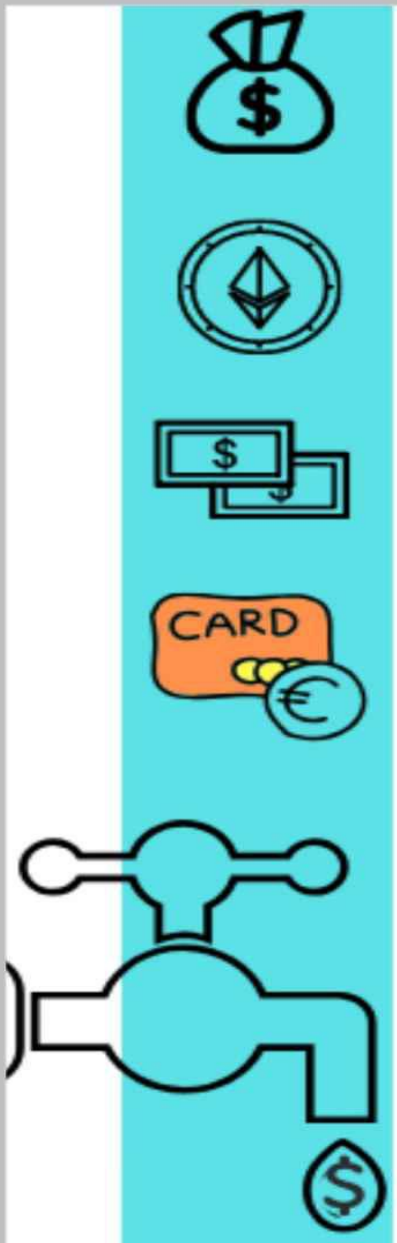
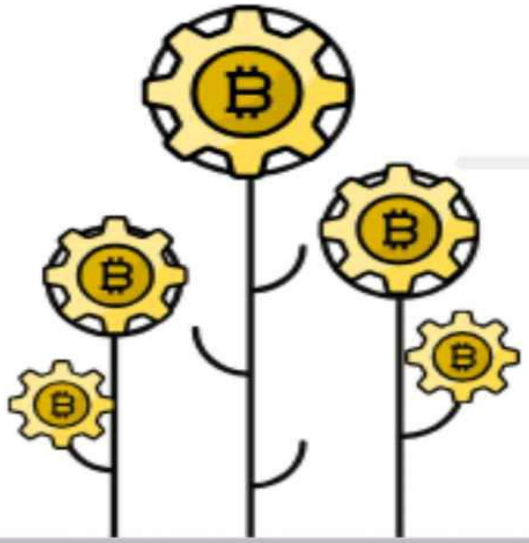


GUIDA RAPIDA ALLA COMPRENSIONE DELLA PIÙ GRANDE INNOVAZIONE TECNOLOGICA, DOPO INTERNET

IL BITCOIN E LA BLOCKCHAIN

L'EVOLUZIONE DELLA MONETA NELL'ERA DIGITALE



GIANLUCA MONTESANTO

GIANLUCA
MONTESANTO

IL BITCOIN E LA BLOCKCHAIN:

L’evoluzione della moneta

nell’era digitale

ISBN: 9798603304465

Revisione e copertina a cura di Monica Spatola (Il Velo Dipinto: Agenzia di servizi editoriali)

Independently published

Agli arditi, ai rivoluzionari, ai nostri figli

INDICE

2 La Blockchain e il Bitcoin

2.1 Cosa è e perché nasce la tecnologia Blockchain
2.2 La prima criptovaluta: il Bitcoin
2.3 Gli algoritmi crittografici, il mining e la generazione di monete Pow, Pos, Poi

3 Il Cripto capitalismo – Le Initial Coin Offering I.C.O.

3.1 Gli smartcontracts e il criptocapitalismo
3.2 Cosa sono le Initial Coin Offering ICO
3.3 La Regolamentazione e i risvolti monetari economico-

Capitolo 1

PREMESSA: STORIA E FUNZIONE DELLA MONETA DALLE ORIGINI AD OGGI

Possiamo assumere come concetto

generale e massimamente sintetico che la moneta, in tutte le sue forme, è, ed è stata, la risposta pratica ai bisogni, via via emergenti, nell'evoluzione della gestione degli scambi nella civiltà umana.

