (novembre 2013), *The Bitcoin Bible*, Books On Demand, ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, (2015) *Sulle tracce del geniale Nakamoto*" Edizione 10/2015, ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, (2017), *Da Nakamoto a Wright: chi si cela dietro l'inventore*, Edizione 02/2017, ultima data consultazione 16 giugno 2018.

J.P. Morgan, (9 febbraio 2018), *J.P. Morgan Perspectives - Decrypting Cryptocurrencies: Technology, Applications and Challenges*, ultima data consultazione 16 giugno 2018.

Kharpal, Ellyatt A. H., (19 gennaio 2018), *Bitcoin could be here for 100 years but it's more likely to 'totally collapse,' Nobel laureate says*, CNBC, Url: "https://www.cnbc.com/2018/01/19/bitcoin-likely-to-totally-collapse-nobel-laureate-robert-shiller-says.html", ultima data consultazione 16 giugno 2018.

Lavalle, C., (25 novembre 2017), *Arriva il bancomat per pagare con Bitcoin anche al supermercato*, La Stampa, Url: "http://www.lastampa.it/2017/11/25/tecnologia/news/arriva-il-bancomat-per-pagare-con-bitcoin-anche-al-supermercato-pdaAABrgxwvPdfQ4sPGtEK/pagina.html", ultima data consultazione 16 giugno 2018.

Lexicon, H., (2015), Hacker Lexicon: What Is the Dark Web?, "https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/", ultima data consultazione 16 giugno 2018.

Liberatore, L., (17 gennaio 2018), *Stellar, l'astro nascente delle criptovalute: sarà nuovo Bitcoin?*, Wall Street Italia, Url: "http://www.wallstreetitalia.com/stellar-lastro-nascente-delle-criptovalute/", ultima data consultazione 16 giugno 2018.

Liberatore, L., (9 gennaio 2018), *Bitcoin, Dimon di JP Morgan: "pentito di averlo definito frode*, Wall Street Italia, Url: "http://www.wallstreetitalia.com/bitcoin-dimon-di-jp-morgan-pentito-di-averlo-definito-frode/", ultima data consultazione 16 giugno 2018.

Lops, V., (8 febbraio 2018), *Bitcoin e i suoi fratelli: le criptovalute che rischiano di scomparire*, Url: "http://www.ilsole24ore.com/art/finanza-e-mercati/2018-02-07/criptovalute-selezione-darwiniana-vista-ecco-cosa-puo-accadere-180236_PRV.shtml?uuid=AEVxZ8vD", ultima data consultazione 16 giugno 2018.

Luongo, L., (9 marzo 2018), *1 miliardo di $ investiti su EOS. Ecco tutti i dettagli*, Yahoo Finanza, Url: "https://it.finance.yahoo.com/notizie/1-miliardo-investiti-eos-tutti-093000218.html?guccounter=1", ultima data consultazione 16 giugno 2018.

Marro, E., (5 gennaio 2018), Bitcoin accerchiato dalle autorità di regolamentazione: chi vincerà?, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/notizie/2018-01-05/bitcoin-accerchiato-autorita-regolamentazione-chi-vincera-065314.shtml?uuid=AEV2GFcD", ultima data consultazione 16 giugno 2018.

Masciandaro, D., (16 settembre 2017), *Sì alla moneta digitale ma con regole anti-rischio*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/commenti-e-idee/2017-09-15/si-moneta-digitale-ma-regole-anti-rischio-220501.shtml?uuid=AEmdc4TC", ultima data consultazione 16 giugno 2018.

Mason, B., (27 febbraio 2018), *IOTA: Cos'è e Come Comprare la Criptovaluta*, Yahoo Finanza, Url: "https://it.finance.yahoo.com/notizie/iota-cos-%C3%A8-e-come-082026529.html?guccounter=1", ultima data consultazione 16 giugno 2018.

Mason, B., (27 febbraio 2018), *IOTA: Cos'è e Come Comprare la Criptovaluta*, Yahoo Finance, Url: "https://it.finance.yahoo.com/notizie/iota-cos-%C3%A8-e-come-082026529.html", ultima data consultazione 16 giugno 2018.

Metz, Wohlsen C. M., (8 giugno 2014), *NEW DIGITAL CURRENCY AIMS TO UNITE EVERY MONEY SYSTEM ON EARTH*, Wired, Url: "https://www.wired.com/2014/08/new-digital-currency-aims-to-unite-every-money-system-on-earth/", ultima data consultazione 16 giugno 2018.

