Dipartimento di Impresa e Management

Cattedra Finanza Aziendale corso avanzato

FINANZA 3.0

La Finanza decentralizzata – Blockchain & Cryptocurrencies

RELATORE

PROF. LUIGI GUBITOSI

CANDIDATO

JACOPO DE SANTIS

MATR. 684291

CORRELATORE

PROF. BRUNO RICCARDO

ANNO ACCADEMICO 2017/2018

"Never invest in a business you cannot understand."

-Warren Buffett-

INTRODUZIONE

Il titolo "Finanza 3.0" deriva da una personale classificazione del comparto finanziario sulla base di eventi che più di altri lo hanno rivoluzionato, decretandone di fatto un cambio di paradigma.

Il primo evento lo identifico con l'affermazione della Borsa valori avvenuta nella seconda metà dell'ottocento, spinta dalla seconda rivoluzione industriale.

I progressi nelle comunicazioni e l'uso dell'elettricità consentirono la conoscenza simultanea dei prezzi di Borsa, il che comportò l'incremento del numero degli investitori e l'espansione del mercato finanziario.

Un secondo fondamentale passaggio riguarda la creazione di prodotti e contratti finanziari "atipici" ed innovativi, in particolare gli strumenti derivati.

Ad oggi il mercato finanziario capitalizza circa 780 trilioni di dollari, e di questi, circa il 65 % è rappresentato dai derivati, con un valore stimato di circa 500 trilioni di dollari. Questo peso ha ampi effetti sull'economia, si pensi ad esempio al caso dei derivati, di natura obbligazionaria, creati dalla cartolarizzazione dei mutui subprime durante la crisi del 2008 negli USA.

Il terzo momento è ancora in divenire, ed è rappresentato dai recenti sviluppi della finanza relativamente al concetto di sistema decentralizzato.

Questo nuovo paradigma finanziario ha trovato nell'informatica un driver di sviluppo oltre che un partner fondamentale, infatti con la creazione di nuovi protocolli informatici come la blockchain, specificatamente dedicati al comparto finanziario, sono stati realizzati modelli di elaborazione delle transazioni basati su sistemi decentralizzati, si pensi in tal caso alle criptovalute come il Bitcoin.

Il lavoro, strutturato in modo deduttivo, all'interno di quattro capitoli, espone tematiche collegate ed incrementali.

La trattazione, nel primo capitolo, affronta un'analisi storica della moneta, esponendo le principali caratteristiche nella sua accezione tradizionale. Il secondo, invece, illustra approfonditamente la tecnologia blockchain, il suo funzionamento, l'estensione al campo finanziario e i diversi utilizzi, evidenziandone pregi e difetti. Gli ultimi due capitoli sono focalizzati sull'intero mondo delle crittovalute, fornendo, in prima battuta, un quadro completo del sistema Bitcoin, e successivamente conducendo un'analisi trasversale sulle principali criptomonete, le relative caratteristiche e le loro applicazioni nel sistema finanziario.

Il seguente elaborato persegue due distinte finalità. In primo luogo, fornire una visione d'insieme dell'intero comparto delle criptovalute, congiuntamente alla tecnologia che ne regola il funzionamento.

Il secondo fine, invece, è quello di analizzare l'intero sistema crypto da diversi punti di vista, con un focus particolare sui principali punti di forza e le debolezze di un mondo in continua evoluzione, cercando di coglierne rischi ed opportunità future.

CAP I - LA MONTETA TRADIZIONALE

1.1 Nascita e fasi principali (dal Gold Standard alla moneta fiduciaria)

Identificare la moneta come un'invenzione implica commettere un grande errore. Essa, invece, rappresenta il risultato di un processo evolutivo che, in momenti diversi, abbraccia i vari mezzi di scambio susseguitisi nella storia.

Nell'antichità le relazioni commerciali si realizzavano mediante l'archetipo dei protocolli di scambio e commercio: il baratto.

Quest'ultimo consiste nello scambio di beni e servizi, subordinato ad una condizione di vantaggio reciproco, ma questa non è l'unica condizione necessaria.

Di fondamentale importanza, infatti, è in questo contesto la convergenza e la coincidenza dei bisogni, condizioni fondamentali per la realizzazione dello scambio.

All'interno del suddetto protocollo di scambio, primordiale, si susseguirono due modalità di pagamento che gli studiosi identificarono come pre-moneta.

La prima fu la cosiddetta "moneta naturale", rappresentata dalla mercanzia, che in condizioni di sovrabbondanza, veniva utilizzata per regolare gli scambi. Mentre il secondo esempio di pre-moneta è rappresentato dalla moneta utensile. Questa tipologia di mezzo di pagamento si affermò dal IX secolo a.C. e comprendeva strumenti ed oggetti sia di uso quotidiano, sia di lavoro, che venivano impiegati nello scambio, pur mantenendo la propria funzione originaria.

Affiancato alle pre-monete, c'è un filone di pensiero, storicamente confermato che identifica come elemento fondante delle prime economie non tanto il baratto, quanto il debito[1].

In Mesopotamia, infatti, i Sumeri, conoscendo la scrittura, incidevano su tavole di argilla i debiti esistenti tra i vari soggetti, commisurandoli con un determinato quantitativo di mercanzia.

Nasce in questo modo la problematica relativa agli scambi differiti nel tempo, basando quindi l'interazione economica sui rapporti sociali e la fiducia reciproca, elementi invece esterni nel baratto.

Ben presto le due tipologie di pre-moneta divennero obsolete a causa della difficoltà di regolamento degli scambi aventi ad oggetto ingenti quantità, si passo quindi all'utilizzo di metalli, i quali venivano marcati per assolvere una funzione di garanzia del valore, anche se realizzata da privati.

I primi esempi dell'utilizzo della moneta metallica si ebbero, in primis in Lidia attorno al 500 a.C., e precedentemente in oriente, nello specifico in Cina, nel 1200 a.C.

A differenza dei precursori cinesi, per i greci, persiani e infine i romani, la scelta ricadde sui metalli preziosi, portando quindi la moneta ad avere un valore intrinseco.

[1] David Graeber, "*Il Debito*", Il Saggiatore, 2012

Sotto l'impero romano di Augusto la moneta preminente fu rappresentata dall'oro, affiancato da quelle in argento, aventi proprio corso legale.
In questo sistema, risulta chiaro come il valore delle monete fosse agganciato indiscutibilmente alla grande presenza di metallo fruibile per la coniazione. Tale relazione portò nel tempo al fenomeno dell'inflazione strisciante, che intaccò il valore delle monete riducendolo[2].
Questo fenomeno venne contrastato con la riduzione della quantità di metallo prezioso presente nelle monete; tale processo, in un'ottica storia, è uno dei primi esempi di signoraggio, messo in atto dalle zecche imperiali.
Con il trascorrere dei secoli il sistema monetario subì molte evoluzioni dovute ad eventi come la scoperta di ingenti giacimenti di argento, che porto il sistema a convergere verso il bimetallismo.
Così fu in Europa fino al 1661, quando le monete metalliche furono sostituite dall'emissione di banconote realizzata dalla Svezia, mentre il più antico utilizzo di banconote si attribuisce alla Cina nel 800 d.C., dove il processo si arrestò in breve tempo a causa della spirale inflazionistica dovuta all'eccessiva emissione.
Questi effetti si replicarono in tutta l'Europa in cui l'emissione di monete avveniva senza che il loro valore fosse agganciato ad un bene rifugio, come ad esempio l'oro.
Le riserve auree infatti rappresentarono la base e il parametro di emissione solo nel 1816 in Inghilterra, dove l'unità di conto era rappresentata dalla sterlina d'oro, definita come 113,0016 grammi di oro puro.
La legge istitutrice del regime aureo definiva tre condizioni:[3]

- La zecca reale era obbligata a comprare o vendere quantità illimitate di oro a prezzo fissato;
- Non era ammesso nessun freno o limitazione all'importazione e all'esportazione di oro;
- La banca d'Inghilterra era tenuta a convertire, ove sia richiesto, banconote e depositi in oro.

Le quantità d'oro detenute da quest'ultima determinavano la quantità di credito che poteva essere concessa sotto forma di depositi o banconote, questi a loro volta incidevano sulla capacità di concessione del credito da parte delle banche.
Perciò, guardando alla bilancia dei pagamenti, le movimentazioni in entrata e uscita di oro per ogni paese determinarono scostamenti nel valore delle riserve monetarie, impattando direttamente sui prezzi delle monete. Infatti, ingenti flussi in entrata di oro avrebbero causato una spirale inflazionistica, mentre grandi prelevamenti avrebbero portato a un panico monetario.
Il regime aureo puro, alfine di controllare l'inflazione dei prezzi, sarebbe stato dominante nello scenario internazionale dal 1870 al 1914, infatti nel 1900, negli Stati Uniti, fu promulgata la legge Gold Standard, la quale tra l'altro porto alla costituzione della banca centrale (Federal Reserve Act, 1913)

---

[2] Roland Nitsche, "*Alla scoperta della Moneta*", 1970, Rizzoli editore.

[3] "*I sistemi monetari dal Gold Standard all'età contemporanea*" – URL: http://old.unipr.it/arpa/facecon/StoriaEc/11-Moneta_contemporanea.htm

All'interno di questo regime monetario, il sistema di cambi ancorato alle riserve auree, in cui ogni moneta aveva una parità metallica fissa, determinava un meccanismo di aggiustamento automatico, che risultava in un regime a cambi fissi fra le diverse divise nazionali.

Nel corso del primo conflitto mondiale il Gold Standard fu sospeso per diverse motivazioni. In primis a causa dell'impatto che la guerra ha avuto sui flussi commerciali e finanziari, ma anche per l'impossibilità, per molte nazioni, di dimostrare la conformità e la corrispondenza delle riserve auree in relazione all'ingente quantità di banconote emesse per sostenere le spese belliche. Un altro fattore che portò alla crisi del sistema Gold Standard, indiscutibilmente, fu la scarsità dell'oro, che non poteva dunque soddisfare le esigenze dei vari sistemi economici.

Per questi motivi, verificatisi a cavallo tra le due guerre mondiali, si optò per il Gold Exchange Standard, un regime monetario aureo che rappresentava però una variante del Gold Standard.

Nei paesi che lo adottarono la valuta nazionale non era più convertibile in oro, ma bensì in valuta estera (il dollaro) a sua volta convertibile in oro.

Questo regime consentiva infatti l'accumulazione di riserve anche in divise estere e non solo in oro, con la finalità di ridurre la pressione su quest'ultimo.

Molti economisti, successivamente alla prima Guerra mondiale e alla Grande Depressione, riscontravano nel regime Gold Standard molte inefficienze, come l'impossibilità per gli stati di espandere l'offerta di moneta per sostenere la ripresa economica a causa dell'obbligo di corrispondenza tra riserve di oro e banconote emesse.

Al fine di risolvere l'instabilità valutaria di quel contesto, nel 1944 avvenne la stipula dell'accordo internazionale di Bretton Woods, che sanciva il passaggio al Gold Exchange Standard.

In questo regime, come detto prima, venivano definite parità fisse tra le valute dei vari paesi, il valore di ogni valuta infatti era agganciata al dollaro americano, l'unico che poteva essere convertito in oro, con un rapporto di conversione fissato a 35 dollari l'oncia.

Con gli accordi di Bretton Woods, in modo indiscutibile, il dollaro veniva posto come l'ago della bilancia dell'intera economia internazionale. Tale convenzione comportò una forte pressione sulla moneta statunitense, che unitamente alle spese sostenute dagli USA per il conflitto in Vietnam, determinarono un clima di sfiducia nei confronti del dollaro, che portò molte banche centrali a convertirne le proprie riserve in oro.

La situazione per la moneta americana divenne insostenibile fino a che nell'Agosto del 1971, l'allora presidente Richard Nixon, decretò l'inconvertibilità del dollaro in oro, portando alla fine del sistema a cambi fissi.

Questo importante passaggio ha condotto all'introduzione delle monete fiat, ossia strumenti di pagamento non coperti da beni come le riserve auree, e quindi prive di valore intrinseco.

In questo contesto gioca un ruolo fondamentale la fiducia che ogni singolo individuo ha nelle istituzioni, infatti i garanti del valore delle monete fiat sono il governo e la banca centrale emittente, e il loro utilizzo è regolato e garantito dalla legge.

Si parla in questo contesto di sistema monetario fiduciario proprio perché ogni individuo accetterà moneta fiat in cambio di beni e servizi sulla base della fiducia che essa sarà successivamente accettata nelle transazioni future.
Aspetto curioso e fondamentale è che proprio la fiducia caratterizza e lega il sistema monetario tradizionale con le valute alternative, frutto di importanti avanzamenti tecnologici, come le criptovalute.

1.2 Le Funzioni della moneta

1.2.1 Mezzo di scambio e pagamento

Nell'attuale sistema monetario, come descritto nella precedente sezione, la moneta viene definita fiat, per la necessità di fiducia come elemento fondante del sistema.
La moneta fiat viene anche definita come uno strumento di pagamento avente corso legale, ossia in un territorio ogni individuo è tenuto ad accettarla per l'adempimento di un debito (potere liberatorio).
La prima funzione attribuita alla moneta[4] è quella di intermediario degli scambi e mezzo di pagamento.
La moneta infatti è un'attività accettata da ogni venditore di beni e servizi, con la consapevolezza che essa sarà riaccettata a sua volta in uno scambio futuro.
La funzione di intermediario degli scambi, permette il superamento di tutte le problematiche relative al baratto, come la coincidenza dei bisogni e gli elevati costi di transazione associati ad uno scambio. Come mezzo di pagamento, invece, la moneta permette l'adempimento dei debiti.
Questo potere è garantito dalla legge o da una convenzione sociale di equivalente forza.

1.2.2 Unità di conto

La seconda fondamentale funzione della moneta è quella di unità di conto, cioè uno strumento numerario.
Questo si traduce nella capacità di misurare costi e ricavi, di quantificare crediti e debiti, e quindi agevola lo scambio di beni e servizi rendendoli direttamente comparabili e commensurabili tra loro.
Non è comunque detto che una singola moneta svolga da sola entrambe le funzioni, sia di unità di conto sia di intermediario degli scambi, nel caso in cui questo non avvenisse si parlerebbe di moneta parziale.
Questo fu il caso dell'Euro, nel periodo della sua introduzione tra il 1999 e il 2002, in cui aveva la funzione di unità di conto, ma non di intermediario degli scambi nelle transazioni al dettaglio.

[4] Paesani P., "*Lezioni di Economia*", 2012, Giappichelli editore, Torino

1.2.3 Riserva di valore

La capacità di costituire una riserva di valore rappresenta la terza funzione della moneta.
Tale funzione si riferisce alla caratteristica di mantenimento del potere d'acquisto nel tempo, chiaramente in relazione al tasso di inflazione, che riflette l'andamento generale dei prezzi.
Di fatto, la funzione di riserva di valore pone la moneta in concorrenza con le attività finanziarie, quali titoli azionari e obbligazionari di varia scadenza, e con le attività reali come beni immobili, opere d'arte e beni rifugio come l'oro. A differenza però delle attività finanziarie e quelle reali, la moneta ha il maggior grado di liquidità, concetto che si traduce nell'attitudine di un asset a trasformarsi rapidamente in potere di acquisto, senza il sostenimento di eccessivi costi.
La moneta infatti, rispetto alle altre attività finanziarie si posiziona quasi nel punto di origine guardando la curva di Tobin (rischio / rendimento), essa ha come rischio implicito il tasso di inflazione, mentre come rendimento implicito la deflazione, ossia la crescita del potere di acquisto della moneta nel tempo, entrambi solitamente prossimi allo zero.

1.3 La centralizzazione del Potere (il Sistema Monetario Europeo)

All'interno del sistema monetario un ruolo preminente spetta al potere pubblico, il quale gioca un ruolo fondamentale in termini di garanzia e funzionamento del sistema stesso.
Assolvendo efficientemente queste funzioni, risulta un divieto per i cittadini, residenti nello Stato in cui la moneta è emessa, di rifiutarla per l'estinzione di un'obbligazione di tipo pecuniario.
Nel continente europeo, ogni decisione di politica economica e nello specifico monetaria spettava ai singoli Stati, i quali detenevano la sovranità di ogni provvedimento in termini di:

- Autorizzazione nell'emissione di banconote all'interno del territorio nazionale.
- Determinare il potere comparativo della propria moneta in relazione alle divise estere (tasso di sconto e politiche di cambio).
- Determinare il tasso di interesse guida, che influenza la capacità di concessione del credito da parte del sistema bancario.

Tali poteri, esclusivi degli Stati, nel tempo vennero meno con l'entrata in vigore nel 1979 dei Sistema Monetario Europeo.
L'accordo, sottoscritto dai membri dell'allora Comunità Europea (1957), imponeva il mantenimento di una parità di cambio prefissata fra le valute all'interno di un intervallo stabilito (± 2,25%).

I governi, le cui valute si discostavano da tale intervallo, avevano l'obbligo di intervenire con strumenti di politica monetaria al fine di ristabilire l'equilibrio.
Con l'Atto Unico Europeo del 1986 veniva predisponeva la libertà di movimento di merci, servizi, persone e capitali; condizioni che rappresentavano la premessa all' Unione Economica e Monetaria.
Il passaggio da premessa a realtà si realizzo il 1° dicembre 1993, anno in cui entrò in vigore il Trattato di Maastricht (Trattato sull'Unione Europea) che istituisce l'Unione politica e detta le linee guida dell'eurosistema.
Obbiettivi del Trattato sono la crescita sostenibile, il rispetto dell'ambiente e la stabilità monetaria, in termini di un valore obbiettivo dell'inflazione intorno al 2%. Gli obbiettivi sarebbero stati raggiunti con due mezzi, il mercato comune e l'Unione economico-monetaria.
Negli anni 1999-2000 l'euro è entrato in vigore in modo virtuale (unità di conto europea) sotto forma di applicazione dei cambi fissi irrevocabili tra le monete e tra queste e l'euro.
Questo passaggio segnò la fine della sovranità monetaria e l'adozione di politiche monetarie individuali per gli Stati dell'euro zona.
Infatti, dal 1° gennaio 2002, con l'immissione in circolazione dell'euro, le competenze in materia monetaria sono state traslate dai singoli Stati verso gli organi comunitari. Nello specifico, la BCE ha il diritto esclusivo nell'autorizzare l'emissione di banconote, fornisce parere al Sistema Europeo delle Banche Centrali sulla definizione dei tassi di interesse guida, e viene impedito agli stati, con l'introduzione della moneta unica, di modificare il potere comparativo della propria moneta. Spetta pertanto agli organi comunitari di indicare il rapporto di cambio con le altre valute.

1.4 Monete alternative: Moneta elettronica e valute virtuali

Per condurre un accurato confronto, l'analisi deve partire definendo le varie tipologie di moneta.
All'interno dei sistemi economici attuali esistono principalmente due tipi di moneta:

- La moneta legale, ossia banconote e monete metalliche
- La moneta bancaria, rappresentata dai depositi bancari

Dall'unione delle due tipologie risulta l'offerta di moneta (M), proprio come risultante della somma tra circolante e depositi bancari.
Sulla base della definizione fornita dalla BCE la moneta può essere definita utilizzando il concetto di aggregati monetari. Essi rappresentano grandezze stock e sono indicati con sigle alfanumeriche.
Il primo aggregato, definito come M1, comprende le banconote, le monete metalliche e i depositi a vista.
L'aggregato M2, invece, comprende sia M1, ed aggiunge a quest'ultimo i depositi con durata prestabilita fino a due anni e quelli rimborsabili con un preavviso di 3 mesi.

Il terzo, M3, include oltre a M2, anche i titoli di debito con scadenza fino a due anni, le partecipazioni in fondi comuni monetari e gli strumenti pronti contro termine.
Mentre, prende il nome di base monetaria, la somma del valore delle banconote, monete metalliche e il valore delle riserve liquide tenute dalle banche centrali presso la BCE.
Importante anche sottolineare che ci si riferisce soltanto a moneta metallica e cartamoneta quando si parla di moneta avente corso legale; a differenza della moneta documentale, come assegni o carte di pagamento, che possono essere rifiutate dal creditore al di sotto di alcuni importi, non avendo corso legale.
Passando al confronto tra valute elettroniche e digitali, si riscontra spesso una generale confusione tra le due tipologie, nonostante tra i due metodi di pagamento intercorrano delle differenze sostanziali.
In relazione alle monete elettroniche possono essere individuati due tipi:

- Monete elettroniche card based
- Monete elettroniche software based

Nella prima tipologia le disponibilità liquide vengono registrate dal microchip presente sulla carta, mentre nel secondo caso sono registrate su un file in locale fruibile online. Tra i sistemi di pagamento elettronici più noti rientrano i bonifici bancari, i pagamenti con carte di credito, debito e i pagamenti online.
Per completare l'analisi, esaminando le valute virtuali, bisogna riconoscere come esse siano il frutto di un costante avanzamento tecnologico nel campo dell'Information & Communication Technology e nell'e-payment.
Il D.Lgs. 25 maggio 2017, n. 90 da una definizione di "valuta virtuale", disponendo che la stessa debba intendersi come un "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, negoziata e archiviata elettronicamente".
Una definizione che non lascia alcun'ombra di dubbio e che dovrebbe far comprendere una volta per tutte, la sostanziale differenza con la moneta elettronica, quest'ultima descritta dal TUB (Testo Unico Bancario) come "il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento; e che sia accettato da persone fisiche e giuridiche diverse dall'emittente".
In relazione alle valute virtuali viene altresì precisato cosa siano, e quali attività svolgano, i prestatori di servizi relativi all'utilizzo di valuta virtuale, ossia "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".
Il collegamento tra la moneta elettronica e quelle tradizionali ha una base giuridica, con una domanda e un'offerta ancora controllate dalla banca centrale; inoltre l'unità di conto è la stessa.
Le valute virtuali, invece, sono collegate al denaro reale attraverso un tasso di cambio, finendo con l'essere esposte alle fluttuazioni dello stesso.

Le fluttuazioni sono amplificate dal fatto che l'offerta di moneta si trova nelle mani di istituzioni non finanziarie e addirittura decentrate. Se ne deduce che i sistemi di moneta elettronica e moneta virtuale affrontano diversi tipi di rischi, maggiori negli ultimi, soprattutto a causa dell'assenza di regolamentazione. I regimi di valute virtuali sono una forma di sistema di pagamento al dettaglio. E ne mostrano tutte le caratteristiche. Fra le valute virtuali sono ricomprese le cosiddette "criptovalute", tra cui il Bitcoin, conosciuto con la sigla BTC.

Per effettuare una classificazione delle valute virtuali verrà richiamata la relazione del 2012 della BCE dal titolo "Modelli di moneta virtuale". Si parla di valute digitali in termini di schemi o di sistemi.

Un sistema di moneta virtuale analizza come una particolare moneta virtuale interagisca all'interno della comunità a cui appartiene, e, nell'economia reale, grazie al suo specifico sistema di pagamento al dettaglio (BCE 2012). In questo modo, possono essere identificati tre diversi tipi di valute virtuali come mostrato nella Figura 1.

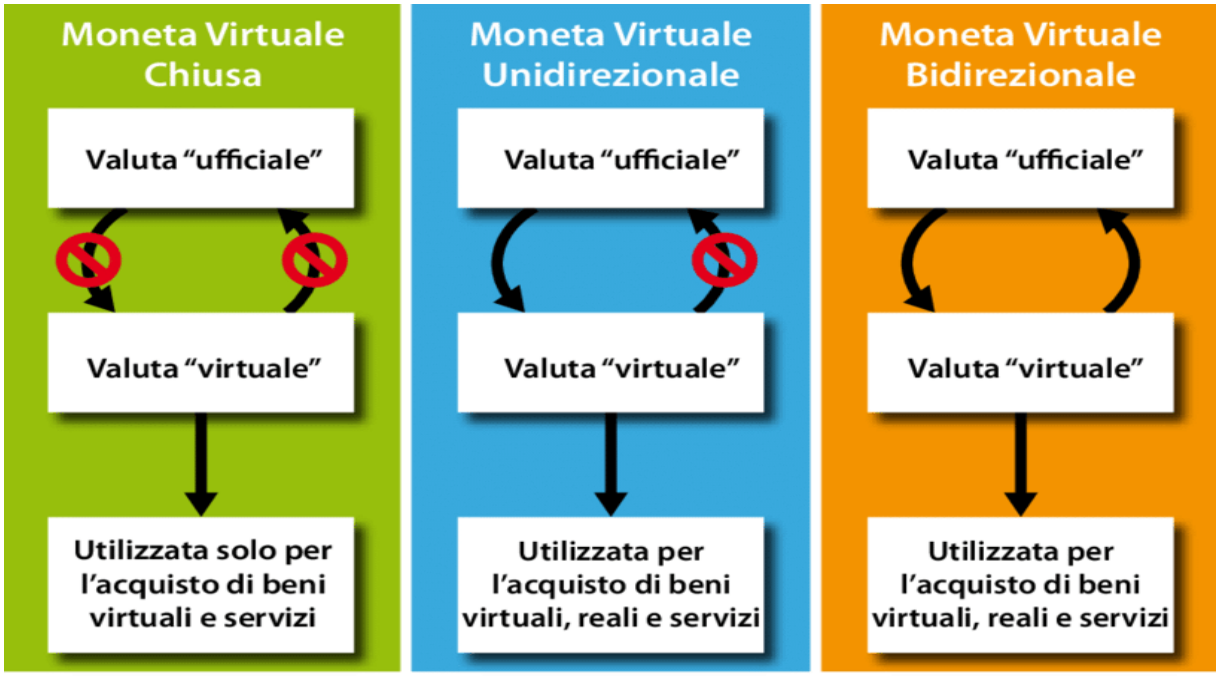


Figura 1 - I tre tipi di moneta virtuale (Fonte BCE 2012)

1. Sistemi di valuta virtuale chiusi: non c'è un collegamento tra la moneta digitale e l'economia reale. Appartengono a questo tipo schema le valute dei giochi online. I giocatori pagando un canone di abbonamento, ottengono la moneta virtuale, eseguendo missioni all'interno del gioco. La valuta guadagnata ha valore solo all'interno della comunità virtuale di riferimento.

2. Schemi di moneta virtuale con flusso unidirezionale: la moneta virtuale può essere acquistata mediante denaro reale ad un certo tasso di cambio. Lo scambio inverso non è consentito. La moneta digitale ottenuta, può essere utilizzata per comprare beni e servizi offerti da specifiche comunità virtuali che accettano tale

moneta come forma di pagamento. In alcuni di questi schemi è anche possibile acquistare beni reali con la moneta virtuale. Un esempio di questo schema è quello di Facebook credits.

3. Schemi di moneta virtuale con flusso bidirezionale: la moneta virtuale può essere scambiata con quelle reali e viceversa. L'uso della moneta virtuale nel mondo reale è molto simile a quello di qualsiasi altra valuta reale, permette infatti l'acquisto di beni e servizi, sia digitali che reali. Bitcoin e le altre criptomonete, ad esso surrogate, appartengono a questo schema (BCE 2012). I modelli di moneta virtuale non devono essere confusi con la moneta elettronica.

CAP II - UN NUOVO PARADIGMA TECNOLOGICO: BLOCKCHAIN - MINING - ICO

2.1 Definizione, Caratteristiche e tipologie di Blockchain

Negli ultimi anni il numero di investitori e appassionati di criptovalute è aumentato in modo vertiginoso. È importante sottolineare che, in questo ambito, oltre agli investitori, sono presenti molti sostenitori ed appassionati della materia. All'interno dei non addetti ai lavori, però, spesso ci si ferma all'innovazione nel comparto finanziario delle transazioni, non capendo che le cryptocurrencies rappresentano solamente la punta dell'iceberg se rapportate al ventaglio delle applicazioni innovative offerte dalla tecnologia blockchain. Per poter inquadrare la nuova tecnologia è importante partire dal concetto di sistema distribuito illustrato nella Figura 2.

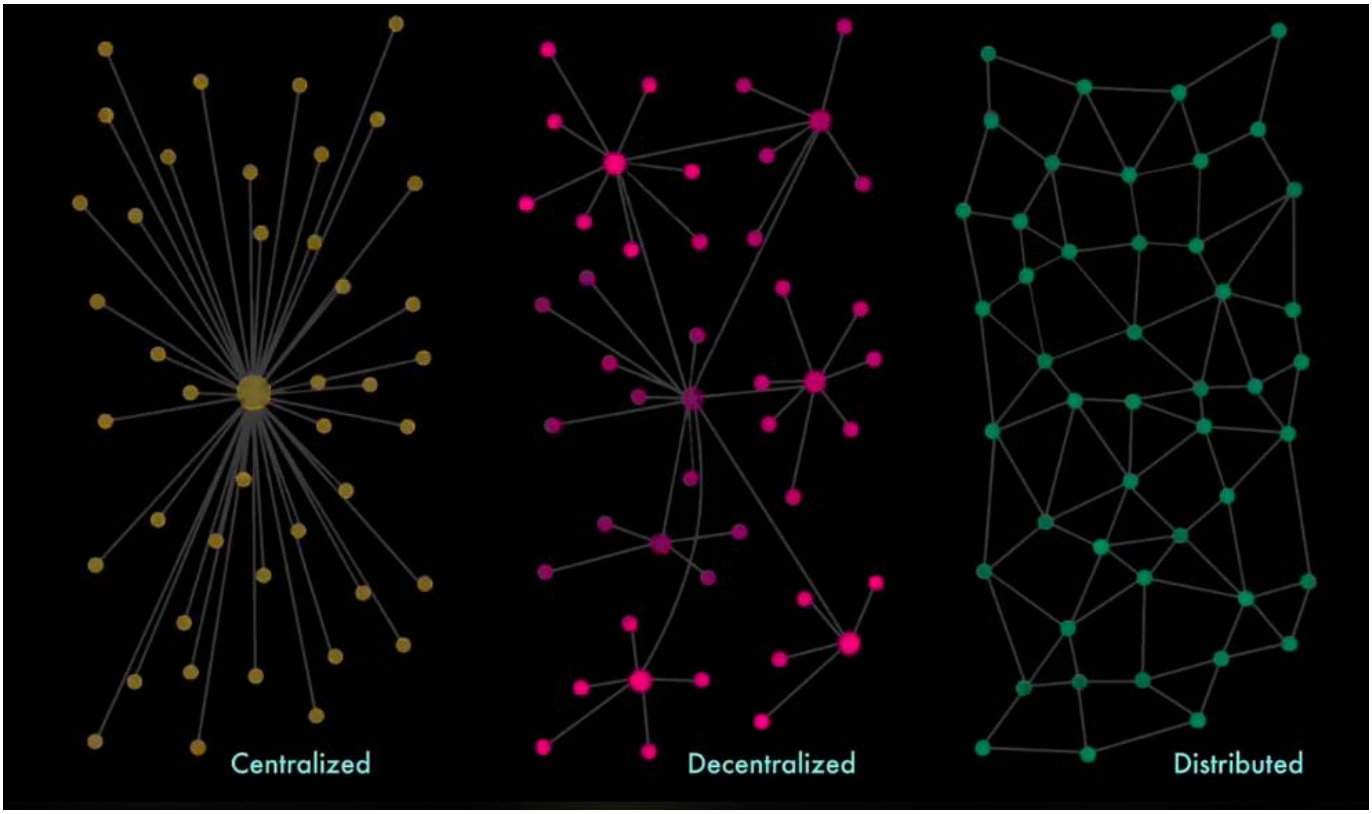


Figura 2 - Tipologie di Sistema

La prima rappresentazione raffigura un sistema centralizzato del tipo one-to-many, simile al nostro sistema economico, in cui le decisioni, gli input vengono forniti da un'istituzione centrale che assume un ruolo preminente nella rete. La seconda connotazione è quella di sistema decentralizzato, si pensi in tal caso ad un'impresa che, operando in vari contesti geografici, lascia autonomia alle sue subsidiaries nell'intraprendere decisioni strategiche, creando quindi diversi centri di responsabilità locali e decentralizzati. La terza tipologia è quella propria della blockchain, ossia un sistema distribuito.

In questo contesto ogni partecipante della rete, chiamato in gergo informatico "nodo", viene posto in posizione paritaria con gli altri partecipanti e concorre con essi al processo di formazione della volontà, sulla base della maggioranza formatasi all'interno di uno schema democratico, attraverso l'approvazione da parte del 50% + 1 dei nodi.

Per poter spiegare in modo accurato la blockchain è fondamentale fornire diverse definizioni.

Nel linguaggio tecnico informatico essa è definita come un protocollo di comunicazione decentralizzato e distribuito che sfrutta la crittografia; ma questa definizione, per i non addetti ai lavori, ha una carente funzione esplicativa.

Passiamo, dunque, a una seconda definizione, inquadrando la blockchain come un'architettura di rete Peer-to-Peer (P2P) alla base di svariate applicazioni informatiche. Con l'espressione P2P si intende un sistema in cui ogni partecipante alla rete (nodo) ha lo stesso peso, e la responsabilità viene, tra i nodi, condivisa. La caratteristica principale di un protocollo informatico P2P è proprio l'assenza di gerarchie e di servizi o posizioni centralizzate nella rete.

Avendo chiarito alcuni concetti portanti alla base della tecnologia, possiamo pertanto fornirne una definizione più pragmatica. Come implementazione del "Distributed Ledger", la blockchain (letteralmente catena di blocchi) rappresenta un libro mastro o database decentralizzato, distribuito e crittografato in cui vengono registrate, in modo immutabile, tutte le interazioni che avvengono tra i nodi partecipanti alla rete[5]. Tale tecnologia consente di trasferire tramite internet non più solo informazioni, ma bensì anche proprietà come avviene con le cryptocurrencies.

Nella spiegazione fornita da "The Economist" la blockchain viene definita come un foglio di calcolo sequenziale di operazioni, costantemente aggiornato su una rete globale di computer, che assolve la funzione di libro mastro distribuito.

Dalle varie definizioni fornite si evince una panoramica delle più importanti caratteristiche della tecnologia:

- <u>Tracciabilità</u>

Il database è articolato in blocchi collegati tra loro, tali che ogni operazione avviata nella rete sia validata dai nodi che la compongono. Questi ultimi infatti assolvono diversi compiti, tra cui osservare le operazioni/transazioni degli altri nodi, effettuare un check sulla coerenza delle operazioni, ed infine approvarle.

- <u>Immutabilità</u>

Il database, lo storico, comprendente tutte le operazioni viene scaricato e replicato da ogni nodo che entra a far parte della rete. Per essere presente sulla rete ed approvata da essa, infatti, ogni transazione è immutabile; a meno che essa sia riproposta per una nuova approvazione.

[5] Gates Mark, "*Blockchain, la guida definitiva per conoscere Blockchain, Bitcoin, Criptovalute, Contratti Smart e il futuro del denaro*", Prima Edizione, 2017

- Sicurezza

Oltre che dall'immutabilità, la sicurezza del sistema è garantita dalla crittografia applicata alle transazioni, tema che sarà affrontato approfonditamente nella successiva sezione del capitolo.
La sicurezza è inoltre garantita dal fatto che tutte le informazioni contenute nel database siano accessibili a tutti i partecipanti della rete, i quali avranno uno storico di tutte le operazioni contenute nei blocchi.
Questo denota come il database sia dislocato su diversi calcolatori (pc) collegati tramite un sistema distribuito.

Chiaramente tale Database Management System rispetto a un database situato localmente o gestito da un singolo soggetto, assicura l'affidabilità nella gestione dei dati e nella loro conservazione anche in caso di malfunzionamento, oltre che la loro riservatezza, proteggendo i dati e il libro mastro, che li contiene, da azioni non autorizzate volte ad alterarli. Infatti, dato che il database è replicato per tutti i nodi, se qualcuno volesse modificare le informazioni in esso contenute avrebbe bisogno di almeno la metà del potere di calcolo (computazionale) di tutti i computer connessi alla rete, i quali cercheranno di correggerlo.
Dal primo rilascio della tecnologia blockchain avvenuto nel 2008 con l'introduzione di Bitcoin, relativamente all'applicazione nelle transazioni, le implementazioni della stessa si sono estese, aumentandone il grado di personalizzazione.
A questo punto diventa necessario per giungere a una più esaustiva comprensione della tecnologia definire le diverse tipologie di blockchain:

- Blockchain Pubbliche

Anche dette "permissioned distributed ledgers", o semplicemente "Public", rappresentano delle reti Peer-to-Peer aperte a tutti i potenziali partecipanti in cui è assente il controllo di qualsiasi autorità centrale. Quest'architettura permette a tutti i nodi della rete di contribuire attivamente all'aggiornamento dei dati registrati nel database e di ottenere la copia di ogni operazione intervenuta sullo stesso. Ogni nodo, infatti, può partecipare al processo di consenso, ovvero controllare ed approvare le transazioni facenti parte di un determinato blocco da inserire nella catena (block-chain).
A differenza di un sistema centralizzato in cui la trasparenza e l'osservanza delle regole è garantita da un determinato soggetto, in una public blockchain queste caratteristiche sono assicurate dalla combinazione fra la risoluzione di problemi informatici e incentivi economici.
In questo contesto il grado con cui ogni nodo della rete può contribuire alla formazione del consenso è commisurato alle risorse che può investire (potenza computazionale) nel processo di approvazione delle transazioni.
Questo tipo di reti vengono classificate come totalmente decentralizzate.

- Blockchain Private

In questa tipologia, l'approvazione delle operazioni, e quindi il processo di formazione del consenso non è demandato alla maggioranza dei partecipanti al sistema, ma bensì è assegnato ad un'organizzazione, che rappresenta l'autorità centrale totalmente assente nelle reti "Public", precedentemente descritte.
D'altro canto, le modalità con cui viene gestita la catena è identica, infatti la gestione dei blocchi segue un determinato ordine, ma la lettura del database può essere pubblica o ristretta dall'organizzazione centrale.
Siamo perciò difronte a un sistema centralizzato ma con l'aggiunta di un sistema di verificabilità informatico-crittografica.

- Consortium Blockchain

Rappresenta la tipologia di rete in cui il "consensus process" viene condotto da un set predeterminato di nodi. Anche in questo contesto la lettura della blockchain può essere pubblica o limitata ad alcuni nodi della rete. Questa terza tipologia viene definita parzialmente decentralizzata, dato che costituisce un ibrido tra la rete trustless della blockchain pubblica e la rete centralizzata del tipo "Private".

Per terminare la panoramica generale è strumentale soffermarsi ancora sulle tipologie di blockchain, evidenziando vantaggi e criticità nel raffronto tra il tipo "Public" e il "Private".
Nelle reti gestite da un consorzio o da una specifica organizzazione (Private), il protocollo può essere agevolmente modificato da questi soggetti, infatti, possono essere modificate le regole di base così come alterate le transazioni o corretti i saldi. Inoltre, a differenza delle reti "Public", i validatori che concorrono alla formazione del consenso sono noti, questo determina una minimizzazione del rischio derivante da un attacco al sistema condotto da nodi della rete che detengono più del 50% + 1 del potere di calcolo.
Altra grande differenza risiede nella privacy, di fatto nelle blockchain private, la possibilità di limitare i permessi di lettura del database fornisce un alto livello di riservatezza. In ultimo, un altro importante vantaggio risiede nel costo delle transazioni. Infatti, nella tipologia "Private" le transazioni necessitano dell'approvazione di un numero ristretto di nodi, degni di fiducia, comportando perciò una riduzione nei costi di transazione rispetto alle blockchain pubbliche, in cui la verifica è condotta da migliaia di computer.
D'altro canto, un grande vantaggio del tipo "Public" è la protezione fornita agli utenti del sistema dagli sviluppatori dello stesso, che recidendo la loro autonomia nel compiere individualmente modifiche sostanziali al protocollo, alimentano e rafforzano il concetto di "Trustless System".
Nonostante i vantaggi descritti, non esiste una tipologia dominante, ma la validità di ognuna di esse dipende dall'utilizzo e dal contesto in cui la si vuole applicare.

2.2 La Crittografia e la sicurezza dei dati

Precedentemente, definendo la tecnologia blockchain, si è fatto diverse volte richiamo al termine crittografia, concetto che verrà chiarito nella presente sezione.
Per crittografia si intende la scienza che si occupa del processo di codifica dei messaggi, prima che essi siano immessi nella rete, rendendo le informazioni criptate a chiunque dovesse intercettarle. Questo meccanismo determina l'esclusività nella lettura e nella comprensione del messaggio da parte del destinatario, infatti attraverso un processo di decodifica le informazioni vengono rese chiare e comprensibili[6]. Il contenuto del messaggio, da proteggere, viene definito testo in chiaro, mentre il suo contenuto reso non comprensibile viene detto testo cifrato. Il processo volto a trasformare il testo in chiaro in cifrato viene chiamato cifratura, all'opposto l'operazione inversa è detta decifratura.
La perfetta Privacy e la totale riservatezza in uno scambio informatico di dati possono essere ottenute solo attraverso un sistema crittografico perfetto. In tal contesto si identificano due tipi di algoritmi di cifratura perfetti:

- "Computational Secrecy"

Si intende un sistema crittografico inviolabile, tenuto conto delle risorse a disposizione da chi esegue l'attacco informatico.

- "Perfect Secrecy"

Si riferisce ad un algoritmo di cifratura matematicamente inviolabile.

I due modelli perfetti, sopra descritti, rappresentano i due sistemi verso cui un algoritmo crittografico tende per acquisire una sua robustezza. Esistono inoltre due famiglie per quanto riguarda le funzioni di cifratura:

- Algoritmi crittografici per uso ristretto

Il loro funzionamento deriva dal fatto che le funzioni di cifratura e decifratura sono sconosciute, la forza dell'algoritmo deriva, quindi, dalla segretezza dello stesso.

[6] Bruce Schneier, "*Applied Cryptography*", John Wiley & Sons, 1996

- Algoritmi crittografici per uso generale

A differenza del precedente, dato che le funzioni di cifratura e decifratura sono conosciute, basa la sua funzione su un sistema di chiavi, una pubblica e una privata. La prima può essere conosciuta da tutti mentre la chiave privata è personale e deve rimanere segreta.

Come precedentemente descritto, un sistema crittografico, per poter assicurare la consistenza del messaggio e l'autenticità del mittente deve essere caratterizzato da diverse proprietà[7]:

- Integrità delle informazioni

Tale proprietà si traduce nella garanzia che i messaggi non vengano modificati senza la dovuta autorizzazione. Infatti, il valore di un messaggio deriva dalla sua consistenza e integrità.
Il meccanismo maggiormente noto per la conservazione dell'integrità di un messaggio è la firma digitale.

- Disponibilità delle informazioni

Partendo dal fatto che un'informazione ha valore solo se recapitata, al momento giusto, al giusto destinatario, la disponibilità delle informazioni è cruciale.
Essa determina infatti che il messaggio sia recapitato al giusto destinatario, cosa non ovvia dati gli innumerevoli attacchi informatici che tendono ad alterare la disponibilità delle informazioni negli archivi digitali.

- Confidenzialità

Rappresenta la proprietà del sistema che garantisce e tutela la segretezza del messaggio cifrato.
Attraverso proprio gli algoritmi crittografici viene garantito che solamente il destinatario del messaggio possa leggerlo, avendo solo egli gli strumenti per decriptarlo, garantendo quindi la segretezza nelle comunicazioni.

[7] Ozalp Babaoglu, Cryptography System, slides – http://www.cs.unibo.it/~babaoglu/courses/security/lucidi/pdf/

- Non Repudiation

La proprietà di non ripudio rende impossibile negare per il mittente, in un sistema, l'invio del messaggio stesso. Questa caratteristica si lega alla firma digitale, che rappresenta un sottoinsieme delle firme elettroniche.

2.2.1 Crittografia simmetrica (chiave privata)

Come descritto precedentemente, l'algoritmo crittografico permette di nascondere, o meglio cifrare, un testo in chiaro. Questo tipo di trasformazione è detta parametrica, ossia necessita di un parametro per essere portata a termine, detto chiave.
Al fine di decifrare un messaggio, infatti, un utente, oltre a conoscere l'algoritmo di cifratura impiegato nella trasformazione, deve necessariamente possedere la chiave.
L'algoritmo crittografico più antico e semplice, data la sua bassa sicurezza e affidabilità, è chiamato "a chiave simmetrica" o "a chiave privata-segreta". Con questo sistema, il mittente, così come il destinatario, utilizzano la stessa chiave privata, la quale viene quindi impiegata sia nella cifratura che nella decifratura.
Il procedimento è descritto nella Figura 3.

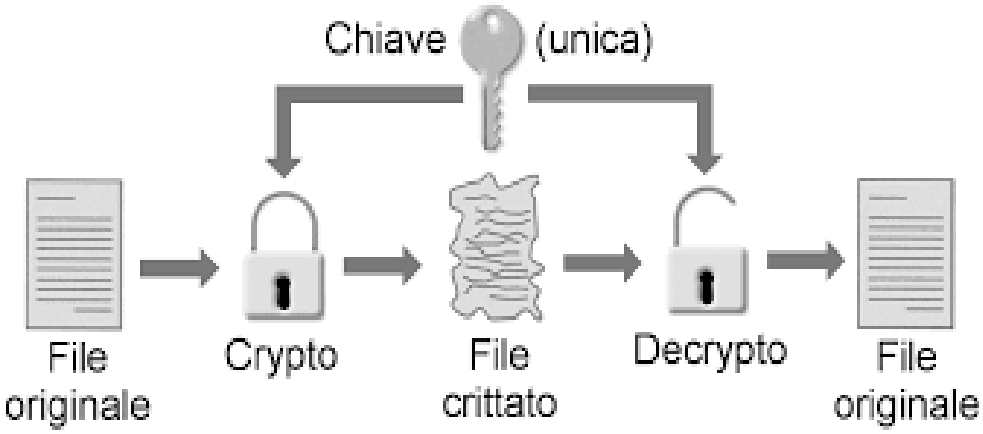


Figura 3 - Esempio di un sistema di crittografia a chiave unica

Il processo descritto, così come l'algoritmo crittografico a cui si riferisce, sono pero caratterizzati da alcuni punti deboli. Primo fra tutti, esso richiede in origine l'incontro tra le parti per accordarsi sulla chiave segreta da utilizzare; questo è dovuto alla bassa sicurezza del canale di trasmissione che ha portato alla necessità di cifrare il messaggio. In secondo luogo, questo meccanismo comporta l'unicità della chiave per ogni coppia di utenti, comportando perciò la generazione di un numero molto elevato di chiavi.

2.2.2 Crittografia asimmetrica (chiave pubblica)

Le falle mostrate dal sistema crittografico simmetrico sono state risolte, attorno agli anni Settanta, con l'introduzione della crittografia "asimmetrica" o a "chiave pubblica".

Seguendo questo algoritmo, ogni utente è detentore di due distinte chiavi: una pubblica e l'altra privata.

La chiave pubblica viene fornita dall'utente ai soggetti con i quali ha intenzione di comunicare, mentre la chiave privata deve essere segretamente custodita.

Le due chiavi assolvono una funzione differente, ossia, quella pubblica permette la cifratura del contenuto del messaggio da inviare; la chiave privata, invece, permette la decifratura del contenuto, che può essere compiuta solo dal proprietario della chiave stessa (privata).

Con questo algoritmo crittografico viene dunque risolto il problema di comunicazione della chiave segreta insito nel meccanismo "simmetrico".

Per chiarire maggiormente il funzionamento del processo si pensi ad una comunicazione informatica tra Bob e Alice.

Per comunicare con Alice, Bob dovrà crittare, cifrare il messaggio con la chiave pubblica di Alice, e solamente quest'ultima, in possesso della sua chiave privata, potrà decriptarlo. Tale procedimento è illustrato nella Figura 4.

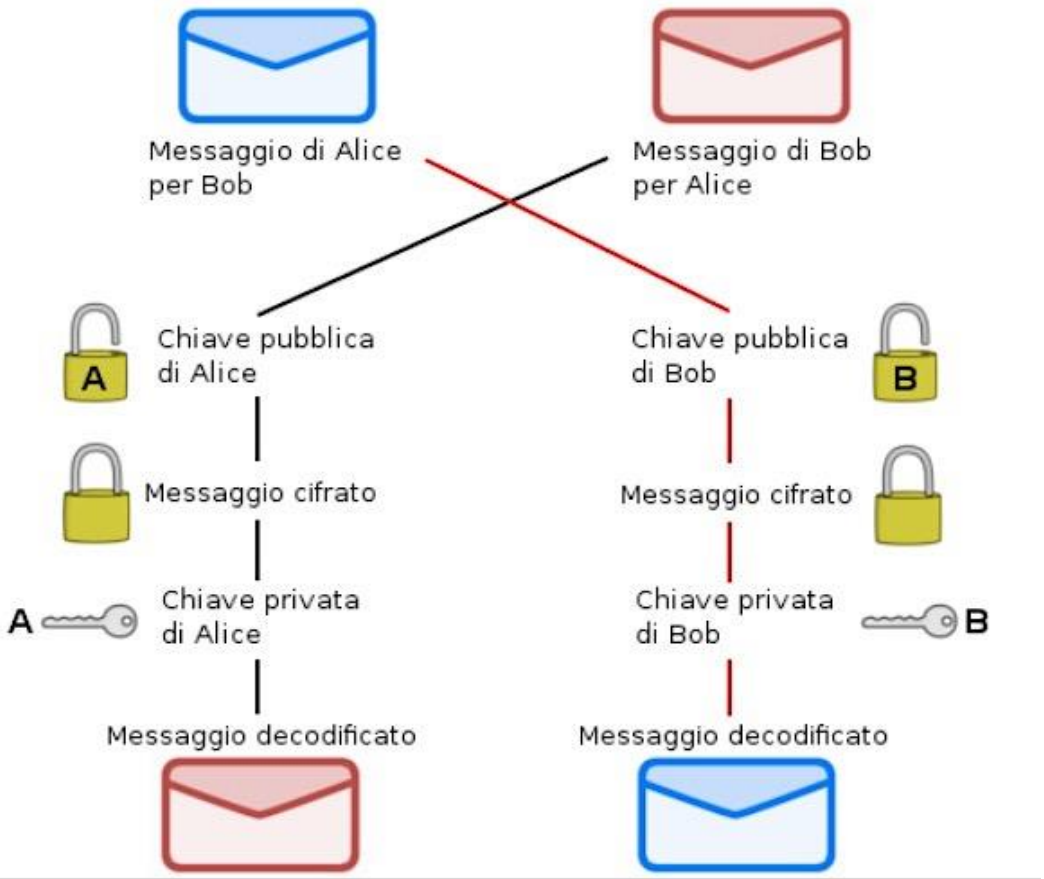


Figura 4 - Schema di crittografia asimmetrica

2.2.3 La funzione Hash nel Bitcoin

All'interno dell'infrastruttura Bitcoin, la crittografia gioca un ruolo fondamentale in diverse operazioni che verranno ampliamente trattate nelle prossime sezioni, come ad esempio nell'attività di "Mining" o per verificare la validità della blockchain.

Gli algoritmi crittografici, però, sono strumentali anche per la creazione di chiavi, indirizzi Bitcoin e per l'autorizzazione delle transazioni. In questo contesto tra i vari algoritmi utilizzati, uno dei più importanti è la funzione hash.

La funzione hash è un algoritmo matematico che permette la mappatura di dati di lunghezza arbitraria in una stringa binaria di lunghezza fissata chiamata in inglese "message digest" oppure valore hash.

Tale algoritmo, dunque, accetta un valore di lunghezza arbitraria e ne restituisce uno di lunghezza fissa, di solito inferiore. Per ottenere questi risultati vengono utilizzati vari algoritmi, uno tra i più noti è SHA (Secure Hash Algorithm).