Mi sembra doveroso, perciò, introdurre, con un breve sunto, il percorso storico della nascita e dell'evoluzione della moneta e delle relative politiche monetarie che ne regolamenteranno la stabilità, lo scambio e il valore, ma soprattutto, vedremo cosa essa rappresenta nella civiltà.

1.1 Il Baratto e il concetto di moneta

A un certo punto della storia, assistiamo al passaggio dallo stile di vita nomade a quello sedentario. Piccoli gruppi di persone iniziarono a aggregarsi e a insediarsi presso uno stesso luogo, formando una sorta di **mercato chiuso** in cui gli scambi di prodotti avvenivano direttamente tra i membri di questi gruppi, in base alle esigenze contingenti.

Avvennero i primi scambi commerciali. Più semplicemente, se occorreva del latte, ad esempio, si

andava dall'allevatore e in cambio del latte si offriva ciò di cui si disponeva. Questi scambi consentivano la conversione dei beni con altri beni, per mezzo del baratto.

Le prime tracce di questa pratica risalgono addirittura alla preistoria. Anche dalle antiche civiltà degli Egizi giungono testimonianze sulla grande importanza di questa forma di scambio.

I più famosi commercianti dell'antichità furono i Fenici, che si distinsero per la loro abilità nel baratto già nel XVI secolo a.C. Il baratto, però, presentava degli inconvenienti, infatti era difficoltoso confrontare efficacemente il valore tra i beni scambiati, lo scambio dei prodotti non

trasportabili creava disagi e, infine, per ottenere tutto il necessario bisognava fare numerosi atti di scambio.

In risposta a queste esigenze di natura pratica, le comunità iniziarono ad accettare e utilizzare dei prodotti "neutri" come pelli, sale, bestiame o ciò che comunemente era chiamato "pecunia" (pecùnia s. f. [dal lat. pecunia, der. di pecus «bestiame», ricordo di un'economia primitiva a carattere pastorizio])[1].

Si trattava di prodotti facilmente trasportabili e che potevano essere misurati, il cui valore era di semplice attribuzione, per questo furono comunemente accettate come merce di scambio o come moneta-merce.

Questa evoluzione del baratto segnò la nascita del primordiale concetto di **moneta,** intesa come bene comunemente accettato in cambio di prodotti o servizi, misurabile e di cui ci sia una quantità massima, determinata e non infinita, la quale possa mantenere il suo valore nel tempo.

1.2 Il Metallismo

Intorno all'VIII secolo A. C., insieme agli altri beni sopra descritti, s'iniziarono a utilizzare, a tale scopo, i metalli preziosi che, grazie alle loro caratteristiche intrinseche, presero il sopravvento sugli altri beni.

I metalli preziosi presentavano, e presentano tutt'ora, dei vantaggi e delle caratteristiche che rispondono in maniera più adeguata a ciò che rappresenta la moneta: **Omogeneità**, perché un pezzo d'oro è esattamente uguale a un altro; **divisibilità** e **duttilità**, fondendo questo metallo prezioso è possibile ricomporlo senza perdita di

peso e valore di quest'ultimo; **non deperibilità,** perché non si assiste al suo deterioramento nel tempo; **malleabilità**, perché la sua lavorazione è agevole. Infine, tutti i metalli preziosi sono **facilmente trasportabili** e **comunemente accettati** come bene di scambio.

Furono coniate le prime monete, il cui valore facciale o nominale corrispondeva al valore intrinseco della quantità di metallo di cui erano costituite.

Già nell'antica Grecia, ciascuna Polis (città-stato) aveva coniato la propria moneta ed esisteva un'officina che le produceva, o meglio le coniava. Questo tipo di officine erano, e tutt'oggi

sono chiamate, la **Zecca**.

Le prime tracce della Zecca italiana sono riconducibili a Roma, in Campidoglio, nel 390 a.C., presso il tempio di Giunone Moneta.