Metz, Wohlsen C. M., (8 giugno 2014), Wired, Url: "https://www.wired.com/2014/08/new-digital-currency-aims-to-unite-every-money-system-on-earth/?mbid=email_onsiteshare", ultima data consultazione 16 giugno 2018.

Morici, M., (11 gennaio 2018), *Tutto quello che c'è da sapere sulla criptovaluta Ripple*, Panorama, Url: "https://www.panorama.it/economia/soldi/tutto-quello-che-ce-da-sapere-sulla-criptovaluta-ripple/", ultima data consultazione 16 giugno 2018.

Morici, M., (11 gennaio 2018), *Tutto quello che c'è da sapere sulla criptovaluta Ripple*, Panorama, Url: "https://www.panorama.it/economia/soldi/tutto-quello-che-ce-da-sapere-sulla-criptovaluta-ripple/", ultima data consultazione 16 giugno 2018.

Morici, M., (19 gennaio 2018), *La blockchain, spiegata bene*, Panorama, Url: "https://www.panorama.it/economia/soldi/la-blockchain-spiegata-bene/", ultima data consultazione 16 giugno 2018.
Nakamoto, S., (31 ottobre 2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, ultima data consultazione 16 giugno 2018.

Nembri, A., (22 febbraio 2017), *M-Pesa i pagamenti mobile che cambiano la vita in 10 Paesi*, Vita, Url: "http://www.vita.it/it/article/2017/02/22/m-pesa-i-pagamenti-mobile-che-cambiano-la-vita-in-10-paesi/142559/", ultima data consultazione 16 giugno 2018.

Nepori, A., (3 dicembre 2017), *Bitcoin e criptovalute: 9 domande e risposte per sapere cosa sono e come funzionano*, La Stampa, Url: "http://www.lastampa.it/2017/12/03/tecnologia/idee/bitcoin-e-criptovalute-domande-e-risposte-per-sapere-cosa-sono-e-come-funzionano-SgPtqzi8tDmG2y6m9EMQVN/pagina.html", ultima data consultazione 16 giugno 2018.

Nepori, A., (3 gennaio 2018), *Bitcoin e le altre: ecco le 12 criptovalute più importanti*, La Stampa, Url: "http://www.lastampa.it/2018/01/03/multimedia/tecnologia/bitcoin-e-le-altre-ecco-le-criptovalute-pi-importanti-jrsdnGhjPtNihrbzYI7I7K/pagina.html", ultima data consultazione 16 giugno 2018.

Nicotra, M., (2 marzo 2018), *Le norme su Bitcoin e crittovalute nei diversi Paesi: il quadro*, Agenda Digitale, Url: "https://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-crittovalute-nei-diversi-paesi-quadro/", ultima data consultazione 16 giugno 2018.

O'Hagan, A., (30 giugno 2018), *The Satoshi Affair*, Url: "https://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair", ultima data consultazione 16 giugno 2018.

Paletta, A., (14 luglio 2017), *Criptovalute: diritto e finanza delle monete virtuali senza Stato sovrano e prima sentenza sull'uso di Bitcoin*, Il Sole 24 ORE – Diritto 24, Url: "http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2017-07-14/partnership-professionisti-e-imprese-reti-miste-113003.php", ultima data consultazione 16 giugno 2018.

Paletta, A., , (14 luglio 2017), *Criptovalute: diritto e finanza delle monete virtuali senza Stato sovrano e prima sentenza sull'uso di Bitcoin*, Sole 24 ORE – Diritto 24, Url: "http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2017-07-14/partnership-professionisti-e-imprese-reti-miste-113003.php?refresh_ce=1", ultima data consultazione 16 giugno 2018.

Papa, F., (maggio 2013), Speech del Santo Padre, Vaticano, Url: "https://w2.vatican.va/content/francesco/it/speeches/2013/may/documents/papa-francesco_20130516_nuovi-ambascaitori.html", , ultima data consultazione 16 giugno 2018.

Pelizzari, Morini T. M., (27 novembre 2017), *Il boom di Bitcoin non è per tutti*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/commenti-e-idee/2017-11-27/il-boom-bitcoin-non-e-tutti-164205.shtml?uuid=AEdjw2ID", ultima data consultazione 16 giugno 2018.