Caratteristica principale di tale funzione è essere non iniettiva, il che si traduce nel non poter invertire la funzione, o meglio l'unico modo per risalire dai dati di output a quelli di input è quello di condurre una "brute force research". Tale operazione consiste nella ricerca di un dato valore tra tutti i possibili input cercando, dunque, una corrispondenza.

Il protocollo Bitcoin risolve diverse problematiche e difficoltà con la crittografia asimmetrica come il sistema di chiavi (pubbliche e private) e gli indirizzi.

Con riguardo alla crittografia asimmetrica, descritta nella sezione precedente, bisogna aggiungere che il processo in una comunicazione può risolversi con una modalità differente da quella descritta nella Figura 4 - Schema di crittografia asimmetrica Infatti, se Bob volesse crittare un messaggio da inviare ad Alice, alternativamente potrebbe codificarlo con la propria chiave privata ed inviarlo ad Alice, la quale potrebbe decifrare il messaggio con la sola chiave pubblica di Bob, accertandone pertanto l'origine.

In sostanza le chiavi sono dei numeri, la chiave privata viene generata in modo randomizzato, mentre quella pubblica viene trovata dalla chiave privata mediante una funzione ellittica unidirezionale.

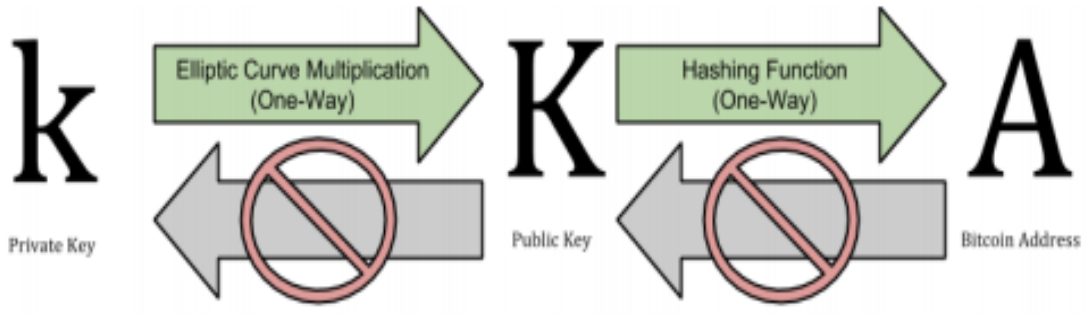


Figura 5 - Sistema di chiavi usate nella blockchain (Fonte: Mastering Bitcoin)

La chiave pubblica, che discende dalla chiave privata come mostrato nella Figura 5, è formata da un codice di 512 bit generato dall'algoritmo crittografico ECDSA (Elliptic Curve Digital Signature Algorithm), ed è utilizzata nella verifica delle firme digitali, relativa alla validità delle transazioni, senza che quindi sia resa nota la chiave privata.
Infine, dalla chiave pubblica viene generato l'indirizzo Bitcoin, ossia il wallet su cui ricevere crittomoneta, mediante algoritmi di hashing, che garantiscono la sicurezza.
Di seguito verrà descritta una transazione Bitcoin con le sue implicazione crittografiche, da un punto di vista tecnico.
Una transazione in Bitcoin tra Bob (pagante) e Alice (ricevente) si articola nei vari step:

1. Alice genera in modo casuale una chiave privata (sequenza casuale di cifre) che viene salvata sul suo computer.

2. La chiave privata viene convertita in chiave pubblica con l'algoritmo matematico della curva ellittica.

3. La chiave pubblica viene criptata e convertita in un hash. La nuova chiave pubblica è chiamata "public key hash", mentre quella originaria prende il nome di "full public key" Il sistema Bitcoin utilizza la funzione hash chiamata SHA-256.

4. L'hash della chiave pubblica viene convertito in una riga di massimo 35 caratteri che rappresenta l'indirizzo del portafoglio di Alice (ad esempio: 15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC).

   - I primi 4 passaggi avvengono istantaneamente -

5. Alice (ricevente) spedisce l'indirizzo a Bob.

6. Bob (pagante) decodifica l'indirizzo in hash della chiave pubblica.

7. Il pagante crea la transazione specificando l'output (quantità di bitcoin trasferiti e un "pubkey script" che contiene le condizioni che rendono spendibili quei determinati Bitcoin, come ad esempio la necessità di utilizzare la chiave privata per firmare la transazione). Oltre agli output Bob dovrà inserire anche il "signature script" ossia le informazioni che il ricevente dovrà fornire per convalidare la transazione.

8. Il pagante conferma la transazione, inviando i Bitcoin all'indirizzo wallet di Alice.

9. Bob (pagante) trasmette la transazione a tutta la rete, ovvero ad altri nodi che ne valutano la correttezza e la comunicano ad un nodo-minatore (miner) affinché la confermi.

10. I “Miners” inseriscono nella blockchain la transazione inserendola in un blocco, la quale diventa riconosciuta e approvata dalla comunità.

11. Alice, il ricevente, firma con la propria chiave pubblica e privata il “signature script”, dimostrando di essere il proprietario dell’output della transazione.
    Va menzionato che il procedimento di firma è del tutto automatizzato dal software Bitcoin. A questo punto Alice potrà spendere l’output della transazione con Bob, come input in una successiva transazione.

Nel sistema Bitcoin, viene introdotto il concetto di “gettone elettronico”, rappresentato come una catena di firme digitali.
Il detentore di un certo ammontare di BTC ricevuti, che voglia trasferirli a un determinato destinatario, deve digitalmente firmare con la propria chiave privata l’hash della transazione precedente (condizione di spendibilità dei BTC, che ne testimonia il possesso) e la chiave pubblica del destinatario (indirizzo a cui spedire), aggiungendo queste informazioni alla transazione che sta avviando come illustrato in Figura 6.

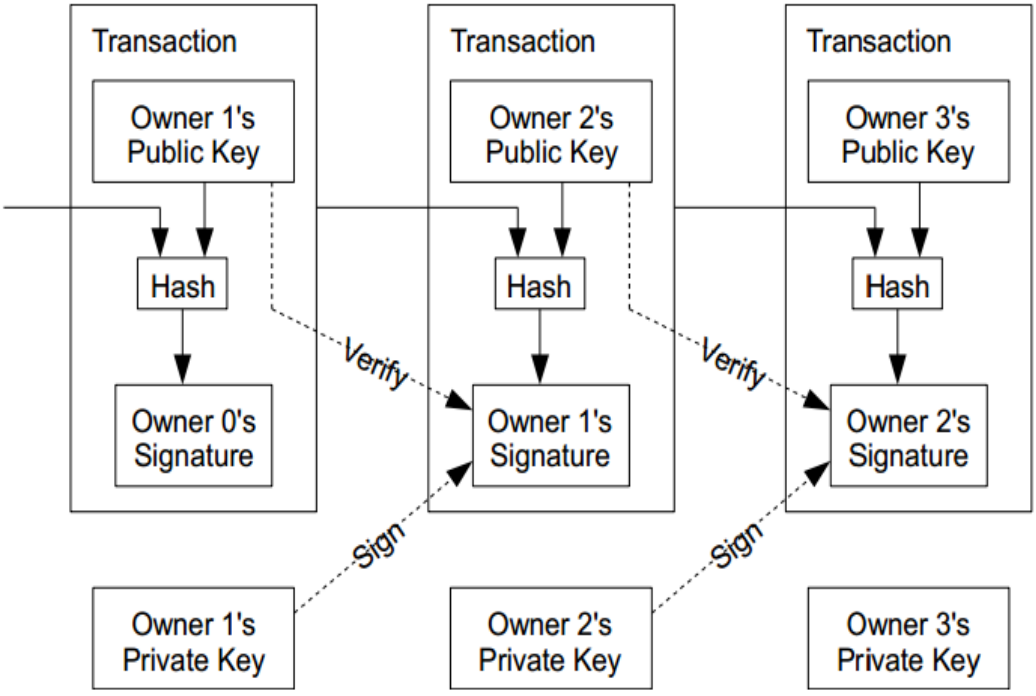


Figura 6 - Catena di transazioni

Il ricevente, in una transazione, può condurre un controllo sui vari passaggi di proprietà della valuta digitale, verificando a ritroso le firme presenti in ogni transazione. Infatti, se venisse modificata anche solo una transazione, tutte le transazioni precedenti sarebbero invalide, in quanto gli hash non corrisponderebbero più, ad esempio a causa del fatto che sono stati spesi dei BTC che non si possedevano.

2.3 La Blockchain applicata alla Finanza

La blockchain applicata al sistema Bitcoin, ha attirato a sé, negli anni successivi al rilascio della crittomoneta, l'interesse di un numero sempre crescente di aziende nell'industria finanziaria.
Moltissimi operatori del comparto finanziario, rimanendo titubanti nei confronti della principale criptomoneta, il bitcoin, hanno studiato la tecnologia che ne regola il funzionamento, comprendendone l'importanza e la capacità di rivoluzionare in diversi comparti e processi, tra cui quelli finanziari.
Le intuizioni riguardo il potenziale tecnologico della blockchain si sono tradotte in investimenti milionari in R&D volti ad ottenere le conoscenze per lo sviluppo di una propria architettura P2P.
Le ragioni riguardano i vari impatti che la tecnologia avrebbe sul mercato finanziario, come ad esempio la riduzione dei costi di transazione e delle tempistiche nelle transazioni, la capacità di processare rapidamente le informazioni, oltre che effetti in termini di disintermediazione in molti processi in cui un'autorità "trust" sembra imprescindibile.
Le implicazioni tecnologiche sopra descritte hanno la forza di rivoluzionare trasversalmente l'intero sistema finanziario, applicando la blockchain alle attività che rappresentano il nucleo operativo delle istituzioni finanziarie, quali trasferimenti di valuta, pagamenti, trading nel mercato azionario, e molte altre operazioni finanziarie.
In tal caso si pensi ad una transazione cross border, in cui il trasferimento di denaro tra due soggetti, oltre ad essere relativamente costoso, potrebbe richiedere tempistiche lunghe.
Con l'adozione di un database, di un registro, basato su tecnologia blockchain, si potrebbero sia ridurre i costi di transazione associati al trasferimento, ma anche le tempistiche, tagliando i canali attraverso cui le informazioni passano per validare la transazione.
In ottica bancaria, tradizionalmente, le transazioni vengono memorizzate su registri interni, e ciò può essere fatto in momenti diversi dalle diverse banche, determinando che i fondi, eliminati dal registro di una banca, non compaiano sul registro di un'altra per diversi giorni.
La tecnologia blockchain, permette di ovviare a questi problemi, sostituendo i tradizionali canali di autenticazione nelle transazioni con la trasparenza fornita da un registro distribuito e condiviso, permettendo di leggere la transazione a tutti i partecipanti alla rete.
L'idea di fondo è che le funzionalità della blockchain possano essere utilizzate per registrare, confermare e trasferire ogni tipo di contratto o proprietà, sostituendo molti servizi di intermediazione con una rete P2P.
Chiaramente, valute e pagamenti rappresentano la prima e la più ovvia applicazione, ma non esauriscono il campo applicativo relativamente alla finanza.
Infatti, l'innovazione può essere estesa a svariate tipologie di transazioni finanziarie, reinventando ad esempio il mercato azionario, il Private Equity, il mercato obbligazionario, gli strumenti di investimento, i derivati, e molti altri.

All'interno del comparto bancario, molte istituzioni si stanno preparando alla rivoluzione tecnologica, investendo, in primis in ricerca per valutare gli impatti sul proprio modello di business, ma anche su vari progetti applicativi per cavalcare l'onda tecnologica.

Un esempio di ciò è rappresentato dalla Deutsche Bank, che nel 2015 ha trasformato l'interesse verso la tecnologia in un progetto consistente nel lancio di diversi Innovation Lab, con lo scopo di accelerare lo sviluppo del settore Fintech e di startup blockchain a livello mondiale

Un altro importante progetto condotto dalla società Fintech R3 Cev ha sperimentato la validità e l'efficacia dell'emissione, commercializzazione e riscatto di un'obbligazione corporate attraverso l'utilizzo di un registro condiviso blockchain. Al progetto hanno partecipato, mettendo a disposizione i loro servizi di cloud computing e data mining, colossi come Amazon, IBM cloud e Microsoft Azure, ma anche appartenenti al comparto bancario, tra i più importanti Bank of Ameria, Banco Santander, Goldman Sachs, J.P. Morgan e molte altre.

Anche all'interno del mercato azionario e obbligazionario la blockchain potrebbe reinventare le transazioni. Esempio di questo si ha avuto il 30 dicembre 2015, quando NASDAQ, principale indice di titoli tecnologici della borsa americana, ha lanciato NASDAQ Linq, un servizio per la negoziazione di titoli obbligazionari basato su blockchain. Obbiettivo del servizio è la velocizzazione del regolamento per le transazioni in mercati pubblici.

Successivamente, NASDAQ Linq ha interessato anche il comparto azionario, nello specifico per le transazioni pre-IPO, testando il commercio di azioni di società private mediante un registro distribuito contenente tutte le informazioni gestite oggi con modalità tradizionali.

Oggetto di queste transazioni basate su blockchain sono quindi quote di azione di società private, prima che esse si quotino.

Questo meccanismo evita il coinvolgimento di una serie di intermediari quali legal advisor, revisori dei conti, consulenti, e custodi di libri, precedentemente indispensabili in una fase di pre-IPO.

L'applicazione NASDAQ Linq, agendo da registro digitale, fornirà uno storico di ogni trasferimento di titoli tra gli utenti della blockchain, semplificando i controlli e garantendo trasparenza nelle transazioni azionarie.

A sostegno di quanto detto va ricordato come NASDAQ, Citibank, Visa e Capital One abbiano investito oltre 30 milioni di dollari su Chain.com, per la realizzazione di registri distribuiti che gestissero le transazioni interbancarie.

Infine, va ricordata la dichiarazione di Bob Greifeld[8]: "La tecnologia blockchain continua a ridefinire non solo il modo in cui opera il settore del mercato azionario, ma l'economia finanziaria globale nella sua interezza".

[8] Bob Greifeld, amministratore delegato di NASDAQ

2.3.1 Il P2P cash system (L'applicazione nelle transazioni)

Il primo utilizzo stabile a livello mondiale della tecnologia blockchain, si è avuto nel settore delle transazioni, grazie alla sua implementazione nel sistema Bitcoin, definito dal suo anonimo ideatore: "A Peer-to-Peer Electronic Cash System". È importante ricordare come il "Distributed Ledger Transaction" sia solo una delle applicazioni derivanti dalla blockchain; l'errore comune infatti è confondere un elemento dell'insieme con l'insieme stesso.

La blockchain consente la creazione di un database per la gestione delle transazioni avvenute tra i nodi che compongono la rete. Sintetizzando, si tratta di un database articolato in blocchi, contenenti al loro interno diverse transazioni, tra loro collegati in modo che ogni transazione intervenuta sulla rete sia approvata dai nodi che ne fanno parte. Questo meccanismo permette la realizzazione di un archivio in cui ogni transazione è chiaramente tracciabile. (Figura 7)

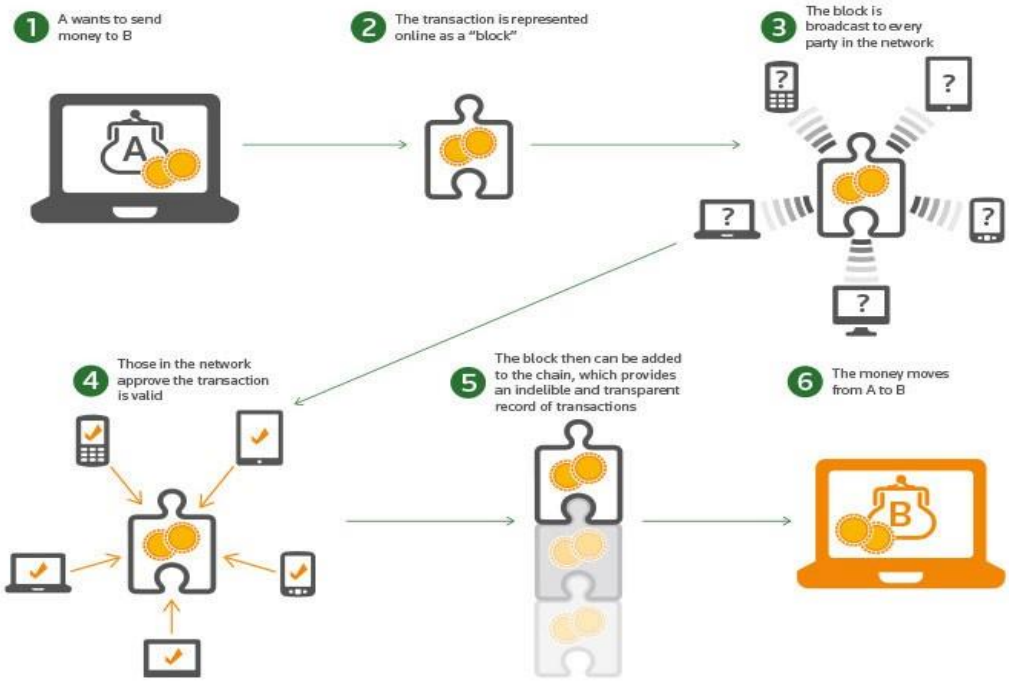


Figura 7 - Funzionamento della Blockchain nelle transazioni

Avendo affrontato nella sezione 2.2.3 i vari step che caratterizzano una transazione BTC tra due ipotetici nodi della rete (Bob e Alice), verranno in questo paragrafo discussi alcuni ulteriori concetti ed effetti relativi ad una transazione nel sistema Bitcoin.

Partendo dal fatto che, in questo contesto, una transazione è un trasferimento notificato a tutta la rete e salvato in un determinato blocco della catena, va menzionato che ogni transazione può essere formata da più input e output.

Gli input non sono altro che riferimenti ad output di transazioni precedenti. Infatti, un indirizzo bitcoin può aver ricevuto n pagamenti, e quindi detiene n output da utilizzare come input in una successiva transazione. In questa ottica si crea un vero e proprio sistema dei resti e delle commissioni.

Analizziamo due casi.

Nel primo caso, considerato caso base, un utente che ha precedentemente ricevuto ad esempio 5 BTC, deve a sua volta pagare in una transazione 5 BTC. In questo caso l'input della transazione conterrà l'id dell'output precedente (di 5 BTC precedentemente ricevuti da un singolo output) e l'indirizzo del destinatario del pagamento unito alla quantità da inviare (sempre 5 BTC). In questo caso banale tutti i Bitcoin posseduti dall'utente vengono trasferiti al destinatario.

La situazione è del tutto diversa nel caso in cui i BTC da inviare non siano tutti quelli posseduti dall'utente, ma solo una parte. Considerando il sistema di input/output come dei blocchi di Bitcoin divisibili solamente con le transazioni, i blocchi devono essere inseriti interi nella transazione, non potendo quindi inviare solo parte dei Bitcoin posseduti.

Tornando all'esempio, se nella transazione l'utente dovesse inviare solamente 3 dei 5 BTC posseduti, dovrebbe comunque trasferire la totalità dei suoi BTC. Per ovviare a questa problematica viene utilizzato un indirizzo dei resti, vale a dire che viene aggiunto all'output della transazione un ulteriore indirizzo, appartenente all'utente che ha compiuto la transazione, al quale vengono inviati i BTC di resto.

Una problematica comune agli utenti inesperti, nel caso non forniscano un indirizzo di resto, è che i BTC di resto non tornino all'utente, ma siano considerati come costo di transazione, e quindi guadagnati dai "Miners" che hanno verificato la transazione.

Questo complesso procedimento viene spesso semplificato da alcuni software che gestiscono portafogli Bitcoin, che automaticamente generano un indirizzo dei resti al quale affluiscono le crittomonete possedute, eccedenti la quantità che si vuole inviare.

2.3.2 Il problema del "Double Spending" (caso Bitcoin)

L'intero sistema Bitcoin è gestito da un database, replicato fra tutti i nodi, che registra e memorizza tutti gli scambi di moneta digitale, senza la necessità di un'autorità centrale. Parlando di digitale, si pensi ora ad un file digitale, che nel caso in cui sia copiato, non permette di distinguere la copia dal file originale, essendo costituiti entrambi da bit.

Traslando il ragionamento nel sistema Bitcoin, si parla di double spending quando esiste la possibilità di spendere due o più volte uno stesso "gettone digitale", considerando questo fenomeno come l'elemento di maggiore criticità all'interno delle valute digitali.

Il funzionamento di Bitcoin, come sistema decentralizzato, è rimesso all'onestà dei nodi-minatori che compongono la rete, i quali verificano e convalidano le transazioni ("Miners").

Può essere considerato onesto un nodo-miner che mette a disposizione la propria potenza di calcolo (computazionale) per creare blocchi che non contengano transazioni considerate inconsistenti, contrastanti tra loro, e tra esse e quelle precedentemente registrate sulla blockchain.

Il problema del double spending si configura quando un nodo malevolo della rete persegua il fraudolento obbiettivo di spendere una stessa unità di valuta digitale diverse volte.

Tale problema dovrebbe essere risolto con la corretta tenuta della blockchain, un registro immutabile e condiviso, che utilizza una marcatura temporale per timbrare ogni blocco, ossia una sequenza specifica di caratteri che identificano in modo univoco e indelebile una data/orario per accertare l'effettivo avvenimento di un evento.

Ogni marca temporale include e ricorda la precedente nella propria hash form, formando così una catena (Catena di blocchi). L'applicazione della marca temporale nella blockchain è detta Timestamp.

Questo meccanismo però non evita la vulnerabilità del sistema ad attacchi come quello del double spending.

Passando agli aspetti tecnici, quando un nuovo blocco di transazioni viene risolto e approvato dai miners, le transazioni in esso contenute sono approvate una volta, e con l'aggiunta a quest'ultimo di ulteriori blocchi, si ottengono via via ulteriori conferme per le transazioni contenute nei blocchi precedenti.

Dato che esiste la possibilità che si creino delle biforcazioni nella catena di blocchi, ogni transazione non può quindi definirsi estranea al fenomeno del double spending fino a che non abbia ricevuto un buon numero di conferme.

Si pensi dunque al caso in cui uno stesso soggetto, nodo malevolo della rete, avvii quasi contemporaneamente due diverse transazioni, pagamenti, utilizzando pero la stessa unità di valuta digitale. Esistono dunque due transazioni: A e B.

Dal momento in cui il nodo malevolo avvia l'operazione A essa sarà successivamente inserita in un blocco della blockchain, visibile per il destinatario, ricevendo quindi una prima conferma.

Prima che la transazione A sia inserita in un blocco, il nodo potrebbe segretamente lavorare alla creazione di un altro blocco che però contiene la transazione B, che invia gli stessi BTC a un altro indirizzo, rendendo inconsistente l'operazione A.

Ma il nodo malevolo non comunicherà al network la transazione B, ma solo quella A, altrimenti gli altri nodi si renderebbero conto del contrasto tra le due operazioni, e quindi il ricevente del pagamento si accorgerebbe del raggiro non vedendo alcuna conferma alla transazione A.

Questa operazione fraudolenta è detta "Selfish-mining". Consiste in una strategia con cui un minatore crea volutamente una biforcazione della blockchain. (Figura 8).

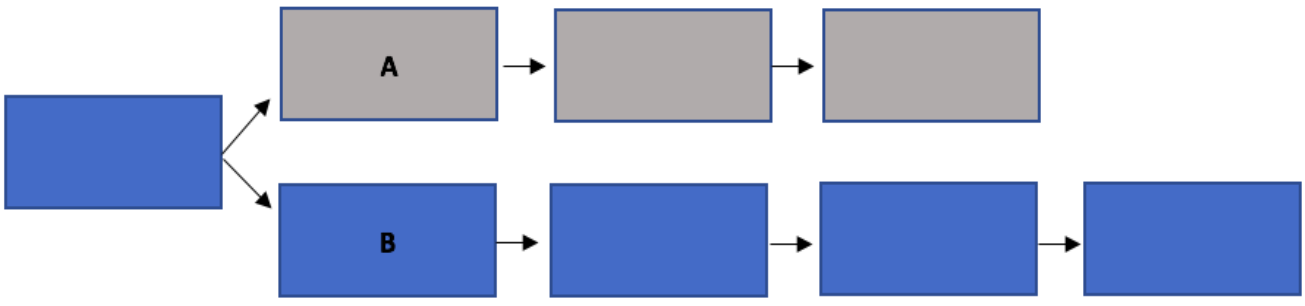


Figura 8 - Double Spending Attack andato a buon fine, in cui la transazione B è correttamente registrata, a differenza di A

Non comunicando la risoluzione di un blocco agli altri miner (transazione B), i minatori onesti continueranno a sviluppare la catena pubblica, mentre il nodo malevolo genererà nuovi blocchi da agganciare alla sua catena privata (catena B della Figura 8), con lo scopo di rilasciarla nel network quando sarà più lunga di quella pubblica, diventando perciò la catena dominante. Rendendo, così, gli altri blocchi, non facenti parte della catena principale, orfani, ed invalide le transazioni in essi contenute. Questa strategia, di difficile attuazione, è comunque possibile, determinando una vulnerabilità nel sistema.
Il double spending attack rappresenta quindi una gara, tra il nodo malevolo e tutti gli altri, a chi produce più blocchi a partire da quello corrente, prima che la transazione A sia approvata, dunque effettiva.
Anche se è remota la possibilità di un attacco simile, esso avrebbe successo, con certezza, nel caso in cui il nodo malevolo detenga da solo una potenza di calcolo, computazionale, superiore al 50% +1 della capacità di calcolo dell'intera rete.
Per completezza, è importante chiarire che parlando di potenza computazionale ci si riferisce all'hash rate come percentuale di essa, ed esprime la quantità di hash al secondo, che un dispositivo è in grado di generare. Ad esempio, una potenza di 1GH/s corrisponde alla capacità di produrre 1 miliardo di hashes al secondo.

2.3.3 La struttura dei blocchi

Come precedentemente accennato, la blockchain si articola in un insieme di blocchi, contenenti un determinato numero di transazioni, collegati tra loro. Questo permette la creazione di un registro condiviso in cui appare lo storico di tutte le transazioni avvenute ed approvate dal sistema, chiaramente non in contrasto tra loro (come nel fenomeno del double spending).
Entrando nello specifico, è importante descrivere l'articolazione di ogni blocco, andando ad analizzare le parti che lo compongono.
Ogni blocco si compone di due parti fondamentali: il block header e la lista di transazioni ricomprese nel blocco stesso[9]. Analizziamole nello specifico.

- Block Header

Rappresenta il documento di identità del blocco e contiene varie informazioni:

1. Numero o altezza del blocco: rappresenta il numero progressivo del blocco aggiunto alla catena. Il primo blocco della catena è detto genesis block, a cui è associato il numero zero.

[9] Antonopoulos Andreas, "*Mastering Bitcoin: Programming the Open Blockchain*", 2017

2. Hash: è il codice identificativo di uno specifico blocco e deriva dall'hashing di diverse informazioni come il numero di versione del software di verifica utilizzato nel protocollo, l'hash del blocco precedente affinché risulti collegato, il tempo in cui il blocco è stato risolto, il merkle root, la memoria utilizzata e il nonce (concetti che verranno di seguito affrontati).

3. Hash del blocco precedente: comprende tutte le informazioni relative al blocco precedente.

4. Hash del blocco successivo: visibile solo se tale blocco è stato agganciato alla catena.

5. Marca temporale (timestamp): data e ora in cui il blocco è stato risolto.

6. Difficoltà: intesa come il tempo di elaborazione necessario a risolvere il problema crittografico nell'operazione di mining. È la difficoltà di risolvere il blocco, ovvero convalidarlo e registrarlo.

7. Transazioni: numero delle transazioni ricomprese nel blocco.

8. BTC totali: rappresenta il numero di bitcoin inviati in tutte le transazioni del blocco, comprese le commissioni associate alla transazione.

9. Size: indica la memoria occupata da tutti i dati delle transazioni comprese nel blocco.

10. Merkle Root: rappresenta l'hash che sintetizza tutte le transazioni presenti nel blocco, in cui le diverse transazioni rappresentano foglie del "Merkle Tree".

11. Nonce: (number used once) garantisce che i dati presenti nel blocco non possano essere riutilizzati, ad esempio in un attacco informatico, ma verrà trattato più nello specifico in seguito.

- Lista di Transazioni

Rappresenta uno schema in cui sono presenti tutte le transazioni comprese nel blocco, indicando per ogni transazione il relativo hash, la commissione, la memoria occupata e gli indirizzi delle transazioni.

È importante, inoltre, aggiungere che la prima transazione che compare in ogni lista di qualunque blocco è chiamata "coinbase". Essa, immessa nel blocco dal miner vincitore, colui che ha risolto per primo il blocco, crea bitcoin nuovi di zecca (creazione di moneta), pagabili a quel miner come ricompensa per aver risolto il blocco, ossia validato e approvato le transazioni in esso presenti, svolgendo l'attività di "Mining", la quale verrà approfonditamente analizzata nella sezione successiva.

2.4 Il Consenso in una rete trustless: Il Mining

Il concetto di consenso nella blockchain viene associato al processo di validazione e verifica delle transazioni, che si realizza con la potenza di calcolo messa a disposizione dai partecipanti alla rete.
Questo potere computazionale è finalizzato alla risoluzione di complessi problemi informatico-matematici, veri e propri puzzle crittografici, e permette al sistema di basarsi su un consenso decentralizzato e distribuito, a differenza del consenso che si formerebbe in un sistema con la presenza di un'istituzione centralizzata garante.
Alcuni nodi della rete, che attivamente partecipano alla risoluzione dei puzzle crittografici, validando quindi i blocchi di transazioni, sono chiamati "Miner", i quali svolgono un'attività molto dispendiosa di risorse, e per questo vengono ricompensati con la generazione di nuova valuta digitale.
La logica che sta alla base del meccanismo di consenso/approvazione deriva dalla necessità di creare ostacoli e complicazioni durante tutto il processo di validazione, con la finalità di evitare tentativi di frodi da parte dei nodi che compongono la rete P2P.
I problemi di carattere informatico-matematico sono stati ideati per porre in competizione fra loro tutti i nodi, poiché tutti, con la loro potenza di calcolo, tentano di raggiungere la risoluzione del problema.
Il nodo che, fra tutti gli altri, riuscirà per primo a risolvere il puzzle crittografico otterrà il diritto alla validazione del blocco di transazioni presentando alla rete la soluzione del puzzle. L'impegno speso nella risoluzione, e il risultato ottenuto determinano per il miner vincitore un compenso in valuta digitale, che rappresenta emissione e creazione di nuova valuta virtuale.

2.4.1 L'attività di Mining nel Bitcoin: Procedimento di consenso, incentivi e costi.

All'interno del sistema Bitcoin, l'invenzione principale di Satoshi Nakamoto, anonimo inventore della più nota fra le principali crittomonete, è sicuramente il meccanismo decentralizzato di consenso.
Si parla in tal caso di "consenso emergente", poiché esso non è ottenuto esplicitamente, infatti, non c'è ad esempio nessun tipo di elezione o momento certo in cui esso sarà raggiunto.
Il consenso, invece, viene creato e raggiunto attraverso l'interazione asincrona di un elevatissimo numero di nodi (user della rete P2P), i quali accettano e seguono le regole su cui si fonda il protocollo informatico che gestisce le transazioni.
È inoltre importante sottolineare come la criptovaluta bitcoin, le sue varie proprietà, le transazioni e la sicurezza del sistema, derivino tutte dal meccanismo decentralizzato del consenso.
Ogni transazione avviata nel sistema viene divulgata sulla rete P2P di Bitcoin, non entra a far parte del

registro condiviso fino a quando essa non viene verificata e inclusa in un blocco della catena attraverso il processo di mining.
Tale processo nel sistema Bitcoin persegue due importanti finalità:

- Il processo di mining crea nuovi bitcoin con la validazione dei blocchi di transazioni che vengono inseriti nella catena. La generazione di nuova moneta assolve la funzione di ricompensa per il lavoro svolto dai miner, ossia validazione e approvazione delle transazioni.

- Il mining genera fiducia subordinando la conferma delle transazioni all'utilizzo di una potenza di calcolo sufficiente a validare il blocco che le contiene. In questo contesto, è importante aggiungere che un maggior numero di blocchi della catena determina l'utilizzo di maggiore potenza di calcolo necessaria per il meccanismo di approvazione, assicurando perciò maggiore fiducia nel sistema.

Come detto in precedenza, il processo di mining determina la generazione di nuovi BTC che si sommano alla valuta digitale già in circolazione, inoltre, tale attività fornisce una protezione dalle transazioni fraudolente, come ad esempio nel fenomeno del double spending, precedentemente descritto.
I miner compiono tali attività fornendo la loro potenza computazionale, di calcolo, al sistema Bitcoin sulla base dell'opportunità di essere ricompensati.
Per partecipare all'attività di mining è necessario connettersi alla rete Bitcoin scaricando un software che implementa tale protocollo e permetta lo svolgimento delle attività crittografiche coinvolte nell'estrazione.
Un nuovo blocco, contenente le transazioni avvenute nel sistema successivamente alla risoluzione del blocco precedente, si può considerare "mined" o risolto e quindi aggiunto al registro blockchain, in media ogni 10 minuti.
Questa condizione è prevista dal protocollo di funzionamento del sistema Bitcoin.
Le transazioni contenute nel blocco "risolto", aggiunto al registro, si considerano perciò approvate, consentendo ai nuovi proprietari di BTC di spenderli in transazioni successive.
I nodi della rete che partecipano al meccanismo di approvazione/consenso (miner) ricevono due categorie di ricompense per la loro attività.
La prima è rappresentata dalla creazione di nuovi BTC nel momento in cui un blocco viene confermato e aggiunto alla catena.
La seconda, invece, è costituita dalle commissioni (fee) relative a tutte le transazioni incluse in un determinato blocco.
Per ottenere queste ricompense, i miner competono nella risoluzione di un difficile problema matematico-informatico basato su un algoritmo crittografico di hashing.
La soluzione a tale problema rappresenta la prova di lavoro (proof of work) del miner, il quale ha impiegato nel processo una potenza di calcolo adeguata.

Il processo di generazione di nuova crittomoneta, così come nell'estrazione di metalli preziosi, segue un andamento decrescente.

Infatti, la massa monetaria creata dal procedimento di estrazione, che rappresenta parte della ricompensa dei miner, decresce approssimativamente ogni quattro anni, o più nello specifico con l'aggiunta di 210.000 blocchi risolti nella blockchain di bitcoin.

In termini pratici, la generazione di BTC è iniziata nel 2009 con la generazione di 50 BTC per ogni blocco risolto, dimezzandosi a 25 BTC nel novembre 2012, fino ad arrivare a 12,5 BTC nel 2016, ossia la ricompensa attuale per il miner vincitore nella risoluzione del puzzle crittografico.

Formalizzando questo processo, la ricompensa del mining nel sistema Bitcoin, e quindi la generazione di nuova moneta, decrescerà in modo esponenziale, verosimilmente, fino all'anno 2140, quando quasi tutti i bitcoin saranno stati emessi, ricordando il limite di 21 milioni di unità. In relazione alla ricompensa dell'attività di mining, la probabilità di ottenerla, risolvendo quindi il blocco, dipende dal rapporto fra la potenza computazionale che ogni singolo nodo apporta e quella totale della rete.

Per quanto riguarda i guadagni relativi alle fee di transazione, essi rappresentano ad oggi meno dello 0,5% dei guadagni complessivi di un miner, dato che la maggior parte delle ricompense è formata dalla generazione di nuova moneta. Ma, considerando che quest'ultimo tipo di ricompensa è decrescente nel tempo, e che gli sviluppi del sistema Bitcoin aumenteranno la size (byte) di ogni blocco, potendo contenere un maggior numero di transazioni, la maggior porzione di guadagni per un miner sarà rappresentata proprio dalle commissioni associate alle transazioni. Infatti, dopo l'anno 2140, terminato il conio di nuova crittomoneta, tutti gli introiti dei miner saranno rappresentati dalle fee nelle transazioni, dunque i guadagni dipenderanno dalla diffusione del sistema Bitcoin all'interno del mercato dei pagamenti.

Il termine mining, in un certo senso, è ingannevole poiché sposta l'attenzione sul processo di generazione di nuova moneta, il quale è solo una ricompensa per il lavoro svolto.

Invece, il primo scopo di tale attività è chiaramente quello di creare di un meccanismo di consenso, tradotto nell'approvazione delle transazioni, che fornisce sicurezza all'intero sistema Bitcoin.

Lo schema di incentivi, le ricompense, sono solamente uno strumento per allineare la funzione obbiettivo di ogni nodo-miner della rete con la stabilità e la sicurezza del protocollo informatico P2P, incentivando l'onestà dei nodi che proteggono il registro da chi vorrebbe alterarlo (nodi disonesti).

Passando ad analizzare in modo più specifico l'attività di mining nel sistema Bitcoin, è importante menzionare che sulla base delle regole del protocollo, indipendentemente dal numero di transazioni avviate nella rete, ogni due settimane devono essere prodotti in media 2.016 nuovi blocchi, ossia uno ogni 10 minuti, a prescindere da quante transazioni sono state effettuate.

Identificando i 2.016 nuovi blocchi da produrre ogni 14 giorni come il numero obbiettivo (target), è importante parlare dell'esistenza di un meccanismo di ribilanciamento. Infatti, ogni due settimane, nel caso in cui il numero dei blocchi di transazioni prodotti si discostasse dal numero target (2.016), la difficoltà di risoluzione del puzzle crittografico, ovvero di produzione di un nuovo blocco, viene modificata a seconda che il numero di nuovi blocchi prodotti sia maggiore o minore del numero target. Nel caso in cui sia minore

la difficoltà verrà rivista verso il basso, all'opposto se il numero è maggiore del target, la difficoltà di produzione sarà alzata.

Vista la forte competizione tra i nodi nel cercare di trovare la soluzione al puzzle crittografico, è naturale aspettarsi un incremento nel tempo della capacità di calcolo della rete, hash-rate[10], a cui seguirà un parallelo aumento della difficoltà richiesta ai miner per risolvere il problema crittografico.

Infatti, la difficoltà, che esprime la complessità di minare un blocco, cambia in relazione all'intera potenza computazionale della rete, allo scopo che la produzione di ogni blocco avvenga mediamente ogni 10 minuti.

Analizzando il processo da un punto di vista procedurale, ogni qual volta delle transazioni vengono avviate nella rete Bitcoin, e notate dai nodi, se esse non sono considerate contrastanti con altre, vengono inserite in una pool temporanea costituita da transazioni non verificate. Tale pool viene mantenuta da ogni singolo nodo che conserva l'intero storico delle transazioni (blockchain).

Tutti i miner che cercheranno di generare un nuovo blocco, attingono a questa pool prendendo le transazioni non verificate in essa presenti, e inseriscono le transazioni nel nuovo blocco che stanno individualmente lavorando. Ovvero, cercheranno di trovare la soluzione a un difficile problema crittografico, conosciuta come "proof of work", per poter validare il blocco di transazioni e inserirlo nel registro blockchain.

Ogni miner, aggiungendo le transazioni sulla base di criteri come la fee (commissione) associata più alta, cercherà di trovare la soluzione per poter validare il blocco ed incassare la ricompensa associata alla risoluzione del problema.

L'inserimento di blocchi successivi, risolvendo altri puzzle, aumenterà la fiducia e il consenso relativo ai blocchi inseriti precedentemente, visto che ogni nuovo blocco è basato sul blocco precedente, mediante un collegamento a cascata di firme digitali.

Passando all'analisi dei costi che derivano dall'attività di mining, argomento che verrà trattato anche nella successiva sezione, bisogna in primis ricordare che la rete Bitcoin sfrutta la potenza di calcolo derivante dai dispositivi hardware messi a disposizione dai nodi del network.

Inizialmente il mining veniva svolto con l'utilizzo di processori dei normali computer, le CPU, successivamente, questi sono stati sostituiti da schede grafiche 3D simili a quelle utilizzate nei videogiochi. I sistemi di tale tipo più diffusi sono quelli ASICS. Tale passaggio è dovuto al vantaggio, dei secondi sistemi rispetto ai primi, in termini di operazioni compiute per unità di energia consumata. Infatti, tra CPU e schede grafiche 3D lo spread in termini di consumo energetico, per "estrarre" la stessa quantità di bitcoin, è elevatissimo a svantaggio dei primi sistemi.

Sulla base di quanto detto, bisogna aggiungere un secondo elemento di costo nell'attività di estrazione, ossia il consumo energetico. Ma, tale elemento, è soggetto a forti variazioni in funzione del paese in cui si vuole fare mining, lasciando quindi spazi ad arbitraggi geografici.

La descrizione prettamente tecnica dell'attività di mining è rimandata alle seguenti sezioni del capitolo.

[10] Indica il numero di hash calcolati in un secondo (hash/s)

2.4.2 Proof of Work (Funzionamento, sicurezza e impatto energetico)

Come specificato in precedenza, il mining rappresenta l'insieme di operazioni crittografiche svolte dai miner, finalizzate all'approvazione delle transazioni comprese in un blocco, alla validazione dello stesso, e quindi al suo inserimento nel registro blockchain.

All'interno dei metodi volti al raggiungimento del consenso in una rete trustless, la proof of work è sicuramente il principale procedimento alla base dell'attività di mining.

Procedendo ad un'analisi tecnica, l'algoritmo proof of work (POW) può essere definito come un procedimento probabilistico finalizzato alla risoluzione del problema del consenso in una rete decentralizzata. Il raggiungimento del consenso si traduce nella validazione dei blocchi da inserire nella catena.

Nell'algoritmo POW, alla base del mining nel sistema Bitcoin, ogni nodo della rete può esercitare un potere decisionale proporzionale alla potenza di calcolo controllata e messa a disposizione della rete.

Per i partecipanti alla risoluzione del problema, la probabilità di risolverlo prima degli altri, e quindi di aggiungere il nuovo blocco alla catena, è direttamente proporzionale alla potenza di calcolo controllata e impiegata nella risoluzione.

Il consenso si realizza con la risoluzione di un problema informatico-matematico, un puzzle crittografico, la cui soluzione può derivare solamente da un procedimento "brute force", cioè attraverso continui tentativi fino all'ottenimento di una soluzione accettabile. Tali problemi crittografici sono di difficile soluzione, ma, trovata una soluzione è banale verificarne la correttezza.

La risoluzione del problema viene trovata modificando le informazioni presenti nel blocco in modo tale che l'hash calcolato sintetizzando tali informazioni, abbia una forma ben definita, chiamata target, ossia si giunga ad una delle soluzioni del problema. Questo processo si articola sottoponendo ad hashing alcuni campi di informazione che compongono il block header, come illustrato nella Tabella 1, e, affinché l'hash risultante sia valido, deve rispettare alcuni criteri.

BLOCK HEADER	**SIZE (Bytes)**
Version Number	4
Hash Blocco Precedente	32
Merkle Root	32
Time (marcatura temporale)	4
Bits	4
Nonce	4
	TOT. 80

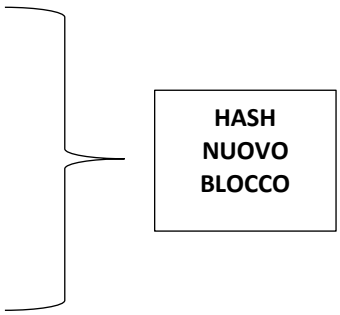


Tabella 1 – Campi da sottoporre ad hashing per generare l'hash del nuovo blocco

Nel caso di Bitcoin, per risolvere il problema crittografico, l'hash risultante dalla sintesi dei dati illustrati nella Tabella 1 deve avere un determinato numero di zeri, consecutivi e iniziali, almeno uguali a quelli che compongono il target, dove quest'ultimo rappresenta la difficoltà del problema crittografico[11].
Prima di chiarire quest'ultimo punto procediamo ad un'analisi dei principali campi di informazioni che devono essere sottoposti ad hashing per la risoluzione del problema crittografico:

- Merkle root

Come precedentemente descritto, esso rappresenta l'hash che sintetizza tutte le transazioni ricomprese nel blocco, inclusa la prima transazione, la "coinbase". È importante sottolineare come il mining di un blocco che contiene una sola transazione, non rende tale processo più semplice o veloce, per cui i miner sono incentivati ad includere un elevato numero di transazioni nel blocco, assicurandosi in questo modo i margini commissionali associati ad ogni operazione.

- Bits

Rappresenta la codifica del target, ossia della difficoltà di risoluzione del problema, intesa come l'ulteriore tempo richiesto per la validazione di un blocco, rispetto a quello in cui la difficoltà è settata al valore minimo, cioè 1.
Affinché un nuovo blocco sia validato e il miner vincitore mostri la soluzione alla rete, la prova del lavoro, è necessario che venga trovato un hash, sintetizzante le informazioni contenute nella Tabella 1, che inizi con un determinato numeri di zeri pari, almeno, a quelli con cui inizia il target.
In altri termini, il target indica lo sforzo computazionale (potenza di calcolo) necessario per la risoluzione del problema crittografico, e quindi l'aggiunta del blocco.

- Nonce

Letteralmente, "numero usato una volta", identifica un parametro che viene modificato tutte le volte che l'hash del blocco ottenuto si discosta dal valore target che permette la risoluzione del problema.
Infatti, in caso di non corrispondenza fra l'hash calcolato e il valore target, l'unico parametro che può essere modificato nei campi informativi del block header è il nonce. Quest'ultimo viene solitamente settato al valore zero e incrementato di volta in volta mentre si calcola la funzione hash del blocco, fino a che non viene trovato un valore hash compatibile con il target assegnato, ossia con un numero di zeri iniziali e consecutivi almeno uguale al target.

[11] Satoshi Nakamoto, "*Bitcoin: A peer to peer electronic cash system*", 2008 – URL: https://bitcoin.org/bitcoin.pdf

Data l'impossibilità di prevedere il valore di hash generato dalla sintesi delle informazioni contenute nel block header, l'unica strada è modificare il parametro nonce, provando tutte le possibili combinazioni, per trovare un hash del blocco che sia compatibile con il target assegnato, in termini di numero di zeri iniziali. In questo processo la difficoltà di risoluzione del problema cresce, in modo esponenziale, all'aumentare del numero di zeri iniziali richiesti dal target.

Per dare un'idea, attualmente nel sistema Bitcoin occorrono in media 2^{68} tentativi per giungere alla soluzione del problema crittografico e quindi "minare" un nuovo blocco.

Chiariamo i concetti espressi con un esempio.

Senza tener conto della reale lunghezza, in termini di bit, delle stringhe che compongono le informazioni sopra descritte, si ipotizzi che il target corrente sia 00000011.

Nel caso in cui un miner, sottoponendo ad hashing le informazioni del block header, ottenga un hash pari ad esempio a 0004p685, la soluzione trovata non sarebbe considerata valida, dato che il target contiene 6 zeri iniziali mentre il risultato solamente 3.

Per ottenere la soluzione valida, il nodo-miner dovrà progressivamente incrementare il parametro nonce, fino a che il risultato dell'algoritmo crittografico hash non inizi con 6 zeri.

Da un punto di vista statistico, trovare un hash che rispetti il target può essere accumunato ad una lotteria, infatti, ad ogni tentativo, realizzato incrementando il nonce, è associata una probabilità di risoluzione del problema costante.

Dunque, il mining è un'attività da realizzare attraverso un procedimento di forza bruta, nel senso di continui tentativi sino al raggiungimento di una soluzione accettabile.

Il funzionamento e le regole alla base del mining, nel sistema Bitcoin, determinano la validazione e l'inserimento nella catena di un nuovo blocco di transazioni in un orizzonte temporale medio di circa 10 minuti, che rappresenta la tempistica prestabilita.

Procediamo ora ad analizzare l'algoritmo "prova di lavoro" sotto il profilo della sicurezza.

La proof of work rende molto difficile, oltre che onerosissimo, la modifica delle transazioni passate già inserite nei blocchi della blockchain. Infatti, la modifica di transazioni pregresse richiederebbe al miner disonesto, intenzionato ad alterare il registro, la dimostrazione di una proof of work valida per ogni blocco successivo a quello modificato.

Per ottenere un esito positivo dall'azione fraudolenta volta a modificare transazioni già verificatesi, un nodo-miner dovrebbe detenere la maggioranza assoluta (51%) della potenza di calcolo dell'intera rete P2P. Controllando la maggioranza del potere di calcolo, è possibile che un determinato miner crei intenzionalmente una biforcazione della catena, il cosiddetto "fork" della blockchain, volto a modificare transazioni pregresse.

Nello specifico, il controllo del 51% del potere computazionale totale, permetterebbe al miner disonesto la risoluzione più rapida dei puzzle crittografici rispetto agli altri nodi del network, consentendogli di creare una catena di blocchi più lunga rispetto alle altre, dopo la biforcazione.

La maggiore lunghezza della catena portata avanti dal nodo disonesto la consacrerebbe come ufficiale, dato che, in caso di fork, la catena dominante o principale risulta essere quella su cui si spesa maggiore potenza di calcolo, e quindi più lunga.

Le blockchain basate sulla proof of work garantiscono un alto livello di sicurezza quando il potere di calcolo è equamente distribuito fra i partecipanti della rete, in caso contrario, come abbiamo esaminato, il rischio è quello di subire un attacco informatico come quello descritto, chiamato "51% Attack". La probabilità associata al rischio di un attacco del genere è chiaramente maggiore nelle blockchain più giovani, caratterizzate da una potenza di calcolo complessiva relativamente bassa, in cui è più semplice raggiungere la maggioranza assoluta di essa.

Anche se verrà trattata nelle successive sezioni, si pensi ad una mining farm, ossia ad un'impresa che possiede moltissimi dispositivi hardware per svolgere l'attività di mining. In tal senso quest'impresa potrebbe sfruttare i vantaggi derivanti dall'economie di scala, conseguendo elevatissimi profitti, a differenza di un miner indipendente proprietario di un solo hardware.

Un altro caso particolare che è importante analizzare è quello che si verifica quando due nodi-miner trovino contemporaneamente due soluzioni valide, anche se diverse, al puzzle crittografico da risolvere. Questo provocherebbe la biforcazione della catena (fork), infatti per un breve periodo esisterebbero due versioni, valide e parallele, della blockchain. In questo particolare caso, la proof of work di Bitcoin permetterebbe la formazione del consenso, stabilendo quale delle due versioni è la catena dominante.

Tecnicamente, in caso di fork, ogni nodo liberamente sceglie una delle due catene di blocchi, utilizzandola come base di partenza per la creazione di nuovi blocchi successivi. Si determina cosi una divisione della potenza computazionale della rete fra le due blockchain concorrenti; decretando come ufficiale la catena che è stata estesa più velocemente, aggiungendo per prima il blocco successivo, poiché su essa è stata impiegata la maggior parte del potere di calcolo dell'intero sistema.

Le transazioni presenti nei blocchi della catena più corta, detta "orfana", se considerate valide (no double spending), torneranno a far parte del pool di transazioni in coda, che verranno incluse successivamente nel blocco da agganciare alla blockchain principale. La catena più corta, detta orfana, non sarà usata da nessun miner come base per inserire altri blocchi di transazioni. Questo è dovuto alla teoria dei giochi, nello specifico ad una situazione in cui ogni giocatore (miner) è convinto che non sia profittevole continuare la blockchain più corta, che, non essendo la versione ufficiale, non permetterebbe di conseguire ricompense e fee. Quest'ultime, nel protocollo Bitcoin, vengono ottenute dal miner, che nel processo competitivo inserisce per primo il blocco successivo alla catena, solo dopo 100 conferme, ossia dopo l'aggiunta di 100 blocchi successivi a quello da lui inserito. A causa dei possibili fork, affinché una transazione possa essere considerata eseguita è fondamentale attendere l'inserimento, nella catena, di un buon numero di blocchi successivi a quello in cui è inclusa la transazione che stiamo esaminando; avendo quindi certezza che essa non venga annullata in caso di fork.