Dal nome della zecca romana deriva il nome di MONETA, diffuso in Italia e in tutto il mondo.

1.3 La moneta-segno, la nota di banco e la nascita delle prime banche

A partire dal Medioevo le esigenze mutarono, si estesero i confini geografici dei mercati e gli scambi avvenivano con regioni distanti. Durante questi lunghi viaggi, le monete potevano essere rubate o, a seconda della quantità, potevano risultare difficilmente trasportabili. Fu allora che nacque la "moneta-segno" con le prime lettere di cambio o "nota di banco". Le note di banco o **banconote** erano dei documenti rilasciati da orafi che custodivano, e quindi certificavano, l'esistenza e il possesso di un certo

numero di monete. Questi "certificati" erano accettati da altri orafi in altre città e potevano essere utilizzati come strumento di pagamento o essere scambiati con il corrispettivo quantitativo di monete certificato.

In questo passaggio storico possiamo riconoscere i primordi della nascita delle future banche commerciali e, al contempo, s'inserisce un concetto fondamentale della futura politica monetaria: la **fiducia**. Acquisito un diffuso consenso, le "note di banco" favorirono la nascita delle prime forme di prestito. Un mercante poteva rivolgersi a questi proto-banchieri per avere oro in prestito. Questi primi banchieri emettevano note di banco a

propria discrezione, quindi anche in eccesso rispetto all'oro effettivamente posseduto nei forzieri. Analizzando tali processi, si evince che, non solo venivano concessi dei prestiti, ma si creava nuova moneta proprio nell'accezione che abbiamo enunciato prima, considerando moneta tutto ciò che viene diffusamente accettato per porre in essere degli scambi.

Le proto-banche furono le prime a creare, dunque, nuova moneta emettendo più note rispetto all'oro posseduto e aumentando, di conseguenza, l'ammontare complessivo dei mezzi di pagamento. Evidentemente, questo comportamento esponeva gli orafi a un notevole rischio di illiquidità.

Immaginiamo, ad esempio, che tutti i possessori delle note di banco le avessero messe all'incasso contemporaneamente, il banchiere non avrebbe potuto far fronte alle richieste perché non possedeva nei propri forzieri tutto l'oro necessario.

Fu a Genova, nel 1406, durante il periodo rinascimentale, che assistemmo alla nascita della prima banca, intesa in senso moderno: il Banco di San Giorgio.

Questa nacque inizialmente come istituzione deputata della gestione del debito pubblico, ma con il passare del tempo e la decadenza dei banchi privati, si affermò anche come "banca commerciale".

Solo nel 1694, assistiamo alla

nascita della prima vera e propria banca di emissione: la Banca d'Inghilterra, alla quale seguirono le banche di emissione degli altri Stati, con lo scopo principale di finanziare i mercati e favorire gli scambi commerciali.

Con l'avvento della rivoluzione industriale, nacquero nuovi tipi di istituzioni bancarie, sia per la raccolta dei depositi che per la concessione di varie forme di credito. Ciò segnò un'espansione dei crediti bancari senza precedenti. Le banche finanziarono la spesa pubblica per le varie opere di urbanizzazione, prime fra tutte quelle ferroviarie, e accompagnarono le imprese nello sviluppo dell'industria tessile, meccanica e siderurgica.

1.4 Il Gold Standard

Nella seconda metà dell'ottocento, considerato che la quantità di oro presente nelle riserve auree delle Banche Centrali di ogni singolo Stato determinava la quantità massima di credito accordabile in certificati di deposito e di moneta emettibile, al fine di mantenere costante il valore delle valute negli scambi monetari, sia nei mercati interni che nei mercati internazionali, si adottò come parametro di riferimento l'oro.

Per ogni unità di valuta si stabilì un corrispettivo quantitativo di oro, determinando di fatto dei tassi di cambio

fissi a livello internazionale per tutte le valute.

Questa impostazione economico-valutaria prese il nome di Gold Standard Exchange, il primo Stato ad adottarlo fu proprio la Gran Bretagna. Una delle caratteristiche fondamentali che decretò il successo dell'adozione, a livello internazionale, del Gold standard era l'obbligo assunto da parte delle Banche centrali di convertire, su richiesta, le monete, banconote o certificati di prestito in oro e viceversa a livello internazionale, come abbiamo detto prima, a tassi di cambio sostanzialmente fissi.