Peterson, B., (14 dicembre 2017), *La blockchain spiegata bene. Ecco la nuova tecnologia informatica che potrebbe essere dirompente quanto internet, Business Insider*, Url: "https://it.businessinsider.com/la-blockchain-spiegata-bene-ecco-la-nuova-tecnologia-informatica-che-potrebbe-essere-dirompente-quanto-internet/?refresh_ce", ultima data consultazione 16 giugno 2018.

Porcu, V., (15 gennaio 2015), Silk Road chiuso, TOR e crittografia inutili, tom's Hardware, Url: "https://www.tomshw.it/silk-road-chiuso-tor-crittografia-inutili-63586", ultima data consultazione 16 giugno 2018.

Prezioso, R., (9 marzo 2018), *Universo Crypto: fra un anno o due resteranno solo i migliori*, Yahoo Finanza, Url: "https://it.finance.yahoo.com/notizie/universo-crypto-anno-due-resteranno-100000863.html?guccounter=1", ultima data consultazione 16 giugno 2018.

Romano, Tucci R. U. (1983), *Storia d'Italia. Annali 6. Economia naturale, economia monetaria*, Giulio Einaudi editore, ultima data consultazione 16 giugno 2018.

Rossi, A., (2017), *Ethereum*, Amazon, ultima data consultazione 16 giugno 2018.
S., A., (30 novembre 2017), *La Bce demolisce il Bitcoin: "Non è una valuta"*, Corriere Comunicazioni, Url: "https://www.corrierecomunicazioni.it/finance/la-bce-demolisce-bitcoin-non-valuta/", ultima data consultazione 16 giugno 2018.

Sabella, M., (10 gennaio 2018), *Perché piacciono alle aziende,* Corriere della Sera, Url: "https://www.corriere.it/economia/18_gennaio_10/buffett-le-criptovalute-faranno-brutta-fine-81090898-f622-11e7-9b06-fe054c3be5b2.shtml", ultima data consultazione 16 giugno 2018.

Samuelson, P.A., (1983), *Economia*, Zanichelli, ultima data consultazione 16 giugno 2018.

Savevski, V., (31 gennaio 2018), *La tecnologia dietro al Bitcoin potrebbe cambiare il mondo della sanità*, Wired, Url: "https://www.wired.it/scienza/medicina/2018/01/31/blockchain-sanita/", ultima data consultazione 16 giugno 2018.

Shwartz, D., (2014), *The Ripple Protocol Consensus Algorithm*, Ripple Labs Inc., ultima data consultazione 16 giugno 2018.

Sideri, M., (2 gennaio 2018), La scalata di Ripple, l'anti Bitcoin Ecco perché ora piace alle banche, Corriere della Sera, url: "http://www.corriere.it/economia/18_gennaio_02/scalata-ripple-l-anti-bitcoin-ecco-perche-ora-piace-banche-97077066-f001-11e7-ae90-7494db7ac3d7.shtml", ultima data consultazione 16 giugno 2018.

Sideri, M., (2 gennaio 2018), Ecco perché ora piace alle banche, Corriere della Sera, Url: "https://www.corriere.it/economia/18_gennaio_02/scalata-ripple-l-anti-bitcoin-ecco-perche-ora-piace-banche-97077066-f001-11e7-ae90-7494db7ac3d7.shtml", ultima data consultazione 16 giugno 2018.

Signorelli, A. D, (4 marzo 2018), Questa fabbrica di Bitcoin guadagna più dei colossi tech, La Stampa, Url: "http://www.lastampa.it/2018/03/04/tecnologia/questa-fabbrica-di-bitcoin-guadagna-pi-dei-colossi-tech-tOKIljDpmI4zlzpAXP1TJI/pagina.html", ultima data consultazione 16 giugno 2018.

Signorelli, A., (22 febbraio 2018), *Che cos'è Litecoin, la prima rivale dei Bitcoin*, Esquire, Url: "https://www.esquire.com/it/news/attualita/a18494503/che-cose-litecoin-la-vecchia-rivale-dei-bitcoin/", ultima data consultazione 16 giugno 2018.

Soldavini P., (23 gennaio 2018), *Bitcoin, la Corea del Sud vuole mettere fine all'anonimato*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/tecnologie/2018-01-23/bitcoin-corea-sud-vuole-mettere-fine-all-anonimato-102350.shtml?uuid=AEqsURnD", ultima data consultazione 16 giugno 2018.