Viene di fatto dimostrato come la probabilità di rimozione di un blocco di transazioni, a causa di una biforcazione della catena, è esponenzialmente ridotta ogni qualvolta viene aggiunto un blocco ad esso

successivo. Nella rete Bitcoin questa probabilità si assume prossima allo zero dopo l'inserimento di circa sei blocchi alla catena, considerando così realmente effettuata la transazione.
A questo punto appare chiaramente più comprensibile come l'attività di mining realizzata con il meccanismo di proof of work rappresenti un procedimento per raggiungere il consenso in una rete trustless.
Procediamo ad analizzare l'impatto energetico dell'attività di mining.
Sicuramente la più grande debolezza dell'algoritmo proof of work è l'elevato consumo di risorse energetiche necessarie al suo funzionamento.
La risoluzione dei problemi crittografici che garantiscono la sicurezza della blockchain comporta un elevato costo energetico, che per molti esperti rappresenta un punto debole in grado di limitare la scalabilità delle blockchain basate su proof of work.
Questo limite ha rappresentato il punto di partenza per lo sviluppo di nuovi algoritmi, impiegati nel procedimento di consenso, più efficienti sotto il profilo energetico, i quali verranno trattati nelle successive due sezioni di questo capitolo.
Ora risulta sicuramente più chiaro il senso della "prova di lavoro", intesa come il meccanismo che consente la soluzione al puzzle crittografico; soluzione da mostrare a tutti i partecipanti della rete, sulla quale si basa il procedimento di consenso nella blockchain. In questa logica il consenso è considerato progressivo poiché i nodi, ai quali viene comunicata la soluzione da parte del miner che ha risolto per primo il puzzle, controllano che il blocco non contenga transazioni tra loro contrastanti e lo confermano ulteriormente utilizzandone l'hash nella produzione del blocco successivo, sviluppando così la catena.

2.4.3 Proof of Stake, un metodo alternativo (Possibili problematiche)

Come esposto nella sezione precedente, in risposta all'inefficienza energetica della proof of work è stato sviluppato un metodo alternativo per il raggiungimento del consenso nella blockchain, l'algoritmo proof of stake, letteralmente "prova che si ha una posta in gioco".
Attraverso questo algoritmo, il consenso nel network viene raggiunto attraverso una votazione svolta tra i suoi partecipanti (nodi)[12].
Ogni nodo ottiene il diritto di voto semplicemente possedendo valuta digitale nella blockchain, e il numero di voti esercitabili è proporzionale alla quantità di criptomoneta posseduta.
Rispetto agli algoritmi di tipo proof of work, quelli proof of stake comportano vantaggi non solo in termini di consumo energetico, elevatissimo nel primo tipo, ma anche in termini di minori tempistiche nella creazione dei blocchi. Questo si deve al fatto che una votazione, rispetto alla risoluzione di problemi

[12] Blokdyk Gerardus, "*Proof-of-Stake: The One Essential Checklist*", 2018

crittografici, necessità di molta meno potenza di calcolo, viene eseguita più rapidamente e garantisce quindi prestazioni più efficienti.

D'altro canto, anche in questo differente metodo per raggiungere il consenso condiviso è presente il rischio di un attacco al sistema, del tipo "Attacco 51%".

Bisogna però far presente che questo tipo di attacco è molto meno probabile rispetto al caso di una blockchain che implementi la proof of work.

Infatti, in un sistema proof of stake il costo dell'attacco sarebbe onerosissimo. Per metterlo in atto un nodo dovrebbe di fatto possedere la maggioranza della crittomoneta in circolazione.

Tale requisito è chiaramente molto più difficile da soddisfare rispetto a quello della proof of work, in cui per condurre un attacco al sistema è sufficiente detenere 51% della potenza computazionale di tutta la rete.

Ma, anche ipotizzando che un nodo arrivi a detenere oltre la metà della crittovaluta in circolazione, la probabilità che egli attacchi la rete rimane molto bassa, poiché sarebbe egli stesso a sopportare il rischio maggiore.

Infatti, l'attacco informatico potrebbe destabilizzare la rete, facendo crollare la fiducia attorno al sistema, con chiarissime e negative conseguenze sul prezzo della crittomoneta.

Se ciò accadesse, il danno maggiore lo subirebbe proprio l'attaccante (nodo disonesto), possedendo la maggioranza della valuta disponibile.

Passiamo all'analisi delle problematiche relative agli algoritmi proof of stake.

Essi, infatti, rispetto a quelli proof of work, sono molto più complessi in termini di sviluppo e implementazione.

Nonostante questa problematica, la questione principale è sicuramente la penalizzazione dei nodi che si comportano in modo disonesto nel processo di consenso.

Prendendo ad esempio il caso in cui avvenga una biforcazione della blockchain, la strategia migliore, che ogni nodo seguirà, è quella di votare entrambe le versioni della catena, data l'assenza di costi da sostenere per partecipare alla votazione.

Viene cosi a verificarsi una situazione di blocco, in cui il raggiungimento del consenso è impossibile, dato che nessuna delle due versioni della catena di blocchi sarà riconosciuta come ufficiale/principale.

È importante ricordare che una situazione del genere non può verificarsi in una blockchain che implementi la proof of work, poiché ogni nodo sceglierà una sola delle due versioni della catena, impiegando le proprie risorse economiche (acquisto di hardware) per risolvere i problemi crittografici relativi alla catena scelta.

Ogni nodo-minatore concentrerebbe quindi la propria potenza di calcolo sulla catena che, secondo lui, ha maggiori probabilità di diventare quella dominante.

2.4.4 Tipologie di Nodi

Fino a questo punto della trattazione, ogni qualvolta è stato usato il termine "nodo", si è fatto riferimento a un qualsiasi partecipante al network peer-to-peer della blockchain, ovvero computer connessi al network. Avendo precedentemente affrontato i concetti più importanti della tecnologia, possiamo procedere ad esaminare le differenze che intercorrono fra i vari partecipanti alla rete, detti, in termini informatici, nodi. Esistono precisamente tre tipologie di nodi:

- Nodo solo Mining
- Nodo Full
- Nodo SPV

La prima categoria di nodi partecipa attivamente alla creazione dei blocchi di transazioni risolvendo dei problemi matematico-informatici. Fra i nodi di mining, quelli che più velocemente risolvono il problema, validando quindi un blocco da aggiungere alla catena, concorrono alla costruzione del consenso e sono quindi ricompensati con unità di crittomoneta, secondo uno schema di incentivi ben stabilito. Ad esempio, nel sistema Bitcoin, come precedentemente detto, la ricompensa del mining assolve anche la funzione di creazione della moneta.

I nodi completi, definiti "full", sono simili ai nodi solo mining, ma rispetto ad essi conservano tutto il registro blockchain, dal blocco genesi (1° blocco) fino all'ultimo blocco inserito nella catena, prima di quello che stanno lavorando per essere validato. Conservano la storia dei blocchi risolti dai miner, e vengono contattati ogni volta che viene avviata una transazione, in modo tale che venga propagata nella rete fino ad arrivare ai miner che, inserendola nel blocco, la confermano.

La terza categoria è quella dei nodi SPV, dove SPV sta per "Simplified Payment Verification" ovvero verifica dei pagamenti semplificata. Questa tipologia di nodi detti anche nodi leggeri, "light node", non custodisce l'intero registro blockchain, ma solo due elementi: l'header dei blocchi e il merkle root. Custodendo solo questi elementi, un nodo SPV si impegnerà a verificare solamente le proprie transazioni, e non tutte quelle avviate nel network. Nel sistema Bitcoin, ogni nodo leggero deve rivolgersi ad un nodo pieno affinché la transazione sia accettata, se non incompatibile con la storia mostrata dalla blockchain, e propagata nella rete. Successivamente i nodi pieni spediscono le transazioni ai miner, affinché le confermino definitivamente inserendole nella blockchain.

2.4.5 Modalità di Mining (Solo – Pool – Cloud)

L'attività di mining, volta alla validazione dei blocchi di transazioni da inserire nella blockchain, può essere svolta secondo 3 principali modalità:

- Solo-Mining

Quando l'attività di mining è svolta individualmente, perseguendo lo scopo di trarre profitto dalle ricompense derivanti dalla validazione dei blocchi e dalle fee associate alle transazioni in essi incluse.
Questa specifica modalità richiede importanti investimenti individuali in termini di dispositivi hardware per detenere un buon livello di potenza di calcolo, e quindi concorrere nel meccanismo competitivo di mining. Chiaramente, ad una maggiore potenza computazionale controllata, corrisponde una maggiore probabilità di risolvere i puzzle crittografici per aggiungere ulteriori blocchi alla catena, traendo così dei profitti. Tuttavia, questa modalità non garantisce flussi di cassa continui nel tempo.

- Pool-Mining

All'opposto del mining individuale, sopra descritto, è possibile compiere questo processo in modo collettivo, unendosi ad esempio ad una mining pool, dove diversi soggetti mettono a disposizione la propria potenza di calcolo, ed i profitti ottenuti vengono suddivisi in base al contributo fornito, in termini di potenza computazionale apportata al pool. Questa modalità, a differenza della prima, permette di partecipare al mining anche non controllando un'elevata capacità di calcolo (hardware), e garantisce flussi di cassa continui nel tempo, anche se di piccolo importo.

- Cloud-Mining

Esistono alcune società, chiamate Mining Farm che spesso, a fronte di un abbonamento, consentono il noleggio di un ammontare determinato di potenza di calcolo dei propri dispositivi hardware per uno specifico periodo. Dunque, il pool mining permette di partecipare all'attività di mining anche non disponendo degli appositi strumenti hardware, eliminando inoltre i problemi di manutenzione e collocazione di tali dispositivi.
In questa modalità i profitti sono commisurati al contributo fornito, sulla base del tipo di contratto sottoscritto.

2.5 Nuove possibilità di finanziamento: Le Initial Coin Offering

Uno dei più recenti sviluppi della blockchain e della cryptocurrencies coinvolge il tema della raccolta fondi per le startup che lavorano in questo ambito o sviluppano soluzioni basate su blockchain.
Dato che si parla di imprese giovani, a volte appena costituite, la raccolta fondi si configura nella forma di Venturing rivolto alle startup.
Per iniziare l'analisi di questa innovativa forma di finanziamento, si può pensare ad una ICO come ad una sorta di IPO (Initial Public Offering) gestita con crittovalute basate su blockchain, nonostante le due tipologie presentino delle sostanziali differenze che verranno successivamente esaminate. Un parallelismo più calzante è sicuramente quello con il mondo del crowdfunding, infatti nelle ICO le nuove imprese si rivolgono direttamente al pubblico di potenziali investitori retailer.
Concretamente, una ICO consiste nella vendita di crittovalute o token digitali, la cui differenza sarà spiegata nella prossima sezione, da parte di un'impresa che ha necessità di raccogliere fondi per sviluppare uno specifico progetto, molto spesso tecnologico[13].
Specifiche quantità di crittovaluta o i token vengono vendute a fronte di un pagamento diretto da parte dell'investitore, che può realizzarsi con moneta avente corso legale, o nella maggior parte dei casi attraverso altra crittovaluta, come bitcoin o ethereum.
Emettendo una crittomoneta o dei token digitali, collegati ad uno specifico progetto, molte startup tecnologiche hanno così espanso le modalità di raccolta di capitali, utilizzando perciò le ICO come l'alternativa più semplice, veloce ed economica rispetto alle modalità tradizionali.
Chiaramente l'andamento del progetto associato alla vendita di criptomoneta determina il futuro della stessa, infatti, nel caso in cui il progetto sia di successo, tutti coloro che hanno investito su di esso otterranno un vantaggio finanziario, vedendo cosi la crittomoneta acquisita conseguire consenso ed affermazione sul mercato. Nel caso negativo in cui il progetto fallisca, gli investitori avranno nel proprio portafoglio una valuta digitale senza valore.
Grazie allo sviluppo tecnologico e alle logiche della blockchain, tramite le ICO è possibile agganciare il valore dell'investimento, ossia della moneta emessa a fronte di un progetto, al valore della comunità che crede in quello specifico progetto.
Come ormai chiaro, la finalità delle ICO è la raccolta di risorse economiche da parte di startup tecnologiche, le quali spesso fissano un ammontare obbiettivo di fondi da raccogliere all'interno di un periodo prefissato. Nel caso in cui l'obbiettivo di raccolta sia raggiunto nel periodo previsto, tali fondi sono utilizzati per portare avanti il progetto dichiarato nel "White Paper" iniziale, in caso contrario, non avendo raggiunto il livello minimo fissato, i fondi vengono restituiti agli investitori, decretando così il fallimento della ICO. Trovandoci all'interno di un settore del tipo "Far West", caratterizzato dalla completa assenza di

[13] *"Fenomeno ICO"* – URL: https://www.blockchain4innovation.it/esperti/fenomeno-ico-punto-opportunita-rischia-truffa/

regolamentazione, uno dei pochi criteri per compiere una valutazione delle varie ICO fra cui scegliere di investire è rappresentato dal "White Paper".
In questo documento la startup interessata a raccogliere capitali tramite ICO inserisce una descrizione del progetto, il business plan, la vision dell'impresa, il funzionamento e le regole della criptovaluta o dei token messi in vendita, il team di sviluppatori e altre informazioni che possono guidare il potenziale investitore in una scelta più consapevole.
Partecipando ad una ICO si entra però in ambito totalmente privo di regolamentazione in cui i casi di truffe o schemi Ponzi sono diffusissimi. il meccanismo delle ICO, infatti espone gli investitori interessati al rischio che l'emittente di crittovaluta persegua obbiettivi disonesti.
Un esempio è la strategia di "Pump e Dump", con la quale l'emittente gonfia il valore della crittomoneta o dei token venduti attraverso dichiarazioni molto positive riguardo il progetto, con la finalità di incrementare considerevolmente la quantità e il prezzo di vendita della moneta digitale. Una volta realizzata la vendita, il prezzo della moneta cadrà a picco, generando perdite fra gli investitori.
A causa delle molte truffe realizzate con il meccanismo delle ICO, molti istituti regolatori e di vigilanza come la SEC o la UK Financial Conduct Authority hanno messo in guardia gli investitori, definendo le ICO come operazioni molto rischiose e speculative, in cui non esiste tutela o protezione per chi vi partecipa.
Un'azione più decisa si è avuta dalla People's Bank of China, la quale nel settembre 2017 ha ufficialmente vietato le ICO, definendole come uno strumento che mette a rischio la stabilità economica e finanziaria, proibendo inoltre alle banche di fornire servizi collegati a questo tipo di operazioni.
Da un altro punto di vista non bisogna criminalizzare il fenomeno. In tal senso basti pensare che ethereum, una fra le principali crittovalute che presenta anche ottime prospettive future, si è finanziata con questo meccanismo.
Per terminare l'analisi generale sulle ICO è importante descrivere come si articola l'operazione, esaminando le fasi che solitamente la compongono:

1. Creazione di un sito Web in cui è descritto il progetto imprenditoriale, spesso basato su blockchain, e la futura ICO.

2. Pubblicazione del White Paper che descrive tecnicamente la ICO, il token digitale che verrà emesso e il progetto nel dettaglio (business plan, business model e altri aspetti tecnici).

3. Realizzare una buona campagna di marketing, in particolare sul Web.

4. Pre-vendita privata dei token, applicando degli sconti rispetto al prezzo in sede di ICO.

5. Pre-vendita pubblica finalizzata a definire precisamente il prezzo in fase di ICO, comprimendo il range di prezzo.

6. Realizzazione della Initial Coin Offering, cioè vendita pubblica dei token digitali.

7. Emissione dei token.

8. Creare un mercato secondario di scambio inserendo tali token in un sito di Exchange, nel quale essi possono essere scambiati con altre crittovalute o con moneta fiat. Quest'ultimo passaggio è subordinato all'affermazione, della valuta digitale emessa, nel mercato e alla fiducia sul loro valore.

2.5.1 Differenza Crittovaluta – Token

Nel descrivere il fenomeno delle ICO si è parlato più volte della vendita di crittomoneta oppure di token per il finanziamento di un progetto. In questa sezione verrà affrontata la differenza che intercorre tra le due tipologie.
Per crittomoneta si intende una "digital coin" che è lanciata e basata su una propria tecnologia blockchain nativa, definita in tal senso: blockchain proprietaria.
È questo il caso di bitcoin, che si appoggia sulla propria blockchain proprietaria, che, nata insieme alla crittovaluta, ne regola il funzionamento.
I token, invece, sono delle unità secondarie, cioè degli asset che si appoggiano su una blockchain già esistente, né nativa né proprietaria.
Ad esempio, esistono ad oggi migliaia di token basati sulla tecnologia utilizzata da altre criptovalute. Moltissimi di questi utilizzano la blockchain Bitcoin, ma soprattutto quella di Ethereum. Questo è molto frequente nelle operazioni di ICO in cui vengo rilasciati dei token, aventi proprio nome e valore, ma gestiti sulla blockchain di altre criptomonete, non potendo quindi essere definiti tali.
Inoltre, poiché le modalità attraverso cui i token vengono generati e rilasciati sono previamente stabilite, a differenza di quanto avviene per le criptovalute, come il Bitcoin, non possono essere minati, ovvero non possono essere "estrarre" ulteriori unità.
All'interno della categoria token esistono 3 differenti tipologie:

- <u>Token di pagamento</u>

In questa categoria sono inclusi i token che vengono accettati come mezzo di pagamento per l'acquisto di beni e servizi. Questa categoria è molto simile alle crittovalute come il bitcoin con la differenza che non utilizzano una propria blockchain proprietaria.

- Utility Token

Letteralmente token di utilizzo, permettono di acquistare ed usufruire di servizi o prodotti realizzati dalla stessa impresa che li ha emessi in sede di ICO, escludendo quindi la finalità di natura monetaria.

- Security Token

La terza categoria rappresenta un vero strumento finanziario come le obbligazioni e le azioni. I token d'investimento rappresentano quindi una partecipazione nella società emittente in termini di diritti di voto, dividendi come percentuale degli utili oppure tassi di interesse.
L'emissione di questa categoria di token, assoggettata alla disciplina per l'emissione di strumenti finanziari, è severamente vietata dalle autorità finanziarie di molti paesi a causa della bassa trasparenza di tali operazioni.

2.5.2 Un'Alternativa al Venture Capital e alla perdita di controllo

Le ICO rappresentano un rivoluzionario strumento di raccolta fondi per startup innovative, che sta stravolgendo le modalità tradizionali di finanziamento per questo tipo di imprese.
Infatti, affianco alle forme tradizionali di finanziamento, equity e debito, l'emissione di crittomonete o token sta diventando una modalità sempre più diffusa, basti pensare che attualmente le cryptocurrencies presenti sul mercato[14] sono oltre 1200, e molte di queste derivano da recenti ICO.
Attraverso le ICO si potrebbero di fatto evitare le innumerevoli regole, requisiti e processi di valutazione richiesti per ottenere fondi da banche o dai Venture Capitalist.
Nell'ottica delle imprese tecnologiche di nuova costituzione, il finanziamento tramite debito, ad esempio attraverso il canale bancario, è spesso proibitivo. Questo è dovuto al fatto che tali startup, nella maggior parte dei casi, operano in ambiti molto volatili e non hanno raggiunto la necessaria massa critica per ottenere finanziamenti a condizioni vantaggiose.
Dal lato equity, l'impatto sicuramente maggiore da parte delle ICO si ha avuto sui fondi di Venture Capital e sugli investitori individuali che operano nel comparto Venturing, come gli angel investor.
Per rendersi conto di questo impatto basti pensare che, nel terzo trimestre del 2017, i finanziamenti ottenuti tramite ICO di startup blockchain ammontavano ad oltre 1,3 miliardi di dollari, cifra 5 volte superiore agli investimenti realizzati da fondi di Venture Capital in questo comparto.

[14] Dati CoinMarketCap – URL: https://coinmarketcap.com/

Questo rapporto è mostrato dalla Figura 9, nella quale vengono raffrontati gli investimenti in equity dei Venture Capital con quelli realizzati tramite ICO.

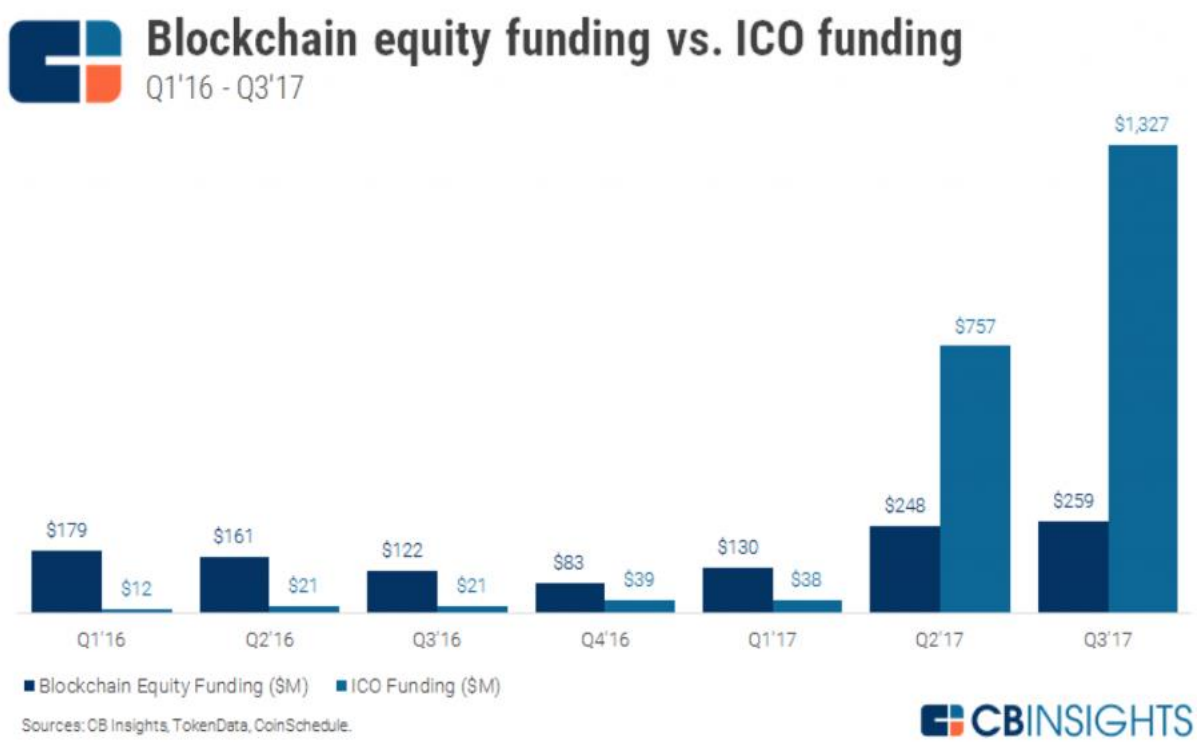


Figura 9 - Investimenti Venture Capital VS ICO Funding

Dal grafico si evince chiaramente come già nella fine del 2017 molte startup innovative, nel campo blockchain, preferiscano finanziarsi tramite ICO piuttosto che dai classici fondi di Venturing, che tradizionalmente rappresentano la principale fonte di finanziamento per le nuove società.

Uno dei motivi di questo passaggio è sicuramente l'assenza di regolamentazione. Infatti, con le ICO si possono ottenere risorse economiche senza dover passare attraverso le regolamentazioni che disciplinano la raccolta dei fondi da investire da parte dei Venture Capital.

La mancanza di regolamentazione si è tradotta in una vendita molto aggressiva di criptovalute tramite ICO, in termini di numerosità e modalità.

Nonostante questo, la motivazione che più di tutte sta determinando il passaggio dai Venture capital alle ICO per ottenere fondi, è relativa al concetto di controllo.

Quando un fondo di VC acquisisce le azioni di una startup, inserendola nel proprio portafoglio di investimenti, la finalità è esercitare il controllo sull'impresa, attraverso ad esempio la nomina di diverse cariche amministrative.

Lo scopo è quello di controllare e gestire l'impresa per migliorarne il business, al fine di poter rivendere le azioni, in sede di way out, ad un prezzo maggiore di quello a cui sono state acquistate nella fase di investimento del fondo.

Attraverso le ICO, invece vengono vendute monete digitali per finanziare un determinato progetto corporate, senza dover cedere le azioni della società, mantenendone quindi la proprietà e soprattutto il controllo. Questo meccanismo, quindi, rappresenta una grande opportunità per le startup e i suoi imprenditori, i quali possono così evitare diluizioni nella proprietà, riduzioni dei diritti di voto, e di fornire tutele per gli investitori.
Proprio l'assenza di regolamentazione e la tutela per gli investitori, oltre che l'altissimo rischio, rappresentano il punto critico delle ICO, che nella maggior parte dei casi si rivelano essere legate a progetti non meritevoli, con una percentuale superiore al 90%.

2.5.3 Differenze con le Initial Public Offering

Dal punto di vista delle finalità, c'è una forte convergenza tra ICO e IPO, sotto altri aspetti ci sono delle differenze sostanziali.
Una Initial Public Offering rappresenta l'operazione con cui una società chiusa o semi chiusa, entra a far parte dei mercati borsistici quotandosi in borsa per la prima volta.
Questa operazione consiste in una sollecitazione al pubblico risparmio, che, per essere eseguita, richiede la conformità a moltissime regole dei mercati finanziari. Di fatto per compiere una IPO è necessario soddisfare diversi requisiti, in termini di, condizioni patrimoniali, capitalizzazione, requisiti di governance, informativa al mercato, e molti altri.
Il rispetto di tale regole, volte alla tutela degli investitori, è garantito dal controllo fornito da un'autorità di vigilanza, che in Italia è rappresentata dalla CONSOB, la quale vigila sulla correttezza delle transazioni e sulle operazioni delle imprese coinvolte.
Per le ICO, invece, non esiste ancora un istituto di vigilanza che eserciti una funzione di controllo. Questo determina un mercato totalmente non regolamentato e caratterizzato da un altissimo coefficiente di rischio associato agli investimenti in esso effettuati.

2.5.4 Le Hot ICOs (Caso Telegram)

Come detto nelle precedenti sezioni, il fenomeno delle ICO si sta diffondendo in tutto il mondo, portando il numero delle crittovalute presenti sul mercato a livelli difficilmente prevedibili fino a poco tempo fa.
Il titolo della sezione deriva da un personale parallelismo fra determinate ICO e alcune quotazioni in borsa di maggior successo, caratterizzate da una domanda di azioni da parte del pubblico di gran lunga superiore a quelle offerte dalla società emittente, dette per questo motivo Hot IPOs.
Tra le varie Initial Coin Offering avvenute negli ultimi anni, ce ne sono alcune che hanno rappresentato un vero successo, sia in termini di progetti ad esse associati, sia per quanto riguarda i capitali raccolti.
In quest'ambito non può che farsi riferimento a una fra le più importanti ICO della storia, ossia, quella che ha lanciato sul mercato Ethereum nel 2014, la seconda criptomoneta per importanza dopo il Bitcoin.
La ICO, vendendo la crittomoneta che finanziava il progetto, su essa basato, raccolse, in un solo mese e mezzo, 18,4 milioni di dollari.
Proseguendo, fra le ICO monstre sono da citare quella di Tezos e quella di Filecoin.
La prima rappresenta un progetto volto a realizzare un'infrastruttura di Information Technology Management, che ha raccolto presso il pubblico 232 milioni di dollari di finanziamento. Di questi fondi, una parte, 50 milioni, sono stati utilizzati per costituire un fondo volto a supportare ed a investire nelle nuove iniziative che utilizzano la piattaforma Tezos.
Un secondo esempio è quello di Filecoin, promosso da una startup americana chiamata Protocol Labs Inc., che ha progettato una piattaforma che consente lo storage distribuito di file, ottenendo in sede di ICO 257 milioni di dollari. Il token Filecoin associato al progetto permette l'acquisto di spazio di archiviazione sulla piattaforma, inquadrandosi così, come un utility token.
Un esempio più recente, e per certi versi controverso, è sicuramente quello di Telegram.
Uno degli eventi più attesi dal vasto pubblico di investitori del mondo crypto durante il 2018 è con certezza la ICO di Telegram, famosa piattaforma di messaggistica istantanea online. Eppure, nel mese di maggio, il Wall Street Journal[15] ha riportato che, molto probabilmente, non sarà condotta nessuna ICO pubblica, dato che in sede di pre-sale privata sono stati raccolti oltre 1,7 miliardi di dollari.
Tale ripensamento è avvenuto nonostante molte indiscrezioni attribuissero alla ICO di Telegram un target di fondi pari a 5 miliardi, da raccogliere tramite vendite private ed una ICO pubblica.
Il progetto di Telegram, su cui si basa la ICO, concerne la realizzazione di un sistema di messaggistica rivoluzionario e decentralizzato, che teoricamente si configurerebbe come un'opzione alternativa a Visa e Mastercard, all'interno dell'economia decentralizzata. Infatti, il progetto Telegram Open Network (TON) è finalizzato alla progettazione di un protocollo blockchain per lo sviluppo di applicazioni e contenuti, che potranno essere acquistati con la crittovaluta precedentemente emessa e venduta per finanziare il progetto.

[15] The Wall Street Journal, *"ICO"* – URL: https://www.wsj.com/articles/telegram-messaging-app-scraps-plans-for-public-coin-offering-1525281933?mod=searchresults&page=1&pos=1

Il token emesso, chiamato Gram, permetterà, oltre che a compiere un investimento con la speranza che il progetto abbia successo, anche di acquisire i contenuti che saranno realizzati e venduti nel marketplace della piattaforma Telegram.
Nonostante questa ICO sia stata un evento molto atteso dall'inizio del 2018, i dettagli ufficiali sono realmente pochi, a differenza dei rumors. Tuttavia, alcuni documenti depositati presso la SEC (Securities and Exchange Commission) mostrano come, tra gennaio e marzo, siano stati effettuati due cicli di investimenti, che hanno permesso al progetto di raccogliere 1,7 miliardi di dollari.
Basandosi sulle informazioni reperibili, la vendita dei token è stata limitata a meno di 200 investitori, fra istituzionali e privati con alto patrimonio, come il miliardario russo Roman Abramovich.
La vendita, riportata alla SEC, è stata realizzata ai sensi dell'articolo 506 del regolamento D del Securities Act, il quale permette alle società di vendere titoli non registrati attraverso una vendita ai soli investitori qualificati.
La marcia indietro dell'azienda sulla relativa vendita pubblica dei token, chiamati Gram, molto probabilmente, è dovuta alla stringente regolamentazione in atto, oltre che ai controlli intensi da parte della SEC relativamente al tema ICO.
Motivazioni che, quasi con certezza, hanno fatto tentennare Telegram riguardo la vendita pubblica, fino a culminare nella quasi certa cancellazione della ICO.

2.6 Vantaggi e criticità della Blockchain

Avendo fornito una completa panoramica sul funzionamento, caratteristiche ed applicazioni della blockchain, nella presente sezione verranno schematicamente descritti i punti di forza e quelli deboli della tecnologia.
Iniziamo descrivendo i vantaggi:

- Trasparenza

Rispetto ai registri attuali, un database basato su blockchain garantisce una maggiore trasparenza. Questo è dovuto al fatto che ogni cambiamento avvenuto nel registro, ad esempio l'aggiunta di un blocco di transazioni, è visibile da tutti gli utenti sulla rete, e le informazioni presenti nella catena non possono essere rimosse o alterate, a differenza di quanto potrebbe accadere in un registro gestito centralmente.

- Eliminazione degli Intermediari

Nel sistema tradizionale, molte operazioni e transazioni hanno bisogno della presenza di un intermediario affinché sia garantita fiducia e sicurezza del sistema. Un vantaggio della tecnologia blockchain è proprio l'eliminazione degli intermediari, che si realizza, ad esempio, permettendo a due individui di avviare direttamente una transazione senza coinvolgere una terza parte, cosa che accade nelle crittovalute come il bitcoin. Questo sistema rappresenta un'ottima alternativa nei contesti caratterizzati da bassa fiducia negli intermediari, ad esempio a causa della corruzione.

- Decentralizzazione

Questa caratteristica permette che la blockchain sia mantenuta su un unico registro condiviso, quindi leggibile da tutti gli utenti della rete, a differenza dei tradizionali registri multipli gestiti privatamente da diverse istituzioni. Essi, infatti, richiedono di porre fiducia nell'ente che lo custodisce.

- Fiducia

Come precedentemente trattato, il sistema di transazioni attuale, richiede di prestare fiducia in un intermediario che realizzi il processo. Con il meccanismo della Proof of Work utilizzato dalla blockchain di Bitcoin, il processo di consenso volto a stabilire la fiducia nel sistema, è totalmente decentralizzato e democratico. La fiducia in questo sistema non è garantita da un ente terzo, ma bensì da un insieme di regole crittografiche, accettate e condivise fra gli utenti che vi partecipano.

- Sicurezza

I dati che vengono inseriti nella blockchain sono immutabili, ossia non possono essere alterati o cambiati. Tutti i computer sulla rete hanno una copia aggiornata della blockchain, riducendo quindi il rischio di una perdita di dati. Per manipolarli, infatti, sarebbe necessario hackerare oltre il 50% dei computer sulla rete nello stesso istante, il che rende l'attacco informatico quasi impossibile. Inoltre, ogni blocco di dati presente nella catena, può essere tracciato all'indietro fino al primo blocco, definito blocco genesi, grazie alla catena di firme digitali che collegano ogni blocco con il precedente e il successivo. Il tracciamento a ritroso,

definito backward induction, rappresenta il percorso da seguire per ricostruire tutte le transazioni della blockchain.
È da aggiungere che la sicurezza di questa tecnologia non è perfetta, ma è sicuramente maggiore di molti sistemi tradizionali attualmente usati.

- Riduzione dei Costi

Risulta chiaro come il processo di disintermediazione, portato avanti dall'implementazione di questa tecnologia, concorra fortemente nella riduzione dei costi associati alle transazioni. Infatti, un aumento dei livelli di intermediazione comporta un incremento nel costo del processo.

- Aumento della Velocità nelle Transazioni

I registri basati su blockchain, a differenza dei database tradizionali, sono in grado di registrare le transazioni in maniera istantanea. All'opposto, utilizzando un classico strumento di pagamento come il bonifico, le disponibilità da inviare verranno decurtate dal conto del pagante e non saranno trasferite a quello del beneficiario prima di qualche giorno.

Avendo descritto i principali vantaggi, procediamo ad analizzare le criticità della blockchain[16]:

- Mancanza di Privacy

Anche se in molte crittovalute basate su blockchain l'anonimato sembra essere uno dei punti di forza, è dimostrabile il contrario.
Nel sistema Bitcoin ad esempio, tutte le informazioni sulle transazioni sono facilmente accessibili in ogni momento a tutti i partecipanti al network; e scoprire l'identità di un account, una volta che si è ricevuto da esso un pagamento, è relativamente semplice.
Per chiarire utilizziamo un esempio.
Se un soggetto facesse un acquisto con i suoi bitcoin in un negozio fisico, il negoziante sarebbe in grado di leggere la transazione sulla blockchain.

[16] Steve Wilson, "*Oltre l'Hype: Comprendere gli anelli deboli della Blockchain*", 2017

Le informazioni sulla transazione indicherebbero il portafoglio (wallet) da cui sono stati inviati i bitcoin.
La conoscenza dell'indirizzo bitcoin del pagante, permetterebbe al commerciante di leggere il suo saldo e tutte le transazioni in entrata e in uscita che hanno interessato quell'account.
Questo determina una effettiva mancanza di privacy, che si manifesta soprattutto negli acquisti effettuati fisicamente, ossia quelli in cui è possibile collegare l'identità di un soggetto al suo account bitcoin, e quindi conoscere le transazioni effettuate o ricevute. È da aggiungere che esistono blockchain che assicurino maggiore privacy nelle transazioni, ma non è questo il caso di Bitcoin o Ethereum.

- Sicurezza

Attraverso l'utilizzo della crittografia asimmetrica, con la blockchain viene assolta la sua funzione di sicurezza del sistema.
Ogni partecipante, infatti, ha due chiavi, una pubblica ed una privata. Mentre la prima consente solamente di vedere il proprio saldo in crittovaluta, la chiave privata invece consente di disporre dell'ammontare di valuta posseduta, ad esempio per un pagamento.
Paradossalmente l'elevata sicurezza di questo sistema può rappresentare un ostacolo alla sicurezza stessa. Si pensi in tal caso alle moltissime persone, che perdendo le loro chiavi d'accesso, non hanno più la disponibilità della loro moneta digitale.
Rispetto ai conti correnti tradizionali, in cui in caso di smarrimento della password dell'online banking o del codice della carta di credito, basta provare la propria identità per ottenerli, nelle crittomonete basate su blockchain questo non è possibile.
Infatti, smarrendo la propria chiave privata, un utente bitcoin perderebbe definitivamente l'accesso ai suoi fondi, poiché essa non può essere resettata.
Lo stesso ragionamento va applicato anche alle frodi.
Si pensi al caso in cui un soggetto conoscendo il codice e i dati della vostra carta di credito, prelevi o spenda vostre disponibilità. In questo caso basta contattare la banca per bloccare la carta di credito, ed evitare altre operazioni non autorizzate.
Nelle crittovalute basate su blockchain, invece, le transazioni non possono essere alterate o annullate, e non esiste nessun intermediario che offra tutela in caso subiate delle frodi.
Se vengono inviati ad esempio dei bitcoin ad un indirizzo (portafoglio) errato della blockchain, quelle disponibilità devono essere considerate perse.
Così come se qualcuno scoprisse la vostra chiave privata, potrebbe prelevare tutte le crittomonete presenti sul conto, senza che vi sia possibilità, per la parte lesa, di annullare l'operazione o chiedere un rimborso.

- Assenza di un Controllo Centralizzato

I sistemi blockchain sono ideati per rimuovere gli intermediari, attribuendo la responsabilità e il controllo ai partecipanti della rete. Il controllo è di fatto affidato alla maggioranza delle persone presenti nel network, attribuendogli quindi un'accezione democratica.
Nelle reti tradizionali, se un'organizzazione volesse apportare un cambiamento, dovrebbe prima ottenere l'approvazione da parte dei suoi dipartimenti. In un network blockchain, come quello di bitcoin, eventuali cambiamenti dovranno essere accettati dalla maggioranza del potere computazionale del network. Tale maggioranza non è facilmente ottenibile, e un esempio di ciò è la divisione avvenuta sulla rete Bitcoin riguardo dei cambiamenti al protocollo, argomento che verrà approfonditamente esaminato nel capitolo successivo.

- Rischio di attacco 51%

Nel contesto degli attacchi informatici è importante citare quanto detto da Robert Sams, fondatore e AD di Clearmatics: "Nei mercati finanziari c'è sempre un meccanismo per correggere un attacco. In una blockchain non c'è un meccanismo per correggerlo, le persone devono accettarlo."
Secondo molti esperti, invece, la blockchain è stata ideata per prevenire molti attacchi informatici come quello della doppia spesa del denaro elettronico, senza ricorrere a un'autorità centrale.
Ricollegandoci al concetto di controllo, se un nodo del network controllasse oltre il 50% del potere di calcolo dell'intera rete, sarebbe in grado di modificare il registro, ad esempio eliminando alcune transazioni o spendendo due volte la stessa unità di crittovaluta.
Nonostante sia molto difficile controllare il 51% del potere di calcolo della rete, va sottolineato come esistono grandissime farm di mining in Russia e Cina, le quali controllano singolarmente un grandissimo potere computazionale. Mettendo insieme la loro potenza di calcolo, potrebbero potenzialmente controllare e manipolare la blockchain.

- Early Stage della Tecnologia

I sistemi basati su blockchain, rappresentano una tecnologia nuova, applicata principalmente alle crittovalute. Mancano quindi altre applicazioni al mondo reale che consacrerebbero la validità della tecnologia. Infatti, nonostante il grandissimo potenziale racchiuso nella blockchain, nulla assicura che verrà preferita alle opzioni tecnologiche esistenti. Stessa cosa successe al sistema di videoregistrazione magnetica

Betamax, sviluppato da Sony, al quale venne preferito dai consumatori il VHS, nonostante sia tecnicamente inferiore.

- Costo

Come descritto nella sezione dedicata alla proof of work, la risoluzione dei problemi crittografici per la validazione di un blocco di transazioni, da un punto di vista computazionale-energetico, è onerosissima.
L'elevato costo è dato sia dall'alto prezzo dei dispositivi hardware finalizzati all'attività di mining, sia dalla grandissima componente energetica richiesta, ossia la corrente consumata in tali processi.

- Limiti di Scalabilità

Considerando che la difficoltà di risoluzione dei problemi crittografici nella rete Bitcoin cresce nel tempo, potendo minare moneta fino al limite di 21 milioni di unità, questo determina chiaramente un incremento nel consumo di elettricità nell'attività di mining.
Tralasciando questo fattore, al tasso di consumo attuale di energia, il costo dell'elettricità necessaria per far funzionare una blockchain che utilizza l'algoritmo proof of work, rende impossibile gestire un numero di transazioni pari a quello delle grandi compagnie di carte di credito, come Visa o Mastercard.

- Reputazione e Regolamentazione

La totale assenza di regolamentazione unita ad un sentiment negativo da parte dei potenziali utilizzatori, possono rappresentare un grande freno per l'affermazione della blockchain.
Infatti, essa è troppo spesso associata, soprattutto da chi non è del settore, alla crittovaluta Bitcoin, generando un effetto boomerang.
Questo è dovuto all'associazione delle crittovalute, specialmente bitcoin, ai mercati del crimine, a causa della garanzia di anonimato. Traslando le insicurezze relative al sistema Bitcoin e le sue pecche alla blockchain, non solo non si capisce a fondo la tecnologia, ma soprattutto si creerebbero luoghi comuni che contrasterebbero la sua affermazione.

2.7 Applicazioni e Prospettive della Blockchain

Come menzionato nella prima parte del capitolo, la blockchain, con il rilascio di Bitcoin, ha trovato nelle transazioni la sua prima e principale applicazione.

Attraverso la Distributed Ledger Transaction, infatti, è consentito ad ogni transazione di essere iniziata e completata direttamente fra due individui tramite internet, senza la necessità di un ente certificatore centrale al quale demandare fiducia e consenso del sistema. Ma, l'impiego nelle transazioni rappresenta solo uno dei possibili utilizzi, all'interno del vasto ventaglio di applicazioni offerto dalla blockchain.

Per comprendere l'ampiezza applicativa di tale tecnologia, bisogna pensare a tutti quei contesti in cui si formano due categorie di soggetti: controllanti e controllati.

Le due categorie sopra citate fanno riferimento ad un sistema chiaramente centralizzato, che rimanda l'affidabilità, la fiducia e la sicurezza del sistema stesso ad un ente sovraordinato, rappresentato dai controllori.

Ricordando che la blockchain, basata ad esempio su proof of work, permette di realizzare un registro condiviso e leggibile da tutti, in cui la fiducia e il consenso sono raggiunti attraverso un procedimento decentralizzato, appare chiaro come questo sistema, in molti casi, possa sostituire quelli centralizzati, superando la dicotomia fra controllori e controllati, a favore di un meccanismo più democratico, in cui ogni soggetto concorre attivamente per conseguire la fiducia e il consenso nel sistema.

Le prospettive di utilizzo della blockchain, non riducendosi al comparto delle transazioni, abbracciano un vasto insieme di possibili campi applicativi, nei quali, in un futuro prossimo, questa tecnologia sarà disruptive. (Figura 10)

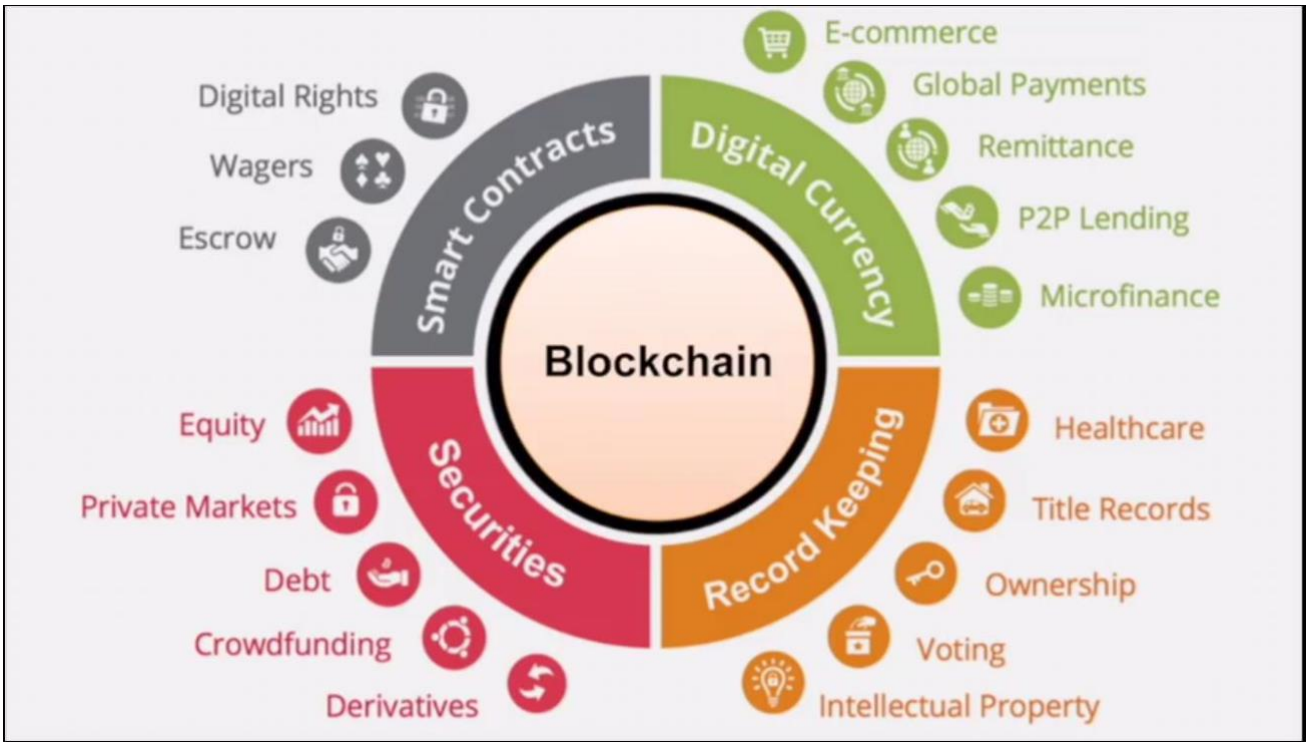


Figura 10 - Potenziali Applicazioni della Blockchain

Sulla base delle valutazioni compiute dai maggiori esperti nel comparto blockchain, procediamo ad analizzare i settori in cui, prospetticamente, l'implementazione di tale tecnologia avrà i maggiori impatti[17]:

- Settori Finanziari

Un esempio classico di mercati, caratterizzati da un sistema centralizzato, sono quelli finanziari.
In essi infatti sono sempre presenti autorità pubbliche e/o private che conducono un processo di validazione, volto a stabilire la legittimità delle azioni messe in atto, assolvendo quindi una funzione di garanzia e fiducia nel sistema. In questi settori, la blockchain può rappresentare una vera minaccia a causa della sua capacità di disintermediare processi tradizionalmente intermediati, portando alla scomparsa di molti ruoli che, ad oggi, sembrano imprescindibili. Un esempio di questo è il comparto bancario, il quale perderebbe il suo primato nelle transazioni, in termini di intermediazione, se esse avvenissero in modo decentralizzato tramite le criptovalute. D'altro canto, sono da riconoscere anche i grandi vantaggi che la blockchain comporterebbe nel comparto finanziario riguardo l'efficienza nei processi, in termini di velocità e costi.
Celebre è il caso di Ripple Lab, argomento che sarà esaminato nell'ultimo capitolo, che con la sua crittovaluta sta rivoluzionando gli scambi e i rapporti interbancari.
Oltre al caso già analizzato di NASDAQ Linq, dove viene impiegata la blockchain nelle transazioni azionarie e obbligazionarie, la tecnologia più aiutare il comparto bancario e assicurativo nel creare un'identità digitale del cliente, immagazzinando ogni informazione in un registro immutabile e condiviso. Permettendo quindi di generare un profilo di rischio da valutare ad esempio durante la concessione di un mutuo oppure per stipulare un contratto assicurativo.
Un rilevante caso di investimento su blockchain e crittovalute, da parte del sistema bancario, è sicuramente quello di Goldman Sachs[18]. La più grande banca d'affari del mondo, infatti, tramite la società Circle, da essa controllata, ha acquistato per 400 milioni di dollari Polinex, Exchange storico di Bitcoin, ovvero una borsa d'Affari dove gli utenti comprano e vendono BTC, Ethereum ed altre criptovalute, ma anche dollari, euro ed altre valute tradizionali. L'obiettivo dell'investimento, compiuto dalla banca d'affari, è ottenere una posizione dominante nel mondo crypto, come dichiarato dall'attuale direttore degli investimenti, il quale, nonostante ciò, identifica nelle crittovalute una bolla finanziaria.
Un altro settore finanziario che sarà investito dall'ondata innovatrice della blockchain è quello del crowdfunding. In esso, infatti, la rivoluzione consiste nell'eliminare l'ente centrale necessario ad abilitare la campagna di crowdfunding, ad esempio Kickstarter, permettendo alle startup di finanziarsi in autonomia, come avviene nelle ICO.

[17] Report UBS, "*Cryptocurrencies, Beneath The Bubble*", 12 October 2017 – URL: https://www.ubs.com/magazines/wma/insights/en/investing/2017/beneath-the-bubble.html

[18] *"Banche e Criptovalute: Goldman Sachs acquista un exchange Bitcoin per 400 milioni di dollari",* EconomyUp – 2018

- Smart Contract

I settori che verranno regolati dagli innovativi "contratti digitali e intelligenti" sono moltissimi. Nonostante il tema degli smart contract sarà affrontato nell'ultimo capitolo, trattando la crittomoneta Ethereum, introduciamo in questa sede alcuni tra i concetti fondamentali.
Per smart contract, si intende un particolare contratto informatico, creato e gestito sulla rete, che si attiva automaticamente e diventa efficace al verificarsi di situazioni ricomprese fra le sue clausole, senza la necessità che le parti diano un input per attivarlo, e senza possibilità di truffe.
Requisito fondamentale nei contratti tradizionali è la fiducia reciproca, ossia che ognuna delle due parti rispetti l'obbligazione assunta.
Con gli smart contract, invece, la fiducia non deriva dalla certezza dell'impegno della controparte, ma è data dall'esecuzione programmata, informatica e automatica del contratto, la quale non è soggetta a discrezionalità.
Gli smart contract gestiti tramite una piattaforma blockchain, rappresentano quindi dei codici informatici, che garantendo la certezza d'esecuzione, può essere utilizzato non solo nelle transazioni valutarie, ma in tutte quelle in cui avvenga un qualsiasi tipo di passaggio di proprietà.

- Smart Property e Diritti Digitali

La blockchain può essere utilizzata come un database, un inventario, dove tenere traccia di ogni tipo di transazione o informazione, disciplinando e registrando quelle che hanno ad oggetto sia asset tangibili (es. valute, immobili), sia asset intangibili come le proprietà intellettuali.
Le proprietà, codificate tramite il registro blockchain, diventano così smart property, che possono essere quindi gestite e trasferite attraverso gli smart contract.
Parlando di diritti come quello del copyright, applicato a musica e libri, esso può essere digitalmente registrato con un protocollo blockchain, permettendo a chiunque di controllare la proprietà dello specifico diritto, e al titolare la possibilità di trasferirlo, cedendo la propria chiave privata a cui è associato il digital right. In questo ambito è interessante citare l'acquisto di Mediachain da parte di Spotify, colosso nella musica digitale, che ha permesso la realizzazione di un registro blockchain per una gestione più trasparente ed efficiente delle royalty, pagate agli artisti per la loro musica.
Un altro esempio di gestione "digital" delle proprietà è quello di un finanziamento per l'acquisto di un veicolo, un semplice caso di leasing finanziario.
Potrebbe, infatti, essere regolato da uno smart contract, che subordinerebbe automaticamente il trasferimento della proprietà del veicolo, dalla compagnia finanziatrice al soggetto finanziato, al pagamento dell'ultima rata prevista nel contratto di leasing.