Un altro aspetto di fondamentale importanza, nell'adozione di questo

sistema, fu l'utilizzo dell'oro come unico mezzo per il riequilibrio e la liquidazione della bilancia dei pagamenti tra i vari Stati.

Il Gold standard risultò essere un meccanismo straordinariamente efficiente ed efficace per lo sviluppo degli affari finanziari internazionali e accompagnò e, probabilmente favorì, la nascita della seconda Rivoluzione Industriale e del conseguente Imperialismo.

Questo, per la stabilità dei tassi di cambio. Di contro, però, questo sistema presentava alcuni risvolti che andavano a modificare il valore della moneta.

La dinamicità del saldo delle riserve auree determinava oscillazioni

direttamente collegate al valore totale di moneta disponibile e, conseguenzialmente, potevano manifestarsi, nei mercati domestici, alternativamente momenti di relativa inflazione o deflazione.

Durante l'Imperialismo, le politiche espansive coloniali spesso prevedevano l'assunzione d'importanti risorse del territorio conquistato che andavano ad arricchire la riserva aurea del Paese conquistatore e, in funzione del riequilibrio della bilancia dei pagamenti, avvenivano trasferimenti di oro tra i singoli Stati.

Questa concatenazione di scambi determinava una notevole dinamicità delle corrispettive riserve auree e

giocava un ruolo fondamentale sul valore effettivo della moneta e sulla conseguente inflazione o deflazione della stessa.

1.5 Bretton Woods e il Dollar standard

Il Gold standard ebbe una fase di arresto con l'avvento della grande guerra, nei primi decenni del XX secolo, fino al suo definitivo abbandono.

A seguito della grande depressione degli anni '30, durante la seconda guerra mondiale, nel 1944 si riunirono le 44 nazioni alleate per la conferenza monetaria e finanziaria delle Nazioni Unite (United Nations Monetary and Financial Conference) e furono firmati gli Accordi di Bretton Woods.

Lo scopo della conferenza fu quello di regolamentare la politica monetaria

internazionale, si decise di adottare per ogni nazione un tasso di cambio fisso nei confronti, non più dell'oro ma del dollaro, che mantenne il suo tasso di cambio con l'oro, ma ne prese il suo posto e divenne il nuovo parametro di riferimento, per questo si parla di Dollar Standard.

In quell'occasione, i rappresentanti delle nazioni riunite decisero, tra l'altro, d'istituire, il Fondo Monetario Internazionale e la Banca Mondiale, con lo scopo di supportare gli stati in crisi con prestiti strutturali da rimborsare nel tempo.

Questa nuova struttura di cambi durò fino al 15 agosto 1971, quando, l'allora Presidente degli Stati Uniti, Richard

Nixon, a Camp David comunicò al mondo la decisione di sospendere la convertibilità del dollaro in oro, sancendo in tal modo la svalutazione del dollaro, la fine del sistema aureo e dando inizio alla nuova fluttuazione dei cambi.

La fluttuazione dei cambi gettò le basi del nuovo sistema monetario che, ormai slegato dalle riserve auree dei singoli Stati, collegava il valore di una moneta alle logiche di mercato e alle dinamiche tra domanda e offerta.

Le Banche centrali, il Fondo Monetario Internazionale e la Banca Mondiale acquisirono, in questo nuovo contesto, un ruolo fondamentale di salvaguardia della stabilità dei prezzi,

quindi dell'inflazione e del valore delle monete, non solo per i mercati domestici, ma anche per quelli internazionali, per questo, in armonia con i Governi si determinarono politiche monetaristiche per mitigare e correggere le varie oscillazioni del valore monetario. Per svolgere questa fondamentale funzione, le Banche centrali assunsero anche il compito di vigilare sul sistema bancario e sulle normative di riferimento, affinché queste fossero rispettate, e laddove necessario sanzionare gli operati illeciti o non conformi, cercando di evitare situazioni di squilibri finanziari.