Soldavini, P., (16 gennaio 2018), *Ecco come e perché Cina e Corea del Sud dichiarano guerra al bitcoin*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/notizie/2018-01-16/cina-e-corea-dichiarano-guerra-bitcoin-ecco-perche-123645.shtml?uuid=AEbqtZjD", ultima data consultazione 16 giugno 2018.

Soldavini, P., (17 settembre 2017), *Dimon condanna il bitcoin, ma poi JP Morgan è tra i principali acquirenti*, Il Sole 24 ORE, "http://www.ilsole24ore.com/art/finanza-e-mercati/2017-09-17/dimon-condanna-bitcoin-e-fa-cadere-ma-poi-jp-morgan-e-i-principali-acquirenti-181620_PRV.shtml?uuid=AEdNalUC", ultima data consultazione 16 giugno 2018.

Soldavini, P., (20 luglio 2017), *Ico per 1,3 miliardi $ nel 2017: ecco come si finanziano le startup in criptovalute*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/tecnologie/2017-07-20/ico-13-miliardi-$-2017-ecco-come-si-finanziano-startup-criptovalute-114507.shtml?uuid=AEJutH0B", ultima data consultazione 16 giugno 2018.

Soldavini, P., (23 gennaio 2018), *Bitcoin, la Corea del Sud vuole mettere fine all'anonimato*, Url: "http://www.ilsole24ore.com/art/tecnologie/2018-01-23/bitcoin-corea-sud-vuole-mettere-fine-all-anonimato-102350.shtml?uuid=AEqsURnD", ultima data consultazione 16 giugno 2018.

Soldavini, P., (3 gennaio 2018), *Criptovalute, Ripple batte Bitcoin: +39.600% in un anno e +124% in una settimana*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/notizie/2017-12-31/e-ripple-criptovaluta-momento-35000percento-un-anno-un-nuovo-sistema-pagamenti-153450.shtml?uuid=AEDP6NZD", ultima data consultazione 16 giugno 2018.

Soldavini, P., (5 gennaio 2018), *Chris Larsen, il padre di Ripple nella top ten dei Paperoni globali*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/notizie/2018-01-05/chris-larsen-padre-ripple-top-ten-paperoni-globali-150105.shtml?uuid=AE90UecD", ultima data consultazione 16 giugno 2018.

Solvadini, P., (12 agosto 2017), *Tra frodi e speculazioni è boom di criptovalute*, Il Sole 24 ORE, Url: "http://www.ilsole24ore.com/art/finanza-e-mercati/2017-08-11/fra-frodi-e-speculazioni-e-boom-criptovalute--211749.shtml?uuid=AEOJPACC", ultima data consultazione 16 giugno 2018.

Spagnuolo, E., (12 gennaio 2018), *Chi è davvero Satoshi Nakamoto, l'inventore dei bitcoin?*, Wired, Url: "https://www.wired.it/economia/finanza/2018/01/12/satoshi-nakamoto-bitcoin/", ultima data consultazione 16 giugno 2018.

Spagnuolo, E., (4 maggio 2018), *"Bitcoin come una moneta estera": il Fisco tassa i guadagni da criptovalute*, Wired, Url: "https://www.wired.it/economia/finanza/2018/05/04/bitcoin-criptovalute-agenzia-entrate/", ultima data consultazione 16 giugno 2018.

Spinelli, F., (1999), *La moneta dall'oro all'euro – un viaggio fra storia e teoria*, Etas, ultima data consultazione 16 giugno 2018.

Teodoro, F., (2018), *Blockchain 3.0*, Amazon Kindle Edition, ultima data consultazione 16 giugno 2018.

Tessa, M., (6 marzo 2018), *Da Harvard: "Tra 10 anni è più probabile che Bitcoin sia a $100 che a $100mila"*, Wall Street Italia, Url: "http://www.wallstreetitalia.com/da-harvard-tra-10-anni-e-piu-probabile-che-bitcoin-sia-a-100-che-a-100mila/", ultima data consultazione 16 giugno 2018.

Tremolada, L., (30 dicembre 2017), *Bitcoin: ecco quanta energia elettrica consumano*, Il Sole 24 ORE, Url: "http://www.infodata.ilsole24ore.com/2017/12/30/bitcoin-quanta-energia-elettrica-consumano/", ultima data consultazione 16 giugno 2018.