Un'altra considerazione, relativamente agli asset fisici, può essere fatta per gli immobili, le cui transazioni sono caratterizzate da una pesante burocrazia.
Infatti, la gestione degli atti notarili, e degli altri documenti, potrebbe avvenire tramite un database blockchain, aumentando così velocità e trasparenza delle compravendite immobiliari e riducendo i costi di transazione associati.
Il registro condiviso potrebbe quindi funzionare come un catasto, nel quale, senza la necessità di un ente certificatore, possono essere registrati gli atti di proprietà, le compravendite, i permessi edilizi e tutti gli altri documenti attualmente gestiti dalle pubbliche amministrazioni.

- Gestione Digitale dell'Identità

Anche in questo contesto la realizzazione di un registro condiviso, immutabile e sicuro, grazie alla crittografia, permetterebbe una più efficiente gestione digitale. Questo è dovuto alla vulnerabilità dei database centralizzati agli attacchi informatici, che consentono l'accesso a tutti i dati dei clienti salvati nel sistema, come ad esempio l'identità online.
Invece, un sistema di identificazione basato su blockchain, permetterebbe, con le firme digitali derivanti dalla crittografia, una gestione più sicura ed inoppugnabile delle identità digitali. Quest'applicazione tecnologica è in fase di sviluppo da parte di varie imprese e governi, come quello dell'Estonia, che potrebbero estendere la gestione decentralizzata oltre che alle identità digitali anche a patenti di guida, passaporti, certificati di nascita e matrimonio.

- Voto Digitale

Continuando il ragionamento usato per le identità digitali, mediante un registro blockchain risulta semplice autenticare l'identità di un determinato soggetto per una serie di altre operazioni online, come ad esempio per il voto digitale.
L'applicazione di quest'ultimo è fallita in molti paesi a causa dei rischi sulla sicurezza e sulla privacy. Tra gli stati che hanno provato a rendere digitale il tradizionale processo di voto sono da citare Danimarca, Norvegia ed Estonia. Ma, solo quest'ultimo, è riuscito a realizzare un voto digitale su larga scala con successo. Attraverso un meccanismo di voto basato su blockchain, verrebbe data a qualsiasi elettore la possibilità di controllare l'effettiva ricezione del suo voto, consentendogli di mantenere anonimato e privacy. Inoltre, questo renderebbe accessibile il voto a molte più persone, aumentando potenzialmente la partecipazione dei cittadini al processo politico.

- Sharing Economy

L'economia della condivisione si sta configurando, negli ultimi anni, come un paradigma sempre più accettato e diffuso. Si pensi, in questo contesto, ai servizi di ride-sharing come Uber, oppure a quelli home-sharing come Airbnb. Tuttavia, nelle più note piattaforme di sharing, vi è la presenza di un intermediario in tutte le interazioni e transazioni.
Con l'implementazione della tecnologia blockchain, che ben si adatta alle logiche dell'economia condivisa, sarebbe possibile eliminare ogni tipo di intermediario, permettendo la creazione di app, basate sullo sharing, totalmente decentralizzate.
In particolare, la blockchain garantirebbe l'integrità e la veridicità delle recensioni, discriminante fondamentale nella scelta d'acquisto, rendendole immodificabili.

- Servizi Pubblici (Utilities)

Oltre ai servizi pubblici come la gestione delle identità digitali o al catasto, le applicazioni della blockchain, potrebbero essere estese anche alle utilities, come la fornitura energetica. In futuro, infatti, potrebbero essere realizzate delle reti intelligenti che permetterebbero alle famiglie, oltre a consumare energia sulla base delle proprie esigenze, anche di vendere l'energia in eccesso, non consumata, al network. Creando quindi un mercato secondario in cui ogni utente potrebbe realizzare transazioni peer-to-peer con gli altri membri della rete.

- Settore della Sanità

Una blockchain è un database distribuito in cui ogni cambiamento effettuato su una copia del registro viene istantaneamente aggiornato su tutte le copie, permettendo a tutti i partecipanti alla rete di avere dati e informazioni costantemente aggiornati, su ogni copia del database. Questa caratteristica suggerisce una potenziale futura applicazione nel campo della sanità.
Basti pensare che ogni paziente, che si interfaccia con un nuovo medico o con un nuovo ospedale, deve compilare vari moduli per formare la sua cartella clinica, che non è condivisa fra i vari soggetti ed enti della sanità. La possibilità di salvare le cartelle cliniche dei pazienti in un registro condiviso, permetterebbe a medici, ospedali e compagnie di assicurazioni sanitarie una comunicazione rapida efficiente basata sulla condivisione dei dati.

- Predizioni e Gioco d’azzardo

Molte startup che sviluppano soluzioni blockchain, stanno tentando di rinnovare il settore del gioco d’azzardo, ovvero quello delle predizioni, relative ad esempio al meteo o all’andamento dei mercati finanziari. Fra le criptovalute che stanno crescendo maggiormente, bisogna citare Augur, che sta sviluppando un mercato di predizioni in cui ogni utente può, tramite la sua previsione, trarre profitto dal risultato di un evento. Augur, quindi, svilupperà una piattaforma decentralizzata per calcolare la probabilità che un determinato evento si verifichi, fornendo la possibilità di scommessa per i suoi utenti.

- Processi di Produzione

Anche all’interno dei processi produttivi molte operazioni potrebbero essere ri-ingegnerizzate, permettendo di conseguire risparmi o incrementi di valore. I processi produttivi più attrattivi per l’adozione della blockchain riguardano sicuramente la supply chain. All’interno di una catena di fornitura, un database distribuito consentirebbe una migliore gestione delle scorte e aumenterebbe la trasparenza su tutto il ciclo di vita del prodotto, registrando in modo immutabile le sue tappe e la provenienza della merce.
Walmart, il colosso statunitense delle vendite al dettaglio, utilizza già la tecnologia blockchain per monitorare le forniture di carne di maiale dagli allevamenti in Cina ai suoi negozi.

CAP III - L' ARCHETIPO DELLE VALUTE DIGITALI: IL BITCOIN

3.1 Excursus Storico: Satoshi Nakamoto

L'inarrestabile passaggio nell'era digitale ha determinato bisogni sempre maggiori di sicurezza e privacy. In tal contesto un ruolo determinante è stato giocato dalla crittografia. Quest'ultima trova i suoi maggiori sviluppi negli anni settanta con lo scopo di garantire la privacy nei nuovi sistemi digitali, come quelli che interessano i pagamenti.

Un esempio è rappresentato dal crittografo americano David Chaum, che negli anni ottanta realizza un sistema di "blind signatures", una particolare forma di firme digitali, volto a incrementare la privacy nei servizi di pagamento elettronici offerti dal sistema bancario dell'epoca.

L'interesse di David Chaum riguardo la sicurezza nei pagamenti elettronici si tradusse nella realizzazione della DigiCash Inc., un sistema di pagamento anonimo, negli anni novanta.

Il sistema di pagamenti elettronici chiamato e-cash, che permetteva di compiere transazioni anonime, utilizzava denaro virtuale controllato crittograficamente dalle banche associate al sistema e-cash.

La principale caratteristica di tale sistema era il controllo centralizzato da parte delle banche, nonostante fosse basato sulla crittografia, la quale negli anni successivi fornirà grandi spunti per la realizzazione di sistemi decentralizzati.

Nonostante l'avveniristico progetto, il sistema di denaro elettronico e-cash non decollò a causa della scelta conservativa delle banche, che prediligevano le carte di credito. Questo determinò il fallimento della Digicash Inc. nel 1998.

Sempre nello stesso anno, Wei Dai e Nick Szabo lanciano sul mercato, a poca distanza di tempo l'uno dall'altro, due diversi sistemi di pagamento decentralizzati.

Nonostante entrambi i sistemi di pagamento rimasero progetti teorici, rappresentano i due progetti più simili al sistema Bitcoin, ideato da Satoshi Nakamoto dieci anni più tardi.

Il progetto b-money di Wei Dai puntava alla realizzazione di un network anonimo in cui gli utenti, identificati da pseudonimi, conservavano separatamente un registro delle transazioni e potevano compiere transazioni con il meccanismo delle firme digitali. Mentre, la generazione di moneta del sistema era subordinata alla risoluzione di problemi attraverso la potenza computazionale dei calcolatori.

Se questo meccanismo condivideva molte idee di fondo con l'attuale sistema Bitcoin, il sistema sviluppato da Szabo, chiamato bit-gold, ne rappresentò una premessa.

Il sistema di pagamento teorizzato da Szabo, così come il Bitcoin utilizzava la proof of work per validare le transazioni. Finalità della "prova di lavoro" era quella di trovare una stringa di bit, chiamata "challenge string", che risolvesse il puzzle crittografico.

Ogni challenge string, che può essere trovata da un solo utente una sola volta, fornisce un input per trovare quella successiva.

Le transazioni avvenivano tramite la firma digitale delle stringhe di bit trovate, e ogni ricevente di un determinato pagamento, poteva controllarne la regolarità consultando il registro condiviso delle transazioni.
Fra gli eventi che hanno contribuito alla nascita del sistema Bitcoin è sicuramente da citare la nascita della corrente cypherpunk alla fine degli anni '80.
Questo movimento sosteneva fortemente la crittografia come la tecnologia in grado di cambiare lo status quo, conducendo a un cambiamento politico e sociale. Più nello specifico, gli aderenti a questo movimento sostenevano l'importanza della crittografia, e quindi della privacy, negli aperti sistemi digitali.
Missione dei cypherpunk, come scritto nel 1993 in "A Cypherpunk Manifesto", era quella di creare sistemi anonimi volti a difendere la privacy attraverso la crittografia, i sistemi di messaggi anonimi, le firme digitali e la moneta virtuale.
Tra i più importanti partecipanti a questo movimento va ricordato, oltre a citati Wei Dai e David Chaum, anche Adam Back, ideatore di hashcash, un noto sistema di proof of work per prevenire lo spam via mail.
Nell' ideazione del sistema Bitcoin convergono proprio le idee del cypherpunk, come la difesa del diritto alla privacy attraverso la creazione di un sistema di pagamento anonimo, realizzato attraverso la matematica e la crittografia.
L'influenza dei precedenti contributi, relativamente alla crittografia e ai sistemi di pagamento decentralizzati, nei confronti di Bitcoin, è certificata dal fatto che il suo ideatore, Satoshi Nakamoto, abbia citato nel suo famosissimo paper[19] proprio Wei Dai, per b-money, e Adam Back per hashcash.
Bitcoin venne presentato il 31 ottobre del 2008 attraverso la pubblicazione del white paper su internet da parte di un anonimo, sotto il nome di Satoshi Nakamoto.
All'interno della Cryptography Mailing List del sito metzdowd.com, nel quale venivano affrontate discussioni relative allo sviluppo tecnologico della crittografia, Satoshi Nakamoto allegò e pubblicò il documento: "Bitcoin: A Peer-to-Peer Electronic Cash System".
Il paper descrive un innovativo sistema per trasferire denaro digitale senza la presenza di servizi o istituzioni centralizzate, risolvendo per la prima volta in maniera distribuita il problema comune a tutte le valute digitali, quello del double spending, ossia il tentativo fraudolento di impiegare la stessa quantità di valuta in due o più transazioni. Nel paper veniva inoltre messa in primo piano l'indipendenza del sistema di pagamento da terze parti e l'anonimato nelle transazioni.
Il primo gennaio 2009 venne rilasciata la prima versione del client Bitcoin, "Bitcoin v0.1" un software open-source.
Mentre la teoria è frutto del lavoro privato di Nakamoto, il software è stato sviluppato con la collaborazione della community online.
Infatti, le conversazioni per lo sviluppo del client-software Bitcoin sono tutt'ora pubbliche sul forum "bitcointalk", dove si possono leggere i post di Nakamoto che ha sviluppato il software fino alla versione 0.3.19.

[19] Satoshi Nakamoto, "*Bitcoin: A peer to peer electronic cash system*", 2008 – URL: https://bitcoin.org/bitcoin.pdf

Satoshi Nakamoto, considerato l'ideatore del sistema Bitcoin, in realtà è uno pseudonimo, mentre la reale identità dell'ideatore, o del gruppo di ideatori, è rimasta un mistero.

Per riuscire ad identificare la mente dietro la nascita della crittovaluta sono state condotte molte ricerche, che si sono unite ai moltissimi rumors sull'identità dell'ideatore.

Tra i nomi dei vari esperti accostati all'anonimo ideatore di Bitcoin vanno menzionati Nick Szabo, ideatore di bit-gold, il quale ha smentito, e l'imprenditore australiano Craig Wright. Quest'ultimo, dopo essere stato indagato, a causa delle pressioni della Fed americana, ha dichiarato la sua estraneità e la volontà di prendere le distanze dal fenomeno.

Ad oggi non è stato possibile appurare chi si nasconda dietro lo pseudonimo di Satoshi Nakamoto, o se questo rappresenti in verità un nome collettivo che identifica un gruppo di persone. Le uniche certezze sono date dal fatto che egli abbia continuato a lavorare con altri sviluppatori del sistema Bitcoin sino a metà 2010. Infatti, risalgono al 2011 le ultime notizie di Nakamoto, quando con una mail mandata agli sviluppatori e alla comunità Bitcoin scrisse: "Sono passato ad altro", consegnando il controllo del codice sorgente Gavin Andresen, uno tra i primi sviluppatori ad unirsi a Bitcoin, nonché il suo collaboratore più stretto fino a quel momento.

Questo messaggio ha decretato la fine del coinvolgimento di Satoshi Nakamoto nel progetto, avvenuto sino alla versione 0.3.19 del software, nonostante le registrazioni della blockchain di Bitcoin mostrano come i portafogli da egli detenuti contengano circa un milione di bitcoin.

Lasciando alla community lo sviluppo del software, si è spontaneamente creato un gruppo di lavoro aperto, che da allora propone nuovi aggiornamenti di quel software, il quale successivamente prenderà il nome di Bitcoin Core, attualmente alla versione 0.14.2.

Come precedentemente detto, Bitcoin nasce ufficialmente a gennaio del 2009 con il rilascio del primo client (software) che ha avviato l'attività di mining e la relativa generazione di valuta.

La prima transazione avvenuta nella blockchain di Bitcoin, registrata il 12 gennaio, fu realizzata proprio da Satoshi Nakamoto, il quale inviò ad Hal Finney, cypherpunk esperto di crittografia, una somma di 10 BTC.

Ma, per circa due anni, dal 2008, i bitcoin vengono solamente considerati come una curiosità tecnologica.

Infatti, le compravendite avvenivano solamente sul forum del progetto Bitcoin, bitcointalk.org.

Il primo storico pagamento, avvenuto proprio nel forum, risale al 22 maggio 2010, quando Laszlo Hanyecz, un programmatore informatico, offrì 10.000 BTC a chiunque gli avesse consegnato due pizze della catena Papa John's.

All'epoca il valore stimato di una singola unità di bitcoin si attestava al di sotto di un centesimo di dollaro, ma solo otto anni dopo, il prezzo avrebbe ampiamente rotto il tetto dei 10.000 $, determinando, a posteriori, un costo milionario per le pizze di Laszlo.

L'incredibile transazione acquisì moltissima notorietà nel web, al punto che tutt'ora, ogni anno, viene festeggiato il "Bitcoin Pizza Day". Ad ogni modo, in un'intervista del New York Times, Laszlo Hanyecz affermò di non aver rimpianti per l'acquisto fatto, essendo stato soddisfatto di aver scambiato un bene tangibile come la pizza con qualcosa che, all'epoca, era considerato senza valore.

Nonostante si sia dovuto aspettare il febbraio del 2011 per veder raggiungere al bitcoin il valore di 1 $, nel luglio del 2010 divenne operativo il primo sito di exchange sul dominio Mtgox.com, che permetteva il cambio fra bitcoin e valuta tradizionale.

Ad agosto 2010 venne scoperta una grave falla relativa al sistema di sicurezza del protocollo Bitcoin, a causa della quale le transazioni non erano correttamente verificate prima del loro inserimento nella blockchain.

Tale malfunzionamento avrebbe permesso agli hacker, che attaccavano il sistema, di generare arbitrariamente quantità di BTC.

La falla venne sfruttata generando dal nulla 184 milioni di bitcoin, ma nel giro di poche ore gli sviluppatori risolsero il problema e annullarono le transazioni invalide.

Negli anni successivi la popolarità di Bitcoin aumentò esponenzialmente, portando il valore per unità da 1 dollaro a oltre 1000 nel 2014, con un trend di prezzo caratterizzato da altissima volatilità.

Sempre nel 2011, tra le associazioni che iniziarono ad accettare bitcoin per le loro donazioni c'era WikiLeaks, fondata da Julian Assange.

Quest'ultimo, attraverso la sua organizzazione, nel giugno del 2011, rese pubbliche scottanti informazioni riservate relative alla guerra in Afghanistan. Tali rivelazioni causarono il divieto, da parte di molti gestori di servizi di pagamento online, come Visa, Mastercard e PayPal, nei confronti dei sostenitori di WikiLeaks, di effettuare donazioni attraverso i propri servizi. Il divieto fu chiaramente il risultato delle pressioni del governo USA su molti gestori di servizi di pagamento, volto a fermare le donazioni a favore dell'associazione.

Questo portò Julian Assange ad accettare contributi e donazioni in bitcoin, concentrando così l'interesse pubblico e dei media attorno alla crittovaluta.

A cavallo tra il 2012 e il 2013 la popolarità del sistema Bitcoin aumentò sensibilmente grazie ad applicazioni di pagamento come Coinbase e Bitpay, che permettevano a qualsiasi sito o commerciante di accettare pagamenti in BTC, e di convertirli in valuta locale attraverso un cambio fisso.

Infine, tra gli eventi che hanno caratterizzato la storia di Bitcoin va menzionato il fallimento, del noto Exchange Mt.Gox, la cui insolvenza ammontava a circa 800.000 BTC di proprietà degli utenti.

Il fallimento dell'allora più importante piattaforma di Exchange fu dovuto ad un attacco informatico, con il quale sono state depredate le crittovalute possedute dagli utenti di Mt.Gox, al quale però vanno anche sommati gli errori e le negligenze del suo management.

Evento che insieme ad altri ha minato la sicurezza e la fiducia nel sistema Bitcoin, traducendosi in una eccessiva volatilità del prezzo della crittovaluta. Nonostante questo avvenimento negativo, va comunque detto che nel 2014 gli investimenti Venture Capital nell'ecosistema Bitcoin ammontarono a 335 milioni di dollari, contro i 96 dell'anno precedente.[20]

[20] Fonte BitPay.

3.2 Concetti principali: Differenza Blockchain – Protocollo – Moneta

La terminologia attorno al Bitcoin può generare confusione soprattutto tra i meno esperti, infatti il nome della crittomoneta è usato simultaneamente per esprimere tre nozioni differenti.
In primis, il termine Bitcoin, con l'iniziale maiuscola, si riferisce alla tecnologia sottostante, la blockchain. In secondo luogo, il nome Bitcoin viene anche usato per identificare il protocollo che lavora al di sotto della tecnologia. Per ultimo, il termine bitcoin, con l'iniziale minuscola, è riferito alle unità di valuta digitale, le quali sono anche comunemente identificate dalla sigla BTC.
Il sistema Bitcoin dunque si articola in tre differenti strati, come mostrato dalla Tabella 2.

TECNOLOGIA	Blockchain: registro decentralizzato sottostante
PROTOCOLLO	Software che esegue transazioni – insieme di regole che disciplinano il sistema Bitcoin
MONETA	bitcoin (BTC)

Tabella 2: I Diversi Strati del Sistema Bitcoin

Il primo strato è rappresentato dalla blockchain, la tecnologia sottostante. Come precedentemente trattato, essa consiste in un database pubblico, decentralizzato e condiviso fra tutti i nodi della rete, nel quale vengono registrate le transazioni fra essi avvenute. Il registro blockchain oltre a poter essere monitorato da qualunque partecipante alla rete, viene aggiornato costantemente dai miner che registrano al suo interno blocchi di transazioni, controllando e validando la loro correttezza e unicità (no double spending).
Lo strato intermedio è rappresentato dal protocollo che opera al di sotto della tecnologia, ovvero l'insieme di regole rappresentato dal software che disciplina le transazioni di crittomoneta e la loro registrazione nella blockchain. Mentre l'ultimo strato del sistema Bitcoin è rappresentato dalla valuta stessa (bitcoin o BTC).
Il concetto importante è che i tre strati sopra descritti, rappresentano la struttura di ogni moderna criptomoneta.
Tipicamente ogni crittovaluta rappresenta sia la valuta digitale che un protocollo. Mentre, per quanto riguarda la tecnologia, una crittovaluta potrebbe basarsi sulla propria blockchain come nel caso di Bitcoin, definita in tal caso "proprietaria", oppure utilizzarne una già esistente. In questo contesto il token digitale avrebbe comunque il suo registro decentralizzato, rappresentato della blockchain esistente che viene scelta. L'utilizzo di una blockchain esistente per una nuova crittovaluta è molto frequente in sede di Initial Coin Offering, dove le più utilizzate sono quella di bitcoin e quella di ethereum.
Aver chiarito la terminologia relativa al sistema Bitcoin, oltre che gli strati in cui si articola, spiega perché nel corso della trattazione, in contesti apparentemente simili, il nome della crittovaluta è stato scritto usando a volte l'iniziale maiuscola, a volte quella minuscola.

3.3 L'Ecosistema Bitcoin

Quando si menziona il sistema Bitcoin si fa riferimento al sistema di pagamento, creato nel 2009, che regola il trasferimento di valuta digitale. Infatti, molti esperti di finanza, non inquadrano il bitcoin come una moneta pura, ma bensì come un mezzo di scambio altamente volatile.
L'avanzamento tecnologico e lo sviluppo di Bitcoin ha dato vita a un vero ecosistema attorno all'innovativo sistema di pagamento.
Lo sviluppo dell'ecosistema Bitcoin ha condotto alla comparsa di nuovi attori, rispetto a quelli presenti nei sistemi di pagamento tradizionali, e nuovi modelli di business, focalizzati sull'offerta di servizi relativi all'utilizzo, lo scambio e l'investimento nel comparto delle crittomonete.
Nonostante l'ecosistema Bitcoin sia recente e in continuo sviluppo, esso si snoda attraverso il coinvolgimento di vari Stakeholders:

- Il Team di Sviluppatori

I quali lavorano al continuo sviluppo del protocollo Bitcoin, migliorando il sistema da un punto di vista tecnico e risolvendo le falle e le vulnerabilità che lo mettono a rischio.

- I Minatori

Garantiscono il funzionamento del sistema, validando e registrando le transazioni nei blocchi della blockchain, attività che determina la creazione di nuova moneta. Tale generazione assolve la funzione di sistema di incentivi, finalizzato a far assumere un comportamento onesto ai miner.

- Gli User

L'insieme degli utilizzatori, ossia i soggetti che con finalità diverse utilizzano la crittomoneta bitcoin, come ad esempio i commercianti che accettano BTC per l'acquisto di beni e servizi, oppure gli investitori che li detengono per finalità speculative.
È importante chiarire che per utilizzare i bitcoin, ad esempio per un pagamento o per inviare denaro, non è necessario diventare un nodo della rete Bitcoin.
I nodi sono necessari a rendere possibili le transazioni, ad esempio controllandole oppure validandole con l'attività di mining, mentre per i semplici utilizzatori della crittovaluta non obbligatorio partecipare attivamente al network. Infatti, basta solamente creare un indirizzo bitcoin, molto simile ad un account email.

- Fornitori di servizi di Wallet

Offrono diverse soluzioni in termini di portafogli elettronici per le diverse esigenze dell'utilizzatore.
I wallet elettronici consentono la ricezione, l'invio e la conservazione dei bitcoin.

- Le Piattaforme di Exchange

Tali piattaforme offrono un "luogo" in cui è possibile tradare le crittomonete più famose. Il trading si realizza sia nello scambio fra diverse crittomonete, sia nella compravendita di monete digitali in cambio di valute tradizionali.
Questo permette, oltre alla possibilità di strutturare un portafoglio diversificato di crittovalute, anche l'opzione di disinvestimento, scambiando le crittomonete possedute in cambio di valute tradizionali ($, €).
Le piattaforme di Exchange sono solitamente gestite da società non finanziarie.

- Fornitori di servizi finanziari

I quali gestiscono piattaforme online che consentono l'investimento in crittovalute, senza entrare concretamente nel sistema Bitcoin, un esempio è la piattaforma di trading over the counter "Plus 500".
Tali soggetti facilitano l'accesso al mondo delle crittovalute, consentendo di investire in diversi prodotti finanziari, come ad esempio gli ETFs o gli strumenti derivati che scommettono sul futuro andamento del bitcoin. Un esempio di questi ultimi sono gli strumenti derivati CDF (contract for difference), i quali sono fortemente levereggiati e i cui pay-off derivano dall'andamento futuro del sottostante.

- Processori di pagamento

Identificano l'insieme di servizi che agevolano l'accettazione di bitcoin come pagamento sia per gli acquisti tradizionali che online.
Tra i più importanti servizi offerti per i merchant, va citata la conversione immediata in valuta legale delle crittomonete incassate, immunizzando così il commerciante dall'alta volatilità del prezzo delle crittovalute come il bitcoin.
Questo meccanismo permette quindi al commerciante di evitare i rischi di svalutazione associati al mantenimento in portafoglio delle criptomonete ottenute dalla vendita di beni e servizi.

- Altri Soggetti

In questo insieme rientrano tutti i soggetti che sono indirettamente coinvolti nel sistema Bitcoin, ma contribuiscono al giro d'affari complessivo. Tra i più importanti della categoria vanno menzionate le imprese produttrici di hardware specifici per l'attività di mining, le aziende che realizzano gli ATM per le crittomonete, quelle che sviluppano software e applicazioni per l'utilizzo di valuta digitale, ed infine l'insieme di startup che sviluppano soluzioni basate su blockchain, anche diverse dall'applicazione nelle transazioni.

3.3.1 Principali caratteristiche del Bitcoin

Il bitcoin può essere definito come la prima valuta digitale decentralizzata, ideata con la finalità di velocizzare e rendere anonime, oltre che più sicure, le transazioni online.
Il sistema, infatti, consente il possesso e il trasferimento anonimo della crittomoneta a chiunque disponga di un indirizzo bitcoin; e i dati necessari per disporre dei bitcoin posseduti sono salvati in uno o più personal computer sotto forma di portafogli elettronici (digital wallet).
Il processo si realizza attraverso una rete peer-to-peer caratterizzata dall'assenza di un'autorità centrale. Questo si traduce nell'impossibilità, per qualsiasi ente centrale, di bloccare le transazioni, oppure effettuare un sequestro di bitcoin, o ancora avviare un processo di svalutazione della crittovaluta.
Caratteristica comune alle monete complementari, infatti, è proprio il porsi al di fuori degli schemi di regolazione tradizionali e centralizzati, e di avere così una matrice anarchica, che promuove il bitcoin in ottica antisistemica.
L'algoritmo di funzionamento della crittovaluta bitcoin, realizzato da Satoshi Nakamoto, è basato su un concetto fondamentale: la creazione della valuta stessa è un fenomeno condiviso dalla comunità, dato che la "produzione" di bitcoin significa al tempo stesso contribuire attivamente alla sicurezza del sistema; in termini tecnici "mining". Il controllo e la validazione delle transazioni, il loro inserimento nei blocchi da agganciare al registro blockchain, insieme alla generazione di moneta come sistema di incentivi, rappresentano infatti due lati della stessa medaglia, ossia dell'attività di mining svolta dai nodi miner.
Per una descrizione tecnica e approfondita dell'attività di mining si rimanda al secondo capitolo, dove, per analizzare la tecnologia di fondo, è stato utilizzato il caso della blockchain di Bitcoin basata sulla proof of work (2.4).
La generazione di moneta, non controllata da un ente centrale e basata su un meccanismo peer-to-peer puro, è regolata dall'algoritmo di creazione che ne definisce caratteristiche e limiti di emissione.
L'idea alla base dell'algoritmo di creazione è la scarsità della crittomoneta, condizione derivante dal fatto che l'emissione di bitcoin è limitata e anticipatamente stabilita.

Infatti, il trend relativo alla generazione di bitcoin è stabilito da un algoritmo che segue un andamento a rendimenti marginali decrescenti nel tempo.

Quanto appena detto è rappresentato nella Figura 11, in cui l'asse delle ordinate indica il numero di BTC che saranno generati in totale, l'asse delle ascisse indica sia la variabile tempo sia il numero di blocchi che verranno progressivamente aggiunti alla blockchain, mentre i numeri sulla curva di generazione rappresentano le ricompense, via via minori nel tempo, che spettano al miner che per primo valida ed inserisce nel registro un nuovo blocco di transazioni.

Tali ricompense rappresentano anche la quantità di bitcoin generati dalla risoluzione di ogni singolo blocco che viene inserito nella blockchain.

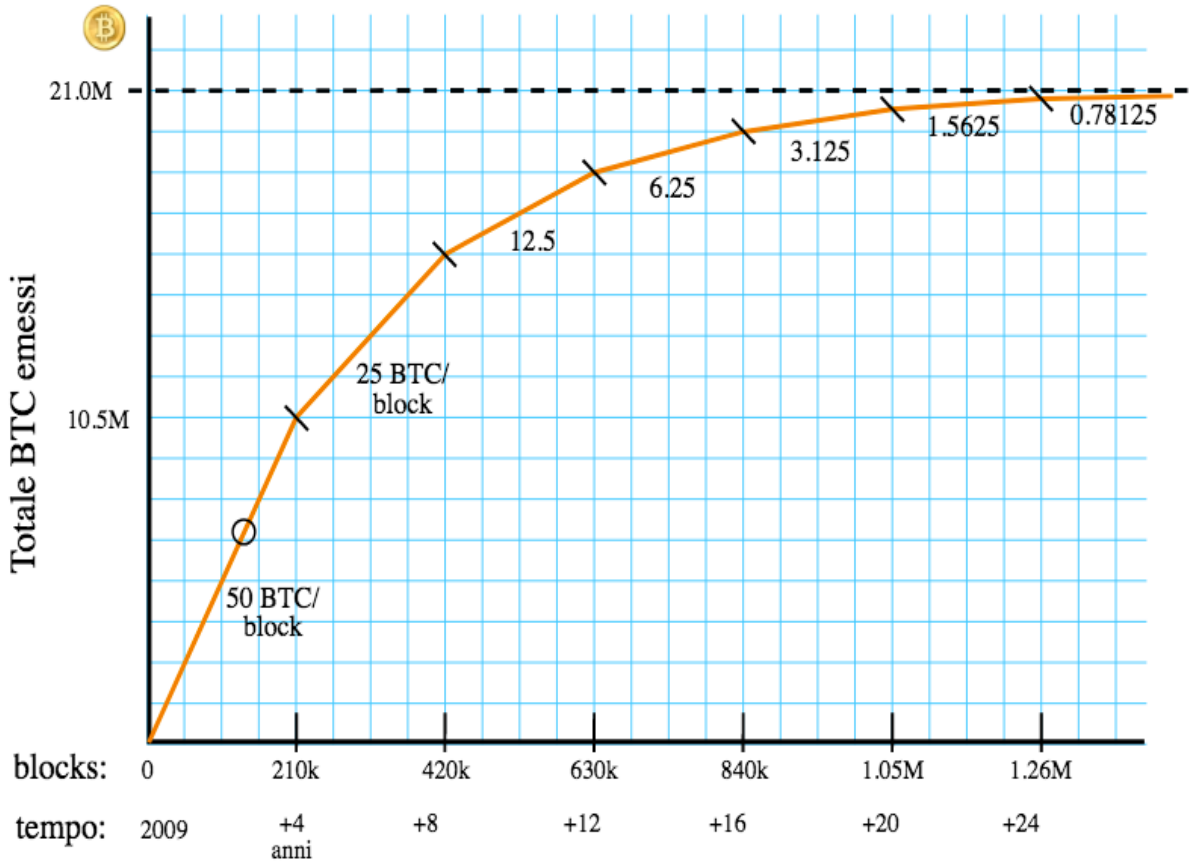


Figura 11 - Rappresentazione semplificata dell'Algoritmo di Generazione Bitcoin

Il numero totale di bitcoin, nel tempo, tende asintoticamente al limite di 21 milioni di unità, e i BTC in circolazione aumentano seguendo una serie geometrica ogni quattro anni.

Ciò implica che lo stock di moneta aumenta a un tasso decrescente, infatti dal 2009 al 2013 è stata generata la metà dei bitcoin possibili (21 milioni), mentre nel 2017 si è arrivati a tre quarti.

Seguendo l'algoritmo di crescita corrente, il tasso di crescita dei bitcoin convergerà a zero intorno al 2140[21], ossia quando la quantità in circolazione raggiungerà il limite di 21 milioni di unità.

Tornando alle caratteristiche qualitative del bitcoin, è importante notare che nonostante non ci sia un

[21] https://bitcoin.org/it/faq

intermediario che consente la circolazione e assicura che la valuta non sia duplicata, il sistema Bitcoin e la tecnologia su cui si basa garantiscono che il double spending sia quasi impossibile, come trattato in precedenza.
Inoltre, non avendo un supporto fisico, i bitcoin possono essere memorizzati in portafogli installati localmente su pc, smartphone o tablet, oppure in portafogli online gestiti da chi offre questo tipo di servizi.
Non essendoci un'autorità centrale che sia garante e svolga funzioni di vigilanza, i costi delle transazioni (fee) nel sistema Bitcoin devono solamente coprire quelli di compensazione dell'attività di mining. Esulando quindi dal calcolo i vari costi associati alle transazioni di valute tradizionali, come ad esempio quelli relativi allo stoccaggio, autenticazione e sicurezza.
Questo determina che i costi per avviare una transazione peer-to-peer nella rete Bitcoin si attestano in media tra lo 0% e l'1%, mentre quelli relativi ad una transazione di valuta standard oscillano intorno al 2-5 %.
Oltre quanto detto, l'assenza di supporti fisici e di un ente centrale si traduce in una maggiore rapidità nel processare le transazioni, in media tra i 10 e i 60 minuti, rispetto ai sistemi di pagamento online tradizionali.
Altra caratteristica fondamentale è l'anonimato, infatti per compiere transazioni in bitcoin non è necessario fornire nessuna informazione personale.
La tecnologia peer-to-peer, unita all'uso di algoritmi crittografici, rende estremamente complesso riuscire ad intercettare chi si celi dietro gli indirizzi utilizzati per compiere transazioni.
Concetto in apparente contrapposizione con l'anonimato è quello della trasparenza. Intendendo con quest'ultima la possibilità per chiunque di seguire in tempo reale la catena di transazioni, infatti tutti i pagamenti, nonostante siano criptati, hanno una storia tracciabile sul registro pubblico che può essere liberamente visualizzato, ovvero la blockchain.
Riassumiamo i concetti espressi attraverso una schematizzazione delle principali caratteristiche del bitcoin:

- Decentralizzazione

Il sistema Bitcoin non è controllato da autorità centrali di natura pubblica o privata. Il controllo sulla validità delle transazioni è condotto da molte entità indipendenti, in modo decentralizzato e distribuito.

- Pseudo-Anonimato

Qualsiasi individuo può scaricare il software e compiere transazioni, senza comunicare la propria identità o dati personali. Le transazioni avvengo tra indirizzi pubblici a partire dai quali è molto difficile risalire all'identità della persona fisica o giuridica che trasferisce o riceve bitcoin. Il sistema è definito pseudo-anonimo poiché esiste comunque la possibilità di risalire all'identità di un utente nel caso non vengano presi

degli accorgimenti per effettuare transazioni, come ad esempio creare sempre un nuovo indirizzo per inviare e ricevere bitcoin.

- Trasparenza

Ogni transazione è memorizzata nella blockchain, un registro visibile da tutti.
Analizzando la blockchain è possibile conoscere quanti bitcoin sono detenuti in uno specifico indirizzo (wallet) in un preciso momento, potendo inoltre risalire agli indirizzi che gli hanno precedentemente inviato le crittovalute.

- Limite alla creazione di moneta

Essendo un sistema decentralizzato, Bitcoin non è soggetto a politiche monetarie come l'aumento o la riduzione della quantità di valuta in circolazione.
L'offerta di moneta è fissata a priori nel protocollo, sulla base di un aumento progressivo della moneta in circolazione, fino al raggiungimento del limite di 21 milioni di unità.

- Velocità delle transazioni

Ogni transazione avvenuta nel sistema Bitcoin impiega in media 10 minuti per essere confermata. Conferma che avviene con l'inserimento di un blocco successivo a quello in cui la transazione in esame è inserita.

- Bassi Costi di transazione

L'assenza di intermediari coinvolti nelle transazioni determina l'abbattimento dei costi ad esse associati.
Le fee relative alle transazioni di bitcoin mediamente sono nell'ordine di 0,0001 BTC, circa 2 centesimi di euro a carico del mittente.

- Irreversibilità delle transazioni

Quando viene realizzata una transazione e inserita nella blockchain, essa è irreversibile, ossia non può essere annullata nemmeno dal mittente.

- Non ha corso legale

I bitcoin vengono accettati come strumento di pagamento solo su base volontaria, non possono quindi essere usati per estinguere un'obbligazione pecuniaria nel caso il creditore rifiuti di accettarli.

- Rete Peer-to-Peer

Nella rete informatica di Bitcoin, i nodi non sono gerarchizzati sotto forma di client o server (clienti e fornitori), al contrario tutti i nodi sono paritetici, ossia possono fungere sia da client che da server nei confronti degli altri nodi, attraverso un metodo di comunicazione diretto.

- Immunità dalla confisca

Infatti, soltanto l'utente per mezzo della sua chiave privata può disporre dei bitcoin custoditi nel suo wallet digitale, impedendo così la confisca o il blocco dei fondi da parte di un'autorità esterna.

3.3.2 Il Protocollo Bitcoin

Quando si parla di protocollo Bitcoin si fa riferimento all'insieme di regole che definiscono il funzionamento del sistema, che si esplica nell'utilizzo del software Bitcoin, il più noto è "Bitcoin Core".
Una delle principali caratteristiche del software Bitcoin è la sua natura open-source. Infatti, il protocollo è aperto nei confronti degli sviluppatori che intendano migliorarlo.
Nonostante ciò risulta essere quasi impossibile per gli sviluppatori realizzare un profondo cambiamento del protocollo.
Questo è dovuto dal fatto che ogni nodo della rete è libero di scegliere quale software e versione utilizzare, con la condizione però che il software da lui utilizzato sia compatibile con quelli impiegati dagli altri nodi, ovvero conforme alle stesse regole.
Questa condizione rimanda l'efficienza e il corretto funzionamento di Bitcoin all'allineamento e al consenso tra sviluppatori e utilizzatori.
La fiducia nel sistema Bitcoin, realizzata mediante un meccanismo di raggiungimento del consenso, è subordinata all'accettazione da parte dei nodi del protocollo stesso, ossia l'insieme di regole informatico-crittografiche che consentono di ottenere il consenso fra i partecipanti alla rete. Le transazioni, seguendo il protocollo Bitcoin, avvengono attraverso il trasferimento delle crittomonete da un indirizzo/wallet a un

altro. L'argomento digital wallet verrà affrontato nelle successive sezioni, mentre per quanto riguarda la descrizione tecnica di una transazione bitcoin si rimanda alle sezioni 2.2.3 e 2.3.1 del secondo capitolo, dedicato alla blockchain.

Ogni volta che si avvia una transazione, il computer la trasmette ai nodi (peer) della rete più vicini, i quali eseguiranno una serie di controlli formali, circa una ventina, per accertarne la validità, e successivamente inoltreranno la transazione agli altri utenti. Con questo meccanismo dunque ogni transazione viene propagata nella rete.

A questo punto entrano in gioco i nodi-miner, i quali avendo ricevuto e verificato la transazione, la inseriscono in un pool di memoria insieme a tutte le transazioni non ancora verificate. In questa fase ogni miner inizierà ad assemblare un blocco di transazioni, selezionandole dalla pool di transazioni non ancora confermate.

Nella blockchain di Bitcoin, mediamente, un blocco contiene dalle 200 alle 300 transazioni.

Una volta creato e validato il blocco di transazioni, attraverso l'attività di mining, il miner lo trasmette alla rete inserendolo nella blockchain, consentendo così ad ogni utente di verificarne la validità, data la natura condivisa e pubblica del registro.

Di seguito una sintesi del funzionamento del sistema Bitcoin e del lavoro svolto dai nodi miner:

- Le nuove transazioni vengono inviate a tutti i nodi della rete.
- Ogni nodo-miner verifica che le transazioni siano valide e le raccoglie in un blocco insieme all'hash del blocco precedente.
- Ogni miner lavora per trovare una proof of work valida per il proprio blocco.
- Quando un minatore trova una proof of work valida, la invia insieme al blocco a tutti gli altri nodi.
- I nodi accettano il nuovo blocco solo se contiene transazioni valide e non incluse precedentemente in altri blocchi.
- I minatori dimostrano di accettare come valido il nuovo blocco utilizzandone l'hash nel calcolo della proof of work del blocco successivo da inserire nella catena.

I nodi minatori, in caso di biforcazione della catena, considerano sempre la blockchain più lunga come quella valida e lavorano per estenderla, poiché su essa è stata impiegata la maggioranza del potere di calcolo dell'intera rete.

Può infatti accadere che due nodi-miner trovino contemporaneamente due differenti versioni dello stesso blocco, ambedue valide, ed entrambi trasmetteranno la propria versione al resto dei nodi. In questo caso ogni nodo-miner lavorerà sul blocco che ha ricevuto per primo, ma conserverà l'altro nel caso diventi parte del ramo più lungo della catena.

Per concludere la panoramica sul protocollo Bitcoin va introdotto il concetto forse più importante, ossia quello di sviluppo continuo. Il software Bitcoin infatti, nel quale si esplica il protocollo, non è ancora giunto ad una versione ufficiale, ma bensì è ancora in versione beta, con molti fattori incompleti in fase di sviluppo attivo.

Dunque, parlando di sviluppo continuo, ci si riferisce ai nuovi strumenti, fattori e servizi che verranno implementati per rendere il sistema Bitcoin più accessibile e sicuro.

3.3.3 Funzione monetaria del Bitcoin

Tipicamente una moneta, per essere definita tale, deve svolgere tre funzioni principali: mezzo di scambio, unità di conto e riserva di valore.

Al fine di verificare se il bitcoin possa essere considerato una valuta o meno, analizziamo le tre caratteristiche della moneta in relazione alla principale valuta digitale.

Per quanto riguarda la funzione di mezzo di scambio, va ricordato che il bitcoin, non avendo corso legale, può essere utilizzata per adempiere ad un'obbligazione pecuniaria solo se accettata, su base volontaria, dal creditore.

Così come le monete fiat, dopo l'uscita dal Gold Standard, anche il bitcoin è privo di valore intrinseco, il quale dipende principalmente dall'utilità percepita dagli utilizzatori attuali e potenziali.

L'efficacia dei bitcoin come strumento di pagamento, dunque, può essere misurata, oltre che dal numero di operazioni effettuate, soprattutto dal numero di soggetti disposti ad accettarli come strumento risolutorio.

Relativamente al numero di transazioni in BTC, secondo i dati disponibili su blockchain.com, la fonte più attendibile della blockchain di Bitcoin, a fine 2017 il volume giornaliero delle transazioni è pari circa 347.319. Ma, la maggioranza di queste transazioni è relativa a speculazioni, e non all'acquisto di beni e servizi.

Per valutare l'accettazione del bitcoin come strumento di pagamento, facciamo riferimento a "Coinmap", la piattaforma utilizzata da tutti gli esercenti che vogliano mostrare all'utenza la loro adesione al circuito Bitcoin.

Dall'analisi dei dati[22] si evince un incremento sostanziale degli esercenti che accettano bitcoin nell'intervallo di tempo che va da fine 2017 a maggio 2018.

[22] https://coinmap.org/#/world/45.46013064/-7.03125000/2

Infatti, se nel 2017 a livello mondiale i merchant aderenti al sistema bitcoin erano poco più di 9.000, ad oggi (maggio 2018) se ne stimano già 12.549, come mostrato nella Figura 12.

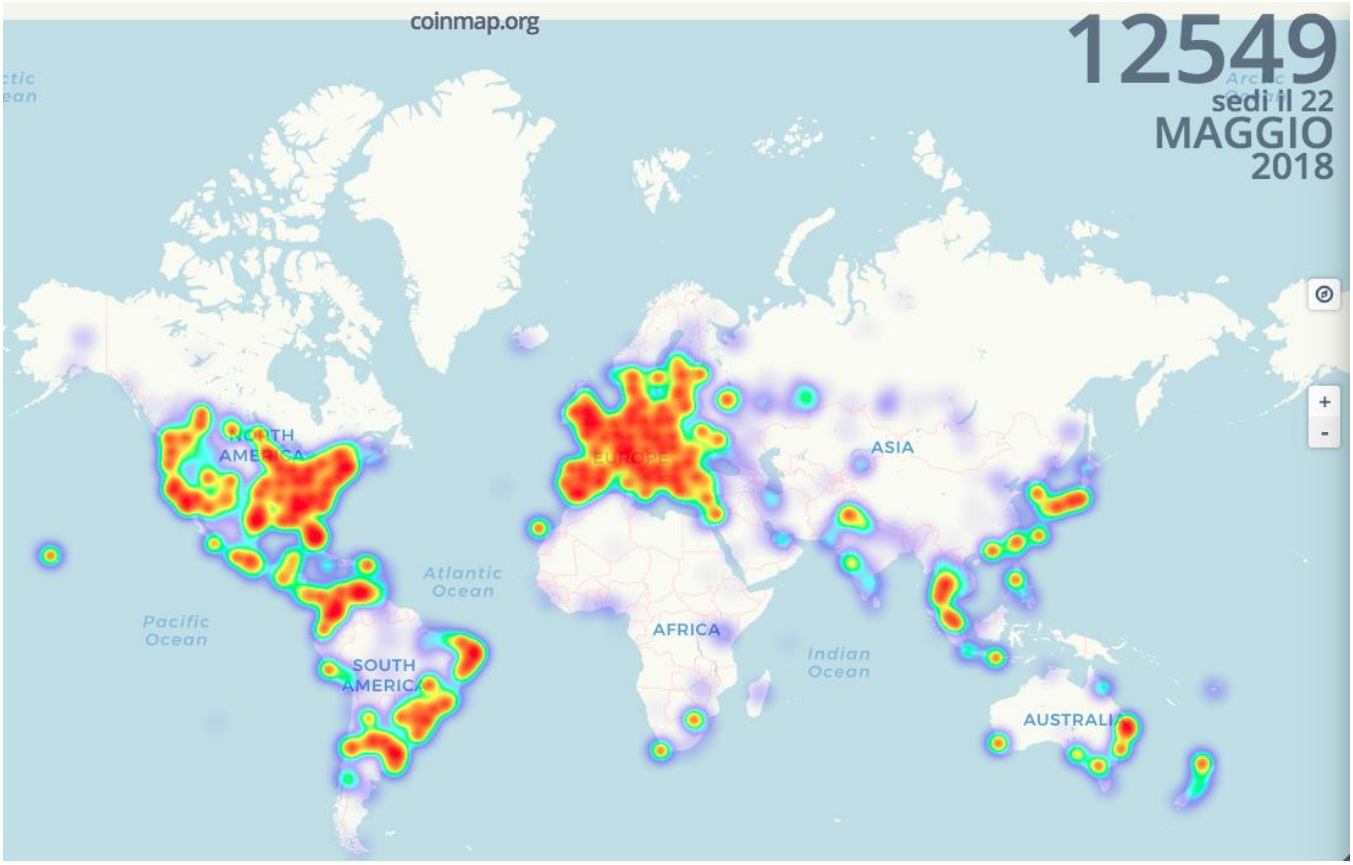


Figura 12 - Esercenti che accettano Bitcoin nel mondo

Una svolta importante nell'utilizzo di bitcoin, come mezzo di scambio e pagamento, si è avuta da marzo 2016, quando Wirex Limited, piattaforma bancaria londinese, ha lanciato una carta di debito che permette il pagamento in bitcoin sfruttando i circuiti internazionali di Visa e Mastercard.

Questo progetto fu chiaramente innovativo ma presentava alcuni limiti relativi all'utilizzo quotidiano dei bitcoin come mezzo di scambio, come ad esempio un importo minimo di transazione pari a 10 dollari e tempistiche lunghe per convertire la valuta legale in bitcoin, oltre 5 giorni lavorativi.

Relativamente alla funzione di unità di conto, una delle maggiori perplessità sulla valuta ideata da Nakamoto deriva dalla sua eccessiva volatilità.

Affinché una valuta assolva la funzione di unità di conto, è necessario che essa sia considerata un bene numerario, ossia venga considerata come unità di base per misurare il valore di altri beni.

L'ostacolo principale nel definire il bitcoin come unità di conto deriva dalla sua estrema volatilità, data dai repentini e profondi cambiamenti di valore rispetto alle più stabili valute tradizionali.

Si pensi in tal senso alla difficoltà per un esercente nel dover continuamente ricalcolare i prezzi dei suoi beni espressi in bitcoin, nel caso li accettasse per il pagamento.

L'instabilità del prezzo dei bitcoin comporta anche problematiche in tema di pagamenti differiti. Infatti, una valuta soggetta a forti oscillazioni di prezzo, nel caso in cui si rivaluti agevolerebbe molto i

prestatori di fondi, mentre pregiudicherebbe la situazione patrimoniale dei soggetti con saldi finanziari negativi, limitando così il ricordo al credito.

Le maggiori oscillazioni del prezzo di mercato derivano spesso dalle dichiarazioni rilasciate da governi, autorità monetarie o banche.

Negli ultimi anni un lampante esempio è stato il divieto, e il successivo unbanning, dei bitcoin da parte della Cina.

Un ulteriore ostacolo all'identificazione del bitcoin come unità di conto è rappresentato dai prezzi differenti riscontrabili sul mercato, in uno specifico istante.

In uno specifico istante, infatti, diversi siti di Exchange riportano prezzi per unità di bitcoin molto differenti, con un'oscillazione nell'ordine del 5-6 %.

Questo, in totale contrapposizione con la legge del prezzo unico, apre le porte a svariate opportunità di arbitraggio, sfruttando quindi le differenze di prezzo nei diversi mercati.

Ultimo ostacolo alla funzione di unità di conto del bitcoin sembra essere rappresentato dal cospicuo valore per unità, circa 8.400 dollari a maggio 2018[23], eccessivamente alto se comparato con il valore di beni e servizi ordinari, come potrebbe essere il costo del caffe.

Ma, a risolvere questa problematica, entra in gioco la divisibilità del bitcoin. Infatti, una singola unità di crittovaluta bitcoin può essere frazionata fino all'ottava cifra decimale.

Dunque, l'importo di 0,000001 BTC, definito anche "satoshi", in onore del suo fondatore, rappresenta l'importo minimo che può essere elaborato in una transazione.

Riguardo la funzione di riserva di valore, una valuta tradizionale consente al proprietario di spenderla in un momento futuro, evitando di farlo incorrere in perdite da svalutazione, o in eccessive rivalutazioni.

Le valute tradizionali, come euro o dollaro, presentano oscillazioni nel tasso di cambio tra lo 0,5% e l'1%, mentre il bitcoin, nel cambio con il dollaro, ha un tasso di volatilità che ha assunto valori anche superiori al 30-35 %.