1.6 La crisi dei mutui subprime

È in questo scenario di organizzazione monetaria mondiale che approdiamo, nell'autunno 2008, a Wall Street, il simbolo della finanza americana e sinonimo della supremazia globale degli Stati Uniti d'America fondata sul dollaro, dove avviene il collasso, a seguito dalla crisi dei mutui Subprime. L'inadeguata regolamentazione della normativa bancaria ed in particolare sul *leverage* o leva finanziaria, che non imponeva alcun limite relativo ai parametri d'indebitamento, permise alle banche di concedere prestiti senza alcun freno.

Il caso di Bear Stearns fu alquanto significativo: la banca arrivò a reggere un rapporto tra impieghi e capitale del 33 a 1. Ciò significa, sostanzialmente, che con ogni dollaro detenuto, essa impiegava o investiva 33 dollari. Una leva così elevata consente di moltiplicare i profitti quando le cose vanno bene, ma è anche un rischio enorme per la stabilità della banca. Se ho una leva di 33 a 1, per ogni 100 dollari che investo sui mercati finanziari, 3 sono miei, gli altri 97 sono presi a prestito. Visto che i debiti vanno restituiti, basterà, allora, una perdita del 3% sui miei investimenti per azzerare il mio patrimonio. Sfruttando la crescita del mercato immobiliare americano,

quindi sfruttando l'elevata domanda di prestiti per acquisto di case, favorita anche dai bassi tassi d'interesse, le banche consentirono di accendere mutui anche a chi non aveva un adeguato *cash flow* per il regolare rientro del debito contratto. Si arrivò a finanziare anche i cosiddetti mutui NINJA (*No Income, No Job or Asset).*

Per avere un'idea della portata di tale fenomeno, basti pensare che in California un raccoglitore di fragole messicano, con un reddito annuo di 14.000$, ottenne da una finanziaria, legata a Washington Mutual, un mutuo da 720.000$ per comprare casa. (Storia tratta dall'Herald Tribune, 27-11-2008).

Altro fattore fondamentale della crisi

dei mutui Subprime fu il meccanismo della cartolarizzazione dei crediti, che consentì alle banche di trasferire il rischio di insolvenza del credito a terzi, e quindi pulire i bilanci dai *bad credit* e rientrare dell'intero capitale più il relativo guadagno, potendo così reinvestire le somme ottenute.

I mutui venivano ceduti alle *Special Purpose Vehicle* o Società Veicolo. Le Società Veicolo trasformavano i mutui in titoli obbligazionari *Mortgage Backed Securities* (MBS), le cui cedole venivano rimborsate con i soldi delle rate pagate dal debitore originario che aveva contratto il mutuo. Allo scopo di sfruttare al massimo questi strumenti finanziari ed espanderne il più possibile

il mercato, avvenne una seconda fase di cartolarizzazione: la cartolarizzazione sulla cartolarizzazione. Con questo nuovo processo, i titoli strutturati sui mutui furono rimpacchettati e cartolarizzati a loro volta in nuovi titoli obbligazionari che, avendo come *collateral* o sottostante altre obbligazioni MBS, furono definiti *Collateralized Debt Obligations* (CDO). Le obbligazioni *Collateralized Debt Obligations* presentano le stesse caratteristiche e si basano sullo stesso meccanismo dei *Mortgage Backed Securities*, con l'unica differenza che, mentre questi ultimi hanno come sottostante i mutui, i CDO sono titoli obbligazionari che hanno come

sottostante altri titoli. Inoltre, similmente al meccanismo di rimborso degli MBS (finanziato con l'incasso delle rate dei mutui), il rimborso e le cedole dei CDO sono finanziati con i rimborsi e il pagamento delle cedole degli MBS da parte della società veicolo di primo livello.