Tremolada, L., (30 dicembre 2017), *Bitcoin: ecco quanta energia elettrica consumano*, Il Sole 24 ORE, Url: "http://www.infodata.ilsole24ore.com/2017/12/30/bitcoin-quanta-energia-elettrica-consumano/", ultima data consultazione 16 giugno 2018.

Vedishchev, A., (11 novembre 2017), *Proof of stake, mining di criptovalute a basso costo*, tom's Hardware, Url: "https://www.tomshw.it/proof-of-stake-mining-criptovalute-basso-costo-89574", ultima data consultazione 16 giugno 2018.

Velcich, F., (29 gennaio 2018), *Un maxifurto da 500 milioni di dollari in criptovalute innesca la grande fuga da Bitcoin & Co.*, Business Insider Italia, *Url:* "https://it.businessinsider.com/un-maxifurto-da-500-milioni-di-dollari-in-criptovalute-innesca-la-grande-fuga-da-bitcoin-co/", ultima data consultazione 16 giugno 2018.

Wasik, J., (8 novembre 2017), *Perché per Buffett quella dei bitcoin è solo una bolla*, Forbes Italia, Url: "https://www.forbes.it/sites/it/2017/11/08/buffett-bitcoin-bolla/#20a466f12e40", ultima data consultazione 16 giugno 2018.

Wilmoth, J., (12 settembre 2012), *What is an Altcoin?*, CCN, Url: "https://www.ccn.com/altcoin/", ultima data consultazione 16 giugno 2018.

Zmudzinski, A., (28 febbraio 2018), *Bill gates: Le criptovalute sono causa diretta di morti*, CoinList, Url: "https://coinlist.me/it/notizie/bill-gates-le-criptovalute-sono-causa-diretta-di-morti", ultima data consultazione 16 giugno 2018.

Sitografia

Amazon.it, Url: "https://www.amazon.it/Bitmain-antminer-14TH-lestrazione-bitcoin/dp/B004GEJU84", ultima data consultazione 16 giugno 2018.

Ansa, (13 febbraio 2018), *Bitcoin: Islanda rischia restare al buio, causa boom miner*, Ansa, Url: "http://www.ansa.it/sito/notizie/economia/criptovalute/2018/02/13/bitcoin-islanda-rischia-restare-al-buio-causa-boom-miner_a87d8223-c018-4d02-a788-4580e77a2000.html", ultima data consultazione 16 giugno 2018.

Aquini, F., (22 gennaio 2018), *Nvidia: chi vuole arricchirsi con le criptovalute fa salire il prezzo delle GPU*, DDay, Url: "https://www.dday.it/redazione/25507/nvidia-chi-vuole-arricchirsi-coi-bitcoin-fa-salire-il-prezzo-delle-gpu", ultima data consultazione 16 giugno 2018.

Bitaddress.org, Url: "www.bitaddress.org", ultima data consultazione 16 giugno 2018.

Bitcoin Wiki, Url: "https://en.bitcoin.it/wiki/Protocol_documentation#Hashes", ultima data consultazione 16 giugno 2018.

Bitcoin Wiki, Url: "https://en.bitcoin.it/wiki/Units#cite_note-4", ultima data consultazione 16 giugno 2018.

Bitcoin Wiki, Url: "https://it.bitcoinwiki.org/wiki/Storia_di_Bitcoin", ultima data consultazione 16 giugno 2018.

Bitcoin.org, Url: "https://bitcoin.org/en/glossary/merkle-root", ultima data consultazione 16 giugno 2018.

Bitcoin.org, Url: "https://bitcoin.org/it/", ultima data consultazione 16 giugno 2018.

Bitcoin.org, Url: "https://bitcoin.org/it", ultima data consultazione 16 giugno 2018.

Bitcoinfees, Url: "https://bitcoinfees.earn.com/", ultima data consultazione 16 giugno 2018.

Blockchain.info, Url: "https://blockchain.info/", ultima data consultazione 16 giugno 2018.

Blockchain.info, Url: "https://blockchain.info/it/charts/", ultima data consultazione 16 giugno 2018.

Blockchain.info, Url: "https://blockchain.info/it/charts/hash-rate?timespan=all", ultima data consultazione 16 giugno 2018.