Infine, un'altra peculiarità del bitcoin, oltre alla volatilità, che esclude la funzione di riserva di valore è data dalla sua natura deflattiva, derivante dal limite massimo di unità (21 milioni). Tema che verrà analizzato nelle successive sezioni.

[23] Fonte: https://blockchain.info/markets

3.3.4 Indirizzi Bitcoin (Digital Wallet): Problematiche di sicurezza e privacy

Un potenziale utilizzatore del sistema Bitcoin per poter ricevere, inviare o custodire dei BTC deve necessariamente possedere un wallet Bitcoin, ossia un portafoglio digitale.
Un portafoglio digitale Bitcoin è solo lontanamente simile ad un conto corrente tradizionale, nel quale viene custodito il denaro posseduto. Infatti, i bitcoin tecnicamente non sono custoditi all'interno di un portafoglio, bensì sono memorizzati nel registro pubblico blockchain, sotto forma di specifici indirizzi appartenenti ai diversi utenti del network.
Gli indirizzi rappresentano l'origine o la destinazione di una transazione bitcoin, e si presentano sotto forma di codici alfanumerici lunghi dai 26 ai 35 caratteri, che generalmente iniziano con il numero 1 oppure 3. (es: 14qViLJfdGaP4EeHnDyJbEGQysnCpwn1gd)
Il codice alfanumerico, che rappresenta l'indirizzo a cui ricevere o spedire bitcoin, non contiene nessun riferimento all'utente, garantendo quindi lo pseudo-anonimato del sistema Bitcoin.
Ogni indirizzo deriva da una chiave pubblica, attraverso da un procedimento algoritmico-crittografico spiegato nella sezione 2.2.3, la quale a sua volta deriva algoritmicamente dalla chiave privata.
Questo meccanismo di derivazione è strutturato per essere unidirezionale, ovvero per rendere impossibile che a partire da un indirizzo bitcoin si possa risalire alla chiave pubblica, e successivamente da essa a quella privata.
Attraverso il procedimento crittografico delle firme digitali, il possesso della chiave privata consente all'utente di spendere i BTC associati all'indirizzo da essa derivato.
Ogni utente può avere un numero arbitrario di indirizzi bitcoin, infatti è possibile generare un indirizzo diverso per ogni pagamento, dato che la loro creazione, richiedendo poca potenza di calcolo, non comporta nessuna spesa per l'utente, e può essere compiuta offline, senza nessun contatto con altri nodi della rete.
La tecnica di generare diversi indirizzi è fortemente consigliata dagli esperti al fine di mantenere alta la privacy e la sicurezza, ma questo argomento sarà affrontato nella parte finale della presente sezione.
Avendo fornito una panoramica sugli indirizzi Bitcoin, focalizziamoci sul tema dei digital wallet.
Nei portafogli Bitcoin vengono custodite le chiavi private dell'utente, le quali gli permettono di spendere i bitcoin associati ad uno specifico indirizzo, il quale deriva dalla chiave pubblica, a sua volta derivante da una specifica chiave privata.
Per fare chiarezza è importante aggiungere che, secondo alcuni calcoli, per ogni singolo utente è possibile generare addirittura 10^{77} chiavi private.
Quando viene creato un nuovo wallet, vengono automaticamente generate cento coppie di chiavi private e pubbliche (key-pool), consentendo così all'utente di disporre di un insieme di indirizzi diversi, da dove inviare bitcoin, o dove riceverli.
Inoltre, quando un utente apre il wallet quello che accade è che il wallet contatta un nodo che ha una copia della blockchain e scorre tutti i blocchi alla ricerca del suo indirizzo, per fornire all'utente il bilancio dei bitcoin che ancora non ha speso e che quindi gli appartengono.

I più importanti wallet sono caratterizzati da un'interfaccia user-friendly, che consente all'utente di visualizzare il saldo di bitcoin a disposizione relativo a tutti i diversi indirizzi che egli possiede, permettendogli inoltre di effettuare transazioni in uscita oppure in entrata verso un suo indirizzo.
Esistono diverse tipologie di portafogli bitcoin, dunque la scelta relativa a quale utilizzare si fonda sulle loro differenti caratteristiche, in termini di praticità, sicurezza e funzionalità desiderate:

- Desktop-Software Wallet

Rappresenta un portafoglio software da installare sul pc che consente di memorizzare e custodire le chiavi private all'interno dell'hard disk. Esistono varie tipologie di software wallet per i diversi sistemi operativi, e la loro installazione solitamente richiede il download dell'intera blockchain di Bitcoin, la quale al giorno d'oggi ha una size di oltre 100 Gigabyte[24].
La sicurezza associata a questa tipologia di portafoglio è alta, soprattutto se si utilizzano precauzioni come utilizzare un'ulteriore password per il wallet, installare un antivirus per il pc, o inserire banalmente una password d'accesso al computer. Se non si prendono questi accorgimenti si corre il rischio che qualche hacker rubi le chiavi private del portafoglio, potendo quindi disporre dei bitcoin.
Inoltre, è fortemente consigliato effettuare dei backup periodici del portafoglio con la finalità di recuperare le chiavi private nel caso in cui il computer smetta di funzionare.

- Mobile Wallet

Questa categoria indica le applicazioni wallet per smartphone, rendendo possibile l'invio, la ricezione e la custodia di bitcoin dal proprio cellulare, con modalità semplici e veloci.
Queste applicazioni non richiedono il download dell'intero registro blockchain, ma solo di una parte di essa, facendo così affidamento sulle informazioni provenienti dagli altri nodi del network. Anche per questa tipologia di wallet sono consigliati backup periodici.

- Online Wallet

I portafogli online sono servizi offerti da siti web, i quali e tutelano e custodiscono le chiavi private degli utenti all'interno di server online. Attraverso questi portafogli, l'utente affida la custodia dei propri bitcoin a terzi. Tipicamente i wallet online sono offerti dalle piattaforme di Exchange, dove avviene la compravendita di bitcoin in cambio di valute tradizionali o altre crittovalute.

[24] Fonte: https://blockchain.info/it/charts/blocks-size?timespan=all

La sicurezza degli online wallet non è la loro migliore qualità, si pensi in tal caso ai vari attacchi informatici avvenuti ai danni di molti siti di exchange per rubare le chiavi private, e quindi i bitcoin dei loro utilizzatori. Un esempio è il caso, precedentemente trattato, di Mt.Gox, avvenuto nel 2014.
Le qualità di questi portafogli, invece, risiedono nella velocità e semplicità di utilizzo, data la possibilità di accedervi da un qualsiasi dispositivo connesso ad internet. Per concludere, detenere molti bitcoin in questo tipo di wallet non è consigliato, mentre risulta essere il più pratico per transazioni piccole ma frequenti.

- Hardware Wallet

Sono dei dispositivi creati appositamente per custodire le chiavi private relative ad indirizzi bitcoin o di altre crittovalute, e rappresentano uno dei sistemi più sicuri.
In questa categoria di portafogli, rispetto alle altre, non si fa affidamento ad entità terze per la custodia delle chiavi private, non si corre il rischio che le stesse vengano rubate da hacker, e non è necessario reimpostarle online o in un software per inviare i propri BTC.
Gli hardware wallet consistono in mini computer aventi un'unica funzione, ossia quella di firmare digitalmente le transazioni con la chiave privata dell'utente.
Questi dispositivi si collegano al pc generalmente tramite la porta USB, e interagiscono con i software wallet anche nel caso in cui il pc dove sono stati installati smetta di funzionare.
L'utente verifica dal pc la correttezza dell'indirizzo a cui spedire i suoi BTC e autorizza l'operazione inserendo un pin sul suo hardware wallet, non rintracciabile dagli hacker. Un esempio di hardware wallet è il Ledger Nano S, acquistabile online o nei negozi fisici.

- Paper Wallet

In questo caso l'utente può direttamente conservare le proprie chiavi pubbliche e private su un supporto cartaceo, proteggendole così dagli hacker o da un guasto del proprio computer.
Molti online wallet consentono di esportare in formato cartaceo i propri codici, o alternativamente sul sito bitaddress.org si possono generare casualmente nuove coppie di chiavi (pubblica e privata) che potranno essere utilizzate per ricevere e successivamente spedire bitcoin.
Una volta che il wallet viene esportato su un supporto cartaceo, la chiave privata non è più memorizzata digitalmente, per cui è consigliabile effettuare varie copie per sicurezza. L'indirizzo creato potrà tranquillamente ricevere dei pagamenti, mentre per spendere i BTC ricevuti l'utente dovrà reimpostare la propria chiave privata all'interno di un online o software wallet, per firmare le transazioni in uscita. I paper wallet, insieme ai software e hard wallet, rappresentano la tipologia di portafogli che offrono all'utente la maggiore sicurezza, soprattutto in ottica cassettista, ossia per conservare i bitcoin nel lungo periodo.

Al fine di evitare problematiche di sicurezza nella gestione dei propri portafogli digitali, le precauzioni sono fondamentalmente due.

La prima, come già accennato, è quella di effettuare periodicamente dei backup aggiornati di indirizzi e chiavi private, tenuti localmente ad esempio in dispositivi di storage. Infatti, la perdita delle chiavi private impedirebbe di disporre dei propri bitcoin.

Nonostante questo esistono dei portafogli che esulano l'utente dal dover compiere sempre dei backup aggiornati, essi vengono chiamati portafogli deterministici. Questi wallet utilizzano una sola chiave privata come token iniziale, chiamata "seed", dal quale possono essere generate una serie di chiavi private e quindi di indirizzi Bitcoin. Con questo sistema l'utente deve preoccuparsi di salvare solamente il "seed" del portafoglio, poiché in caso di perdita del portafoglio, basterà questo "seed" per rigenerare le stesse chiavi private, senza così perdere i bitcoin posseduti.

La seconda precauzione per ottenere un buon livello di sicurezza è relativa alla gestione degli indirizzi, usati come punto in cui ricevere bitcoin, o da dove inviarli.

Siccome il contenuto della blockchain è visibile da tutti, è possibile visualizzare tutti i movimenti, in entrata e uscita, che hanno interessato un determinato indirizzo Bitcoin.

In questo senso, è fortemente sconsigliato utilizzare lo stesso indirizzo per più transazioni. Si pensi al caso in cui un utente che utilizza sempre lo stesso indirizzo effettui un pagamento ad un altro utente, quest'ultimo potrebbe analizzare tutti i movimenti relativi a quello specifico indirizzo e risalire addirittura all'identità del pagante.

A tal proposito esistono dei database che hanno analizzato milioni di indirizzi Bitcoin per collegare le informazioni relative alle transazioni a quelle presenti pubblicamente nei siti web, riuscendo in molti casi a delineare l'identità della persona celata dietro l'indirizzo.

L'utilizzo ripetuto dello stesso indirizzo Bitcoin potrebbe dunque portare a rivelare l'identità dell'utente che effettua la ripetizione, ma questo non è il rischio maggiore.

Si pensi infatti che utilizzare lo stesso indirizzo comporta una concentrazione dei bitcoin posseduti, poiché tutti sono associati a quell'unico indirizzo.

Data la natura pubblica e condivisa della blockchain, in cui ogni utente può leggere il saldo di BTC relativo ad ogni specifico indirizzo, potrebbero verificarsi azioni illecite ai danni del soggetto che ha concentrato tutti i suoi BTC in un unico indirizzo, come rapimenti ed estorsioni.

3.3.5 Gli Exchange

Sul web esistono attualmente molti siti che consentono la compravendita di bitcoin in cambio di moneta legale o di altre crittomonete. Tali piattaforme vengono chiamate "Exchange". Esse svolgono una funzione simile a quella dei classici market maker finanziari, ovvero fissano i tassi di cambio a cui l'Exchange è disposto a comprare o vendere bitcoin in cambio delle principali valute tradizionali, o di altre criptomonete. Successivamente alla registrazione nella piattaforma, è possibile dunque effettuare gli scambi tramite il motore di trading interno.

Nella maggioranza dei casi i siti di Exchange offrono, in maniera accessoria, anche il servizio di online wallet agli utilizzatori della piattaforma.

Gli Exchange soffrono spesso di problemi di sicurezza, poiché rappresentano la preda più facile da attaccare per i criminali informatici. È infatti consigliato di utilizzarli esclusivamente per il tempo necessario ad effettuare le conversioni, e non per conservare ingenti somme di crittovaluta.

La maggior parte delle piattaforme di Exchange si sta dotando di procedure di identificazione dell'utente, attraverso la presentazione di documenti e prove di residenza in sede di registrazione al sito.

Questo è dovuto al rispetto delle varie normative in tema di riciclaggio, e determina l'impossibilità di acquistare bitcoin in modo anonimo all'interno di tali piattaforme.

I principali siti di Exchange[25] attualmente operanti e i loro elementi distintivi sono mostrati nella Figura 13.

Bitcoin exchanges

Timespan: 24h 3d 7d 30d **6m** 2y 5y | Market type: all **exchange** derivative OTC | Currency: all **USD** EUR JPY GBP SGD PLN CAD more

	Name	Rank	Volume [BTC]	Spread [%]	Spread 10 BTC[%]	Spread 100 BTC [%]	Volatility (stddev)	Trades per minute
1	Bitfinex	1 7,838	1 9,971,985	2 0.02	2 0.18	1 0.87	53.47	1 101.85
2	GDAX	2 5,234	2 4,001,255	1 0.00	1 0.16	2 1.08	3 49.40	2 73.40
3	Bitstamp	3 3,466	3 2,858,103	0.10	4 0.41	3 1.37	51.50	3 36.95
4	Kraken	4 1,074	5 1,300,445	5 0.07	0.70	5 3.35	50.80	5 20.55
5	HitBTC	5 985	1,153,884	0.10	1.09	10.12	50.32	4 22.59
6	CEX.IO	795	329,277	0.17	1.30	9.43	4 49.48	12.55
7	itBit	646	567,838	4 0.06	5 0.55	4.59	1 47.35	3.71
8	Bit-x	330	322,440	2.26	4.31	7.32	108.74	0.98
9	Gemini	328	4 1,414,694	3 0.04	3 0.39	4 1.55	5 50.27	17.59
10	EXMO	110	121,031	0.26	4.68	35.39	2 49.04	11.82
11	TheRockTrading	3	152	6.42	-	-	90.81	0.01
12	CampBX	2	6	38.80	-	-	1,069.19	0.00
13	BitBay	-	0	2.15	42.44	-	0.00	0.00

Figura 13 - Principali Piattaforme di Exchange

[25] Fonte: http://data.bitcoinity.org/markets/exchanges/USD/6m#rank_desc

3.4 La corsa all'oro: La Bolla del Bitcoin

Per gli studiosi e gli esperti di mercati finanziari, non c'è nulla di più affascinante delle bolle speculative.
In finanza, per bolla speculativa si intende il caso in cui uno specifico asset class o uno strumento finanziario registri una prolungata deviazione del suo prezzo da quelli che sono i suoi fondamentali, ovvero i suoi valori standard.
Lo sviluppo di una bolla speculativa può essere scomposto in tre principali fasi:[26]

- Accumulazione

Nella fase di accumulazione i volumi di compravendita sono elevati poiché gli investitori istituzionali cominciano a prendere posizione sullo strumento finanziario. La crescita dei prezzi è moderata.

- Speculazione

In questa fase iniziano gli investimenti di risparmiatori e investitori retailer. I prezzi sottoposti ad un'accelerazione rialzista portano le quotazioni a livelli molto elevati.
Inizia la fase dell'euforia per gli investitori, che si traduce nel forte ingresso nel mercato da parte di chi non aveva investito, e nell'incremento dell'investimento, guidato dall'avidità di ulteriori guadagni, per chi vi è già dentro.
Al termine di questa fase gli investitori istituzionali, maggiormente esperti ed informati, cominciano a disinvestire parte dell'investimento effettuato nella prima fase.

- Esplosione

In quest'ultima fase comincia il ribasso dei prezzi, il quale può essere graduale con una successiva accelerazione, oppure può configurarsi come un vero e proprio crollo delle quotazioni.
Questo è dovuto da dati o notizie non in linea con le aspettative degli investitori, o a causa di un evento esogeno imprevisto.
A questo punto inizia la fuga degli investitori attraverso una "panic sale", ossia quando le vendite si auto-alimentano in funzione del panico degli investitori.

[26] Psicologia&Mercati – "*Le bolle speculative. La finanza comportamentale applicata ai bitcoin*", 2017 – URL: http://citywire.it/news/psicologiaandmercati-le-bolle-speculative-la-finanza-comportamentale-applicata-ai-bitcoin/a1050826

Avendo trattato le fasi che caratterizzano una bolla speculativa, è importante interrogarsi su processi che originano le bolle finanziarie. Al fine di comprendere l'origine di questi eventi abbiamo bisogno del supporto della finanza comportamentale[27].

A tal proposito, il professore di economia cognitiva Matteo Motterlini ha elaborato il cosiddetto "effetto specchio". Procediamo all'analisi di questa situazione finanziaria-comportamentale.

Se un investitore intorno a sé è circondato da persone eccitate per aver conseguito un guadagno in borsa, subirà inconsciamente una modifica delle proprie preferenze di investimento. Infatti, i guadagni degli altri investitori in borsa causeranno un aumento inconscio della propensione al rischio dell'investitore che stiamo analizzando.

Questo lo potrebbe condurre a commettere l'errore di entrare sul mercato quando le valutazioni sono già troppo elevate, proprio per non avere il rimpianto di non aver conseguito facili guadagni.

Viceversa, se l'investitore ha attorno a sé persone frustrate dalle loro perdite in borsa, tenderà inconsciamente a ridurre la propria propensione al rischio, quindi a non investire o peggio ancora, a vendere causando un potenziale effetto ribassista.

L'economia comportamentale dunque spiega come la prospettiva di guadagni facili, si pensi al caso delle crittovalute come il bitcoin, viene vista a livello inconscio come una generazione di dopamina nel nostro cervello, soprattutto nella parte rettile, quella degli istinti primari. Questo causa uno degli errori principali della maggior parte degli investitori, ovvero l'impulsività.

Impulsività e frenesia sono alla base della formazione e dello scoppio delle bolle finanziarie.

Lo spettro di questi fenomeni speculativi si manifesta da almeno 400 anni nelle forme più diverse, ma per quanto se ne discuta, esorcizzarli sembra essere impossibile.

Infatti, che si tratti di tulipani, di titoli internet (dot-com bubble) o di criptovalute non è rilevante; quando il mercato si muove come un gregge, solamente uno shock traumatico può far cambiare la direzione di marcia.

Tra tutte le bolle registrate nella storia, quella attribuita al Bitcoin rappresenta il territorio più inesplorato in cui gli esperti di finanza si siano imbattuti.

In circa dieci anni, i bitcoin non hanno solamente bruciato ogni record borsistico in termini di prezzo, passando dai 40 centesimi iniziali a oltre 12 mila dollari a metà gennaio 2018, ma hanno anche subito bruschi crolli che ne hanno ridotto fortemente la capitalizzazione.

[27] "*Così la bolla finanziaria nasce nel nostro cervello. Ecco i nuovi segreti della neuroeconomia*", Il Sole 24 Ore, URL: http://www.ilsole24ore.com/art/economia/2010-12-11/cosi-bolla-finanziaria-nasce-121548_PRN.shtml

3.4.1 Trend del prezzo e delle transazioni

Il prezzo del Bitcoin segue, dall'irrisorio valore del 2009, anno di nascita, un forte trend rialzista, caratterizzato però da brusche inversioni di marcia e da una forte volatilità, non comune alle valute tradizionali.

Nel febbraio 2011 il prezzo di un bitcoin raggiunse per la prima volta la parità con il dollaro. Già nel giugno 2011 il prezzo avrebbe toccato il tetto dei 32 dollari circa, per poi scendere e stabilizzarsi a 5 $ nei mesi successivi, in quella che viene chiamata la "Great bubble of 2011".

Valori consistenti del prezzo cominciarono a vedersi dal 2012, superando quota 100 $ per unità nell'inizio aprile 2013, e arrivando, solo 10 giorni dopo, ad un massimo di 266 $.

Ma, il vero boom che ha dato il via alla "corsa all'oro" si è avuto nel marzo 2017, quando il prezzo di bitcoin cominciò ad attestarsi su un valore maggiore dei 1000 $, senza mai più, fino ad ora, scendervi al di sotto.

Il valore massimo raggiunto dalla crittovaluta coincide con un importante accadimento che ha portato i bitcoin nel "mainstream della finanza", ovvero la quotazione dei future aventi come sottostante bitcoin sulla borsa di Chicago.

I primi contratti future su bitcoin sono stati lanciati l'11 dicembre 2017 dal Chicago Board Option Exchange, seconda borsa del mondo per i derivati, e solo una settimana dopo, i future furono disponibili per il trading anche presso il Chicago Mercantile Exchange, la borsa per i derivati numero uno al mondo.

La maggioranza dei contratti future presentava scadenze molto brevi, nell'ordine di un mese.

Il successo del lancio dei future insieme all'attenzione mediatica per l'evento, hanno portato il bitcoin a raggiungere il tetto massimo di quasi 20.000 dollari.

Dal valore massimo raggiunto, a quello attuale di circa 8.400 $ (fine maggio 2018), il trend del prezzo ha subito una forte spinta ribassista, caratterizzata sempre da una forte volatilità.

Sulla base dei dati presenti nel sito blockchain.com, il portale più affidabile nella fornitura di dati sul sistema Bitcoin, Il trend di prezzo è mostrato nella Figura 14.

Figura 14 - Trend del prezzo di Bitcoin

Le motivazioni relative allo scoppio della bolla Bitcoin possono essere di varia natura, ma in questa sede ne verranno trattate due, una motivazione di natura specifica ed una generale.

La motivazione specifica deriva dalla quotazione stessa dei bitcoin attraverso i contratti future. Infatti, la maggioranza degli investitori che ha sottoscritto tali contratti, è stata mossa da meri fini speculativi, volti ad ottenere un guadagno facile quanto veloce.

Un grandissimo numero di investitori ha di fatto sottoscritto contratti future di tipo long (di acquisto) non per detenere i bitcoin successivamente alla scadenza dei medesimi, ma per rivenderli, incrementando ulteriormente il guadagno sperato dai future, dato dalla differenza tra prezzo spot alla scadenza e il prezzo future stabilito. Il meccanismo avrebbe dunque generato un eccesso di offerta seguente alla scadenza dei contratti, portando così al ribasso le quotazioni di BTC.

Per quanto riguarda la motivazione, di natura generale, che spiega il crollo del prezzo di bitcoin, bisogna tener presente che i moltissimi degli investitori che hanno partecipato alla corsa all'oro, spinti dalla febbre del mercato, non avevano compreso la tecnologia blockchain, che regola il funzionamento del sistema Bitcoin. Questo ha portato alla formulazione di aspettative di ritorno economico, tra gli investitori, molto più ottimistiche della realtà, che li ha condotti a subire forti perdite.

Come ogni tecnologia innovativa, anche la blockchain infatti seguirà la curva di Gartner, detta "Hype Cycle" o "fasi del ciclo di vita di una tecnologia"[28].

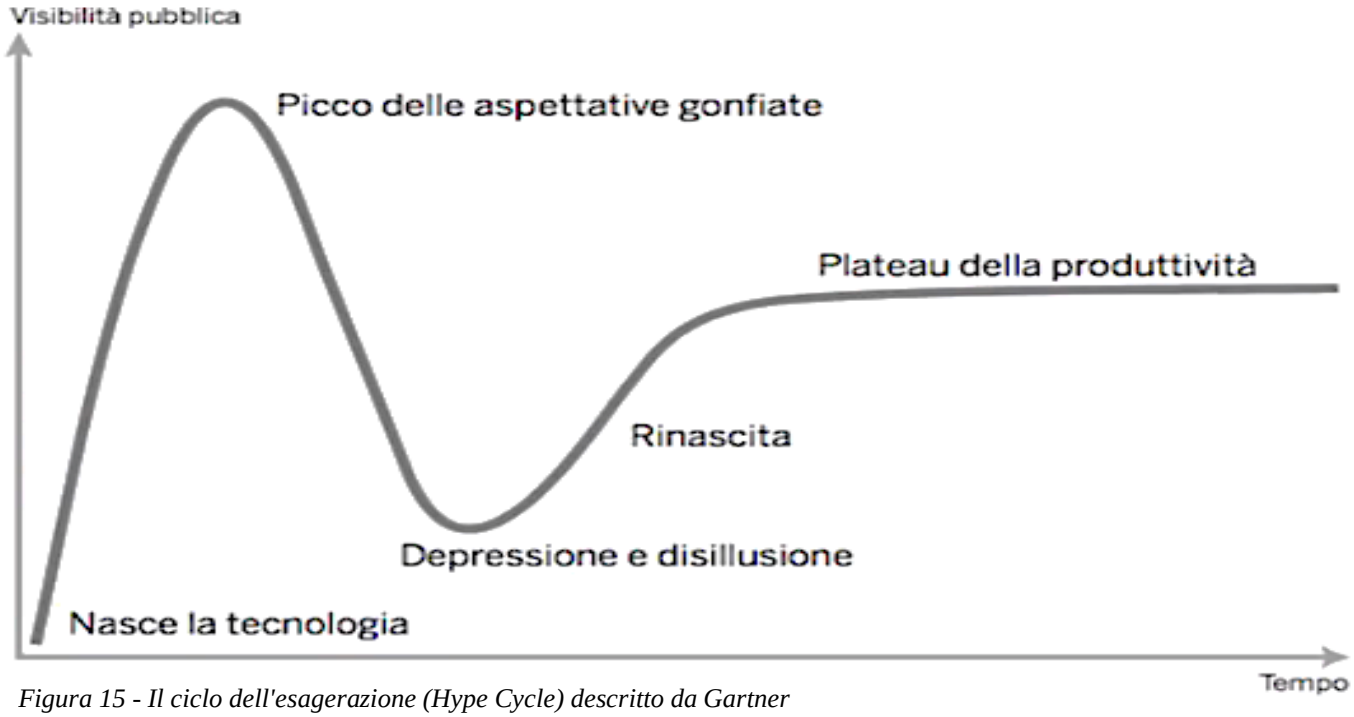


Figura 15 - Il ciclo dell'esagerazione (Hype Cycle) descritto da Gartner

Secondo questa teoria, gli investitori tendono a sovrastimare il valore di una nuova tecnologia nel breve periodo, ed a sottovalutarne l'effetto nel lungo termine. Fino a pochi mesi fa ci trovavamo nella prima curva ascendente, dove investitori poco smart investono miliardi, pensando che la blockchain stravolgerà il mondo

[28] Pistono Federico, "*Startup Zero.0* – Imparare dai fallimenti per creare successi. Dalla Silicon Valley all'Italia", 2017, Hoepli

nei prossimi 2-3 anni. Ovviamente questo non accadrà, ma bensì ci sarà una caduta delle aspettative riguardo la tecnologia, che per i non addetti ai lavori sembrerà un effettivo crollo.
Le aspettative ridimensionate saranno di molto inferiori rispetto al reale valore che la tecnologia assumerà sviluppandosi negli anni.
La veridicità della teoria di Gartner può essere verificata confrontandola con quanto sta accadendo al bitcoin, ovvero relativamente al crollo del prezzo successivo allo scoppio della bolla.
Tutto questo è già successo in passato in vari casi, si pensi alla bolla delle Dot-com avvenuta nel 2000, dalla quale però sono venuti fuori colossi come Google, Amazon e Facebook.
È inoltre importante aggiungere, per fornire una panoramica sul mercato delle crittovalute, che tutte le valute digitali si dimostrano legate al mercato di bitcoin da una forte correlazione.
Questo è dovuto alle caratteristiche del mercato delle crittovalute, quali l'elevata concentrazione e la bassa liquidità, da cui deriva anche l'alta volatilità del prezzo. Si potrebbe in tal senso dire che "quando Bitcoin starnutisce, il mercato delle criptovalute prende un raffreddore".
Per quanto riguarda le transazioni di Bitcoin, invece, bisogna ricordare che esse vengono inserite dai miner all'interno di un nuovo blocco da registrare nella blockchain.
Questo meccanismo rende chiaro che il numero di transazioni che possono essere processate dal sistema Bitcoin è chiaramente funzione della dimensione (size) del blocco.
In relazione alla size, esiste un limite tecnico nella dimensione dei blocchi di Bitcoin pari a 1 MB, il quale permette di raggiungere il limite massimo di 6-7 transazioni per secondo.
Con il recente aumento di popolarità del Bitcoin, il numero di transazioni è aumentato esponenzialmente, trasformando il limite di grandezza del blocco in un vero e proprio ostacolo. Si pensi che il numero di transazioni attualmente si attesta poco sotto le 200.000 al giorno[29], di gran lunga superiore al numero medio di transazioni registrate negli anni precedenti.
Gli utenti della rete, infatti, per veder processate e convalidate le proprie transazioni sono costretti ad aumentare le fee ad esse associate, aumentando quindi la ricompensa per l'attività di verifica svolta dai miner.
Gli eccessivi ritardi nella convalida delle transazioni, uniti all'incremento delle commissioni, hanno nel tempo portato i membri della comunità Bitcoin a dividersi sulla necessità o meno di apportare modifiche al protocollo.
Le modifiche apportate, così come le divisioni all'interno della comunità, saranno affrontate nella sezione ad esse dedicata.

[29] Fonte: https://blockchain.info/it/charts/n-transactions?timespan=all

3.4.2 Le determinanti del Prezzo, Rischi di Svalutazione

Avendo osservato il trend storico del valore di bitcoin, procediamo all'analisi dei principali driver che determinano il prezzo della crittovaluta:

- Le Forze di Mercato: Domanda e Offerta

Data la natura indipendente e decentralizzata del sistema Bitcoin, il suo prezzo non può essere manipolato da un'autorità centrale tramite manovre di politica monetaria.
Infatti, il prezzo di bitcoin, espresso in dollari o euro (BTC/$ - BTC/€), è influenzato dal mercato, ovvero dal meccanismo di domanda e offerta Figura 16[30].

Seguendo la teoria quantitativa della moneta, l'offerta è determinata dallo stock totale di bitcoin in circolazione, che, conoscendo l'algoritmo di generazione della moneta nel sistema Bitcoin, è nota a tutti gli utilizzatori e fissa nel lungo periodo.
Dunque, l'offerta di moneta è stabilita e inelastica, ossia insensibile alla domanda.
Mentre, per quanto riguarda la domanda di crittovaluta, essa è elastica e dipende dallo sviluppo e dall'ampiezza dell'economia Bitcoin.
Questo determina che la domanda sia funzione dell'utilizzo della criptomoneta negli scambi (mezzo di scambio), del numero di transazioni effettuate e del numero di partecipanti al network, ad esempio dato dal numero di digital wallet creati. Infatti, seguendo questo ragionamento, un incremento nell'utilizzo come mezzo di scambio, così come un crescente numero di utilizzatori, determinerà un incremento del prezzo per unità del bitcoin.

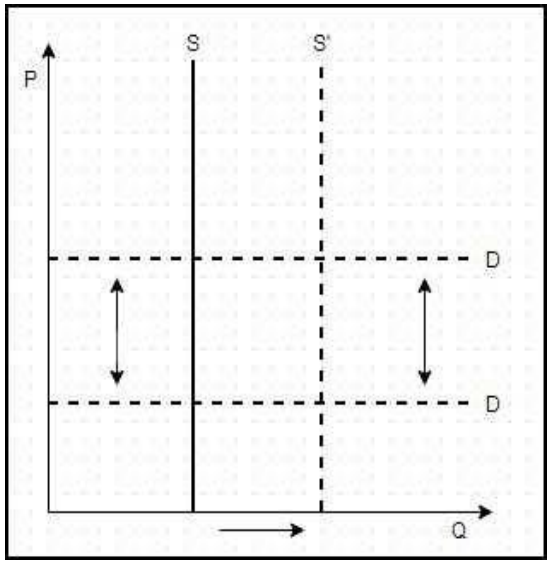


Figura 16 - Domanda e offerta di Bitcoin

- Attrattività del Bitcoin

Seguendo quanto detto, il prezzo del bitcoin è influenzato principalmente dai meccanismi di mercato, dati dall'interazione tra domanda e offerta. Procediamo a valutare i fattori specifici, che, insieme ai tradizionali prima citati, influenzano la domanda di crittomoneta, e dunque il suo prezzo.

[30] "*Bits and Bets – Information, Price Volatility, and Demand for Bitcoin*", Buchholz et al., 2012

Tra i fattori che incidono sull'attrattività della crittomoneta, e quindi sulla domanda, vi è sicuramente la sicurezza del sistema, intesa come impenetrabilità agli attacchi informatici, la fiducia e le aspettative relative alle prospettive di utilizzo della crittovaluta, e l'attrattività come opportunità investimento, paragonando il bitcoin all'oro digitale.

Un altro fattore rilevante per i movimenti della domanda è rappresentato dalle notizie e informazioni rese pubbliche dai media. In questo senso tali notizie possono giocare a favore o contro il bitcoin, influenzando positivamente o in negativo la domanda che incide sul prezzo. Un esempio di notizia che incide negativamente sul prezzo del bitcoin potrebbe essere un attacco informatico ai danni di un noto sito di Exchange, con la conseguente sottrazione dei bitcoin degli utenti, oppure il divieto sull'utilizzo della crittomoneta imposto da uno stato. Mentre, per evento positivo si intende ad esempio l'accettazione della valuta digitale come pagamento da parte di un grande player del commercio.

Inoltre, sulla base di vari studi effettuati da Buchholz e Kristoufek, confrontando le statistiche del numero della digitazione della parola bitcoin sul web con il trend del prezzo, si evince come un aumento dell'interesse sia positivamente correlato con l'incremento del prezzo.

Risulta dunque chiaro come l'interesse generato tra utilizzatori attuali e potenziali rappresenti uno dei principali driver della domanda e quindi del prezzo del bitcoin.

- Andamenti Globali Macroeconomici e Finanziari

Inserendo la crittovaluta all'interno del complesso sistema finanziario, è evidente che alcuni fattori e variabili economico-finanziarie incidano sul prezzo del bitcoin.

L'inflazione è sicuramente uno di questi. Infatti, se il bitcoin ha tra le sue finalità quella di essere una valuta alternativa alle "svalutabili" valute tradizionali, questo comporta che, in periodi caratterizzati da forte inflazione, ci sarà un decremento dell'utilizzo di valute standard a favore del bitcoin, che non risente direttamente di tale variabile. Questo incremento di utilizzo sicuramente spingerà a rialzo il prezzo della crittovaluta. Inoltre, si pensi ad una crisi finanziaria, ad esempio nel mercato azionario, che porterà gli investitori a spostarsi su altri asset class, come potrebbero essere le obbligazioni oppure i bitcoin.

- I Costi di Produzione (Mining)

Una critica molto comune al sistema Bitcoin è dovuta dal fatto che il valore della crittovaluta è basata sulla fiducia in esso riposta dalla comunità di riferimento, e non è garantito da nessuna autorità centrale. Così come il bitcoin anche le valute tradizionali, con l'uscita dal gold standard, non hanno più una base solida a cui agganciare il proprio valore, il quale viene quindi definito corso forzoso sulla base delle decisioni di politica monetaria prese da istituti e autorità centrali.

Questo determina, sia per le valute tradizionali che per il bitcoin, la difficoltà di determinarne il valore intrinseco, ma proviamo a forzare un po' il concetto. Se si pensa alle valute come euro o dollaro, il loro valore reale, non considerando il loro valore forzoso-fiduciario, è rappresentato dal costo di produzione fisica delle banconote e delle monete metalliche. Traslando lo stesso discorso al bitcoin, possiamo identificare come valore intrinseco il costo unitario di produzione del bitcoin, ossia il costo per unità derivante dalla dispendiosa attività di mining, che assolve la funzione di consenso-fiducia del sistema, oltre che di generazione di moneta.
Risulta dunque chiaro che il prezzo del bitcoin è chiaramente agganciato e associato ai costi relativi alla sua produzione, in termini di consumo elettrico-energetico dell'attività di "estrazione".

Per quanto riguarda i rischi di svalutazione del bitcoin, dobbiamo far riferimenti a specifici ed ipotetici eventi. Si pensi ad esempio ad un ipotetico progresso scientifico, riguardo il tema energetico, che permetta di ridurre drasticamente i costi associati alla produzione (mining) dei bitcoin. Un evento compatibile, anche se remoto, potrebbe essere l'utilizzo di una nuova fonte di energia.
Rimanendo sempre nel contesto energetico dei costi di produzione, un altro evento causa della svalutazione della crittomoneta potrebbe coincidere con l'avanzamento tecnico-tecnologico nella produzione dei dispositivi hardware utilizzati specificamente per l'attività di mining. Infatti, la realizzazione di macchinari più efficienti in termini di consumo elettrico, determinerebbe l'abbassamento dei costi di produzione-estrazione, e quindi una svalutazione del bitcoin.
Infine, altri eventuali rischi di svalutazione potrebbero derivare da cambiamenti delle regole del sistema bitcoin, ovvero da modifiche del protocollo.
Pensando ad esempio al limite fissato di unità, che si traduce in un'offerta di moneta massima di 21 milioni di unità, nel caso in cui tale limite venisse espanso, l'incremento di offerta provocherebbe chiaramente la svalutazione della crittovaluta.
Un ultimo caso da prendere in esame è quello di una modifica del protocollo relativa alla dimensione (size) dei blocchi della blockchain su cui si regge il sistema Bitcoin. Un incremento di capacità del blocco permetterebbe a ai miner di inserire un maggior numero di transazioni all'interno dei blocchi da validare. Questo determinerebbe un minor congestionamento della rete, che si tradurrebbe in un minor costo di commissione (fee), associato a ciascuna transazione, per far si che sia validata dai miner in un tempo ragionevole.
Infatti, in una rete congestionata da molte transazioni che devono essere confermate, la discriminante per i miner nella scelta di quali inserire per prime nel successivo blocco si basa sul guadagno derivante dalla fee associata a ogni transazione. I miner, potendo inserire più transazioni all'interno di ogni singolo blocco, valideranno anche quelle con le fee associate più basse, rendendo così più economico e veloce il sistema di pagamento. Al contrario una dimensione del blocco eccessivamente ristretta determinerà alte fee e tempistiche associate alle transazioni per ottenere la loro validazione, condizione che porterà gli utilizzatori a preferire altre crittovalute o sistemi di pagamento diversi, portando alla svalutazione del bitcoin.

3.4.3 Il Limite di unità e i risvolti sulla Deflazione

Come trattato nelle precedenti sezioni, i bitcoin vengono coniati durante la creazione di ogni blocco da registrare nella blockchain, seguendo un algoritmo di generazione prefissato e decrescente nel tempo.
Nei primi quattro anni, dal lancio del sistema Bitcoin, la creazione di un blocco determinava una generazione di 50 BTC, che rappresentano anche la ricompensa per l'attività di validazione svolta dai miner.
Con la creazione di 210.000 blocchi, approssimativamente ogni 4 anni, il tasso di creazione di nuova crittovaluta si dimezza, determinando così un'offerta decrescente nel tempo.
Ad oggi la quantità di bitcoin generati con la validazione e l'inserimento di un nuovo blocco nella blockchain ammonta a 12,5 BTC.
Il numero di nuove unità di valuta emesse diminuirà fino all'anno 2137 circa, quando raggiungerà il valore minimo di 1 Satoshi, ovvero 0,00000001 BTC.
Il limite di generazione verrà raggiunto approssimativamente nel 2140, quando 20.999.999,9769, circa 21 milioni di bitcoin, saranno già stati emessi.
Successivamente a questa data, la creazione di nuovi blocchi non determinerà più la creazione di crittovaluta, determinando come unica ricompensa per i miner le commissioni (fee) associate alle transazioni.
Le valute tradizionali sono solitamente emesse e controllate dalle banche centrali, le quali, nella maggior parte dei paesi occidentali, perseguono una politica monetaria mirata al mantenimento di un'inflazione bassa e costante.
Questo approccio, basato sulla teoria monetaria moderna, è finalizzato a stimolare l'economia e a sostenere un livello occupazionale desiderabile.
Nel sistema Bitcoin, la più importante e dibattuta conseguenza di una offerta di moneta predeterminata e decrescente nel tempo, è rappresentata dalla natura intrinsecamente deflazionaria della crittovaluta[31].
La deflazione, relativa all'aumento del potere di acquisto della crittomoneta, verrà innescata dal momento che la domanda di bitcoin supererà l'offerta, che è fissa e decrescente nel tempo.
Questo processo, data un'offerta di moneta limitata, porterà il valore del bitcoin a crescere nel tempo, connotandolo come una moneta deflattiva, a differenza delle valute tradizionali.
Secondo molti economisti ed esperti, questo aspetto del bitcoin è molto pericoloso, soprattutto per quelli di matrice Keynesiana, i quali definiscono ingiuste sia l'inflazione che la deflazione, attribuendo però a quest'ultima i maggiori rischi per l'economia.
Infatti, in un periodo di deflazione, le aspettative di un ulteriore discesa dei prezzi porteranno le persone a mettere da parte la moneta invece di spenderla, determinando così un collasso della domanda.
Conservare una moneta che aumenta di valore è di fatto molto più conveniente che spenderla.
La riduzione della domanda influenzerà le imprese che, vendendo meno beni e servizi, ridurranno la

[31] Antonopoulos Andreas, "*Mastering Bitcoin: Programming The Open Blockchain*", 2017

produzione e i salari, con chiare e drastiche conseguenze sull'occupazione, che porteranno ad una ulteriore riduzione della domanda e di conseguenza dei prezzi, innescando la spirale deflazionistica.

È importante sottolineare come nel sistema Bitcoin, la deflazione non è causata da un collasso nella domanda, ma bensì da una massa monetaria fissa e sempre prevedibile.

Un altro aspetto importante è rappresentato dal fatto che il bitcoin necessita di un incremento del proprio valore nel tempo per il successo della sua funzione come strumento di pagamento. Proviamo a fare chiarezza su questo punto.

Come descritto nella sezione 2.4.1, affinché una transazione vada a buon fine, deve essere validata dai miner attraverso l'attività di mining. Convalidare le transazioni, però, diventa progressivamente più oneroso e difficile, data la riduzione delle ricompense nel tempo e la forte competizione tra i miner, che causerà nel tempo un incremento della difficoltà per risolvere il puzzle crittografico (proof of work).

Affinché i miner siano incentivati a sostenere spese sempre più elevate per continuare questo indispensabile processo (mining), è necessario che il bitcoin continui ad apprezzarsi, dimostrandosi una moneta deflattiva.

Paul Krugman[32], premio Nobel per l'economia, ritendendo pericoloso un modello monetario deflazionistico, ha affermato: "Quello che vogliamo da un sistema monetario non è di rendere ricche le persone in possesso di denaro, vogliamo facilitare le operazioni e rendere l'economia nel suo complesso ricca".

Dunque, se si vuole configurare il bitcoin come una valuta alternativa, non dovrebbe essere percepito e considerato come un buon investimento a lungo termine, data la sua natura deflattiva.

Come potenziale sistema monetario che gestisce transazioni, il Bitcoin dovrebbe di fatto discostarsi dall'immagine di asset di investimento o di strumento di copertura valutaria, nel caso le monete tradizionali risentano dell'inflazione.

Quanto detto è poco realistico, poiché la volatilità e i risvolti deflattivi della crittomoneta, la allontanano sempre di più dalla classificazione come valuta, connotandola principalmente come un investimento.

Per concludere, il bitcoin rappresenta quindi un tipo di moneta deflattiva, ritenuta dai più esperti come dannosa per un'economia basata sui consumi, poiché l'aumento del suo valore nel tempo non li incentiva.

[32] Paul Krugman, "*Why is deflation bad?*" - URL: https://krugman.blogs.nytimes.com/2010/08/02/why-is-deflation-bad/

3.5 Le Divisioni all'interno della comunità Bitcoin: Hard e Soft Fork

Data la natura open-source del software Bitcoin, all'interno della comunità il dibattito sulla scalabilità del sistema, e sulle modifiche da apportare al protocollo per conseguirla, è sempre stato oggetto di accese discussione e differenti punti di vista.

Le principali questioni riguardo la scalabilità del sistema bitcoin hanno avuto ad oggetto la velocità nel processare e validare le transazioni, e i costi associati a questo procedimento, ovvero le fee di transazione.

Durante la trattazione il concetto di fork è stato discusso analizzando vari casi specifici. Con il termine fork viene identificata la biforcazione della catena blockchain, che avviene attraverso la creazione di due rami distinti a partire dallo stesso blocco. Un fork comincia quindi con la creazione di due blocchi alla stessa altezza (block height).

Come precedentemente discusso, questo evento può verificarsi spontaneamente, ovvero quando due diversi miner trovano la soluzione per validare un blocco, e la comunicano agli altri nodi a distanza di pochi istanti. Tale genere di fork è molto comune e non desta particolari preoccupazioni, poiché, tra le due ramificazioni, la versione ufficiale della catena sarà quella maggiormente estesa, rendendo invalida, "orfana", la catena su cui i miner hanno lavorato di meno, quindi la più corta.

Casi sicuramente più interessanti di fork sono quelli in cui la biforcazione deriva da una proposta di modifica del protocollo[33], ed è sinonimo di upgrade del software Bitcoin. Infatti, cambiando il protocollo, la blockchain cambia le regole e le modalità di costruzione della catena di blocchi sono diverse da quelle basate sulle regole precedenti.

Altro tema interessante è che anche la creazione di una nuova crittomoneta può avvenire attraverso un fork. Infatti, nel caso in cui una parte significativa della comunità si opponga alle modifiche del protocollo proposte, si creerebbe uno split permanente della blockchain, in cui una catena è quella originale, e l'altra è la blockchain di una crittovaluta alternativa. Questo è stato il caso di Bitcoin Cash, che analizzeremo successivamente.

Un fork, relativo ad una modifica del protocollo, può essere classificato come "soft fork" o "hard fork" sulla base dell'impatto che genera sui wallet ed i nodi della rete Bitcoin, in termini di aggiornamento dei client-software. Generalmente un hard fork richiede alla rete l'aggiornamento dei software utilizzati (nodi e wallet), mentre un soft fork è almeno parzialmente retro compatibile con questi software.

Gli hard fork rappresentano un cambiamento del protocollo in grado di condurre a uno split perenne della blockchain.

L'unico modo per evitare tale split è che all'interno della comunità Bitcoin si crei un sufficiente consenso sulle nuove regole del protocollo.

Procediamo ad analizzare più nello specifico le due tipologie di fork.

---

[33] "*Da Nakamoto all'Hard Fork: la storia del Bitcoin, gli upgrade, la politica, gli aneddoti*", Alberto De Luigi, 2018, URL: http://www.albertodeluigi.com/2017/07/17/storia-e-upgrade-del-bitcoin/#6

Un soft fork è un aggiornamento del protocollo Bitcoin che generalmente si traduce nel passaggio da una regola permissiva ad una più stringente. Questa modifica del sistema, solitamente gradita da nodi, miner, client e altri software che operano nella rete, non esclude le regole precedenti e quindi non determina una biforcazione della catena.

Caratteristica principale dell'adottamento di una modifica soft fork è la reversibilità.

Infatti, l'idea di fondo dei soft fork è quella di nascondere le modifiche ai vecchi client-software (pre soft fork), in modo che essi siano in grado di leggere i nuovi dati senza accorgersi delle modifiche effettuate.

L'hard fork, invece, consiste in una modifica del protocollo Bitcoin, generalmente non consensuale, che può provocare una scissione permanente nella blockchain.

Le modifiche del protocollo che si presentano sotto forma di hard fork, nella maggior parte dei casi, permettono una situazione che prima non era valida, ad esempio l'aumento della dimensione del blocco da 1 a 2 MB, oppure la restrizione di alcune regole e il contemporaneo allargamento di altre.

Con un hard fork non è possibile mantenere il vecchio client-software, infatti in caso di adottamento della modifica del protocollo, l'hard fork è irreversibile. Si pensi alla modifica relativa all'aumento della size del blocco fino a 2 MB, dopo che è stato minato il primo blocco maggiore di 1 MB, si creerebbe una divisione della blockchain, in quanto i nuovi e i vecchi software lavorerebbero con regole tra loro incompatibili.

Per riassumere, in caso di soft fork, a differenza di un hard fork, le vecchie versioni del software (vecchio protocollo) riconoscono come validi i blocchi della blockchain generati con il nuovo software (protocollo modificato-nuovo).

La relazione tra protocollo iniziale (legacy chain) e protocolli modificati tramite hard fork e soft fork, che riassume quanto finora detto, è mostrata nella Figura 17.

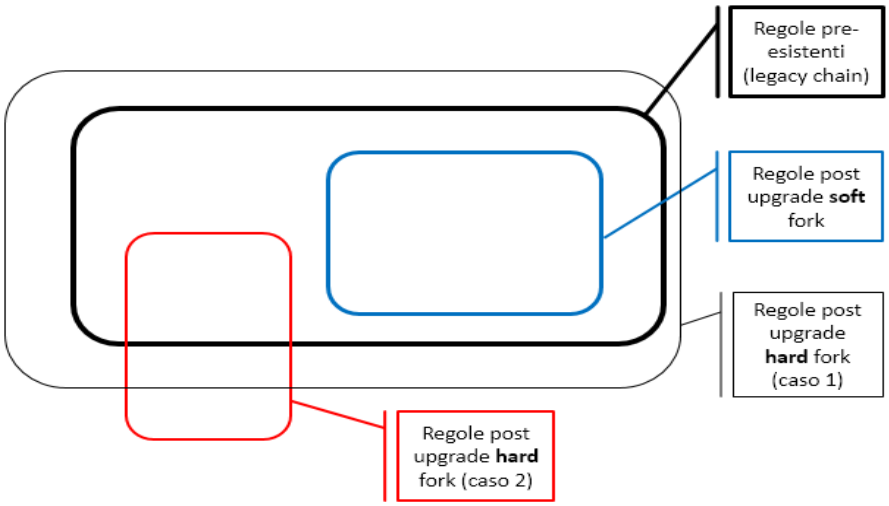


Figura 17 - Relazione tra Protocollo esistente, Protocollo post hard fork e post soft fork

Affinché una modifica del protocollo abbia effetti per l'intera rete è necessario che il nuovo software, che applica le modifiche apportate al protocollo, sia adottato da una maggioranza qualificata della comunità.

Dunque, utenti-nodi e miner devono deliberatamente scaricare la versione aggiornata del software Bitcoin, compatibile con le modifiche del protocollo, spostando il consenso sul nuovo set di regole.
Per concludere, in caso di hard fork relativi al cambiamento del protocollo Bitcoin, gli scenari che si possono configurare sono fondamentalmente tre:

- Se la stragrande maggioranza di nodi e miner, scaricando il nuovo software, adotterà la modifica del protocollo, la blockchain rimarrà unica. Non ci sarà quindi la biforcazione della catena.

- Se la modifica verrà adottata dalla maggioranza della comunità, ma una minoranza significativa non la adotterà, si creeranno due blockchain distinte che seguono regole diverse. Questo determinerà la creazione di una nuova crittomoneta alternativa al bitcoin.