Tutti questi titoli obbligazionari, sia i MBS che i CDO, furono piazzati facilmente sui mercati finanziari di tutto il mondo, grazie al favore delle società di rating, che li classificarono come investimenti "sicuri" attribuendo loro la classe di rischio "AAA". Evidentemente, allo scoppio della bolla immobiliare del mercato americano, e quindi all'impossibilità dei debitori di

rimborsare le rate dei mutui, tutto il sistema, che sostanzialmente si basava su di essi, andò in stallo. La crisi finanziaria, che nasceva in seno al mercato americano, passò oltre i confini nazionali statunitensi e divenne mondiale. La crisi dei mutui subprime scatenò a valanga una crisi finanziaria globale e una crisi nell'economia reale a causa dei vari meccanismi di collegamento tra il mondo finanziario e l'economia reale, tra questi, consideriamo l'effetto leva delle banche e la rottura del rapporto fiduciario. A causa dell'effetto leva, anche una piccola perdita nel settore dei mutui e delle CDO ebbe il potere di causare enormi riduzioni nel patrimonio delle

banche. Il caso di Bear Stearns, sopra riportato, ne è un chiaro esempio. In secondo luogo, le banche iniziarono a fidarsi sempre meno l'una dell'altra, ciò bloccò il mercato interbancario, vale a dire, i prestiti che quotidianamente le banche pongono in essere tra loro, la vera e propria linfa che fa funzionare l'intero sistema finanziario.

Allo scoppio della crisi, le banche iniziarono a temere di ricevere titoli "tossici" in cambio dei prestiti realizzati sul mercato interbancario, proprio nello stesso momento in cui la liquidità serviva di più per tappare le perdite che venivano a crearsi con la crisi dei mutui subprime. L'intero sistema del credito subì un importantissimo arresto, la crisi

coinvolse le banche di tutto il mondo e, a cascata, le imprese che non ebbero più accesso al credito. Per spezzare questa spirale dovettero intervenire governi e banche centrali, iniettando liquidità nel sistema e garantendo i titoli tossici nei bilanci delle banche.

Quello che accade nel 2008, quindi, fu molto più di una catastrofe finanziaria. Insieme alla bolla creditizia scoppiò la bolla del globalismo americano. L'ingloriosa fine di Lehman Brothers, Merryll Lynch, Bear Sterns, la clamorosa multa elevata alla società di rating Standard & Poor's, di 1,5 miliardi di dollari per rating "gonfiati" minarono qualcosa di più importante della ricchezza: la fiducia verso il sistema

bancario da parte di soggetti esterni, ma ancor più grave, da parte di soggetti interni al sistema.

Capitolo 2

LA BLOCKCHAIN E IL BITCOIN.

2.1 Cos'è e perché nasce la tecnologia Blockchain

Nel capitolo precedente abbiamo

ripercorso la storia della moneta, partendo dalla preistoria siamo arrivati fino ai giorni nostri. Questo excursus è stato necessario per riuscire a comprendere cosa è una moneta e, come questa, nelle sue evoluzioni, ha generato reazioni e cambiamenti nella vita dei popoli, nel corso degli anni. Siamo arrivati, alla fine del capitolo, a raccontare ciò che ancora oggi "subiamo", cioè le conseguenze della più grande crisi finanziaria dopo gli anni trenta.

Come abbiamo visto, la conseguenza più grave che ha prodotto questa crisi, oltre alla perdita della ricchezza, è stata la perdita di fiducia verso l'intero sistema bancario, in generale. Per avere

una misura della “catastrofe”, che è nata come crisi finanziaria prima e poi ha ribaltato e contagiato in maniera purulenta l'economia reale, possiamo considerare che, solo nel primo anno di crisi, tra settembre 2007 e ottobre 2008, provocò una perdita di valore delle borse mondiali di 26,4 mila miliardi di dollari e un calo del pil mondiale stimato in 4,7 mila miliardi di dollari (fonte: Il Sole 24 ore Economia, del 6 agosto 2017). Quasi 700 banche, dall'inizio della crisi finanziaria, sono scomparse. Questo dato è quanto emerge dal rapporto sul settore di giugno 2017 della Banca Centrale Europea, che evidenzia come il numero totale delle istituzioni bancarie (tenendo conto di

grandi gruppi e singole istituzioni, anche straniere, con base nell'Unione Europea), sia sceso dalle 3.881 unità di fine 2007 alle 3.154 di fine marzo 2017.