Blockchain.info, Url: "https://blockchain.info/it/pools", ultima data consultazione 16 giugno 2018.

Blockchain4innovation.it, Url: "https://www.blockchain4innovation.it/", ultima data consultazione 16 giugno 2018.

Borsa Inside, (7 febbraio 2018), Url: "https://www.borsainside.com/criptovalute/67342-ripple-e-stellar-oggi-rimbalzano-previsioni-positive-su-quotazioni-2018-grazie-alle-grandi-aziende/", ultima data consultazione 16 giugno 2018.

Buybitcoinworldwide.com, Url: "https://www.buybitcoinworldwide.com/it/indice-di-volatilita/", ultima data consultazione 16 giugno 2018.

Coindesk.com, Url: "https://www.coindesk.com/information/how-to-use-ethereum/", ultima data consultazione 16 giugno 2018.

Coingecko.com, Url: "https://www.coingecko.com/en", ultima data consultazione 16 giugno 2018.

Coingecko.com, Url: "https://www.coingecko.com/it/grafici_del_prezzo/bitcoin/usd", ultima data consultazione 16 giugno 2018.

Coinlist, Url: "https://coinlist.me/it/calendario-ico", ultima data consultazione 16 giugno 2018.

Coinmap.org, Url: "www.coinmap.org", ultima data consultazione 16 giugno 2018.

Coinmarketcap, Url: "https://coinmarketcap.com/", ultima data consultazione 16 giugno 2018.

Coinmarketcap.com, Url: "https://coinmarketcap.com/currencies/bitcoin/#charts", ultima data consultazione 16 giugno 2018.

Coinmarketcap.com, Url: "https://coinmarketcap.com/currencies/ethereum/#chart", ultima data consultazione 16 giugno 2018.

Coinmarketcap.com, Url: "https://coinmarketcap.com/currencies/iota/#chart", ultima data consultazione 16 giugno 2018.

Coinmarketcap.com, Url: "https://coinmarketcap.com/currencies/ripple/#chart", ultima data consultazione 16 giugno 2018.

Coinmarketcap.com, Url: "https://coinmarketcap.com/currencies/stellar/#chart", ultima data consultazione 16 giugno 2018.

Coinmetrics.io, Url: https://coinmetrics.io/charts/#assets=btc, ultima data consultazione 16 giugno 2018.

Corriere Comunicazioni, (15 marzo 2018), *Bitcoin, l'Fmi spinge per la regolazione: "Garantire stabilità finanziaria"*, Url: "https://www.corrierecomunicazioni.it/finance/bitcoin-lfmi-spinge-per-la-regolazione-garantire-stabilita-finanziaria/", ultima data consultazione 16 giugno 2018.

Corriere della Sera, (4 ottobre 2013), *Chiuso Silk Road, il mercato online delle drogh*e, Url: "http://www.corriere.it/tecnologia/13_ottobre_02/chiuso-silk-road-ebay-droghe-df97b220-2b8c-11e3-93f8-300eb3d838ac.shtml", ultima data consultazione 16 giugno 2018.

Corriere della Sera, (settembre 2008), *Lehman Brothers dichiara fallimento*, Url: "http://www.corriere.it/economia/08_settembre_15/lehman_brothers_banca_crisi_credito_Usa_b8805f84-82b3-11dd-9b8b-00144f02aabc.shtml", ultima data consultazione 16 giugno 2018.

Cryptocompare.com, Url: "http://www.cryptocompare.com/", ultima data consultazione 16 giugno 2018.

De Agostini, M., (17 agosto 2017), *Prezzi schede video alle stelle, sta per piovere sul bagnato*, tom's Hardware, Url: "https://www.tomshw.it/prezzi-schede-video-alle-stelle-sta-piovere-bagnato-87643", ultima data consultazione 16 giugno 2018.

Dizionario Cambridge, Url:

"https://dictionary.cambridge.org/it/dizionario/inglese/gamer", ultima data

consultazione 16 giugno 2018.

Dizionario Economico.com, Url: "http://dizionarioeconomico.com/analisi-swot", ultima data consultazione 16 giugno 2018.

Dizionario Garzanti, Url: "https://www.garzantilinguistica.it/ricerca/?q=peer-to-peer", ultima data consultazione 16 giugno 2018.

Dizionario Garzanti, Url: "https://www.garzantilinguistica.it/ricerca/?q=framework", ultima data consultazione 16 giugno 2018.