- Se la stragrande maggioranza della comunità non adotterà la modifica, tutto rimarrà come era prima della proposta (vecchio protocollo)

3.5.1 Le principali modifiche del Protocollo Bitcoin

La continua diatriba sulle modifiche da apportare al protocollo Bitcoin per rendere il sistema scalabile, si è concentrata sulle possibili soluzioni in grado di rendere più efficienti i pagamenti, in termini di velocità e costi.
L'incremento della popolarità del bitcoin, e il conseguente aumento del numero di transazioni, hanno portato la rete a congestionarsi, causando ampi ritardi nella convalida delle transazioni (anche 24 ore), e costi ad esse associati elevati per incentivare i miner a validarle.
Nel corso del tempo, sono stati proposti dalla comunità moltissimi upgrade del protocollo, ma, in questa sede, le proposte analizzate sono due:

- Segregated Witness

Spesso abbreviato in SegWit, rappresenta un soft fork che consente al protocollo Bitcoin di gestire un maggior numero di transazioni.
L'idea di fondo si basa sul separare dai dati di ogni transazione, che vengono registrati nei blocchi, le firme, e di raccoglierle in una struttura separata. In una transazione bitcoin, la firma o "testimone" (witness), realizzata con la chiave privata del mittente, rappresenta la condizione di spendibilità di quei determinati bitcoin, e pesa circa il 60 % della dimensione totale dei dati relativi alla transazione.

Pertanto, separando la firma dagli altri dati della transazione, che verranno inseriti nel blocco, si avrà una riduzione della size (byte) delle transazioni, consentendo così di aggiungerne un numero maggiore all'interno di ogni blocco, il cui limite di memoria è fissato a 1 MB.
Secondo alcune stime, l'adozione di SegWit genererebbe un incremento di capacità del blocco, dovuto al mino peso di ogni transazione da inserire, analogo a quello che si avrebbe se fosse direttamente aumentata la dimensione del blocco a circa 2 MB.
Inoltre, l'adozione della modifica SegWit renderebbe possibile l'applicazione della tecnologia Lightning Network, per rendere le transazioni immediate, anonime e con minori commissioni, ma questa implementazione verrà trattata in seguito nella sezione dedicata alle prospettive future di scalabilità.
La modifica del protocollo Bitcoin Segregated Witness, subordinata ad una adesione dell'80% della comunità, proposta come soft fork, venne attivata il 24 agosto 2017.

- Segregated Witness 2x

La precedente proposta di modifica SegWit ha diviso la comunità Bitcoin tra chi era a favore e chi credeva che la soluzione avrebbe risolto i problemi di scalabilità solo momentaneamente.
Quest'ultima corrente di pensiero, infatti, sosteneva la necessità di un aumento del limite della dimensione dei blocchi (fissato a 1 MB), piuttosto che un alleggerimento del peso relativo ai dati delle transazioni, come proposto da SegWit.
La contro proposta di modifica del protocollo, chiamata Segregated Witness x2, si caratterizzò per accettare SegWit, ma proponendo ulteriormente l'incremento della dimensione del blocco fino al limite di 2MB, da realizzare tramite hard fork.
Il 23 maggio 2017 durante il Consensus a New York chiamato "Bitcoin Scaling Agreement at Consensus 2017", 52 aziende hanno firmato un accordo che stabilisce l'attivazione di SegWit con il consenso del'80% della rete Bitcoin e l'avvio di un hard-fork per portare block size a 2 MB entro 6 mesi.
Il problema di proporre l'ulteriore modifica relativa alla block size, attraverso un hard fork, risiede nel fatto che, nel caso la proposta sia adottata, ogni miner e nodo del network saranno obbligati ad effettuare l'aggiornamento dei software, data l'incompatibilità della modifica con i software precedenti.
L'8 novembre 2017, però, gli sviluppatori di SegWit 2x annunciano la cancellazione dell'hard fork, pianificato il successivo 16 novembre, a causa della mancanza di consenso della rete.

3.5.2 Bitcoin Cash

Come affermato precedentemente, se una modifica del protocollo Bitcoin, tramite hard fork, viene accettata dalla maggioranza della comunità, ma esiste una minoranza significativa che non la adotta, si creeranno a partire dallo stesso blocco due blockchain distinte. Questo evento determina la nascita di una nuova crittomoneta, agganciata alla blockchain sostenuta dalla minoranza qualificata.

Quanto descritto è accaduto il 1° agosto 2017, quando parte degli sviluppatori appartenenti alla comunità Bitcoin, contrari all'implementazione della modifica Segregated Witness, hanno rifiutato tale modifica e in aggiunta proposto l'aumento della dimensione del blocco fino a 8 MB, mediante un hard fork.

Il nome Bitcoin "Cash", deriva proprio dalla volontà, di alcuni sviluppatori, di rendere il bitcoin un sistema più efficiente nei pagamenti reali, incrementando la velocità di validazione delle transazioni e riducendone i costi associati. Tali risultati sarebbero stati raggiunti con l'incremento del limite di dimensione dei blocchi. Attraverso l'hard fork, da cui è nato Bitcoin Cash, tale limite è stato portato a 8 MB, rispetto a quello di 1 MB previsto dai blocchi generati con la versione tradizionale del software Bitcoin.

La motivazione per cui tramite il fork si è venuta a creare una biforcazione della catena e una nuova valuta, risiede nel fatto che la blockchain di Bitcoin Cash, una delle due biforcazioni, accetterà e registrerà come validi solamente blocchi più grandi di 1 MB (vecchio limite), fino al limite di 8 MB. Questo determinerà il rifiuto dei blocchi di massimo 1 MB generati sulla blockchain di Bitcoin, regolata dal protocollo originario, vedendoli quindi rifiutati da nodi e miner Bitcoin Cash.

Viceversa, la blockchain classica di Bitcoin non elaborerà e considererà validi i blocchi della catena di Bitcoin Cash, data la loro dimensione maggiore del limite di 1 MB previsto dal protocollo prima del fork.

Una conseguenza interessante per i detentori di bitcoin prima del fork, è il potenziale guadagno derivante dalla moltiplicazione delle monete possedute. Proviamo a fare chiarezza.

Come precedentemente trattato, i bitcoin posseduti da un utente non sono salvati nei wallet digitali, ma sono registrati nella blockchain sotto specifici indirizzi. Con il fork avviene una biforcazione della blockchain a partire da uno stesso blocco, la quale da vita, oltre alla catena originaria, alla blockchain di Bitcoin Cash.

Sia la catena che segue le nuove regole (Bitcoin Cash), sia la catena originale (Bitcoin), hanno in comune i blocchi della blockchain che vanno dal primo inserito fino all'ultimo prima del fork, dal quale partono le due ramificazioni. Questo fa si che le due catene, fino al momento del fork, abbiano la stessa radice, una storia comune. Dunque, se prima del fork un utente era in possesso di un certo ammontare di bitcoin, associati ad un determinato indirizzo, tale informazione sarà presente in entrambe le catene, una volta avvenuta la biforcazione (post fork). Questo determinerà la moltiplicazione delle crittovalute possedute, poiché i bitcoin riconosciuti di proprietà dell'utente sulla vecchia catena, saranno riconosciuti anche nella nuova blockchain di Bitcoin Cash, questa volta però sotto forma della nuova crittovaluta (Bitcoin Cash).

Il protocollo di Bitcoin Cash è stato aggiornato il 15 maggio 2018 aumentando il limite di dimensione del blocco da 8 a 32 MB.

3.5.3 Bitcoin Private: Una Privacy Coin

Continuando il discorso delle crittovalute nate dai fork, come Bitcoin Cash, non si può non parlare della neonata Bitcoin Private, lanciata sul mercato il 2 marzo 2018.
Bitcoin Private rappresenta il primo caso di "Fork Merger" nella storia delle crittovalute. Per fork merger si intende la catena risultate dalla fusione fra due blockchain, entrambe nate da una biforcazione (fork) delle loro rispettive blockchain originali. Nello specifico caso di Bitcoin Private le due blockchain fuse sono quella derivante da un fork della catena di Bitcoin e quella nata dalla biforcazione della catena di Zclassic, una crittovaluta basata su un'altissima privacy (privacy coin).
La finalità di questa fusione è la creazione di una nuova crittomoneta che avesse caratteristiche e solidità del Bitcoin oltre che la maggiore privacy fornita dalla tecnologia implementata in Zclassic.
L'incremento di privacy è garantito dall'adozione della tecnologia ZK-Snarks (zero knowledge), la quale consente di registrare le transazioni sempre su una blockchain pubblica, ma senza che mittente e destinatario siano identificabili. Questo rappresenta un nuovo sistema di sicurezza impenetrabile, che usa maggiormente la crittografia su blockchain.
In Bitcoin, invece, si ha una condizione di pseudo anonimato, in quanto un utente è identificato da un indirizzo, generato a partire da una chiave pubblica, a cui però non è associata la sua identità.
È importante aggiungere che, così come con Bitcoin Cash, chi fosse stato possessore di una quantità bitcoin precedentemente al fork merger, avrebbe conservato i suoi bitcoin e in più avrebbe ottenuto la stessa quantità di Bitcoin Private. Infine, rispetto al Bitcoin, Bitcoin Private presenta blocchi il doppio più grandi e una velocità nel processare e validare le transazioni 4 volte superiore.

3.6 Vantaggi e Criticità del Bitcoin

Avendo fornito un'accurata panoramica sulla principale crittovaluta, di seguito è proposta una sintesi schematica dei principali vantaggi del Bitcoin:

- Trasparenza

Nel sistema Bitcoin chiunque è in grado di seguire in tempo reale tutta la catena delle transazioni. Infatti, ogni transazione è si criptata, ma ha una storia tracciabile sulla blockchain, ossia sul registro pubblico che può essere liberamente visualizzato. Le transazioni sono catene di firme digitali che possono essere quindi tracciate.

- Anonimato

Si parla di anonimato nel sistema Bitcoin, più correttamente di pseudo anonimato, perché in una transazione, sia pagante che beneficiario sono identificabili solo attraverso i loro indirizzi Bitcoin, rappresentati da stringhe alfanumeriche. In una transazione gli indirizzi sono due, l'indirizzo del mittente da cui sono stati inviati i bitcoin e l'indirizzo di destinazione delle crittovalute, appartenente al beneficiario.
Tali indirizzi sono ricavati dalle chiavi pubbliche degli utilizzatori, senza però che esse siano collegate alle loro identità. Esistono comunque dei rischi per cui è possibile ricollegare un indirizzo Bitcoin all'identità dell'utilizzatore, come descritto nella sezione 3.3.4.

- Costi e Velocità delle Transazioni

In condizioni di non congestionamento della rete, le commissioni associate alle transazioni sono molto più economiche rispetto a strumenti di pagamento tradizionali come carte di credito o bonifici. Nel sistema bitcoin si attestano in media a circa 0,0001 BTC, pochi centesimi di euro.
Mentre per quanto riguarda la velocità di esecuzione delle transazioni, in Bitcoin sono necessari mediamente 10 minuti per far si che una transazione ottenga una prima conferma, attraverso il suo inserimento in un blocco della blockchain. Le ulteriori conferme relative alla transazione si avranno con l'inserimento nella catena dei blocchi successivi. A differenza dei classici bonifici che impiegano giorni, è importante sottolineare che la tempistica indicativa di 10 minuti è si più efficiente, ma è subordinata all'assenza di un elevato numero di transazioni da processare che congestionerebbe la rete.

- Rigidità del Protocollo

La rete Bitcoin è decentralizzata, dunque non esiste nessuna autorità centrale in grado di modificare il protocollo o di costringere gli utenti e minatori ad accettare tali modifiche. Come affrontato nella sezione 3.5, le modifiche al protocollo vengono apportate mediante il rilascio di nuove versioni del software Bitcoin, nel quale il protocollo si esplica. Inoltre, tali modifiche si considerano accettate solo se la maggioranza di utilizzatori, nodi e miner passano alla versione aggiornata dei rispettivi software utilizzati.
Nel tempo si è manifestata la difficoltà di ottenere la maggioranza di consensi sulle proposte di modifica rilevanti del protocollo, connotando quindi la sua rigidità come un vantaggio in termini di democrazia.

- Decentralizzazione

L'indipendenza da autorità centrali come governi o banche, rende Bitcoin un sistema totalmente decentralizzato basato su una rete peer-to-peer, nella quale gli utenti comunicano in modo diretto senza la presenza di intermediari. La correttezza delle transazioni bitcoin è garantita dall'attuazione di regole e operazioni crittografiche presenti nel protocollo.
In questo contesto, la fiducia e il consenso non sono demandati a un'entità centrale, ma si realizzano con dei procedimenti informatici ampliamente accettati e condivisi dalla comunità Bitcoin.

Procediamo l'analisi sintetizzando gli svantaggi e le principali criticità di Bitcoin:

- Irreversibilità delle Transazioni

Nel sistema Bitcoin, quando un utente invia una quantità di crittomoneta ad un determinato indirizzo, e la transazione viene processata e registrata nella blockchain, non c'è possibilità di annullarla.
L'unico modo per riavere i propri bitcoin indietro è chiederne la restituzione, se si conosce l'identità del destinatario a cui sono stati precedentemente inviati.
Se consideriamo l'utilizzo di bitcoin per un pagamento, l'irreversibilità delle transazioni tutela il commerciante, che è certo dell'impossibilità che il pagamento sia annullato, ma non il consumatore, che a fronte di un pagamento effettuato ed irreversibile potrebbe ricevere merce difettosa o addirittura nulla.

- L'onerosità dell'attività di mining

Come descritto nella sezione 2.4.1, l'attività di convalida delle transazioni (mining) determina ingenti costi per i miner, in termini di appositi dispositivi hardware da acquistare e consumo di energia elettrica.
Con la difficoltà attuale, in termini di potenza di calcolo, di risoluzione del puzzle crittografico (proof of work) per validare i blocchi di transazioni, l'attività di mining è redditizia solo se si sfruttano economie di scala, come le Mining Farm.
L'incremento nel tempo della potenza computazionale presente nella rete Bitcoin, determina una maggiore difficoltà nella convalida dei blocchi di transazioni, che rende la competizione tra i vari miner sempre più serrata, costringendo quindi ognuno di loro ad aumentare gli investimenti in dispositivi hardware per ottenere ricompense dal mining, a discapito degli altri miner.

- Rischi di Centralizzazione

La decentralizzazione del sistema Bitcoin è portata in auge dai suoi sostenitori come una delle caratteristiche più lodevoli della crittovaluta. Nonostante questo, se si analizza a fondo l'architettura del sistema e i suoi partecipanti, si evince come la completa decentralizzazione è utopica. Questo può essere appurato sia riguardo il mining, sia per la distribuzione dei bitcoin fra i suoi utenti-utilizzatori.
Dal punto di vista del mining, il problema risiede nel fatto che la maggioranza del potere di calcolo per minare i blocchi è in mano a pochi soggetti[34]. Basti pensare che circa il 40% della potenza computazionale totale è detenuta da Bitmain, una Mining Farm cinese che ha anche il primato nel mondo per la produzione di dispositivi hardware per il mining.
Dato che per funzionare la blockchain di Bitcoin ha bisogno che i miner convalidino i blocchi di transazioni, più il potere di calcolo è accentrato nelle mani di pochi soggetti, più essi potranno decidere quali transazioni accettare, quali blocchi minare, quando e come farlo.
Dunque, affinché una crittovaluta sia realmente decentralizzata, è necessario che la potenza di calcolo sia non concentrata ed equamente distribuita fra tutti i partecipanti della rete.
Invece, dal punto di vista delle monete possedute, è chiaro come alcuni soggetti e player del comparto detengano una quantità tale di bitcoin da poter influenzare il mercato con strategie di "pump e dump".
Basti pensare che l'anonimo ideatore del sistema di pagamento, Satoshi Nakamoto, secondo le stime della rivista specializzata Cointelegraph, possiederebbe circa un milione di bitcoin, rappresentando la più grande fra le balene del bitcoin.

- Costi e tempistiche delle transazioni (Block Size)

Come precedentemente descritto tra i vantaggi, i bassi costi e velocità delle transazioni rappresentano un vantaggio del Bitcoin rispetto agli strumenti di pagamento tradizionali. Quanto detto è vero solo se il numero di transazioni non è così elevato da congestionare il sistema. Nell'ultimo anno, con la maggiore conoscenza e diffusione del Bitcoin, si è arrivati a picchi giornalieri di transazioni avviate nel sistema, talmente alti da congestionare la rete. Tale situazione ha comportato lunghi ritardi nella conferma delle transazioni, anche 24 ore, e costi (fee) di transazione pagati dagli utilizzatori per incentivare i miner, troppo onerosi.
Dal confronto con il circuito di carte di credito Visa, si evince come Bitcoin debba ancora risolvere alcune problematiche e difficoltà per essere un sistema di pagamento scalabile. Infatti, il circuito di carte di credito Visa, ha la capacità di supportare mediamente 2000 transazioni al secondo, fino ad un limite di 4000 Tps, mentre il sistema Bitcoin permette di raggiungere un limite massimo di 6-7 transazioni per secondo.

[34] "*Scenario della Centralizzazione del Mining: perché la Decentralizzazione è fondamentale*", 2018 - URL: https://medium.com

Una soluzione a questo problema di scalabilità nei pagamenti bitcoin, è la proposta di incrementare la size (bytes) del blocco per aumentare il numero di transazioni da includervi, sostenuta da una buona parte della comunità. L'aumento di dimensione del blocco consentirebbe ai miner di inserire molte più transazioni da validare, il che si tradurrebbe in minori tempistiche per processare le transazioni e minori costi ad esse associati, data la minor concorrenza nell'essere validate rispetto al caso di un congestionamento della rete.
L'aumento della size del blocco però produrrebbe degli effetti da non sottovalutare. Infatti, se da una parte incentiva i miner poiché possono ottenere un maggior numero di fee potendo includere molte più transazioni nel blocco da confermare, dall'altra parte riduce la sicurezza del sistema. Questo è dovuto al fatto che un aumento della dimensione di ogni blocco da inserire nella catena, si tradurrebbe nel tempo in un forte appesantimento della blockchain, il che rappresenterebbe un forte svantaggio per i full-node (nodi pieni) che devono conservare/immagazzinare tutta la blockchain.
La minor sicurezza del sistema è data dal fatto che, con l'appesantimento della catena, ci saranno molti meno nodi-pieni nella rete che conserveranno tutta la storia delle transazioni Bitcoin, determinando così una minore condivisione e decentralizzazione del registro pubblico blockchain.

- Volatilità del Prezzo e Deflazione

La forte volatilità che caratterizza il trend del prezzo di bitcoin, scoraggia l'abbandono degli strumenti di pagamento tradizionali a favore della crittovaluta. La volatilità deriva dalle caratteristiche del mercato delle crittovalute, ovvero la ancora bassa liquidità e la mancanza di spessore, che determinano forti oscillazioni del prezzo in corrispondenza di spostamenti della domanda, data la natura limitata e fissa dell'offerta di bitcoin. Una maggiore stabilità del valore di bitcoin favorirebbe una diffusione su più ampia scala, ad esempio aumentando gli esercenti disposti ad accettarla, ovvero facilitando le decisioni di consumo per gli utilizzatori. Inoltre, è importante tener conto che i risvolti deflattivi del bitcoin non permettono di identificarla totalmente come valuta, infatti non lo rendono una semplice riserva di valore, e lo pongono in contrasto con un'economia basata sui consumi (3.4.3)

- Vulnerabilità del Protocollo e Sviluppo Continuo

Il sistema Bitcoin, nonostante la sua sicurezza, è vulnerabile ad attacchi informatici nel caso in cui un soggetto o un insieme di soggetti, di concerto, detengano una potenza computazionale talmente alta da mettere a repentaglio la stabilità dell'intero sistema. I casi principali di attacchi informatici sono quelli descritti nella sezione 2.4.2, ovvero il "double spending attack" e il "51% attack", il cui verificarsi è

subordinato al possesso, da parte del nodo o dei nodi malevoli, della maggioranza del potere di calcolo dell'intera rete.
È inoltre ricordare che ancora non è stato rilasciato il software ufficiale e definitivo di Bitcoin, dato che è ancora in fase beta, con molti fattori incompleti e in fase di sviluppo. Questo se da una parte lascia aperte le prospettive di sviluppo, dall'altra rende il sistema Bitcoin ancora instabile e in fase di maturazione.

- Assenza e difformità della Regolamentazione

La situazione legale e fiscale di Bitcoin, ove non assente, non è omogenea e varia da Stato a Stato. L'analisi sulla regolamentazione del Bitcoin verrà condotta nella sezione successiva.

3.7 Le Prospettive future e la Scalabilità del Bitcoin

Per scalabilità del sistema Bitcoin, si intende la sua capacità di svilupparsi, diffondersi ed affermarsi come un efficiente sistema di pagamento complementare rispetto alle valute tradizionali.
Per ottenere la scalabilità della crittomoneta, da anni la comunità Bitcoin si interroga sugli sviluppi e le migliorie da apportare al protocollo per favorire la completa diffusione dell'innovativo sistema di pagamento tra il pubblico.
Il dibattito sulle modifiche da apportare e i progressi da compiere, ha dato vita a profonde spaccature all'interno della comunità, nella quale sono presenti correnti di pensiero diverse e contrastanti.
Le proposte di modifica del protocollo, volte all'efficientamento del sistema Bitcoin, cercano di perseguire la sua scalabilità attraverso due modalità: scalabilità "on chain" e "off chain".
Per scalabilità on chain si intende la modifica e il miglioramento delle caratteristiche intrinseche della blockchain di Bitcoin, come potrebbe essere ad esempio l'incremento della dimensione (size) di ogni blocco della catena. Mentre, la scalabilità off chain si riferisce alla creazione di un'infrastruttura tecnologica sopra a Bitcoin e la sua blockchain, una "second layer technology".
Tale infrastruttura tecnologia di secondo livello si articola in applicazioni e implementazioni tecnologiche, che in sinergia con il sistema Bitcoin e la sua blockchain, permettono la crescita e la scalabilità della crittovaluta.
Possiamo quindi paragonare la scalabilità on chain ad una crescita e uno sviluppo endogeno del sistema Bitcoin, mentre la scalabilità off chain può essere equiparata ad una sua crescita esogena.

3.7.1 Lightning Network: Progetto di Scalabilità “off chain”

Una delle discriminanti che più influiranno sul futuro delle crittovalute è sicuramente l’usabilità. Infatti, non solo il futuro di Bitcoin, ma anche quello delle altre criptomonete, dipende dalla loro diffusione come strumento di pagamento utilizzato dalle persone nella vita quotidiana.

Ad oggi, non esiste nessuna crittovaluta che possa garantire pagamenti semplici, rapidi e non aggravati da onerose commissioni. Queste problematiche riguardano anche il Bitcoin, in cui il limite di dimensione del blocco, pari a 1 MB, si è tradotto nel dicembre 2017 in un sovraccaricamento della rete, che ha portato a lunghe attese per la conferma delle transazioni, e i costi, ad esse associati, fino al valore di 25 dollari per singola transazione.

Uno dei metodi sostenuti dalla comunità per migliorare il sistema Bitcoin, attraverso una scalabilità off chain, è quello di gestire le transazioni senza trasmetterle e registrarle nella blockchain, gestendole appunto “off chain”. Questo consente la riduzione dei dati caricati nella blockchain e del costo delle transazioni (incentivo per i miner), non essendoci più lunghe file di transazioni da essere approvate.

Un noto progetto che persegue questo tipo di scalabilità è Lightning Network[35], che si fonda sulla modifica del protocollo Bitcoin Segregated Witness, e consiste in un sistema di transazioni certificate gestite temporaneamente fuori dalla blockchain.

Questa tecnologia, sviluppata dal team di sviluppatori di Lightning Labs, consente di realizzare un numero esponenzialmente più grande di transazioni nella rete, senza però appesantire la blockchain, poiché gli scambi avvengono su un secondo strato fuori dalla catena. (off chain - second layer technology).

Con Lightning Network, i nodi della rete aprono un canale fra loro (payment channel) attraverso una transazione on chain, ovvero registrata sulla blockchain.

Dopo l’apertura di tale canale, ogni futura transazione, ad esempio fra due nodi, viene svolta su quel canale e salvata in locale dai singoli nodi, quindi senza la necessità di registrare dati sulla blockchain, evitando di appesantirla.

Altra importante conseguenza è che in tutte le transazioni realizzate nel canale non c’è bisogno di pagare commissioni (fee) ai miner, poiché vengono gestite off chain.

Il canale di pagamento creato, utile soprattutto per i rapporti di pagamento continuativi, può restare aperto a tempo indeterminato. Tutte le transazioni avvenute nel canale fra i due nodi determinano un saldo, ad esempio dopo varie transazioni in entrata ed uscita Bob deve 5 BTC ad Alice. Tale saldo viene, alla chiusura del canale, gestito come una transazione che viene caricata sulla blockchain, come detto, solo alla fine del rapporto. Si pensa che il funzionamento sopra descritto di Lightning Network consentirà alla rete Bitcoin di scalare a migliaia di transazioni al secondo rispetto al limite attuale di 7 Tps, senza aumentare il limite di dimensione dei blocchi, ovvero un esempio di scalabilità on chain.

[35] “*Bitcoin: Il Lightning Network risolverà il problema delle transazioni?*”, 2018 – URL: https://www.advister.it/bitcoin-lightning-network-transazioni/

Evitando l'incremento della size dei blocchi oltre 1 MB, infatti, si consente a tutti i nodi pieni (full-node) di continuare a sincronizzare l'intera blockchain, senza renderla eccessivamente pesante come nel caso di un aumento della block size. Un grande numero di nodi pieni che conservano l'intero registro blockchain è strumentale alla natura decentralizzata del sistema Bitcoin.

La tecnologia Lightning Network, nonostante sia ancora in fase beta e gli sviluppatori stessi ne hanno sconsigliato l'utilizzo, è stata utilizzata già in molte transazioni[36]. Un esempio lampante dei vantaggi che si possono conseguire dall'implementazione di questa tecnologia è dato da una transazione realizzata nella blockchain di Bitcoin in cui sono stati trasferiti 40.000 BTC, all'epoca circa 450 milioni di euro, ad un costo (fee di transazione) pari ad 1 € (0,0001 BTC).

Al fine di fornire un quadro completo dei progetti di scalabilità off chain, oltre a Lightning Network, è doveroso citare anche il caso delle "Side-Chain", dette catene laterali. Tali side-chain sono tecnologie emergenti che consentono a token e crittovalute, appartenenti ad una blockchain, di essere utilizzati in modo sicuro in una blockchain separata e di essere poi spostati nella blockchain originale, se necessario. La funzionalità Side-chain ha un enorme potenziale per migliorare le capacità attuali della blockchain, in termini di tempi e costi.

Va sottolineato che tali progetti, fino ad ora, hanno interessato poche valute digitali, tra cui non rientra il Bitcoin.

3.7.2 Atomic Swap: Un Exchange peer-to-peer decentralizzato

Gli Exchange, come descritto nella sezione 3.3.5, sono delle società private che forniscono una piattaforma in cui gli utenti possono realizzare compravendite di bitcoin in cambio di valute tradizionali, o altre crittovalute listate sull' Exchange.

Risulta chiaro capire che questo è un servizio centralizzato, in cui la piattaforma di scambio è fornita e gestita da una società privata.

Una modalità innovativa e alternativa a quella descritta per realizzare scambi fra le crittomonete, è rappresentata dal progetto Atomic Swap, pronto per essere implementato nel sistema Bitcoin.

Questa innovativa tecnologia offre all'utente la possibilità di effettuare scambi fra diverse crittomonete direttamente dal suo wallet Bitcoin, in modo Peer-to-Peer con gli altri utilizzatori.

Questo sistema evita quindi la necessità di rivolgersi ad un Exchange tradizionale e centralizzato, e permette di realizzare in maniera anonima gli scambi con una spesa irrisoria prossima allo 0 %, rispetto allo 0,5 % applicato in media dai siti di Exchange tradizionali.

[36] "*Lightning Network – Scalable, Instant Bitcoin/Blockchain Transactions*" – URL: https://lightning.network/

La rivoluzione apportata dalla tecnologia Atomic Swap consiste, quindi, nell'affidare al protocollo Bitcoin la funzione di Exchange, e non ad un ente centrale, mettendo in contatto direttamente domanda e offerta di bitcoin, ad esempio attraverso degli smart contract.

3.7.3 La Regolamentazione

L'instabilità del Sistema Bitcoin è dovuta a diversi elementi, fra cui sicuramente rientra l'assenza e la difformità di regolamentazione fra i vari Stati.
Procediamo in questa sezione ad analizzare i vari orientamenti al livello mondiale nei confronti del bitcoin, descrivendo la situazione normativa attuale rispettivamente in Asia, in USA e in Europa, con un focus sull'Italia[37].
È importante sottolineare come uno Stato, difronte ad una nuova tecnologia, possa assumere fondamentalmente tre politiche di regolamentazione:

- Non regolamentare nulla
- Regolamentare in modo restrittivo ed ostile
- Creare un ecosistema che incentivi l'utilizzo della nuova tecnologia, in modo da sfruttarne l'innovazione

Iniziando la disamina dal continente asiatico, quello che risalta, è come la regolamentazione sulle crittovalute proceda a macchia di leopardo.
Infatti, se da una parte la Cina e la Corea del Sud hanno annunciato l'intenzione di regolamentare le crittomonete e assumono posizioni sempre più restrittive, soprattutto per quanto riguarda la scarsa trasparenza delle Initial Coin Offering, in Giappone le crittomonete, come il bitcoin, sono state decretate una forma legale di pagamento dal 2017. A partire proprio da questo anno, in Giappone, diverse società cominciarono a pagare parte dei salari dei dipendenti in valute virtuali, come il bitcoin.
Negli United States, la Commissione per i Titoli e gli Scambi (SEC) si è attivata per bloccare e contrastare diverse attività relative alle crittovalute, con la necessità di tutelare i cittadini, potenziali investitori. Nonostante ciò, la SEC ha comunque riconosciuto pubblicamente il fenomeno delle crittovalute e delle Initial Coin Offering, come un innovativo e valido strumento di raccolta di capitale per le aziende, soprattutto per quelle di piccole dimensioni, oltre che una possibile fonte di stimolo per l'economia e la crescita del paese.

[37] "Le norme su Bitcoin e crittovalute nei diversi Paesi: Il quadro", 2018 – URL: https://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-crittovalute-nei-diversi-paesi-quadro/

Continuando il discorso della regolamentazione per quanto riguarda l'Europa, dal primo incontro fra Commissione europea, i regolatori, i supervisori e gli esperti del settore crypto, è emersa la decisione di rimandare al summit del G20 di marzo 2018, la discussione sulla strategia comune da intraprendere per inquadrare normativamente le crittovalute.

Nonostante queste attese, ci sono state varie prese di posizione, come quella del presidente della BCE Mario Draghi, il quale ha affermato come l'Europa guardi con interesse la tecnologia blockchain, alla base di Bitcoin, come punto di partenza per introdurre innovazioni importanti, distinguendo le valute virtuali dalla tecnologia che ne consente l'utilizzo.

La Commissione europea, seguendo questa direzione, ha istituito l'Osservatorio e Forum sulla blockchain, perseguendo l'obiettivo di monitorare gli sviluppi ed i progetti basati su blockchain nel territorio europeo, mettendo inoltre a disposizione dei finanziamenti per promuovere i progetti di governi ed industrie che sfruttano le opportunità offerte da tale tecnologia. Infatti, la Commissione Ue prevede che la blockchain influirà sui servizi digitali e reinventerà i modelli aziendali in molti settori, come ad esempio quello finanziario, assicurativo, sanitario, logistico, dei pubblici servizi, e nella gestione dei diritti di proprietà intellettuale.

Le conclusioni a cui è giunto il tavolo di lavoro europeo sono sei[38]:

- La tecnologia blockchain è promettente per i mercati finanziari, a detta di Dombrovskis, vice presidente della Commissione europea.
- Le crittomonete, come il bitcoin, sono diventate oggetto di una forte speculazione, e questo espone investitori e consumatori a grandi rischi, come la perdita del capitale.
- Gli allarmi su tali rischi sono importanti e riguardano anche l'Europa.
- Le Initial Coin Offering sono diventate per le imprese innovative del settore una modalità per raccogliere ingenti capitali. Questa, a detta della Commissione europea, rappresenta una grande opportunità che va però valutata alla luce dei rischi relativi alla scarsa trasparenza delle società emittenti e dei business plan sottostanti.
- Va valutato se, per regolamentare il comparto delle crittovalute, conviene adottare la regolamentazione esistente per altre materie, oppure è necessaria una regolamentazione comunitaria ad hoc.
- I cripto-asset incorporano ampi rischi in tema di riciclaggio di denaro derivante da attività illecite e di finanziamento delle attività illegali, tra cui il terrorismo. Infatti, proposta della Commissione è quella di assoggettare alla direttiva sul riciclaggio gli scambi in monete virtuali e i fornitori di portafogli digitali (wallet). Proposta sulla quale è stato raggiunto un accordo fra i co-legislatori europei.

[38] "Bitcoin, niente regole fino al 2019. La Ue aspetta il G20", 2018 – URL: https://www.corrierecomunicazioni.it/finance/bitcoin-niente-regole-al-2019-la-ue-aspetta-g20

L'attuale assenza di una specifica regolamentazione a livello comunitario sulle crittovalute, ha portato i vari paesi dell'Unione a muoversi in modo autonomo.

In Gibilterra, da gennaio 2018, è stato annunciato che le ICO verranno regolamentate, istituendo una figura di sponsor come garante di queste operazioni.

Stessa posizione è stata presa dall'Autorità federale di vigilanza sui mercati finanziari svizzera, sottoponendo a vigilanza prudenziale le operazioni di emissione di nuove crittovalute, ovvero le ICO.

In Germania, l'Autorità federale di supervisione finanziaria ha emanato un comunicato per definire gli obblighi da rispettare per i promotori di ICO, mentre in Francia viene sottolineata la necessità di un'autorizzazione preventiva per l'offerta di derivati su crittovalute. Infatti, in rispetto alla MIFID II, vi è il divieto di offrire tali strumenti derivati attraverso canali elettronici, per una maggiore tutela dell'investitore.

In Italia, invece, le crittovalute sono regolamentate unicamente sotto il profilo del contrasto al riciclaggio di denaro; estendendo di fatto i controlli, oltre a chi effettua attività di conversione tra crittomonete e valute legali (Exchange), anche agli operatori commerciali che accettano valuta virtuale per il pagamento di beni e servizi.

Il recepimento della Quinta Direttiva anti-riciclaggio, in Italia, ha portato ad inserire i bitcoin e le piattaforme digitali di scambio nella categoria delle "valute ed intermediari non finanziari digitali".

Con questa mossa, sono state assoggettate le transazioni in crittovaluta, che resta priva di corso legale, alle stesse regole di vigilanza sulle tradizionali società finanziarie.

Questa posizione potrebbe determinare un ostacolo alla diffusione dell'utilizzo di crittomonete nel nostro paese, disincentivando le aziende che vogliono sviluppare tali prodotti e soluzioni in Italia, le quali preferiranno quindi il collocamento in paesi caratterizzati da una regolamentazione più favorevole ed incentivante.

Nonostante le varie posizioni prese dai diversi Stati sul tema crypto, il problema irrisolto è quello di definire una precisa natura giuridica della crittomonete.

Ci sono Paesi, come il Giappone, in cui si sta procedendo verso una totale parificazione fra il Bitcoin e la moneta legale, ed altri che rifiutano questa direzione per evitarne la diffusione e l'uso criminale, come l'Italia.

Per ultimo, è importante menzionare che, negli Stati Uniti, è recente il caso di una pronuncia giudiziaria sulla base della quale Bitcoin è moneta, e non quindi commodity, come aveva precedentemente decretato la Commodity Futures Trading Commission.

CAP IV - LE PRINCIPALI ALTCOIN: UN SETTORE IN ESPANSIONE

4.1 ETHEREUM: Una Crittomoneta 2.0

L'ondata rivoluzionaria ed innovativa generata dal lancio del Bitcoin ha determinato, negli anni successivi, una forte spinta a convergere verso la traiettoria tecnologica tracciata dalla più nota crittomoneta.
Questo ha portato alla realizzazione e al lancio di una miriade di progetti relativi al mondo crypto, con la speranza di replicare il successo del Bitcoin.
Infatti, gli annunci relativi al lancio di nuove monete digitali avvengono con regolarità, e la continua realizzazione di tutti questi progetti, ha determinato inizialmente la formazione del comparto delle crittovalute, e successivamente la sua incontrollabile espansione.
Basti pensare che, nonostante l'alto tasso di fallimento di questi progetti, il numero delle valute digitali immesse sul mercato è elevatissimo, ad oggi oltre 1.400[39].
Da qui deriva il neologismo "altcoin", termine usato per identificare l'insieme di crittovalute create dopo il bitcoin.
L'elevato numero di altcoin, lascia immaginare come, in questo grande insieme, siano realmente poche le crittomonete che possano replicare o addirittura performare i risultati ottenuti dal bitcoin.
In questa ottica, il seguente capitolo è finalizzato a descrivere due principali altcoin che, più di altre, si stanno delineando come possibili leader nel comparto, attualmente traghettato dal bitcoin.
Le due crittomonete in questione, che verranno analizzate nel presente capitolo, sono rispettivamente: Ethereum e Ripple.

4.1.1 La Storia di Ethereum

Sviluppata circa sette anni dopo il bitcoin, Ethereum sembra essere, a detta degli esperti del settore, la crittovaluta maggiormente in grado di stravolgere le logiche tradizionali, poiché è basata su una tecnologia più innovativa e sostanzialmente migliore di quella del bitcoin.
Il progetto Ethereum fu inizialmente descritto dal suo giovane ideatore, Vitalik Buterin, come il risultato del personale lavoro e della sua ricerca nella comunità Bitcoin.

[39] "*Quante monete come i bitcoin esistono*?", La Stampa – Economia, 2018 – URL: http://www.lastampa.it/2018/01/13/economia/quanti-monete-come-i-bitcoin-esistono//

Successivamente, nel 2013, Vitalik Buterin pubblicò il white paper di Ethereum, nel quale veniva dettagliatamente descritta la progettazione tecnica, la logica alla base del protocollo Ethereum e l'architettura degli smart contract.

Per una descrizione introduttiva di tali contratti digitali si rimanda alla sezione 2.7.

Il progetto Ethereum venne formalmente annunciato dal suo fondatore nel gennaio 2014, nella conferenza nord-americana sul Bitcoin tenutasi a Miami, in Florida.

Proprio durante quel periodo, Vitalik Buterin cominciò a cooperare con il Dottor. Gavin Wood, un programmatore inglese, che divenne, con il primo, co-fondatore di Ethereum.

Una volta sviluppato il software Ethereum, la realizzazione di un progetto come quello di Buterin, e quindi il lancio di una nuova criptomoneta e l'avvio della sua blockchain, è subordinato all'impiego di ingenti risorse sia economiche che umane, come gli sviluppatori.

Con la finalità di avviare e finanziare il progetto, dunque realizzare una rete strutturata di sviluppatori, miner, investitori e stakeholders vari, il team di Ethereum annunciò la sua Initial Coin Offering nel 2014, ovvero la prevendita di crittovaluta "ether", rappresentante l'unita di moneta di Ethereum (ETH). Infatti, nel luglio 2014, l'Ethereum Fundation ha offerto l'allocazione iniziale di ether tramite una prevendita pubblica di 42 giorni; nella quale ha venduto la sua crittomoneta in cambio di bitcoin.

Durante questo breve periodo (42 giorni), Ethereum ha raccolto un patrimonio di 18.439.086 $, in base al cambio BTC/$ nel 2014, ottenendo dagli investitori 31.591 bitcoin in cambio di circa 60.102.000 di ether.

Il grande ammontare di risorse raccolto dalla ICO, è stato inizialmente utilizzato per pagare i debiti legali e i mesi di lavoro svolto degli sviluppatori, e successivamente per finanziare e promuovere lo sviluppo continuo del progetto Ethereum.

Tra il 2014 e il 2015 la comunità di sviluppatori è stata invitata a testare i limiti della rete Ethereum, la quale è stata ufficialmente lanciata, in versione beta, ovvero in fase di sviluppo, il 30 luglio 2015.

Il rilascio del network ha permesso agli sviluppatori di iniziare a scrivere (coding) smart contract ed applicazioni decentralizzate da implementare nella blockchain di Ethereum.

Successivamente, i miner hanno iniziato ad unirsi al network di Ethereum per garantire la sicurezza della sua blockchain e, chiaramente, guadagnare ether dai blocchi "risolti", "estratti".

Ethereum rappresenta un passo successivo nel futuro della blockchain.

Infatti, nonostante sia costruito dalle stesse fondamenta della tecnologia di Bitcoin, amplia considerevolmente le opportunità offerte dalla blockchain, attraverso l'inserimento di smart contract e applicazioni decentralizzate.

Ad oggi la crittovaluta ether è la seconda più grande del mercato, con un valore unitario di circa 530 $ ed una capitalizzazione di mercato pari a 52,5 miliardi di dollari, meno della metà di quella del Bitcoin (123 bn).

Nella pagina successiva, la Figura 18 illustrata il trend del rapporto fra i prezzi di ether (ETH) e bitcoin (BTC).

Figura 18 - Trend del rapporto fra il prezzo di ether (ETH) e il prezzo di bitcoin (BTC)

4.1.2 Principali Caratteristiche: Tecnologia e Differenze con Bitcoin

All'interno di questa sezione, l'analisi è incentrata sull'innovativa tecnologia di Ethereum, ovvero una piattaforma in cui sviluppare applicazioni decentralizzate e smart contract, dove la moneta, gli ether, è utilizzata per la compravendita di servizi all'interno di essa.

La tecnologia blockchain è riuscita a mettere insieme operazioni e processi appartenenti a diversi campi, come l'informatica, l'intelligenza artificiale, le comunicazioni e anche la finanza.

Nell'idea di fondo dell'ideatore del sistema Bitcoin, Satoshi Nakamoto, lo sviluppo completo della tecnologia blockchain avrebbe dovuto seguire tre step, ma nel Bitcoin ne identifichiamo solo due: l'implementazione del registro pubblico delle transazioni, il protocollo Bitcoin, ovvero il sistema di transazioni per trasferire un valore in modo peer-to-peer.

Il terzo step è rappresentato dalla possibilità di gestire, tramite blockchain, anche applicazioni decentralizzate e contratti digitali, ma questo richiedeva forti sviluppi nel sistema di elaborazione. Nakamoto, infatti, non immaginava solamente di inviare denaro senza intermediari fra due soggetti, ma anche di avere una moneta programmabile e ricca di caratteristiche attivabili in modo informatico.

Un progetto tecnologico che sta portando la blockchain al terzo step è proprio quello di Ethereum.

Ethereum rappresenta una piattaforma blockchain aperta, la quale consente ad ogni utilizzatore di costruire ed utilizzare applicazioni decentralizzate, che vengono eseguite sulla blockchain stessa.

Infatti, nel tardo 2013, Vitalik Buterin ha proposto una singola blockchain che ha però la capacità di essere riprogrammata per eseguire qualsiasi computazione arbitrariamente complessa. La programmabilità della tecnologia, ha reso possibile per gli utenti lo sviluppo di contratti "smart" e di applicazioni decentralizzate (DApp), piuttosto che fornire un set predefinito di operazioni, proprio come in Bitcoin. In tal modo, la blockchain di Ethereum è una piattaforma utilizzabile per una vasta gamma di applicazioni decentralizzate Peer-to-Peer, che includono sicuramente le criptomonete, ma non si esauriscono ad esse.
Gli sviluppatori possono dunque creare applicazioni che si eseguono sulla Ethereum Virtual Machine (EVM), ovvero sul cuore della tecnologia, che può eseguire codici di una complessità algoritmica arbitraria, come smart contract o DApp.
Procediamo ad un'analisi tecnica del funzionamento della tecnologia di Ethereum[40].
L'unità di base di Ethereum è il suo conto (account). La blockchain di Ethereum registra e mostra lo stato di ogni conto, e tutte le transazioni avvenute sulla rete Ethereum sono costituite da trasferimenti di valuta (ether) ed informazioni tra i vari conti. Esistono appunto due tipologie di conti:

- Externally Owned Accounts (EOAs): conti controllati da chiavi private, dunque da individui.
- Contract Accounts: conti regolati da codici informatici e possono essere creati solo da un EOA.

È importante sottolineare che gli EOA sono chiaramente controllati dagli umani, con le loro chiavi private, ma anche i contract accounts lo sono. Infatti, nonostante siano regolati da codici informatici, sono programmati per essere controllati da un EOA, a sua volta controllato con le chiave privata da un utilizzatore.
La terminologia più conosciuta per identificare i contract account è "smart contract", ovvero dei programmi che si eseguono quando una transazione è inviata allo specifico conto (contract account).
Gli utenti della rete Ethereum dunque creano nuovi contratti con l'impiego del codice (coding) sulla blockchain.
Gli smart contract associati ai conti compiono una determinata operazione solo dopo aver ricevuto istruzioni di eseguire l'azione da un EOA. Dunque, un contract account esegue l'operazione da esso prevista solo se indotto da un conto EOA.
Come nel sistema Bitcoin, gli utilizzatori devono pagare delle commissioni di transazione alla rete, più nello specifico ai miner che convalidano le transazioni inserendole nella blockchain. Questo meccanismo protegge il registro pubblico blockchain di Ethereum da operazioni contrastanti fra loro e da attacchi informatici.
Queste commissioni vengono pagate in ether e sono identificate con il termine "gas", che rappresenta il guadagno che giustifica il costo della computazione svolta dai miner.

[40] Ethereum Fundation, "*Ethereum White Paper*", 2015 – URL: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper

Detto in parole semplici, il termine “gas” identifica il carburante necessario a far impiegare ad un miner la sua potenza di calcolo per eseguire un determinato smart contract o un’applicazione sulla blockchain.
Ad esempio, nel caso in cui un miner decida di eseguire un contratto, significa che il mittente della transazione, a cui è associato uno smart contract, ha deciso di pagare un certo “Gas-Price”, in ether, superiore o uguale al prezzo a cui il miner ha deciso di mettere a disposizione il proprio potere computazionale e le proprie risorse, in termini di consumo elettrico e tempo. Quando il carburante si esaurisce, i miner terminano l’esecuzione dello smart contract.
Infatti, il mittente di una transazione deve pagare “gas”, ovvero una quantità di ether, per ogni step del programma o del contratto smart attivato, inclusi i calcoli e l’archiviazione in memoria.
I miner sono nodi del network di Ethereum che ricevono, diffondono, verificano ed eseguono le transazioni e le applicazioni decentralizzate ad esse associate. Queste operazioni si realizzano attraverso l’attività di mining, ovvero con il raggruppamento delle transazioni avvenute nella rete all’interno dei blocchi, in un meccanismo concorrenziale in cui i miner si sfidano per far si che il loro personale blocco sia il prossimo ad essere aggiunto alla blockchain.
Oltre alle fee associate alle transazioni (gas), i minatori sono ricompensati anche con un ammontare fisso pari a 5 ether (crittovaluta) per ogni blocco che “minano” con successo, in modo tale che questo meccanismo rappresenti l’incentivo economico per le persone che dedicano risorse come hardware ed elettricità al funzionamento della rete di Ethereum. Gli ether di volta in volta generati in questo modo (5 ether), rappresentano la funzione di generazione di moneta in Ethereum.
Così come avviene nel sistema Bitcoin, i miner hanno il compito di risolvere un complesso problema informatico-matematico per validare-minare un blocco con successo.
Il procedimento di risoluzione del problema crittografico è identificato con l’algoritmo di Proof of Work (sezione 2.4.2).
In questo contesto la prova del lavoro svolto (POW) è l’esecuzione stessa del programma o dell’applicazione decentralizzata, risolvendo così la critica di grande spreco di risorse finalizzato alla mera esecuzione di calcoli, mossa verso Bitcoin.
Inoltre, al fine di scoraggiare la centralizzazione della rete dovuta all’utilizzo di hardware specifici per l’attività di mining, come avviene in Bitcoin, Ethereum affida questo compito alle classiche CPU dei computer. Questo determina la possibilità per tutti, e non solo per pochi soggetti, di contribuire alla sicurezza della rete con il mining, consentendo alla rete di Ethereum di gestire la sua sicurezza in modo più decentralizzato rispetto al caso in cui il mining nella blockchain fosse subordinato all’utilizzo di hardware specifici, come in Bitcoin.
Procedendo nell’analisi delle principali differenze fra la piattaforma Ethereum e il sistema Bitcoin, è doveroso menzionare che, nonostante siano entrambi progetti open-source ai quali collaborano vari sviluppatori, l’elemento di differenza con il protocollo Bitcoin è che la blockchain di Ethereum è disegnata per essere flessibile, adattabile e riprogrammabile, al fine di eseguire qualsiasi applicazione informatica, come ad esempio gli smart contract.

Un'altra importante differenza è rappresentata dall'utilizzo della crittovaluta nei due sistemi. Infatti, se in quello Bitcoin la criptomoneta è utilizzata per le transazioni e i pagamenti, nel sistema Ethereum la valuta, ossia gli ether, sono ideati per essere utilizzati dagli sviluppatori nel pagare la potenza di calcolo del network necessaria ad eseguire le applicazioni decentralizzate, da loro sviluppate.

Dunque, nonostante i due sistemi abbiano entrambi una crittomoneta, quello che differisce è la loro finalità. Gli ether, di fatto, non rappresentano un sistema di pagamento alternativo, come i bitcoin, ma servono ad incoraggiare gli sviluppatori nel creare ed eseguire applicazioni sulla blockchain di Ethereum.

Infatti, dal momento che la blockchain di Ethereum viene eseguita da migliaia di computer in tutto il mondo, le applicazioni possono essere eseguite utilizzando la potenza di calcolo di un gigantesco network globale di pc.

Ulteriori differenze fra il sistema Bitcoin ed Ethereum si evincono anche dalla tempistica di validazione dei blocchi, infatti se per minare e quindi validare un blocco in Bitcoin il tempo previsto dal protocollo è settato a 10 minuti, in Ethereum invece, questa tempistica si riduce a soli 17 secondi.

Sempre relativamente all'attività di mining, uno dei problemi del Bitcoin è rappresentato dal fatto che il potere di calcolo dell'intera rete viene "sprecato" per generare numeri casuali (hash) con la finalità di trovare la proof of work, necessaria ad aggiungere blocchi alla blockchain[41]. Ethereum, invece, utilizza in modo migliore i computer collegati al network e la loro potenza di calcolo, permettendo agli sviluppatori di creare applicazioni da eseguire utilizzando la potenza di calcolo combinata della rete, insieme alla tecnologia blockchain.

Mentre, per quanto riguarda l'algoritmo di generazione di moneta, che sappiamo essere in Bitcoin determinato e agganciato al limite di 21 milioni di unità, in Ethereum vengono generati, come ricompensa per i miner, 5 ether per ogni blocco "estratto", con il limite però di 18 milioni di unità di crittovaluta generata al massimo ogni anno.

Questo determina chiaramente, a differenza dei bitcoin, un'offerta di moneta non limitata nel tempo, che si sgancia così dai suoi risvolti deflattivi, tanto criticati dal pensiero di molti economisti.

Un'ultima importante differenza con il sistema Bitcoin è rappresentata dai portafogli elettronici, o digital wallet, che, a differenza dei numerosi wallet Bitcoin, è unico ed è chiamato Ethereum wallet. Quest'ultimo può essere semplicemente scaricato online dal sito www.ethereum.org.

Per concludere la descrizione sulle caratteristiche di Ethereum, è importante sottolineare come essa sia una piattaforma particolarmente adatta ad applicazioni che automatizzano la diretta interazione fra gli utilizzatori e facilita azioni di gruppo coordinate attraverso la rete.

Ad esempio, le interazioni finanziarie oppure i contratti potrebbero essere eseguiti automaticamente ed in modo affidabile usando linguaggi informatici su Ethereum. Le possibilità di Ethereum non si esauriscono a contratti e operazioni finanziarie, ma bensì si estendono a qualsiasi situazione in cui fiducia e sicurezza

[41] Gates Mark, "*Blockchain, la guida definitiva per conoscere Blockchain, Bitcoin, Criptovalute, Contratti Smart e il futuro del denaro*". Prima Edizione, 2017

sono fondamentali, come ad esempio la gestione di proprietà intellettuali, il voto, i trasferimenti di asset, il crowdfunding, le assicurazioni e molte altre.