Dizionario Treccani, Url: "http://www.treccani.it/enciclopedia/crittografia/", ultima data consultazione 16 giugno 2018.

Dizionario Treccani, Url: "http://www.treccani.it/enciclopedia/open-source/", ultima data consultazione 16 giugno 2018.

Dizionario Treccani, Url: "http://www.treccani.it/enciclopedia/peer-to-peer/", ultima data consultazione 16 giugno 2018.

Dizionario Treccani, Url: "http://www.treccani.it/enciclopedia/sir-thomas-gresham_%28Enciclopedia-Italiana%29/", ultima data consultazione 16 giugno 2018.

Dizionario Treccani, Url: "http://www.treccani.it/vocabolario/criptovaluta_%28Neologismi%29/", ultima data consultazione 16 giugno 2018.

Ethereum.org, Url: "https://ethereum.org/", ultima data consultazione 16 giugno 2018.

Fastweb, (13 gennaio 2018), *Truffe e furti Bitcoin, breve storia*, Url: "http://www.fastweb.it/web-e-digital/truffe-furti-bitcoin", ultima data consultazione 16 giugno 2018.

Fastweb, (13 gennaio 2018), *Truffe e furti Bitcoin, breve storia*, Url: "https://it.businessinsider.com/un-maxifurto-da-500-milioni-di-dollari-in-criptovalute-innesca-la-grande-fuga-da-bitcoin-co/", ultima data consultazione 16 giugno 2018.

Fastweb, (13 gennaio 2018), *Truffe e furti Bitcoin, breve storia*, Url: "http://www.fastweb.it/web-e-digital/truffe-furti-bitcoin/", ultima data consultazione 16 giugno 2018.

Fastweb, (28 gennaio 2017), *Cos'è IOTA, l'alternativa alla blockchain per l'IoT* , Url: "http://www.fastweb.it/web-e-digital/cose-iota-alternativa-blockchain/", ultima data consultazione 16 giugno 2018.

Fastweb, (29 dicembre 2017), *Non solo Bitcoin, le altcoin alternative*, Url: "http://www.fastweb.it/web-e-digital/da-litecoin-a-sexcoin-le-alternative-a-bitcoin/", ultima data consultazione 16 giugno 2018.

Fastweb, "http://www.fastweb.it/internet/cosa-e-come-funziona-p2p/", ultima data consultazione 16 giugno 2018.

Fastweb, "http://www.fastweb.it/web-e-digital/internet-of-things-quali-linguaggi-di-programmazione-imparare/", ultima data consultazione 16 giugno 2018.

Gold.org, Url: "www.gold.org", ultima data consultazione 16 giugno 2018.

Griffith, K., (16 aprile 2014), *A Quick History of Cryptocurrencies BBTC — Before Bitcoin*, Bitcoin Magazine, Url: "https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/", ultima data consultazione 16 giugno 2018.

HDBlog.com, Url: "https://www.hdblog.it/2017/02/24/Google-rompe-per-la-prima-volta-lalgoritmo-di-hashing-SHA-1/", ultima data consultazione 16 giugno 2018.

IBM.com, Url: "https://www-03.ibm.com/press/us/en/pressrelease/53290.wss", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE – Nòva, (3 maggio 2015), *Criptovalute tra opportunità e voglia di regolamentazione*, Url: "http://nova.ilsole24ore.com/frontiere/criptovalute-tra-opportunita-e-richieste-di-regolamentazione/", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, (16 gennaio 2018), La Cina studia la stretta, Bitcoin in picchiata sotto 12mila dollari, Url: "http://www.ilsole24ore.com/art/finanza-e-mercati/2018-01-16/-bitcoin-scivolone-sotto-quota-12mila-dollari-103336_PRV.shtml?uuid=AE47RVjD", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, (21 aprile 2018), Url: "http://argomenti.ilsole24ore.com/parolechiave/criptovaluta.php", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, (31 gennaio 2018), *Criptovalute e bolle, Padoan: «Le banche centrali si stanno attrezzando, il sistema va regolato»*, Url: "http://www.ilsole24ore.com/art/notizie/2018-01-31/criptovalute-e-bolle-padoan-le-banche-centrali-si-stanno-attrezzando-sistema-va-regolato-165542.shtml?uuid=AEJiUEsD", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, "http://www.ilsole24ore.com/art/tecnologie/2018-03-08/con-cosa-si-comprano-bitcoin-201343.shtml?uuid=AEYBUuDE", ultima data consultazione 16 giugno 2018.