4.1.3 DApp e Smart Contract

La caratteristica che rende il progetto Ethereum particolarmente interessante, al di là della sua notorietà e della capitalizzazione della crittomoneta ether, è la sua portata generale, in termini di programmabilità della blockchain sottostante, nell'eseguire contratti e applicazioni decentralizzate (DApp).
Queste ultime sono molto simili alle applicazioni tradizionali, ma con la differenza che sono eseguite direttamente sulla blockchain di Ethereum, e non sono gestite in modo centralizzato. Da questo deriva che le DApp godono di benefici quali la sicurezza delle transazioni e dei dati, i quali non possono essere modificati o cancellati, e il risparmio dei costi per gestirle[42].
Come precedentemente introdotto nella sezione 2.7, gli smart contract hanno la finalità di sostituire i contratti tradizionali per renderne più semplice e veloce l'interpretazione e l'esecuzione, sostituendo al linguaggio naturale un linguaggio informatico elaborabile dal computer.
Tale passaggio consente notevoli risparmi in termini di tempo e costi, poiché gli smart contract vengono automaticamente eseguiti, senza dunque l'intervento delle parti coinvolte per attivarlo, e possono essere utilizzati per scambiare digitalmente qualsiasi cosa abbia un valore.
In termini tecnici, uno smart contract è una funzione automatica identificata da un indirizzo (codice) tramite il quale è possibile eseguirlo, e da un saldo che contiene i proventi delle transazioni inviate all'indirizzo associato al contratto, dal quale vengono detratti gli ether necessari a pagare il "gas" utilizzato per l'esecuzione dello smart contract.
Tali contratti sono pubblicamente visibili sulla blockchain, la quale li rende trasparenti, temporalmente identificabili, funzionanti e impossibili da manomettere e interrompere, se non per specifica volontà delle parti in esso coinvolte.
Risulta importante chiarire che la comunicazione tra le applicazioni decentralizzate sviluppate e la blockchain di Ethereum è definita proprio dagli smart contract.
Un esempio potrebbe essere un'applicazione finanziaria che gestisce i vari finanziamenti emessi a favore di diversi soggetti. Tali finanziamenti sarebbero pubblicamente visibili sulla blockchain, e attraverso l'utilizzo degli smart contract, si potrebbe monitorare lo stato di salute dei vari prestiti e revocarli automaticamente, ottenendo la restituzione, nel caso in cui vengano disattesi alcuni covenant; portando, successivamente alla restituzione dei fondi prestati, la cancellazione dei prestiti dal registro blockchain.

[42] Dr. Gavin Wood, "*Ethereum: A secure decentralized generalised transaction ledger*", 2017 – URL: https://ethereum.github.io/yellow/paper.pdf

Un ulteriore esempio potrebbe essere il caso di un datore di lavoro, il quale potrebbe scrivere il contratto di un suo dipendente sulla blockchain di Ethereum.
In questo modo, alla fine del mese, lo smart contract provvederebbe automaticamente a togliere la cifra pattuita dal saldo del contratto, trasferendola al dipendente tramite una transazione. Questa operazione sarebbe dunque realizzata con il costo di una fee in gas molto bassa, senza affidarsi ad intermediari come banche e pagare commissioni alte come nei bonifici.
Le app decentralizzate e i contratti smart rappresentano il passo successivo nell'evoluzione della tecnologia blockchain. Infatti, attraverso queste innovative implementazioni, la "Blockchain 2.0" potrebbe potenzialmente avere un impatto e un'utilità maggiore di quella avuta da Bitcoin e dalla tecnologia blockchain, su cui si basa.

4.1.4 L'Attacco Informatico: Il Paradosso del Rimedio Centralizzato e il Fork

Uno dei principali rischi di blockchain e criptovalute, così come in molti altri contesti digitali, è quello degli attacchi informatici. La probabilità di tale rischio, unita alla capacità di reagire del sistema nel caso in cui l'evento si verifichi, giocano un ruolo determinante sulla fiducia e sulle percezioni di affidabilità dei sistemi di valute digitali. Infatti, fra i driver che muovono la domanda di crittomoneta da parte del pubblico, le percezioni di sicurezza e resistenza del sistema ad attacchi informatici sono determinanti.
Così come è avvenuto per il Bitcoin, con l'hackeraggio del noto Exchange Mt.Gox, anche Ethereum, nella sua recente storia, fu vittima di un destabilizzante attacco informatico.
Nel maggio 2016, tramite un crowdfunding realizzato con la vendita di crittovaluta ether, venne finanziato e lanciato un importante progetto di Ethereum chiamato DAO[43].
La sigla DAO indica la "Decentralized Autonomous Organization", ovvero una società digitale di venture che permette ai suoi soci di acquistare quote con la finalità di investire in nuovi progetti.
Il DAO, fiore all'occhiello del network Ethereum, creato su un codice open-source, è un'organizzazione virtuale di investimenti strutturata senza management, CEO e consiglio di amministrazione, che si fonda dunque sulla completa decentralizzazione. In questo senso, nel DAO, è il collettivo a prendere le decisioni, attraverso la votazione di ogni membro, il quale può finanziare progetti realizzati da società o sviluppatori e beneficiare di eventuali guadagni futuri.
Dunque, per chiarire, DAO rappresentava un contratto, con decine di migliaia di partecipanti, volto a raccogliere fondi, sulla base delle disponibilità dei partecipanti ad investire, che fungeva da fondo di investimento; cioè, attraverso votazioni regolamentate da un meccanismo di consenso come quello della blockchain, i fondi raccolti venivano investiti in progetti promettenti.

[43] "*What is a DAO*", CoinDesk, 2017 – URL: https://www.coindesk.com

Avendo ottenuto finanziamenti per un valore superiore a 160 milioni di dollari, DAO è stato istanziato e implementato nella blockchain di Ethereum, entrando dunque a far parte del suo network.
Essendo stato implementato nella blockchain, ogni transazione avente ad oggetto le quote del DAO, ovvero investimenti, acquisti e vendite, veniva realizzata e memorizzata sulla blockchain Ethereum.
I problemi cominciarono quando, a giugno 2016, qualcuno fra gli utenti, sfruttò una vulnerabilità nel codice DAO, relativamente al processo di disinvestimento della quota nel fondo.
Questo portò alla sottrazione, dal valore del fondo, di oltre 60 milioni di dollari, rappresentati dai circa 3,6 milioni di ether sottratti.[44]
Nonostante la decentralizzazione sia l'elemento fondante di blockchain, crittomonete e anche dell'organizzazione DAO, le scelte di Vitalik Buterin, cofondatore di Ethereum, presero la direzione opposta. Infatti, per porre rimedio all'attacco informatico che aveva scosso l'intera comunità Ethereum, Vitalik Buterin bloccò tutte le transazioni, sia sui mercati in cui venivano scambiati gli ether (ETH) che su quelli del DAO.
Questo si realizzò attraverso un hard fork, ovvero con il cambiamento strutturale delle regole e dei meccanismi della piattaforma Ethereum, con il quale vennero cancellate le transazioni incriminate dal registro blockchain; impedendo così, all'attaccante di disporre della quantità di criptovaluta sottratta, e privandolo della proprietà degli ether illegittimamente ottenuti.
Tale hard fork dunque avrebbe riportato il sistema al momento precedente a quello dell'attacco informatico, e avrebbe consentito al DAO di riottenere le disponibilità sottratte.
L'azione di forza di Vitalik Buterin, ha mostrato alla comunità alcune contraddizioni nell'ideologia stessa di decentralizzazione, poiché, per risolvere la questione, si è ricorsi ad un'azione centralizzata e autoritaria, decisa e messa in atto dall'ideatore della piattaforma Ethereum in persona.
Questa profonda contraddizione ha dato vita a una grave spaccatura all'interno della comunità Ethereum, che ha portato parte di essa a non accettare le modifiche totalitarie effettuate da Buterin, determinando così la divisione di Ethereum in due parti e il fork della sua blockchain, con la conseguente creazione di una nuova crittomoneta.
Una parte era rappresentata dagli utenti che, considerando i principi di immutabilità di Ethereum, non accettavano i provvedimenti e le modifiche, e volevano quindi tornare alle regole precedenti, l'altra, invece, da chi era disposto a rimanere in Ethereum, accettando i cambiamenti effettuati.
La parte della comunità contraria alle modifiche fondò la crittovaluta Ethereum Classic, mantenendo le regole anteriori all'attacco informatico, la seconda rimase stabilmente in Ethereum, ma con le nuove regole.
Dunque, nella data del provvedimento di Buterin, si è avuta una scissione permanente, che ha portato alla nascita di una nuova crittomoneta, Ethereum Classic (ETC), e della sua relativa blockchain (biforcazione).
La nuova blockchain di Ethereum Classic, nata dalla biforcazione di quella originaria, è del tutto

[44] "*The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*", CoinDesk, 2016 – URL: https://www.coindesk.com

indipendente dalla quella di Ethereum (originaria), ma condivide, con questa, gli stessi blocchi fino alla data dell'hard fork, ovvero della biforcazione.
Ad oggi la capitalizzazione di Ethereum, crittovaluta che presenta le regole modificate per risolvere l'attacco informatico, è circa 30 volte superiore a quella di Ethereum Classic, basata sulle regole originarie non modificate.

4.1.5 DAICO: Initial Coin Offering 2.0

Come descritto precedentemente in tema di ICO (2.5), molte emissioni e vendite di nuove monete digitali si realizzano in un contesto deregolamentato e caratterizzato da un'altissima componente di rischio.
Oltre questo, molti progetti finalizzati alla creazione di nuovi token digitali si basano sull'utilizzo di blockchain già esistenti; e in questo contesto, le più utilizzata è quella di Ethereum.
Per un chiarimento sulla differenza tra criptovaluta e token si rimanda alla sezione 2.5.1.
L'utilizzo di una blockchain non proprietaria, su cui basare una nuova moneta digitale, si fonda sul grande risparmio di risorse relativo alla possibilità di non sviluppare e programmare una propria tecnologia.
Di fatto, anche per motivi di sicurezza, viene utilizzata una blockchain esistente e ben strutturata, come quelle su cui si basano le più stabili e importanti criptomonete.
Data la flessibilità e la programmabilità della blockchain di Ethereum, la scelta di molti team di progetti, finalizzati al lancio di nuovi token digitali, spesso ricade su di essa, preferendola alla blockchain più rigida di Bitcoin.
Scegliendo la blockchain di Ethereum per lanciare un token digitale, i suoi miner valideranno anche le transazioni aventi ad oggetto i nuovi token, non solo quelle relative alla crittomoneta principale ether (ETH).
Infatti, tutti i nuovi token digitali che utilizzano la blockchain di Ethereum possiedono lo stesso standard (ERC20), e ciò ne facilita l'utilizzo poiché li rende compatibili con tutti gli smart contract, le applicazioni decentralizzate e le altre "coin" che supportano lo standard ERC20. È possibile creare il proprio token digitale, relativo ad uno specifico progetto, attraverso il sito www.ethereum.org.
Nel 2017 più di 700 token digitali sono lanciati e distribuiti sulla piattaforma Ethereum, e in generale, circa l'85 % di tutti i token utilizzano la blockchain di Ethereum.
Il grande utilizzo della catena di Ethereum per lanciare nuovi token digitali, venduti in fase di ICO, ha recentemente spinto il suo ideatore, Vitalik Buterin, a compiere l'ennesima innovazione nel settore: le DAICO.
Questa volta si tratta di una sorta di autoregolamentazione volta alla protezione degli investitori in sede di Initial coin Offering.

Le DAICO derivano dalla fusione tra il concetto di governance decentralizzata della DAO e il crowdfunding delle ICO (Figura 19)[45].

La DAICO rappresenta un protocollo, ideato recentemente da Buterin, in grado di autoregolamentare l'insidioso e rischioso mercato delle ICO.

Infatti, i finanziatori-investitori del progetto che utilizza la DAICO, tramite un codice informatico, potranno vedere i loro interessi maggiormente garantiti. In pratica, con la DAICO, i finanziatori possono decidere anticipatamente la quota di fondi che gli sviluppatori del progetto possono prelevare per ogni suo step.

Inoltre, nel caso in cui i finanziatori della ICO non fossero più soddisfatti del progetto, potranno ottenere il rimborso del capitale investito attraverso una votazione aperta a tutti i tokenholders.

Questo protocollo è stato ideato, da Vitalik Buterin, per tutelare maggiormente gli interessi degli investitori e per impedire che i team di sviluppatori approfittino dell'assenza di rapporto fiduciario con i loro finanziatori, spendendo i capitali raccolti in modo inefficiente.

In estrema sintesi, grazie all'invenzione della DAICO, chi investe nelle Initial Coin Offering può subordinare la disponibilità dei fondi, per il team del progetto, al raggiungimento di alcune condizioni (milestone).

Questa rappresenta sicuramente una grande tutela nei confronti degli investitori, contro il team che ha condotto l'ICO.

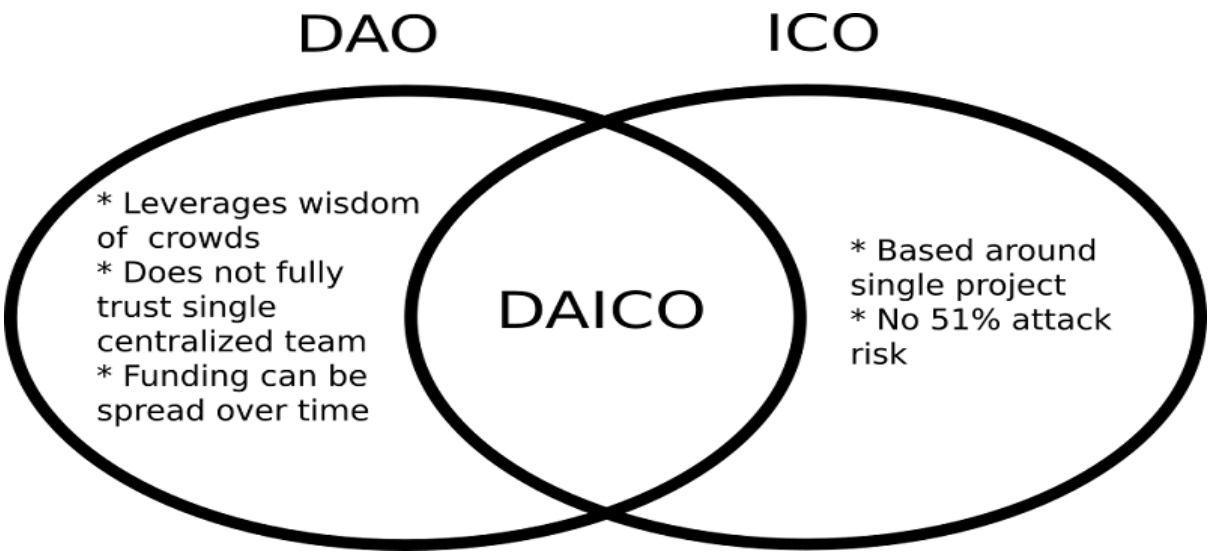


Figura 19 - DAICO: Fusione delle caratteristiche di DAO e ICO

[45] L'assenza del rischio di attacco 51% nelle ICO, come mostrato nella Figura 19, deriva dall'impossibilità di minare i token digitali e soprattutto dall'utilizzo di una blockchain già esistente. Ad esempio, un token venduto in sede di ICO che si basa sulla blockchain di Ethereum verrà gestito proprio su questa blockchain, la quale è caratterizzata da una buona distribuzione del potere di calcolo e dalla presenza di un grandissimo numero di nodi indipendenti. Tali condizioni rendono difficile se non impossibile il rischio di un attacco informatico condotto da uno o più soggetti detentori di oltre il 50% del potere di calcolo dell'intero network Ethereum. Il ragionamento opposto vale in una blockchain dove il potere di calcolo totale è basso e non equamente distribuito, rendendola così penetrabile ad un Attacco 51 %.

4.2 RIPPLE: Una criptomoneta progettata per le banche

Risulta chiaro che, l'ipotetica affermazione nel tempo delle crittovalute, come sistemi decentralizzati e disintermediati, rappresenti uno scenario decisamente avverso all'attuale sistema finanziario e bancario.
Quest'ultimo, decisamente minacciato dal funzionamento Peer-to-Peer delle crittomonete, rischia di perdere terreno nei confronti dei processi meno costosi e più rapidi delle valute digitali, attraverso una disintermediazione del sistema finanziario.
In risposta a questa minaccia, Ripple Lab ha sviluppato e lanciato sul mercato una criptovaluta a misura di banca, che può aiutare il comparto bancario a rispondere alle pressioni, e a cavalcare l'onda crittografica e digitale. La crittomoneta in questione è ripple, nota con la sigla XRP.

4.2.1 Principali Caratteristiche e Funzionamento

Ripple Lab è una società privata che ha sviluppato sia una piattaforma di scambio Peer-to-Peer che una valuta digitale chiamata ripple (XRP), progettata per le banche[46].
Ripple Lab offre agli utenti un suo network chiamato "Ripple Net", le cui regole, definite nel protocollo, sono accettate da tutti i partecipanti, attraverso il quale collega banche, providers e società finanziarie digitali. Il protocollo Ripple, che regola la rete di pagamenti, permette di eseguire transazioni, ovvero trasferimenti di somme di denaro, in qualsiasi valuta. Dunque, il network di Ripple consente alle banche l'esecuzione di transazioni e il cambio fra valute per scambi esteri, senza l'intervento di una camera di compensazione (clearing house), quindi senza un intermediario terzo.
Ripple venne fondata nel 2012 dal programmatore informatico Jed McCaleb, il quale era intenzionato a realizzare un sistema più efficiente, sicuro ed economico per trasferire denaro, rispetto al Bitcoin.
In realtà, l'idea alla base di ripple l'aveva avuta, già nel 2004, il canadese Rian Fugger, e l'aveva chiamata Ripplepay. Dunque, l'idea di Ripple, in un certo senso, è antecedente a quella del Bitcoin.
Per quanto riguarda il numero di crittomonete ripple, tutte le unità sono già disponibili e sono già state tutte generate (pre-minate).
Le unità di crittomoneta sono dunque limitate, e tale limite, codificato nel protocollo, fissa il numero massimo di ripple generati e in circolazione pari a 100 miliardi di unità.
Il fatto che la crittomoneta ripple sia pre-minata, ovvero che tutte le unità sono state già generate, significa che non è possibile fornire hashing power (potere di calcolo) in cambio di nuovi ripple.
Questo determina un basso consumo energetico del network Ripple, rispetto a quello di Bitcoin caratterizzato da un'onerosissima attività di "estrazione" (mining).

[46] "*Ripple, la nuova Crittovaluta sulla bocca di tutti*", Versione Italiana Kindle, 2018

Dei 100 miliardi di unità emesse e disponibili, circa 33 miliardi erano di proprietà del pubblico di investitori, mentre circa 66 miliardi erano di proprietà della stessa società Ripple Lab e di investitori iniziali.

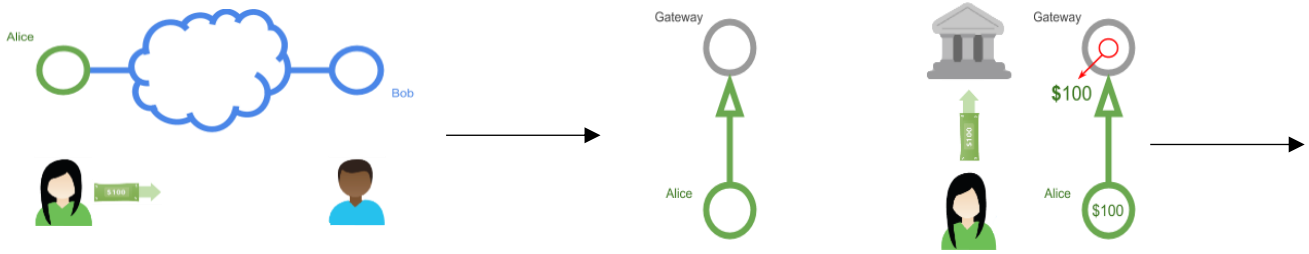
La società che gestisce ripple, di fatto, deteneva più della metà dei ripple in circolazione, e questo preoccupava particolarmente gli investitori che temevano il rischio di una strategia di dump, attuata dalla stessa società Ripple Lab.

In risposta a queste preoccupazioni, ripple ha stipulato degli accordi tramite escrow, ossia un deposito in garanzia, attraverso cui vincolava 55 miliardi di XRP, mediante 55 contratti con scadenze mensili progressive. Ogni mese, alla scadenza di un contratto, per circa 5 anni, Ripple Lab poteva utilizzare un miliardo di ripple (XRP), che, a detta del team della società, sarebbe stato destinato allo sviluppo dell'ecosistema Ripple e alla sua difesa. Infatti, al fine di sostenere il prezzo della crittomoneta e reagire a speculazioni, un miliardo di unità di ripple, vincolati tramite escrow, sarebbero stati mensilmente prelevati per sostenere il prezzo di XRP e mantenerlo al riparo da manovre speculative al ribasso del mercato.

Procediamo ad analizzare il funzionamento tecnico della crittovaluta ripple.

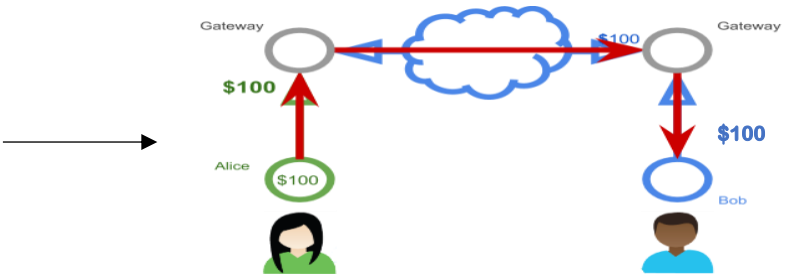
Il Ripple Net consente alle banche, ma fondamentalmente a chiunque, di trasferire valuta tradizionale o digitale. Il funzionamento è basato sulla costruzione di linee di fiducia fra l'utente, che deve effettuare un pagamento a favore di un altro, e altri utenti che hanno il ruolo di gateway, ovvero che aiutano a realizzare la transazione come degli intermediari. Analizziamo il processo nello specifico attraverso la figura 20.

Figura 20 - Fasi e processi di una transazione nel sistema Ripple



1) In una transazione, Alice desidera pagare 100$ a Bob su internet. Alice e Bob sono in paesi diversi e utilizzano valute diverse

2) Alice chiede aiuto a un gateway ripple locale per effettuare la transazione.
Alice crea una linea di fiducia con il gateway, deposita in esso 100$, e in cambio il gateway emette un saldo di 100$ sulla linea di fiducia di Alice



3) Anche Bob ha trovato il suo gateway locale di cui fidarsi. Quindi, per effettuare una transazione, Il network Ripple deve trovare un percorso di fiducia tra Alice e Bob. Tale percorso è rappresentato dai due gateway, rispettivamente di Alice e Bob, che permettono di creare il percorso di fiducia e di realizzare la transazione.
In questa fase il saldo del gateway di Alice viene azzerato e trasferito all'interno del gateway di Bob. Successivamente Bob può decidere se lasciare il saldo sul gateway e utilizzarlo per altre transazioni, oppure riscattare quel saldo e quindi prelevare denaro dal suo gateway, che funge dunque da banca.

La parte interessante del funzionamento di Ripple, è rappresentata dal fatto che esso opera come una sorta di camera di compensazione automatica tra gli utenti del network, permettendo così sia di trasferire denaro, sia di ritirarlo presso altri utenti che hanno il ruolo di gateway, ovvero fungono da banche[47].

Idealmente Ripple si propone come un protocollo in grado di gestire e standardizzare le transazioni tra istituti finanziari tradizionali, e tra loro ed altri utenti.

La flessibilità di Ripple consente di trattare qualsiasi tipo di valuta, consentendo anche lo scambio fra valute attraverso un mercato di valuta integrato nel software Ripple. Quest'ultimo ha anche una propria moneta interna, chiamata ripple (XRP), che a differenza delle altre valute non si basa sul concetto delle linee di fiducia, ma bensì può essere inviata a chiunque liberamente.

Le linee di fiducia instaurate con i vari utenti-gateway del network, finanziariamente, possono essere viste come vere e proprie linee di credito.

Ogni volta che un utente intende avviare una transazione, o aprire una linea di fiducia, consuma una parte dei suoi XRP, che fungono da costi di transazione. Le crittomonete ripple sono inoltre fondamentali per fare da ponte nello scambio fra valute di qualsiasi tipo (bridge-currency), soprattutto per quelle che non hanno un cambio diretto sul mercato.

I bilanci degli utenti, ovvero i saldi, e le linee di credito (fiducia) vengono gestite attraverso un database distribuito, chiamato ledger, simile alla blockchain.

Ogni nodo del network, che ha lo specifico compito di validare e rendere effettive le transazioni, contiene al suo interno una copia dell'ultimo ledger valido, ossia del libro mastro aggiornato in cui sono registrate le transazioni.

Il processo di formazione del consenso, per validare le transazioni, è molto diverso dal mining basato sulla proof of work di Bitcoin.

Infatti, ogni utente di Ripple Net ha una lista di nodi affidabili, ovvero delle entità fidate a Ripple Lab, chiamata UNL (Unique Node List).

Quando vengono avviate delle transazioni nel sistema, ogni nodo propone agli altri nodi le proprie modifiche al libro mastro (ledger). Ogni qualvolta un nodo riceve una proposta di modifica, la accetta solamente se proviene da un nodo presente nella propria lista (UNL).

Una volta che la maggior parte dei nodi ha accettato la modifica, questa viene inclusa nell'ultimo ledger valido, che diventa il medesimo per tutti i nodi.

Da un punto di vista tecnico, ad ogni transazione avvenuta nella rete Ripple il registro (ledger) si aggiorna; i nodi partecipanti firmano e distribuiscono crittograficamente una dichiarazione della loro opinione sulla correttezza del registro, e delle transazioni realizzate nella rete.

Il processo sopra descritto di validazione, ovvero di esecuzione delle transazioni, escludendo ogni forma di mining, è molto più rapido e meno oneroso in termini di risorse rispetto al Bitcoin, permettendo un aggiornamento del registro (ledger) ogni 4-5 secondi, contro i 10 minuti della blockchain di Bitcoin.

[47] "*Ripple for Users*", 2018 – URL: https://wiki.ripple.com/Ripple_for_Users

Inoltre, è possibile installare un nodo-pieno (full node), per validare le transazioni e il registro, su dispositivi poco potenti, quali computer e smartphone.
L'approccio al problema del consenso, per la validazione delle transazioni, presenta però delle debolezze.
Risulta difatti in dubbio se esso possa garantire la correttezza e sicurezza delle transazioni, oltre che l'indipendenza da terze parti. Il punto centrale, in tal senso, è che tutto dipende da come vengono configurate le varie liste di nodi (UNL).
Il team di sviluppatori sostiene che sia sufficiente aggiungere nodi fidati, che non abbiano incentivo ad unire le forze con la finalità di sovvertire il sistema Ripple.
Ad esempio, scegliendo come nodi fidati server gestiti da banche e istituzioni finanziarie, sarebbe poco probabile una loro collaborazione per influenzare la rete Ripple.
Dato il rapporto fiduciario tra Ripple Lab e i nodi validatori, Ripple nasce centralizzata, ovvero di fatto gestita da una società privata, a differenza delle altre crittovalute affrontate nel corso dell'elaborato.
Infatti, Ripple aveva inizialmente solo 25 nodi che convalidavano le transazioni, ed erano palesemente tutti in mano a Ripple Lab.
Per risolvere la problematica dell'eccessiva centralizzazione, del procedimento di consenso, Ripple ha espanso nel tempo il suo network di nodi validatori a 55 entità, non tutte controllate da Ripple.
Questa recente evoluzione è stata letta positivamente dal mercato, come una dichiarazione della volontà del team di decentralizzare il sistema.
Sulla base delle analisi e delle stime di CoinDesk[48], la crittomoneta XRP è considerata "toro", ovvero in ascesa rapida. Infatti, il prezzo di ripple è salito di oltre 1000 % dopo gennaio 2018, arrivando a toccare quota 3,5 $, dopo il valore di 0,3 $ mantenuto stabilmente nel corso del 2017.
Attualmente, stando ai dati di giugno 2018, il prezzo di XRP si aggira attorno a 0,6 $, con una capitalizzazione complessiva di mercato pari a 24 Bn di dollari.

4.2.2 Le Soluzioni sviluppate da Ripple Lab

Alcune delle ragioni alla base della nascita delle crittovalute, in risposta all'attuale sistema bancario e finanziario, sono sicuramente la pesante intermediazione dei processi, gli alti costi di transazione che ne derivano e le basse prestazioni, in termini di velocità del sistema.
Secondo uno studio condotto da McKinsey, big della consulenza, evidenzia che, nelle transazioni bancarie tradizionali, esistono fondamentalmente tre problemi.
Uno è chiaramente la velocità, basti pensare che per effettuare un pagamento tramite bonifico, da una parte all'altra del mondo, il tempo richiesto è mediamente di 3-5 giorni.

[48] https://www.coindesk.com/category/companies/ripple-labs/

Altro importante problema è rappresentato dagli eccessivi costi relativi delle transazioni bancarie; ed infine, è stato stimato che il 4 % di tutte le transazioni, gestite dal sistema bancario, falliscono o presentano degli errori. Le tre problematiche sono illustrate nella Figura 21.

Ripple, invece, con il suo network e la sua crittomoneta XRP, mira proprio a risolvere queste problematiche, e ad offrire alle banche una soluzione per poterli superare. Mediante il sistema Ripple, infatti, le transazioni possono essere gestite abbassando drasticamente i costi, le fee delle transazioni bancarie, si può avere la certezza assoluta delle transazioni bancarie, e la loro velocità aumenta esponenzialmente poiché in 4 secondi Ripple riesce a trasferire fondi da una banca all'altra. Inoltre, Ripple riesce a gestire 1.500 transazioni al secondo, ed è scalabile fino a 50.000 Tps.

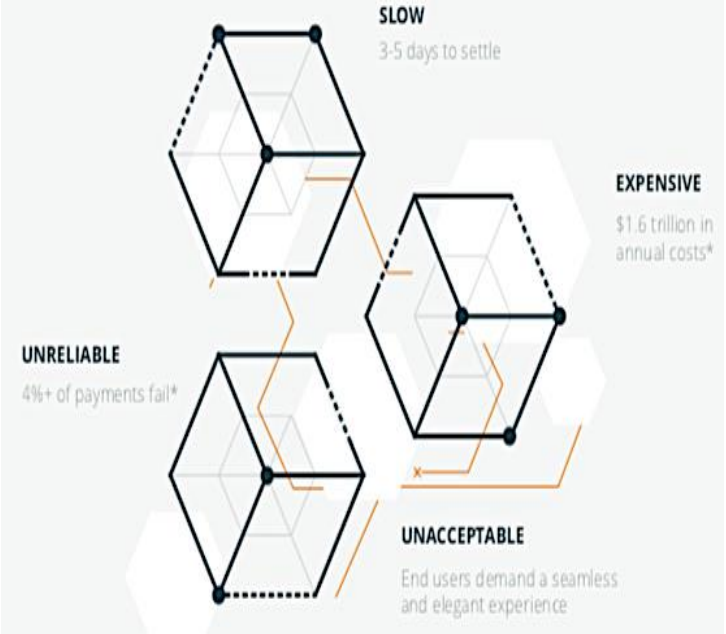


Figura 21 - Problematiche delle Transazioni Bancarie (Studio Mc Kinsey)

I vantaggi per il sistema bancario, forniti dal sistema Ripple, sono illustrati nella figura 22.

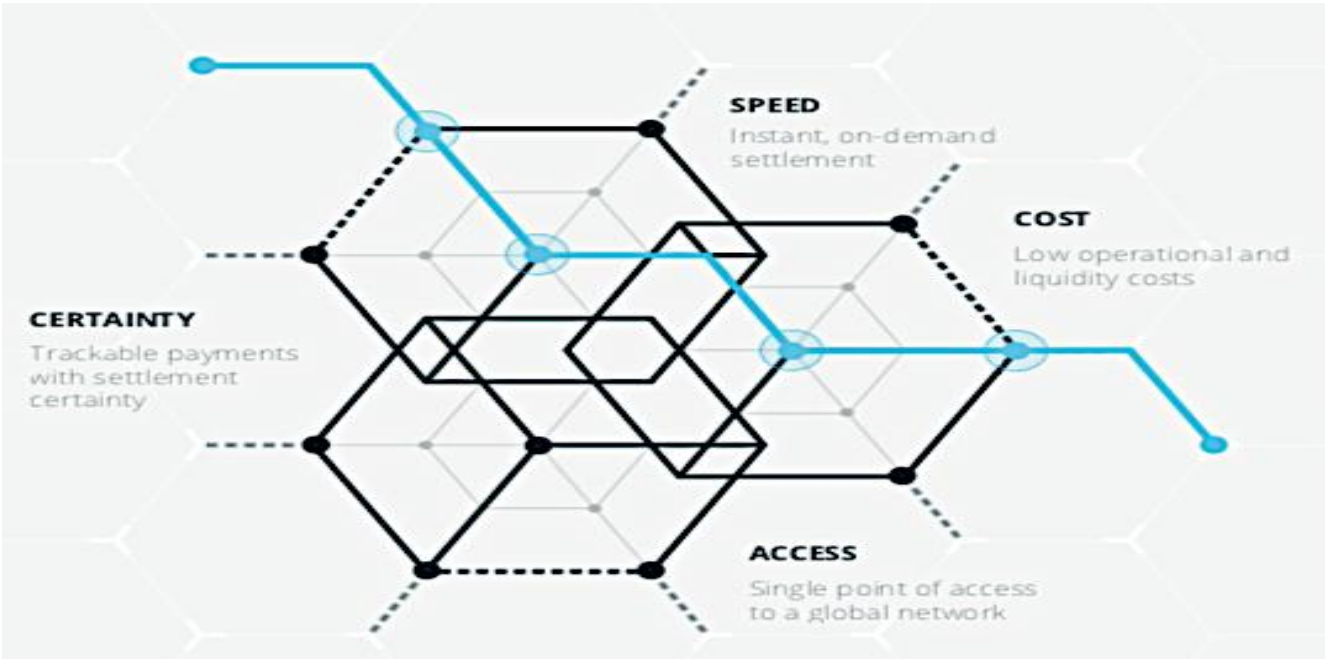


Figura 22 - Caratteristiche e Vantaggi del Sistema Ripple

I mercati finanziari globali riconoscono risparmi per 1,6 miliardi di dollari, che potrebbero essere generati da un'adozione del sistema Ripple per i pagamenti bancari.

Ripple Labs mira, infatti, a semplificare i pagamenti oltre frontiera, e a dotare il sistema bancario di una tecnologia che possa tenerlo in corsa nella competizione fra esso e i sistemi di pagamento decentralizzati

Per rinnovare i pagamenti bancari e per permettere alle banche di cavalcare l'onda crittografica, Ripple Labs ha sviluppato tre soluzioni:

- xCurrent

È la soluzione più avanzata e collaudata di Ripple Labs. Tale soluzione è nata per i pagamenti internazionali, ed è finalizzata a sostituire il processo di comunicazione e di elaborazione delle informazioni nelle transazioni, del sistema di pagamenti esistente (SWIFT). Attraverso xCurrent, infatti, le banche possono scambiarsi comunicazioni e messaggi in tempo reale, al fine di confermare i dettagli del pagamento prima di eseguire la transazione, e per confermare il trasferimento di fondi, una volta che è stata realizzata. Dunque, xCurrent consente l'invio di messaggi bidirezionali tra i soggetti in tempo reale, superando i limiti di velocità e costo del sistema unidirezionale di messaggistica SWIFT, attualmente utilizzato dalle banche.

- xRapid

Ripple Labs si accorse che esisteva un buco di mercato, dal lato dell'offerta, sul business della liquidità nei mercati emergenti. xRapid, in questo senso, permette di fornire liquidità e di convertire le valute, nei mercati emergenti, in modo molto più economico rispetto ai processi attuali, tradizionali. xRapid quindi fornisce una soluzione per i fornitori di servizi di pagamento e altre istituzioni finanziarie che desiderano ridurre al minimo i costi di liquidità, poiché i pagamenti nei mercati emergenti richiedono spesso conti in valuta locale prefinanziati. Il meccanismo di conversione tra valute si basa sulla funzione "ponte" assolta dalla crittomoneta ripple (bridge currency), che nella funzione xRapid rappresenta un pool di liquidità.

- xVia

xVia rappresenta la soluzione meno sviluppata dal Ripple Labs, anche in funzione del suo recente sviluppo. Questa soluzione è diretta ad aziende, fornitori di servizi di pagamento e banche che desiderano inviare pagamenti su varie reti utilizzando un'interfaccia standard. xVia non richiede l'installazione di un software, e consente agli utenti di inviare pagamenti a livello globale, assicurando la trasparenza nello stato di pagamento, e fornendo informazioni dettagliate come le fatture. La soluzione xVia, quindi, consente di effettuare transazioni attraverso un'interfaccia standard senza la necessità che si installi xCurrent.

Per quanto riguarda le fasi di attuazione delle tre soluzioni, nella prima fase xCurrent è stato distribuito alle banche centrali e ai principali fornitori di servizi di pagamento transfrontalieri. Nella seconda fase si sta sviluppando xRapid, come mostrato dall'annuncio di diverse istituzioni finanziarie che ne accettano l'utilizzo, mentre la fase tre, relativa allo sviluppo di xVia, sembra ancora lontana e incerta.

4.2.3 Le Differenze con il Bitcoin

La differenza più marcata tra XRP e BTC è sicuramente la finalità dei due sistemi, che nel caso di ripple da vita ad un vero e proprio paradosso.
Bitcoin è stato creato per rispondere al crollo economico-finanziario del 2008, ed alla mancanza di fiducia del pubblico nei confronti del sistema bancario, percepito come complice delle turbolenze finanziare che hanno caratterizzato gli ultimi anni.
In questo sistema totalmente decentralizzato, le transazioni non sono controllate da un intermediario o un ente centrale, ma bensì sono verificate dai nodi-pieni (full node) della rete, ovvero degli utenti che hanno scaricato l'intero registro blockchain, diventando controllori del sistema Bitcoin.
Ripple invece, gestito in modo centralizzato da Ripple Labs e progettato per le banche, mira a rendere più efficienti le transazioni bancarie in termini di tempi e costi, ed a regolare i rapporti e gli scambi fra istituzioni finanziarie.
Il paradosso della finalità di Ripple è dovuto al fatto che persegue l'obbiettivo di salvare il comparto bancario, adeguandolo a processi più innovativi, quando invece il mondo delle criptovalute è nato proprio per scavalcarlo e disintermediare il sistema. Il sistema Ripple è dunque finalizzato a rendere più competitivi i servizi offerti dalle banche, aiutandole nel confronto con le crittovalute.
Una delle principali differenze tra XRP e BTC è che il primo rappresenta un sistema per trasferire somme di denaro in qualsiasi valuta, mentre il Bitcoin si è dimostrato essere primariamente un sistema per immagazzinare capitale, con finalità di investimento. Questo determina che il sistema Ripple ha un valore più per il protocollo con il quale gestisce le transazioni che per la moneta in sé, diversamente da quanto avviene nel sistema Bitcoin, in cui la criptomoneta è preminente.
Da un punto di vista tecnico, un'importante differenza è data dal fatto che le crittomonete ripple (XRP) sono state immesse sul mercato da Ripple Lab, un ente centrale, e, a differenza dei bitcoin, gli XRP non possono essere minati, cioè non possono essere guadagnati-estratti dagli utenti, miner, contribuendo con il loro potere di calcolo a validare e rendere sicure le transazioni. Infatti, nel network Ripple i miner sono assenti.
Le unità di XRP, dette quindi pre-minate, sono state tutte generate da Ripple Lab, raggiungendo il limite previsto di 100 miliardi di unità, a differenza del limite di 21 milioni di bitcoin in totale, che verrà raggiunto nel tempo, approssimativamente nell'anno 2140.
L'assenza del processo di mining nel sistema Ripple determina, nel confronto con il Bitcoin, ampi vantaggi in termini di costi e velocità del sistema. Infatti, il processo di validazione delle transazioni, che nei sistemi tradizionali può richiedere fino a 3-4 giorni, circa 17 secondi per Ethereum e intorno ai 10 minuti per Bitcoin, viene efficientemente realizzato dal sistema Ripple in 4 secondi.
Inoltre, a differenza della rete Bitcoin, Ripple Net può gestire 1.500 transazioni per secondo, ed è scalabile fino a sostenere 50.000 Tps.
Molti esperti inseriscono erroneamente nell'insieme delle criptovalute anche ripple, mentre sarebbe più opportuno inserirla nell'ambito dei progetti per la digitalizzazione dei processi bancari. Ripple non può

essere considerata una criptomoneta alla stregua del bitcoin, perché, a differenza di quest'ultimo, non è decentralizzata e soprattutto è gestito da un'azienda che può subire pressioni e intimidazioni da forze esterne. Nonostante ciò, come sistema di pagamento, Ripple è più rapido ed economico del Bitcoin.

4.2.4 Un'Opportunità per il Sistema Bancario e le Istituzioni Finanziarie

Come precedente detto, a differenza delle principali crittomonete come bitcoin, ripple non nasce per eliminare il ruolo di intermediazione delle banche ma, al contrario, rappresenta una risorsa importante per queste ultime, che infatti hanno investito in esso ingenti risorse.
Tra i più grandi finanziatori delle soluzioni sviluppate da Ripple Labs vengono annoverati Banco Santander, UBS, ma anche Unicredit.
La soluzione xCurrent, sviluppata da Ripple Labs per innovare il procedimento di messaggistica tra banche, volto all'esecuzione delle transazioni, è stata sperimentata con alcune banche centrali come la Federal Reserve statunitense, la BCE, l'Autorità monetaria di Singapore e la Banca di Indonesia.
Oltre le autorità monetarie citate, anche il più grande generatore di pagamenti oltre frontiera, Singapore, nel 2017 ha utilizzato xCurrent per potenziare le transazioni. Celebre è anche l'utilizzo di questa soluzione da parte di American Express, nota società che opera nel settore delle carte di pagamento e di credito.
La crittovaluta XRP, anche nel 2018, sta continuando a scalare le vette della notorietà, infatti, Ripple Labs ha annunciato altre cinque nuove partnership, stipulate in diversi paesi[49].
In questo senso, a dare fiducia alla crittomoneta XRP sono state innanzi tutto due banche, Itaù Unibanco del Brasile e la IndusInd indiana. Ai suddetti istituti di credito, si sono successivamente unite tre società di money transfer, tra cui la InstaRem a Singapore, la Beetech in Brasile e la Zip Remit dal Canada.
Le società sopra citate adotteranno Ripple Net con l'obbiettivo di migliorare e facilitare i pagamenti internazionali in tempo reale.
Gli sviluppi sul fronte Ripple Net, come xCurrent, secondo gli esperti, genereranno un impatto limitato sul valore della crittomoneta ripple, poiché non richiedono l'utilizzo della moneta virtuale XRP, ma soltanto quello del network. Infatti, le banche e le istituzioni finanziarie non sembrano ancora pronte ad accogliere ad occhi chiusi le criptovalute.
In altre parole, nonostante le partnership realizzate da Ripple Labs e gli investimenti raccolti, la quotazione di ripple (XRP) sul mercato non dovrebbe teoricamente subire variazioni degne di nota.
D'altro canto, c'è da notare come molto spesso gli incrementi di quotazione della "coin" ripple, siano stati sostenuti dalla sua crescente legittimazione, riconosciuta da numerose banche e società finanziarie di tutto il mondo.

[49] "*Ripple scala le vette del successo: annunciate 5 nuove partnership*", Money.it, 2018 – URL: https://www.money.it/quotazione-Ripple-oscilla-5-nuove-partnership

CONCLUSIONI

Gli obiettivi perseguiti dall'elaborato, come menzionato in fase introduttiva, sono fondamentalmente due.
In primis, quello di accompagnare il lettore durante un percorso conoscitivo, finalizzato alla comprensione degli elementi fondanti e distintivi riguardo le principali criptovalute, supportando tale processo con la parallela disamina della blockchain, tecnologia che ne regola il funzionamento.
Il secondo obbiettivo, invece, consiste nello svincolarsi dall'euforia del momento, al fine di valutare, in modo quanto più oggettivo, punti di forza, fragilità, opportunità e rischi delle crittovalute, attualmente leader del comparto, unitamente alla tecnologia che ne è alla base.
Personalmente, in funzione dei temi sviluppati, sono confidente nel conseguimento dei due obbiettivi sopracitati, ma tale risultato è solo parzialmente soddisfacente.
Infatti, esiste un terzo obiettivo, non menzionato e molto ambizioso, che ritengo sia il più interessante, ma anche il più arduo da raggiungere. L'obbiettivo implicito consiste nel fornire una risposta alla gettonatissima domanda, da un milione di dollari o forse anche più: "Quale sarà il futuro delle criptovalute e della blockchain?".
Per tentare di fornire una risposta valida, credo sia fondamentale effettuare una distinzione fra le due realtà, al fine di non confondere un elemento dell'insieme con l'insieme stesso.
Per quanto riguarda l'ambito della blockchain, dove l'applicazione nelle crittovalute rappresenta solamente uno degli utilizzi ricompresi nell'ampio ventaglio applicativo, le prospettive sul suo futuro sono decisamente promettenti.
Infatti, la mia personale opinione, non per comodità, ma per convinzione, converge con la visione del presidente della BCE Mario Draghi; il quale riconosce ed apprezza la capacità innovativa della blockchain nel ridisegnare molti processi, distinguendola nettamente dalle valute virtuali che su essa si basano.
Di fatto, se per la blockchain potrebbe prospettarsi un futuro promettente, lo stesso ragionamento non è detto si adatti alle criptovalute come il bitcoin.
Nonostante i mezzi monetari si siano evoluti nel tempo, passando dalla fase 1, quella "fisica" dell'oro, alla fase 2, quella "fiduciaria", e successivamente alla fase 3 "derivata", degli omonimi contratti, non è detto si compia l'ennesimo passaggio alla fase 4, ovvero relativa alle valute digitali.
Dunque, data l'impossibilità di rispondere a quale sia il futuro delle criptovalute, ho personalmente riscontrato tre elementi fondamentali e strumentali al loro successo.
Il primo è sicuramente l'utilizzo di una blockchain, che ne regola il funzionamento, tale da non confliggere con l'ordine pubblico e la legalità, in relazione alla tracciabilità delle transazioni, all'eliminazione dell'anonimato, e ad un controllo sul protocollo di funzionamento affidato alle autorità.
Da quest'ultimo punto, deriva il secondo elemento strumentale all'affermazione delle crittovalute, ovvero la regolamentazione.
Quest'ultima, è intesa come il controllo da parte della legge sul funzionamento delle valute digitali, e sulle eventuali modifiche migliorative da apportare al protocollo informatico che le disciplina.

Infine, il terzo elemento, strumentale al successo delle crittomonete, è il tempo.

Nonostante sembri banale affidare al tempo la risposta alla domanda sul futuro delle criptovalute, basta pensare che il mercato finanziario, e i suoi sviluppi digitali, hanno avuto circa mezzo secolo di tempo per svilupparsi e giungere all'attuale infrastruttura, nonostante siano presenti ancora delle inefficienze. In appena dieci anni, invece, le crittovalute, nonostante presentino ancora forti criticità e debolezze, sono state sviluppate e migliorate fino a posizionarsi come un reale competitor nei confronti dell'attuale sistema finanziario e bancario.

Immaginare cosa ha in serbo il futuro per il comparto crypto, è solamente un gioco di retorica.

Ad oggi infatti, nessuno, anche fra i più esperti del settore, risulterebbe in grado di prevedere gli sviluppi futuri e l'eventuale affermazione della blockchain e/o delle criptovalute; ma, a tal proposito, l'elaborato cerca di fornire chiavi di lettura e strumenti atti alla formazione, per il lettore, di una personale opinione.

Opinione sicuramente incerta, ma quantomeno consapevole.

INDICE DELLE FIGURE E DELLE TABELLE

BIBLIOGRAFIA & SITOGRAFIA

- Franco Angeli, *"Moneta e banche attraverso i secoli"*, Ennio De Simone, 2011
- David Graeber, *"Il Debito",* Il Saggiatore, 2012
- Roland Nitsche, *"Alla scoperta della Moneta"*, 1970, Rizzoli editore.
- Paesani P., *"Lezioni di Economia"*, 2012, Giappichelli editore, Torino
- *"Virtual Currency Schemes"*, European Central Bank, 2012
- Aron Jacob, "*Virtual money gets real*", New Scientist, 2011
- Gates Mark, *"Blockchain, la guida definitiva per conoscere Blockchain, Bitcoin, Criptovalute, Contratti Smart e il futuro del denaro"*, Prima Edizione, 2017
- Bruce Schneier, *"Applied Cryptography"*, John Wiley & Sons, 1996
- Amato M. e Fantacci L., "*Per un pungo di Bitcoin*", Università Bocconi Editore, 2016
- Caetano R., "*Bitcoin. Guida all'uso delle criptovalute*", Apogeo, 2016
- Pedro Franco, "*Understanding Bitcoin: Cryptography, Engineering and Economics*", 2014
- Antonopoulos Andreas, *"Mastering Bitcoin: Programming the Open Blockchain"*, 2017
- Capoti D., Colacchi E. e Maggioni M., "*Bitcoin Revolution: La moneta digitale alla conquista del mondo*", Ulrico Hoepli Editore, 2015
- Blokdyk Gerardus, *"Proof-of-Stake: The One Essential Checklist"*, 2018
- Steve Wilson, *"Oltre l'Hype: Comprendere gli anelli deboli della Blockchain"*, 2017
- Barber Simon, Boyen Xavier, Shi Elaine & Uzun Ersin, "*Bitter to Better - How to Make Bitcoin a Better Currency"*, Financial Cryptography and Data Security, 2011
- Pistono Federico, *"Startup Zero.0 – Imparare dai fallimenti per creare successi. Dalla Sylicon Valley all'Italia"*, 2017, Hoepli
- Goodman, Leah McGrath (2014), "*The face behind Bitcoin"*, Global Edition, 2014
- *"Bits and Bets – Information, Price Volatility, and Demand for Bitcoin"*, Buchholz et al., 2012
- Halaburda e Sarvary, "*Beyond Bitcoin: The Economics of Digital Currencies"*, 2016
- *"Ripple, la nuova Crittovaluta sulla bocca di tutti"*, Versione Italiana Kindle, 2018

- Dr. Jack Peterson & Joseph Krug, *"Augur: A Decentralized, Open- Source Platform for Prediction Markets"*, 2014
- Vitalik Buterin. "*Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform"*, 2013
- E. G. Sirer e I. Eyal, "*Majority is not Enough: Bitcoin Mining is Vulnerable*", 2014
- Thaddeus Dryja e Joseph Poon, "*The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments",* 2015
- Massimo Bartoletti, Livio Pompianu, *"An empirical analysis of smart contracts: platforms, applications, and design patterns"*, 2017
- "*I sistemi monetari dal Gold Standard all'età contemporanea*" – URL: http://old.unipr.it/arpa/facecon/StoriaEc/11-Moneta_contemporanea.htm
- Ozalp Babaoglu, Cryptography System, slides – http://www.cs.unibo.it/~babaoglu/courses/security/lucidi/pdf/
- Satoshi Nakamoto, "*Bitcoin: A peer to peer electronic cash system*", 2008 – URL: https://bitcoin.org/bitcoin.pdf
- *"Fenomeno ICO"* – URL: https://www.blockchain4innovation.it/esperti/fenomeno-ico-punto-opportunita-rischia-truffa/
- Dati CoinMarketCap – URL: https://coinmarketcap.com/
- The Wall Street Journal, "*ICO*" – URL: https://www.wsj.com/articles/telegram-messaging-app-scraps-plans-for-public-coin-offering-1525281933?mod=searchresults&page=1&pos=1
- Report UBS, "*Cryptocurrencies, Beneath The Boubble*", 12 October 2017 – URL: https://www.ubs.com/magazines/wma/insights/en/investing/2017/beneath-the-bubble.html
- Psicologia&Mercati – "*Le bolle speculative. La finanza comportamentale applicata ai bitcoin*", 2017 – URL: http://citywire.it/news/psicologiaandmercati-le-bolle-speculative-la-finanza-comportamentale-applicata-ai-bitcoin/a1050826
- *"Così la bolla finanziaria nasce nel nostro cervello. Ecco i nuovi segreti della neuroeconomia"*, Il Sole 24 Ore, URL: http://www.ilsole24ore.com/art/economia/2010-12-11/cosi-bolla-finanziaria-nasce-121548_PRN.shtml

- Paul Krugman, "*Why is deflation bad?*" - URL: https://krugman.blogs.nytimes.com/2010/08/02/why-is-deflation-bad/
- "*Da Nakamoto all'Hard Fork: la storia del Bitcoin, gli upgrade, la politica, gli aneddoti*", Alberto De Luigi, 2018, URL: http://www.albertodeluigi.com/2017/07/17/storia-e-upgrade-del-bitcoin/#6
- "*Scenario della Centralizzazione del Mining: perchè la Decentralizzazione è fondamentale*", 2018 - URL: https://medium.com
- "*Bitcoin: Il Lightning Network risolverà il problema delle transazioni?*", 2018 – URL: https://www.advister.it/bitcoin-lightning-network-transazioni/
- "*Lightning Network – Scalable, Instant Bitcoin/Blockchain Transactions*" – URL: https://lightning.network/
- "Le norme su Bitcoin e crittovalute nei diversi Paesi: Il quadro", 2018 – URL: https://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-crittovalute-nei-diversi-paesi-quadro/
- "Bitcoin, niente regole fino al 2019. La Ue aspetta il G20", 2018 – URL: https://www.corrierecomunicazioni.it/finance/bitcoin-niente-regole-al-2019-la-ue-aspetta-g20
- "*Quante monete come i bitcoin esistono*?", La Stampa – Economia, 2018 – URL: http://www.lastampa.it/2018/01/13/economia/quanti-monete-come-i-bitcoin-esistono//
- Ethereum Fundation, "*Ethereum White Paper*", 2015 – URL: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper
- Dr. Gavin Wood, "*Ethereum: A secure decentralized generalised transaction ledger*", 2017 – URL: https://ethereum.github.io/yellow/paper.pdf
- "*What is a DAO*", CoinDesk, 2017 – URL: https://www.coindesk.com
- "*The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*", CoinDesk, 2016 – URL: https://www.coindesk.com
- "*Ripple for Users*", 2018 – URL: https://wiki.ripple.com/Ripple_for_Users
- "*Ripple scala le vette del successo: annunciate 5 nuove partnership*", Money.it, 2018 – URL: https://www.money.it/quotazione-Ripple-oscilla-5-nuove-partnership
- *"Banche e Ciptovalute: Goldman Sachs acquista un Exchange Bitcoin per 400 milioni di dollari"*, EconomyUp , 2018 – URL: https://www.economyup.it

RIASSUNTO

CAPITOLO I

Connotare la moneta come un'invenzione, significherebbe commettere un errore. Essa, di fatti, deriva da un processo evolutivo storico, che si articola in varie fasi incrementali.