Il Sole 24 ORE, Url: "http://finanzamercati.ilsole24ore.com/quotazioni.php?QUOTE=!EURUS.FX", ultima data consultazione 16 giugno 2018.

Investing.com, Url: "https://it.investing.com/crypto/", ultima data consultazione 16 giugno 2018.

Iota.org, Url: "https://iota.org/", ultima data consultazione 16 giugno 2018.

Iota.org, Url: "https://www.iota.org/", ultima data consultazione 16 giugno 2018.

Iotaitalia.com, Url: "https://www.iotaitalia.com/about/", ultima data consultazione 16 giugno 2018.

La Repubblica, (13 febbraio 2018), *Draghi sul Bitcoin: "Attenzione, ma non spetta alla Bce bloccarlo*, Url: "http://www.repubblica.it/economia/2018/02/13/news/bce_askdraghi_bitcoin_crisi-188765722/", ultima data consultazione 16 giugno 2018.

Lamiaprivacy.wordpress.com, Url: "https://lamiaprivacy.wordpress.com/2015/03/07/capire_le_basi_della_crittografia/", ultima data consultazione 16 giugno 2018.

Lecriptovalute.org, Url: "https://www.lecriptovalute.org/2018/01/19/proof-of-work-significato-cos-e-pow-e-il-proof-of-stake-guida/", ultima data consultazione 16 giugno 2018.

Milano Finanza, Url: "https://www.milanofinanza.it/valuta/cambio-euro-dollaro", ultima data consultazione 16 giugno 2018.

Nicehash.com, Url: "http://www.nicehash.com", ultima data consultazione 16 giugno 2018.

Opencoin.org, Url: "https://opencoin.org/Members/jhb/opencoin-and-ripple", ultima data consultazione 16 giugno 2018.Ragazziweb.com, Url: "http://www.ragazzieweb.it/?q=node/41", ultima data consultazione 16 giugno 2018.

Righto.com, Url: "http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html", ultima data consultazione 16 giugno 2018.

Ripple.com, Url: "https://ripple.com/use-cases/corporates/", ultima data consultazione 16 giugno 2018.

Stellar.org, Url: "https://www.stellar.org/about/mandate/#Held_by_Foundation", ultima data consultazione 16 giugno 2018.

Stellar.org, Url: "https://www.stellar.org/about/mandate/", ultima data consultazione 16 giugno 2018.

Stirpe.com: Url: "https://stripe.com/it", ultima data consultazione 16 giugno 2018.

The Nilson Report, Url: "https://nilsonreport.com/index.php", ultima data consultazione 16 giugno 2018.

Tokendata.io, Url: "https://www.tokendata.io/", ultima data consultazione 16 giugno 2018.
Unisa.it, Url: "http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0304/GnuPG/Gnupg.htm", ultima data consultazione 16 giugno 2018.

Valutevirtuali.com, Url: "http://valutevirtuali.com/criptovalute-principali-performance-ed-andamento-prezzo/", ultima data consultazione 16 giugno 2018.

Wikipedia, Url: "https://it.wikipedia.org/wiki/M-Pesa", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://en.wikipedia.org/wiki/Thiel_Fellowship", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Analisi_SWOT", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Gateway_(informatica)", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Macchina_virtuale", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Problema_dei_generali_bizantini", ultima data consultazione 16 giugno 2018.

Wikipedia.org, Url: "https://it.wikipedia.org/wiki/Volatilit%C3%A0_(economia)", ultima data consultazione 16 giugno 2018.

Wired, (22 aprile 2014), *Il creatore di bitcoin è Nick Szabo?*, Url: "https://www.wired.it/attualita/tech/2014/04/22/bitcoin-creatore-nick-szabo/", ultima data consultazione 16 giugno 2018.

Wired, (22 aprile 2014), *Il creatore di bitcoin è Nick Szabo?, Url:* "https://www.wired.it/attualita/tech/2014/04/22/bitcoin-creatore-nick-szabo/", ultima data consultazione 16 giugno 2018.

Worldbank.org, Url: "hhttps://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=NO", ultima data consultazione 16 giugno 2018.

Worldbank.org, Url: "https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=DK", ultima data consultazione 16 giugno 2018.