Nella storia possiamo identificare diversi protocolli e mezzi di scambio, susseguitisi nel tempo; primo fra tutti il baratto, che subordinava lo scambio di beni e servizi alla coincidenza di bisogni delle parti coinvolte nella trattativa. All'interno del suddetto protocollo di scambio, vennero storicamente identificate due forme di pre-moneta: la moneta naturale, rappresentata dalle merci in sovrabbondanza, utilizzate per regolare gli scambi, e dalla moneta utensile, che comprendeva strumenti di lavoro e di uso quotidiano. Le problematiche relative al regolamento di scambi aventi ad oggetto grandi quantità, determinarono l'obsolescenza delle pre-monete, a favore dell'utilizzo di quelle metalliche, utilizzate per la prima volta in Cina nel 1200 a.C. L'utilizzo di metalli preziosi nel processo di coniazione, quali oro ed argento, attribuì alle monete un proprio valore intrinseco.

Fino al 1661 in Europa il sistema dominante si basava sul bimetallismo, ma nello stesso anno, in Svezia, le monete metalliche furono sostituite dall'emissione di banconote. Le emissioni, successivamente, si diffusero in tutta Europa, ma, dato che il valore delle banconote non era agganciato a nessun bene rifugio, le eccessive emissioni determinarono la diffusione di forti spirali inflazionistiche.

Per ovviare a questi effetti, si dovette aspettare il 1861, quando, in Inghilterra, le riserve auree rappresentarono per la prima volta la base e il parametro di emissione, agganciando quindi il valore delle banconote alle movimentazioni di oro, in entrata e in uscita dal paese. Per controllare l'inflazione dei prezzi, il regime aureo puro, introdotto in Inghilterra, divenne dominante nel 1900, quando negli Stati Uniti venne promulgata la legge Gold Standard. In questo regime monetario, ogni valuta aveva una sua parità con l'oro, determinando così un regime di cambi fissi fra le diverse divise nazionali. Tale sistema monetario venne abbandonato nel corso del primo conflitto mondiale. Le principali cause furono gli effetti della guerra sui flussi commerciali e finanziari, l'impossibilità di dimostrare, per molte nazioni, la conformità fra le banconote emesse e le riserve auree detenute, e la scarsità dell'oro.

Per porre fine alla situazione di instabilità monetaria creatasi, nel 1944, con gli accordi di Bretton Woods, si sanciva il passaggio al Gold Exchange Standard. In questo regime monetario, il valore di ogni valuta, non veniva più agganciato alle riserve auree, ma bensì era fissato rispetto al dollaro statunitense, l'unico a poter essere convertito in oro. Le conseguenze furono forti pressioni sul dollaro, poste dal nuovo regime monetario, che, unite alla situazione statunitense relativa alla guerra in Vietnam, portarono ad una forte sofferenza della moneta americana, che spinse il presidente Richard Nixon a decretarne l'inconvertibilità con l'oro.

Questo passaggio condusse alla soppressione del regime a cambi fissi, e all'introduzione delle monete fiat, ossia valute non coperte da riserve auree, e dunque prive di valore intrinseco. Elemento fondamentale delle

monete fiat è la fiducia nelle autorità, quali governi e banche centrali, in relazione al loro valore, appunto fiduciario, e relativamente alla loro accettazione come strumento di pagamento, disciplinata dalla legge.
Nell'attuale sistema monetario, le funzioni riconosciute alla moneta sono tre: la funzione di intermediario negli scambi e mezzo di pagamento, per l'adempimento di debiti; la funzione di unità di conto, che consente di misurare costi-ricavi e crediti-debiti; ed infine quella di riserva di valore, ossia la capacità della moneta di conservare il suo potere d'acquisto nel tempo.
Le decisioni di politica monetaria in Europa, riguardo le emissioni di banconote, le politiche di cambio, e la definizione del tasso di interesse guida, spettavano ai governi e le banche centrali dei singoli stati; ma, con il trattato di Maastricht in vigore dal 1993, e successivamente con l'introduzione dell'euro, avvenuta tra gli anni 1999 e 2002, la sovranità delle politiche monetarie venne trasferita dai singoli stati agli organi comunitari, primo fra tutti la BCE.
All'interno dei sistemi economici attuali esistono fondamentalmente due tipi di monete: la moneta legale, banconote e monete metalliche, e la moneta bancaria rappresentata dai depositi (moneta elettronica).
Lo sviluppo informatico e i costanti avanzamenti tecnologici hanno portato alla nascita di una nuova tipologia, ovvero delle valute dette virtuali o digitali, non emesse e controllate da nessuna banca centrale, le quali vengono spesso confuse con le monete elettroniche. Queste ultime sono collegate alle valute tradizionali da una base giuridica e sono controllate da una banca centrale; una valuta digitale, invece, è collegata al denaro solamente attraverso un tasso di cambio, che la può esporre a forti fluttuazioni. Fra le valute virtuali sono comprese le criptomonete come il bitcoin (BTC).
Sulla base della classificazione dei "Modelli di moneta virtuale", fornita dalla BCE nel 2012, possiamo suddividere le valute virtuali in tre categorie: sistemi di valuta virtuale chiusi, in cui non c'è collegamento tra la moneta digitale e l'economia reale – schemi di moneta virtuale con flusso unidirezionale, dove la "digital coin" può essere acquistata con denaro reale, ma lo scambio inverso non è consentito – e gli schemi di moneta virtuale con flusso bidirezionale, in cui la moneta digitale può essere scambiata con valute reali e viceversa, permettendo così l'acquisto di beni e servizi, se accettata come mezzo di pagamento. Il bitcoin, così come le altre criptomonete, appartengono alla terza tipologia di valute virtuali.

CAPITOLO II

Prima di procedere alla disamina delle principali criptovalute, è fondamentale comprendere la tecnologia su cui si basa il loro funzionamento. La tecnologia blockchain, letteralmente "catena di blocchi" è riferita a sistemi digitali decentralizzati, più esattamente distribuiti, in cui ogni partecipante della rete (nodo) è posto in posizione paritaria con gli altri nodi, e concorre con essi alla formazione della volontà, e del consenso nel sistema, attraverso un procedimento di approvazione democratico. In termini tecnici la blockchain rappresenta un protocollo di comunicazione informatico Peer-to-Peer, che sfrutta la crittografia dei dati, ma, questa definizione, ha un basso potere esplicativo. In modo pragmatico possiamo identificare la

blockchain, nell'applicazione alle valute digitali, come un libro mastro (database) decentralizzato, distribuito tra i partecipanti e crittografato, in cui vengono registrate in modo immutabile tutte le transazioni avvenute tra i partecipanti della rete (nodi). Le principali caratteristiche della tecnologia blockchain sono: la tracciabilità delle operazioni registrate nel database, registro decentralizzato – l'immutabilità dei dati contenuti nel registro blockchain – la sicurezza del sistema, condizione garantita dalla crittografia – e l'accessibilità delle informazioni, contenute nel database, garantita a tutti i partecipanti della rete.

Rispetto ad un registro tradizionale, gestito in modo centralizzato, un database blockchain assicura la sicurezza e la conservazione dei dati, poiché esso non è detenuto da un singolo soggetto, ma bensì è distribuito e replicato fra tutti i partecipanti della rete. Questo determina che, per modificare i dati contenuti nella blockchain, un hacker informatico dovrebbe detenere una potenza di calcolo almeno pari al 51% della potenza computazionale (di calcolo) dell'intera rete, dato che gli altri utenti tenteranno di correggerlo.

Esistono diverse tipologie di blockchain: blockchain pubbliche, ovvero reti P2P aperte a tutti i potenziali partecipanti, in cui è assente il controllo di un ente centrale – blockchain private, ad accesso limitato, in cui, a differenza della prima tipologia, il processo di formazione del consenso, ovvero di verifica delle transazioni, è assegnato ad un ente centrale – e le consortium blockchain, ossia una via di mezzo fra le altre due tipologie.

Precedentemente, definendo la tecnologia, si è fatto riferimento alla crittografia, ossia la scienza che si occupa del processo di codifica dei messaggi, volto a rendere le informazioni criptate.

Le due principali tipologie di crittografia sono: la crittografia a chiave simmetrica, in cui il mittente e il destinatario utilizzano la stessa chiave privata, utilizzata sia per la cifratura che per la decifratura del messaggio – e la crittografia asimmetrica (a chiave pubblica), che attraverso due chiavi, una pubblica e l'altra privata, permette rispettivamente la cifratura e la decifratura del messaggio.

Nell'infrastruttura Bitcoin, la crittografia è fondamentale per la verifica delle transazioni avvenute nella rete (attività di mining), e per verificare la correttezza del registro blockchain. L'algoritmo crittografico asimmetrico utilizzato nel sistema Bitcoin prende il nome di funzione Hash; in sostanza, per compiere una transazione, vengono utilizzate due chiavi, una pubblica e una privata, dove la prima deriva dalla seconda, e da quest'ultima deriva l'indirizzo Bitcoin da cui inviare, o su cui ricevere, criptomoneta.

Infatti, per compiere una transazione in bitcoin, un utente deve digitalmente firmare con la sua chiave privata la transazione precedente (condizione di spendibilità dei BTC, che ne certifica il possesso), e la chiave pubblica del destinatario, ovvero l'indirizzo a cui spedire BTC. Il ricevente, in una transazione BTC, può condurre un controllo sui vari passaggi di proprietà della valuta digitale inviatagli, verificando a ritroso le firme digitali presenti in ogni transazione.

L'applicazione della blockchain nelle transazioni, come nel caso della criptomoneta bitcoin, consente la riduzione dei costi e delle tempistiche, disintermediando quei processi che attualmente sono gestiti in modo centralizzato. Nonostante questi vantaggi, l'utilizzo delle valute digitali implica la presenza di rischi e problematiche connesse a questa categoria di valute, primo fra tutti il problema del Double Spending.

Con questo termine si identifica il rischio, in un sistema di valuta virtuale, relativo alla possibilità che un utente possa spendere due o più volte la stessa unità di valuta digitale. Data la natura decentralizzata del registro, spendere la stessa quantità di BTC due o più volte, rappresenterebbe una contraddizione per tutti gli utenti che possono leggere il database delle transazioni. Infatti, effettuare il double spending, porterebbe gli altri nodi del network a correggere le transazioni che hanno ad oggetto la stessa quantità di criptomoneta, poiché sono tra loro contrastanti; ma, nel caso in cui il nodo malevolo detenga la maggioranza del potere di calcolo dell'intero network, egli sarebbe in grado di modificare il registro blockchain, attuando comportamenti scorretti come la cancellazione o modifica di transazioni pregresse, oppure il double spending di una stessa quantità di bitcoin.

Come si evince dal nome della tecnologia blockchain, il database si articola in una catena di blocchi collegati tra loro, al cui interno vengono ricomprese le transazioni che di volta in volta vengono avviate nella rete. Ogni blocco è composto da due parti fondamentali: il block header, in cui sono comprese varie informazioni come ad esempio la marca temporale, ovvero la data in cui il blocco di transazioni e stato convalidato attraverso l'attività di mining, i collegamenti ai blocchi precedenti e successivi, ed i BTC totali inviati in tutte le transazioni ricomprese nel blocco – e la lista delle transazioni, indicandone commissioni, la memoria occupata e gli indirizzi bitcoin interessati dalle transazioni.

Il procedimento di formazione del consenso nella blockchain viene associato al processo di validazione delle transazioni, che si realizza con la potenza di calcolo messa a disposizione dai partecipanti della rete (computer), attraverso l'attività di "Mining", chiamata così per l'analogia con le estrazioni minerarie.

Il processo di mining nel sistema Bitcoin persegue due importanti finalità: in primis con l'attività di mining vengono creati nuovi BTC, attraverso la validazione dei blocchi di transazioni che vengono registrati nella blockchain, e in questo senso, la generazione di moneta assolve la funzione di ricompensa per il lavoro svolto dai nodi-minatori (Miner), ossia di validazione ed approvazione delle transazioni – in secondo luogo, l'attività di mining genera fiducia e consenso nel sistema, subordinando la convalida dei blocchi di transazioni, alla risoluzione di un difficile problema crittografico di carattere informatico-matematico, che viene risolto attraverso l'individuale potere di calcolo messo a disposizione dai vari nodi-minatori della rete (miner).

Relativamente al metodo di raggiungimento del consenso, realizzato attraverso il mining, la blockchain di Bitcoin si basa sull'algoritmo "Proof of Work", letteralmente prova di lavoro. Questo algoritmo subordina il consenso, ossia la convalida delle transazioni, alla risoluzione di un puzzle crittografico, un problema informatico-matematico, la cui soluzione deriva da un procedimento di "brute force", cioè attraverso continui tentativi finalizzati ad ottenere una soluzione accettabile. Tale soluzione, considerata la prova di lavoro, appunto, viene mostrata dal miner, che per primo l'ha trovata, a tutta la rete, permettendo così la validazione dei blocchi di transazioni, generando fiducia e consenso nel sistema.

Il funzionamento e le regole alla base del mining, nel sistema Bitcoin, determinano la validazione e l'inserimento nella catena di un nuovo blocco di transazioni in un orizzonte temporale medio di circa 10 minuti, che rappresenta la tempistica media prestabilita dal protocollo informatico.

Sotto il profilo della sicurezza, l'algoritmo proof of work, potrebbe essere soggetto ad attacchi informatici, volti alla modifica di transazioni validate, solamente nel caso in cui un nodo arrivi a detenere, da solo o di concerto con altri, il 51 % dell'intero potere computazionale della rete. Questa condizione consentirebbe al nodo disonesto di creare una biforcazione nella catena blockchain (fork), finalizzato a modificare transazioni pregresse.

Infatti, detenendo la maggioranza del potere di calcolo, in gergo tecnico hashing power, il nodo malevolo potrebbe risolvere i puzzle crittografici più velocemente degli altri nodi-miner, consentendogli di creare una catena di blocchi più lunga rispetto alle altre biforcazioni, decretandola come versione ufficiale.

In caso di biforcazione (fork) della blockchain, infatti, la catena considerata dominante è quella su cui è stata impiegata la maggior quantità di potere di calcolo, ovvero la catena a cui viene agganciato il maggior numero di blocchi, attraverso la risoluzione dei problemi crittografici. L'attacco informatico, sopra descritto, prende il nome di "51% Attack".

Da un punto di vista energetico, l'attività di mining, relativa alla risoluzione di complessi puzzle informatico-matematici, è eccessivamente dispendiosa, infatti, gli alti costi sono dovuti sia all'utilizzo di hardware specifici, per eseguire l'altissimo numero di calcoli informatici relativi al mining, sia all'elevato consumo di elettricità.

Per molti esperti del settore, proprio l'elevato consumo elettrico rappresenta un punto debole in grado di limitare la scalabilità blockchain basate su proof of work, come quella di Bitcoin.

Fino a questo punto della trattazione, ogni qualvolta è stato usato il termine "nodo", si è fatto riferimento a un qualsiasi partecipante al network peer-to-peer della blockchain, ovvero computer connessi alla rete. In realtà esistono tre diverse tipologie di nodi: i nodi pieni (full node), i quali scaricano e conservano l'intero registro blockchain, in modo da verificarne la correttezza – i nodi-miner, ossia coloro che convalidano i blocchi di transazioni da agganciare alla blockchain – e i nodi leggeri (light node), che non sono né miner, né conservano l'intera blockchain, rappresentando gli utenti del network meno coinvolti nel sistema.

All'interno della categoria delle valute digitali vengono ricomprese due diverse tipologie: le criptomonete, come il bitcoin, ossia "coin" digitali basati su una propria blockchain nativa, che ne regola il funzionamento, definita in questo caso "proprietaria" – e i token digitali, ovvero delle unità digitali secondarie che, non avendo una blockchain proprietaria, si appoggiano e vengono gestiti sulle catene, blockchain, di altre criptomonete, prima fra tutte quella di Ethereum, ovvero della criptovaluta "ether" (ETH).

Uno dei più recenti sviluppi della blockchain e della sua applicazione alle criptovalute, riguarda il tema della raccolta fondi per startup innovative che sviluppano soluzioni tecnologiche. Infatti, affianco alle tradizionali modalità di finanziamento per queste società, l'emissione di crittovalute o token digitali sta diventando sempre più diffusa. Queste operazioni prendono il nome di ICO (Initial Coin Offering), attraverso cui le startup emettono e vendono al pubblico una determinata quantità di token o criptomonete, per finanziare uno specifico progetto tecnologico. Tale modalità di finanziamento sta, negli ultimi anni, rimpiazzando l'attività di Venture Capital, tradizionalmente diretta proprio all'investimento in progetti e società innovative, e di nuova costituzione. Tale passaggio è dovuto alla mancanza di regolamentazione

delle ICO, che rende più semplice e meno oneroso il finanziamento, rispetto alle stringenti regole e ai requisiti richiesti per ottenere fondi da banche e Venture Capital.
Inoltre, la vendita di crittovalute tramite ICO, consente agli imprenditori di raccogliere fondi senza perdere il controllo della società, cosa che accade nella raccolta di equity, ad esempio attraverso una IPO, ovvero il procedimento di quotazione in borsa, strettamente regolamentato a differenza delle ICO.
Tra le Initial Coin Offering più importanti, è doveroso citare quella di Ethereum, la seconda principale crittovaluta dopo il bitcoin, che nel 2014 permise, ad Ethereum Fundation, di raccogliere 18,4 milioni di dollari, in circa un mese e mezzo.
Avendo fornito una panoramica sul funzionamento e le caratteristiche della blockchain, procediamo ad un'analisi schematica dei punti di forza e delle debolezze della tecnologia.
Per quanto riguarda i vantaggi della blockchain, i più importanti sono: la trasparenza del registro, che può essere letto da chiunque – la disintermediazione dei processi, si pensi alle transazioni bitcoin – la decentralizzazione, di fatto il registro delle transazioni è tenuto e condiviso da tutti i partecipanti al network – la sicurezza, infatti i dati contenuti nella blockchain sono immutabili, a meno di un attacco informatico, comunque di difficile realizzazione – e la riduzione dei costi e delle tempistiche, basti pensare alle crittovalute che consentono di effettuare transazioni direttamente fra due utenti, senza necessità di intermediari.
Relativamente alle criticità della blockchain, invece, le più importanti sono: la mancanza di privacy, nonostante il sistema Bitcoin sia anonimo, è in alcuni casi possibile risalire alle identità degli utenti – la sicurezza, esiste infatti la probabilità, anche se minima, di un attacco informatico al sistema del tipo "51 % Attack" – l'assenza di controllo centralizzato, che non consente un agevole sviluppo del sistema, e determina difficoltà nel modificare con rapidità il protocollo informatico – l'early stage della tecnologia, che rappresenta una novità e deve ancora stabilizzarsi verso un design dominante – il costo elevato dell'attività di mining, volta alla convalida dei blocchi di transazioni – i limiti di scalabilità – la reputazione e la regolamentazione, ovvero troppo spesso la blockchain risente dell'influenza negativa del sentiment relativo alle criptomonete, che su essa si basano, ed inoltre la regolamentazione è spesso assente o difforme fra Stato a Stato.
Come precedentemente menzionato, l'applicazione nelle criptovalute, nonostante sia la prima, è solo una delle possibilità offerte dall'ampio ventaglio applicativo della tecnologia blockchain; è infatti importante non confondere un elemento dell'insieme con l'insieme stesso.
Per comprendere l'ampiezza applicativa di tale tecnologia, bisogna pensare a tutti quei contesti in cui si formano due categorie di soggetti: controllanti e controllati. Le due categorie appena citate fanno riferimento ad un sistema chiaramente centralizzato, che rimanda l'affidabilità, la fiducia e la sicurezza del sistema stesso ad un ente sovraordinato, rappresentato dai controllori. Nei sistemi basati su blockchain, invece, la fiducia e la sicurezza, così come il consenso, sono raggiunti attraverso un procedimento decentralizzato e condiviso tra i vai partecipanti del network.

I principali settori che sono stati rivoluzionati dalla blockchain, o che secondo gli esperti lo saranno, sono: i settori finanziari, basti pensare al caso di Nasdaq, che impiega la blockchain in alcune transazioni azionare ed obbligazionarie – il settore delle smart property e dei diritti digitali, la blockchain infatti potrebbe gestire l'allocazione e il trasferimento di qualsiasi tipo di proprietà, anche digitale, attraverso gli smart contract, i quali saranno esaminati successivamente, analizzando la blockchain di Ethereum - la gestione delle identità digitali – il voto digitale, che in paesi come Norvegia ed Estonia è stato realizzato attraverso un registro blockchain – i settori relativi alla Sharing Economy, come quelli in cui opera Uber o AirBnB – i servizi pubblici, come quello della fornitura energetica – il settore della sanità, riguardo la gestione e la comunicazione delle informazioni sanitare dei pazienti – il settore delle predizioni e del gioco d'azzardo – ed i processi di produzione, relativamente alla filiera produttiva, infatti, la blockchain consentirebbe di registrare in modo immutabile tutte le informazioni riguardo i prodotti, come ad esempio l'origine, gli spostamenti e le altre informazioni relative al ciclo di vita del prodotto. È questo il caso di Walmart, colosso statunitense delle vendite al dettaglio, che utilizza la blockchain per monitorare le forniture di carni.

CAPITOLO III

Bitcoin venne presentato il 31 ottobre del 2008 attraverso la pubblicazione del white paper, ossia una descrizione tecnica del progetto, su internet da parte di un anonimo, sotto il nome di Satoshi Nakamoto. All'interno della Criptography Mailing List del sito metzdowd.com, nel quale venivano affrontate discussioni relative allo sviluppo tecnologico della crittografia, Satoshi Nakamoto allegò e pubblicò il documento: "Bitcoin: A Peer-to-Peer Electronic Cash System".

Il paper descrive un innovativo sistema per trasferire denaro digitale senza la presenza di servizi o istituzioni centralizzate, risolvendo per la prima volta in maniera distribuita, il problema comune a tutte le valute digitali, quello del double spending. Nel paper veniva inoltre messa in primo piano l'indipendenza del sistema di pagamento da terze parti, e l'anonimato nelle transazioni. Il primo gennaio 2009, venne rilasciata la prima versione del client Bitcoin, "Bitcoin v 0.1" un software open-source.

Mentre la teoria è frutto del lavoro privato di Nakamoto, il software è stato sviluppato con la collaborazione della community online.

Infatti, le conversazioni per lo sviluppo del client-software Bitcoin sono tutt'ora pubbliche sul forum "bitcointalk", dove si possono leggere i post di Nakamoto che ha sviluppato il software fino al 2011, quando in una mail inviata agli sviluppatori e alla comunità Bitcoin scrisse: "Sono passato ad altro"; lasciando così alla community lo sviluppo del software. Ad oggi non è stato possibile appurare chi si nasconda dietro lo pseudonimo di Satoshi Nakamoto, o se questo rappresenti in verità un nome collettivo che identifica un gruppo di persone.

La terminologia relativa al sistema Bitcoin può generare confusione, infatti il nome della criptomoneta è utilizzato simultaneamente per esprimere tre diversi strati del sistema. In primis, il termine Bitcoin, con

l'iniziale maiuscola, si riferisce alla tecnologia sottostante, la blockchain, ovvero al protocollo informatico che gestisce l'allocazione e il trasferimento di proprietà, ovvero i BTC. In secondo luogo, il nome Bitcoin viene anche usato per identificare il protocollo che lavora al di sotto della tecnologia, ovvero l'insieme di regole che disciplinano il sistema, le quali si esplicano nel software Bitcoin. Per ultimo, il termine bitcoin, con l'iniziale minuscola, è riferito alle unità di valuta digitale, le quali sono anche comunemente identificate dalla sigla BTC. Il sistema Bitcoin, dunque, si articola in tre differenti strati: tecnologia – protocollo – moneta.

Nonostante l'ecosistema Bitcoin sia recente e in continuo sviluppo, esso opera attraverso il coinvolgimento di vari Stakeholders: il team di sviluppatori, i quali lavorano al continuo sviluppo del protocollo Bitcoin – i minatori, che convalidano i blocchi di transazioni e li registrano nella blockchain, attività che determina la creazione di nuova moneta come ricompensa per i miner – gli utilizzatori, come ad esempio commercianti o investitori – i fornitori di servizi di wallet, ovvero di portafogli digitali nei quali vengono custodite le chiavi pubbliche e private che permettono di disporre dei propri bitcoin – le piattaforme di Exchange, dove è realizzabile la compravendita di crittomonete in cambio di valute tradizionali o altre crittovalute – i fornitori di servizi finanziari, che consentono di investire in crittovalute senza entrare concretamente nel sistema, ad esempio attraverso contratti derivati – i processori di pagamento, ossia l'insieme di servizi che agevolano l'utilizzo e l'accettazione di bitcoin per i pagamenti – e altri soggetti, come ad esempio le imprese che producono i dispositivi specifici per l'attività di mining, aziende che realizzano ATM per le crittomonete, oppure startup che sviluppano soluzioni tecnologiche basate su blockchain.

Il bitcoin può essere definito come la prima valuta digitale decentralizzata, ideata con la finalità di velocizzare e rendere anonime, oltre che più sicure, le transazioni online. L'algoritmo di funzionamento della crittovaluta bitcoin, realizzato da Satoshi Nakamoto, è basato su un concetto fondamentale: la creazione della valuta stessa è un fenomeno condiviso dalla comunità, dato che la "produzione" di bitcoin significa al tempo stesso contribuire attivamente alla sicurezza del sistema; in termini tecnici "mining".

La generazione di moneta, non controllata da un ente centrale e basata su un meccanismo peer-to-peer puro, è regolata dall'algoritmo di creazione che ne definisce caratteristiche e limiti di emissione. L'idea alla base dell'algoritmo di creazione è la scarsità della crittomoneta, condizione derivante dal fatto che l'emissione di bitcoin è limitata e anticipatamente stabilita. Infatti, il trend relativo alla generazione di bitcoin è stabilito da un algoritmo che segue un andamento a rendimenti marginali decrescenti nel tempo. Il numero totale di bitcoin, nel tempo, tende asintoticamente al limite di 21 milioni di unità, e, seguendo l'algoritmo di crescita corrente, il tasso di crescita dei bitcoin convergerà a zero intorno al 2140. In questa data, l'unica ricompensa, per l'attività di validazione delle transazioni, svolta dai miner, saranno le fee di transazione, dato che non verrà generata più moneta come fonte di incentivo per il mining.

Di seguito è proposta un'analisi schematica delle principali caratteristiche della criptovaluta bitcoin: la decentralizzazione del sistema, dovuta all'assenza di controllo di autorità centrali – lo pseudo-anonimato delle transazioni, non è infatti semplicemente rintracciabile l'identità, ma gli utenti sono identificati da indirizzi Bitcoin – la trasparenza, ogni transazione bitcoin è memorizzata nella blockchain, un registro

pubblico – il limite di creazione della valuta, fissato a 21 milioni di unità – la velocità nelle transazioni, infatti il sistema Bitcoin impiega in media 10 minuti per confermare una transazione – i bassi costi di transazione – l'irreversibilità delle transazioni – il bitcoin non ha corso legale, ovvero viene accettato come strumento di pagamento solo su base volontaria – ed infine, è immune dalla confisca.

Quando si parla di protocollo Bitcoin, si fa riferimento all'insieme di regole che definiscono il funzionamento del sistema, che si esplica nell'utilizzo del software open source, il più noto è "Bitcoin Core".

Ogni volta che si avvia una transazione, il computer la trasmette ai nodi (peer) della rete più vicini, i quali eseguiranno una serie di controlli formali, per accertarne la validità, e successivamente inoltreranno la transazione ai nodi-miner. Questi ultimi, inizieranno ad assemblare individualmente un blocco di transazioni, che attraverso la presentazione della "prova del lavoro", verrà convalidato ed inserito nella blockchain, diventando visibile a tutti gli utenti.

Al fine di verificare se il bitcoin possa essere considerato una valuta o meno, analizziamo le tre caratteristiche della moneta in relazione alla principale valuta digitale. Per quanto riguarda la funzione di mezzo di pagamento, l'efficacia del bitcoin, viene misurata dal numero di transazioni effettuate, ma soprattutto dal numero di soggetti disposti ad accettarli come strumento risolutorio. Dai dati disponibili, rispetto al 2017, nell'ultimo anno il numero di esercenti disposti ad accettare BTC come strumento di pagamento è aumentato considerevolmente. Relativamente alla funzione di unità di conto, una delle maggiori perplessità sulla valuta ideata da Nakamoto, deriva dalla sua eccessiva volatilità. Infatti, le ampie oscillazioni di prezzo del Bitcoin, renderebbero difficile ed oneroso, per i commercianti, il continuo ricalcolo dei prezzi dei prodotti espressi in BTC; oltre che a rappresentare una problematica per i pagamenti differiti.

Riguardo la funzione di riserva di valore, se una valuta tradizionale consente al proprietario di spenderla in un momento futuro, evitando di farlo incorrere in perdite da svalutazione, o in eccessive rivalutazioni, il bitcoin invece non sembra limitarsi ad una semplice riserva di valore, anzi, empiricamente sembra essere destinato a crescere di valore, data la sua natura deflattiva, dovuta al limite di unità, fissato nel protocollo, pari a 21 milioni.

Fra tutte le bolle registrate nella storia, quella attribuita al Bitcoin rappresenta il territorio più inesplorato in cui gli esperti di finanza si siano imbattuti. Difatti, in circa dieci anni, i bitcoin non hanno solamente bruciato ogni record borsistico in termini di prezzo, passando dai 40 centesimi iniziali a oltre 12 mila dollari a metà gennaio 2018, ma hanno anche subito bruschi crolli che ne hanno ridotto fortemente la capitalizzazione. Il valore massimo raggiunto dalla crittovaluta, coincide con un importante accadimento, che ha portato il bitcoin nel "mainstream della finanza", ovvero la quotazione dei future aventi come sottostante bitcoin sulla borsa di Chicago. Il successo del lancio dei future insieme all'attenzione mediatica per l'evento, hanno portato il bitcoin a raggiungere il tetto massimo di quasi 20.000 dollari.

Ad oggi, il prezzo è sceso poco sotto i 7.000 $, anche in virtù dei limiti attuali mostrati dal sistema Bitcoin, infatti l'eccessiva congestione della rete, dovuta ad un elevatissimo numero di transazioni avviate, ha

portato a ritardi di oltre 24 ore nella convalida delle transazioni, e a pagare elevatissime fee ai miner, per ottenerne la validazione. Queste problematiche, hanno portato i membri della comunità Bitcoin a dividersi, sulla necessità o meno di apportare modifiche al protocollo, per rendere più scalabile il sistema.

Avendo osservato il trend storico del valore di bitcoin, procediamo all'analisi dei principali driver che determinano il prezzo della crittovaluta: le forze di mercato, infatti, non essendo controllato da nessuna autorità centrale, il prezzo del bitcoin è determinato dal meccanismo di domanda e offerta, con quest'ultima limitata a 21 milioni di unità – l'attrattività del bitcoin, intesa come l'insieme di eventi in grado di far incrementare la domanda di possibili utilizzatori. Un esempio può essere la regolamentazione, l'adozione del sistema Bitcoin da parte di un'importante player commerciale, oppure il divieto all'utilizzo posto da parte delle autorità – inoltre, un importante driver è l'andamento macroeconomico e finanziario, il quale può, come nel caso di periodi ad elevata inflazione delle valute tradizionali, rendere più attrattive le crittovalute – ed infine, i costi di produzione, ossia dell'attività di estrazione, il mining, nel senso che, un' incremento di questi costi, implicherebbe un chiaro aumento del prezzo del bitcoin.

Per quanto riguarda i rischi di svalutazione del bitcoin, dobbiamo far riferimenti a specifici ed ipotetici eventi. Ad esempio, produrrebbero una svalutazione dei bitcoin, l'utilizzo di una fonte energetica meno costosa per svolgere l'attività di mining, oppure l'utilizzo di dispositivi hardware con un minore consumo energetico, o ancora, il rischio che vengano cambiate le regole alla base del protocollo. Una fra tutte, il limite di unità, che, nel caso in cui venisse aumentato, lancerebbe un segnale di abbondanza tale da deprimere il prezzo dei BTC.

Nel caso in cui le regole del sistema Bitcoin non venissero modificate, il limite di generazione della moneta, fissato a 21 milioni di unità, connota il bitcoin come una moneta deflattiva. Infatti, al raggiungimento del tetto di offerta della valuta, un incremento della domanda, genererebbe un apprezzamento della crittomoneta. Questa implicazione deflattiva, a detta dei più importanti economisti, soprattutto keynesiani, rappresenta il più grande limite all'affermazione del bitcoin; poiché una moneta deflattiva risulterebbe non adatta e dannosa per un'economia basata sui consumi, dato che l'aumento del valore della moneta nel tempo non li incentiverebbe.

La continua diatriba sulle modifiche da apportare al protocollo Bitcoin per rendere il sistema scalabile, si è concentrata sulle possibili soluzioni in grado di rendere più efficienti i pagamenti, in termini di velocità e costi.

La scalabilità del sistema bitcoin può essere raggiunta attraverso miglioramenti "on chain" oppure "off chain".

Per scalabilità on chain, si intende la modifica e il miglioramento delle caratteristiche intrinseche della blockchain di Bitcoin, come potrebbe essere ad esempio l'incremento della dimensione (size) di ogni blocco della catena. Mentre, la scalabilità off chain si riferisce alla creazione di un'infrastruttura tecnologica sopra a Bitcoin e la sua blockchain, una "second layer technology".

Le principali proposte di modifica del protocollo Bitcoin sono state: Segregated Witness, con la quale si chiedeva l'alleggerimento dei dati contenuti in ogni blocco, al fine di poter inserire in esso un maggior

numero di transazioni – e Segregated Witness 2x, che, rispetto alla prima proposta, aggiungeva l'incremento della dimensione del blocco da 1 MB a 2 MB, con la finalità di evitare congestioni della rete Bitcoin. Mentre la prima modifica è stata accettata e apportata dalla comunità Bitcoin, nell' agosto 2017, la seconda non è stata apportata data la mancanza di consenso fra i vari stakeholders.

È importante aggiungere che, nel caso di una modifica sostanziale del protocollo, in cui una maggioranza della comunità è disposta ad implementarla, mentre una minoranza qualificata si oppone, si creerebbe una biforcazione (fork) della blockchain, poiché le due catene lavorerebbero sulla base di regole diverse. Questo fork, determinerebbe la creazione di una nuova criptovaluta, come nel caso della Blockchain di Bitcoin, dalla quale, in funzione delle fratture nella sua comunità sulle modifiche da apportare al protocollo, si è creata una catena di blocchi alternativa, dalla quale è nata una nuova crittovaluta: Bitcoin Cash.

Avendo fornito una panoramica sulla crittovaluta leader del comparto, di seguito è proposta una sintesi schematica dei principali vantaggi del bitcoin: la trasparenza, nel sistema Bitcoin ognuno può seguire in tempo reale tutta la catena delle transazioni – l'anonimato nelle transazioni – bassi costi e rapidità delle transazioni, condizioni che sono però subordinate all'assenza di un elevato numero di transazioni da processare che congestionerebbe la rete – e la decentralizzazione, intesa come indipendenza da un'autorità centrale.

Mentre, per quanto riguarda le criticità del sistema Bitcoin, che limitano la sua diffusione, riscontriamo: l'irreversibilità delle transazioni, infatti se si sbaglia indirizzo a cui inviare i BTC non è possibile annullare l'operazione – l'onerosità del mining, l'attività che assolve sia la funzione di convalida delle transazioni, sia di generazione di nuove unità di crittovaluta, è dal punto di vista elettrico, costosissima – i rischi di centralizzazione, legati al concentramento della maggioranza del potere di calcolo del sistema Bitcoin in mano a pochi soggetti ed entità, che consentirebbe di manipolare il protocollo e la blockchain di Bitcoin – i costi e le tempistiche delle transazioni, troppo alti in situazioni di congestionamento della rete, una soluzione potrebbe essere l'aumento della dimensione del blocco che comprende le transazioni – la volatilità del prezzo e i risvolti deflattivi, infatti la crittomoneta bitcoin tenderà ad apprezzarsi, ed è importante che lo faccia, perché con lo sviluppo della rete Bitcoin la difficoltà della convalida dei blocchi tenderà a salire, rendendo più oneroso il mining, che dovrà quindi essere compensato dalla generazione di una valuta il cui prezzo tende a crescere – la vulnerabilità del protocollo e il suo sviluppo continuo, infatti oltre al rischio di attacchi informatici come il "51% Attack", il sistema bitcoin si fonda su un protocollo informatico ancora in fase beta, ossia non ufficiale, ma in sperimentazione – e l'assenza o la difformità di regolamentazione, poiché la situazione legale e fiscale di Bitcoin, ove non assente, non è omogenea e varia da Stato a Stato.

Proprio a riguardo della regolamentazione, anche se la situazione si presenta a macchia di leopardo, in via generale, c'è una forte attenzione delle autorità riguardo i rischi relativi alle operazioni di ICO, non regolamentate. Mentre, per quanto riguarda il Bitcoin, alcuni paesi come il Giappone, lo hanno dichiarato valuta legale, parificandolo a quelle tradizionali; altri, invece, come l'Italia, lo hanno regolato solamente attraverso il recepimento della direttiva europea relativa all'anti riciclaggio, rimanendo di fatto scettici

riguardo il comparto cripto. Questo è dovuto soprattutto alla paura dell'utilizzo del Bitcoin per fini illegali come il cyber-crime.
Inoltre, riguardo la natura giuridica della crittomoneta bitcoin, è importante menzionare che, negli Stati Uniti, è recente il caso di una pronuncia giudiziaria sulla base della quale bitcoin è moneta, e non quindi commodity, come aveva precedentemente decretato la Commodity Futures Trading Commission.

CAPITOLO IV

Con il termine "altcoin", vengono identificate le crittovalute, nate dopo il bitcoin, che compongono il comparto crypto. L'elevato numero di altcoin, ad oggi circa 1.400, lascia immaginare come, in questo grande insieme, siano realmente poche le crittomonete che possano replicare o addirittura performare i risultati ottenuti dal bitcoin.
Per questa ragione, verranno analizzate due principali altcoin che, più di altre, si stanno delineando come possibili leader nel comparto, attualmente traghettato dal bitcoin. Le due criptomonete in questione sono Ethereum e Ripple.
Sviluppata circa sette anni dopo il bitcoin, Ethereum sembra essere, a detta degli esperti del settore, la crittovaluta maggiormente in grado di stravolgere le logiche tradizionali, poiché è basata su una tecnologia più innovativa e sostanzialmente migliore di quella del bitcoin.
L'Ethereum Fundation, con a capo il giovane ed ormai famoso Vitalik Buterin, lanciò la criptomoneta "ether" (ETH) nel 2014 attraverso una delle ICO più importanti della storia. L'operazione, che finanziava il progetto tecnologico dell'Ethereum Fundation, consentì la raccolta di 18 miliardi di dollari, ottenuti dalla vendita delle criptomonete ether. Ad oggi la crittovaluta ether è la seconda più grande del mercato, con un valore unitario di circa 530 $ ed una capitalizzazione di mercato pari a 52,5 miliardi di dollari.
Ethereum rappresenta una piattaforma blockchain aperta, la quale consente ad ogni utilizzatore di costruire ed utilizzare applicazioni decentralizzate, che vengono eseguite sulla blockchain stessa.
La programmabilità della tecnologia, ha reso possibile per gli utenti lo sviluppo di contratti "smart" e di applicazioni decentralizzate (DApp), piuttosto che fornire un set predefinito di operazioni, proprio come in Bitcoin. Infatti, la blockchain di Ethereum è una piattaforma utilizzabile per una vasta gamma di applicazioni decentralizzate Peer-to-Peer, che includono sicuramente le criptomonete, ma non si esauriscono ad esse.
Invece, per smart contract, si intende un contratto digitale che viene automaticamente eseguito al verificarsi di una o più clausole in esso contenute, senza dunque l'intervento delle parti coinvolte per attivarlo, e può essere utilizzato per scambiare digitalmente qualsiasi cosa abbia un valore.
Il procedimento di mining di Ethereum, ossia di risoluzione del problema crittografico per la validazione delle transazioni, è basato sull'algoritmo di Proof of Work, proprio come il sistema Bitcoin.

In questo contesto la prova del lavoro svolto (POW) è l'esecuzione stessa del programma o dell'applicazione decentralizzata, risolvendo così la critica di grande spreco di risorse finalizzato alla mera esecuzione di calcoli, relativi al mining, mossa verso Bitcoin.

Mentre, per quanto riguarda l'algoritmo di generazione di moneta, che sappiamo essere in Bitcoin determinato e agganciato al limite di 21 milioni di unità, in Ethereum vengono generati, come ricompensa per i miner, 5 ether per ogni blocco "estratto", con il limite però di 18 milioni di unità di crittovaluta generata al massimo ogni anno. Questo determina chiaramente, a differenza dei bitcoin, un'offerta di moneta non limitata nel tempo, che si sgancia così dai suoi risvolti deflattivi, tanto criticati dal pensiero di molti economisti.

Un'altra importante differenza è rappresentata dall'utilizzo della crittovaluta nei due sistemi. Infatti, se in quello Bitcoin la criptomoneta è utilizzata per le transazioni e i pagamenti, nel sistema Ethereum la valuta, ossia gli ether, sono ideati per essere utilizzati dagli sviluppatori nel pagare la potenza di calcolo del network necessaria ad eseguire le applicazioni decentralizzate, da loro sviluppate. Ulteriori differenze fra il sistema Bitcoin ed Ethereum si evincono anche dalla tempistica di validazione dei blocchi, infatti se per minare e quindi validare un blocco in Bitcoin il tempo previsto dal protocollo è settato a 10 minuti, in Ethereum invece, questa tempistica si riduce a soli 17 secondi.

Le app decentralizzate e i contratti smart rappresentano il passo successivo nell'evoluzione della tecnologia blockchain. Infatti, attraverso queste innovative implementazioni, la "Blockchain 2.0", di Ethereum, potrebbe potenzialmente avere un impatto e un'utilità maggiore di quella avuta da Bitcoin e dalla sua blockchain.

Risulta chiaro che, l'ipotetica affermazione nel tempo delle crittovalute, come sistemi decentralizzati e disintermediati, rappresenti uno scenario decisamente avverso all'attuale sistema finanziario e bancario.

In risposta a questa minaccia, Ripple Lab ha sviluppato e lanciato sul mercato una criptovaluta a misura di banca, che può aiutare il comparto bancario a rispondere alle pressioni, e a cavalcare l'onda crittografica e digitale. La crittomoneta in questione è ripple, nota con la sigla XRP.

Ripple Lab è una società privata che ha sviluppato sia una piattaforma di scambio Peer-to-Peer che una valuta digitale chiamata ripple (XRP), progettata per le banche. Infatti, Il protocollo Ripple, che regola la rete di pagamenti, permette di eseguire transazioni, ovvero trasferimenti di somme di denaro, in qualsiasi valuta. Dunque, il network di Ripple consente alle banche l'esecuzione di transazioni e il cambio fra valute per scambi esteri, senza l'intervento di una camera di compensazione (clearing house), quindi senza la necessità un intermediario terzo.

Per quanto riguarda il numero di crittomonete ripple, tutte le unità sono già disponibili e sono già state tutte generate (pre-minate), a differenza dei bitcoin e degli ether.

Le unità di crittomoneta sono dunque limitate, e tale limite, codificato nel protocollo, fissa il numero massimo di ripple generati e in circolazione pari a 100 miliardi di unità. Il fatto che la crittomoneta ripple sia pre-minata, ovvero che tutte le unità sono state già generate, significa che non è possibile fornire potere

di calcolo in cambio di nuovi ripple. Questo determina un basso consumo energetico del network Ripple, rispetto a quello di Bitcoin caratterizzato da un'onerosissima attività di "estrazione" (mining).

Il Ripple Net consente alle banche, ma fondamentalmente a chiunque, di trasferire valuta tradizionale o digitale. Il funzionamento è basato sulla costruzione di linee di fiducia fra l'utente, che deve effettuare un pagamento a favore di un altro, e altri utenti che hanno il ruolo di gateway, ovvero che aiutano a realizzare la transazione, come degli intermediari bancari.

La flessibilità di Ripple consente di trattare qualsiasi tipo di valuta, consentendo anche lo scambio fra valute attraverso un mercato di valuta integrato nel software Ripple. Quest'ultimo ha anche una propria moneta interna, ripple (XRP), che a differenza delle altre valute non si basa sul concetto delle linee di fiducia, ma bensì può essere inviata a chiunque liberamente. Le crittomonete ripple sono inoltre fondamentali per fare da ponte nello scambio fra valute di qualsiasi tipo (bridge-currency), soprattutto per quelle che non hanno un cambio diretto sul mercato.

Il processo di formazione del consenso, per validare le transazioni, è molto diverso dalla "proof of work" di Bitcoin. Infatti, ogni utente di Ripple Net ha una lista di nodi affidabili, ovvero delle entità fidate a Ripple Lab, chiamata UNL (Unique Node List), a cui è affidata la convalida delle transazioni.

La differenza più marcata tra XRP e BTC è sicuramente la finalità dei due sistemi, che, nel caso di ripple, da vita ad un vero e proprio paradosso.

Bitcoin è stato creato per rispondere al crollo economico-finanziario del 2008, e alla mancanza di fiducia del pubblico nei confronti del sistema bancario, percepito come complice della turbolenta situazione che ha caratterizzato gli ultimi anni. Ripple invece, gestito in modo centralizzato da Ripple Labs e progettato per le banche, mira a rendere più efficienti le transazioni bancarie in termini di tempi e costi, ed a regolare i rapporti e gli scambi fra istituzioni finanziarie. Il paradosso della finalità di Ripple è dovuto al fatto che persegue l'obbiettivo di salvare il comparto bancario, adeguandolo a processi più innovativi, quando invece il mondo delle criptovalute è nato proprio per scavalcarlo e disintermediare il sistema. Il sistema Ripple è dunque finalizzato a rendere più competitivi i servizi offerti dalle banche, aiutandole nel confronto con le crittovalute.

L'assenza del processo di mining nel sistema Ripple determina, nel confronto con il Bitcoin, ampi vantaggi in termini di costi e velocità del sistema. Infatti, il processo di validazione delle transazioni, che nei sistemi tradizionali può richiedere fino a 3-4 giorni, circa 17 secondi per Ethereum e intorno ai 10 minuti per Bitcoin, viene efficientemente realizzato dal sistema Ripple in 4 secondi. Inoltre, a differenza della rete Bitcoin, Ripple Net può gestire 1.500 transazioni per secondo, ed è scalabile fino a sostenere 50.000 Tps.

Tra i più grandi finanziatori delle soluzioni tecnologiche sviluppate da Ripple Labs vengono annoverati Banco Santander, UBS, ma anche Unicredit, oltre a molte banche centrali, come la BCE e la Federal Reserve statunitense, che hanno sperimentato il Ripple Net.

Proprio in relazione alle partnership stipulate da Ripple Labs, c'è da notare come, molto spesso, gli incrementi di quotazione della "coin" ripple, siano stati sostenuti dalla sua crescente legittimazione, riconosciuta da numerose banche e società finanziarie di tutto il mondo. Attualmente, stando ai dati di

giugno 2018, il prezzo di XRP si aggira attorno a 0,6 $, con una capitalizzazione complessiva di mercato pari a 24 Bn di dollari.

CONCLUSIONI

Ad oggi, cercare di rispondere alla domanda relativa a quale sia il futuro della blockchain e delle criptomonete, è solamente un gioco di retorica. Nonostante il futuro della blockchain, a detta degli esperti, sembra essere davvero promettente, data la sua grande spinta innovativa, quello delle criptovalute rimane decisamente incerto. Allo stato attuale dei fatti, nessuna crittovaluta sembra essere in grado di poter rimpiazzare le valute tradizionali, date le molte criticità e le profonde debolezze che le caratterizzano.
Tra gli elementi, che personalmente ritengo cruciali per l'ipotetica affermazione delle valute digitali, rientrano lo sviluppo e i futuri miglioramenti della tecnologia, su cui esse si basano, una regolamentazione tanto specifica quanto favorevole, ed infine, sicuramente il tempo, variabile fondamentale se si tiene conto della "freschezza" del comparto cripto.