Ancora oggi, la Banca Centrale Europea immette nel mercato nuova moneta, acquistando titoli di stato, continuando a mantenere il costo del denaro ai minimi storici, allo scopo di dare liquidità ad un sistema economico-finanziario che, nel suo complesso, ancora stenta a ripartire ed è ben lontano dai livelli pre-crisi.

Questo contesto disastroso è il fattore scatenante della nascita della Blockchain e, quindi, del Bitcoin. Ecco, come l'uomo, di fronte a questi fatti, innesca il suo sano istinto di

autoconservazione mettendo in campo tutto ciò di cui è capace.

La domanda è: come può la tecnologia Blockchain, essere una risposta alla crisi mondiale? Intanto, cerchiamo di capire cosa sia la blockchain e, proviamo a spiegarlo con un esempio.

Immaginiamo che ai tempi dei primi banchieri, quando nacque la "nota di banco", tutti i trasferimenti di oro a livello mondiale, fossero stati iscritti, in ordine cronologico, su un unico grande registro o libro giornale, e immaginiamo ancora che una copia di questo registro fosse custodita da chiunque possedesse anche solo una piccola quantità di oro e che tutti questi registri venissero

aggiornati costantemente da ciascuno ad ogni transazione, anche se la transazione specifica non lo riguardava: avremmo avuto, in unico registro, il saldo della quantità di oro che ciascuno possedeva e quindi la quantità di oro di cui ognuno poteva disporre.

Abbiamo semplificato, in parole povere, il sistema della blockchain: un grande *ledger* o libro giornale, pubblico, condiviso, decentralizzato e crittografato, con crittografia asimmetrica, che ti consente di avere una chiave pubblica e una chiave privata, all'interno del quale, troviamo scritte tutte le transazioni in ordine cronologico legate tra di loro con un'applicazione indiretta di una marca

temporale.

Oggi, quello che abbiamo immaginato nell'esempio, è attuabile ed è stato realizzato grazie alla tecnologia Blockchain: una catena di blocchi pubblica, condivisa, decentralizzata e crittografata. Ma di quali blocchi parliamo? In questo caso, si parla di blocchi informatici, all'interno dei quali vi sono scritti dei dati o più semplicemente delle transazioni, crittografate per l'appunto. Una volta creati, certificati o "minati" (scopriremo in seguito il significato del termine) e uniti l'uno all'altro, concatenati, questi dati diventano sostanzialmente immodificabili. Questa trasparenza e certificazione delle informazioni

estromette, automaticamente, dal sistema della registrazione dei trasferimenti o degli scambi l'elemento "fiducia" che ai tempi delle note di banco fu essenziale per l'evoluzione dell'intero sistema finanziario. Adesso, questa fiducia è trasferita ad algoritmi matematici e alla tecnologia.

Questo è quello che afferma anche Massimo Chiriatti, Tecnologo, membro di Assob.it, in un interessante articolo su Nova – Il Sole 24 Ore, il 25 febbraio 2018. Con l'utilizzo della Blockchain e la decentralizzazione del *ledger,* le transazioni non sono più scritte e custodite presso un unico ente privato. Oggi, per sapere quanti soldi hai, o se vuoi mandarli a qualcuno in cambio di

qualcosa, lo devi chiedere alla tua banca perché è lì che sono registrate tutte le tue transazioni, nel database della tua banca. Ecco che, ancora, ritorna il concetto di fiducia nel sistema bancario. Con la decentralizzazione del *ledger* pubblico, chiunque può trovare su internet la blockchain di Bitcoin, per esempio, e scaricare l'intero registro fin dalla prima transazione ad oggi.

Chiunque, con le opportune conoscenze informatiche, può avere una "filiale" della Blockchain in casa che si aggiorna automaticamente ad ogni blocco inserito. E chiunque possegga Bitcoin, può trasferire la propria valuta in qualsiasi momento e senza dover chiedere a nessuno di farlo al suo posto.

In realtà, già qualche secolo fa, Nell'isola di Yap[2] in Micronesia (a Nord Est dell'Australia), era possibile riscontrare un qualcosa che assomiglia molto alla Blockchain di oggi. Una legenda racconta di un dio che introdusse su quest'isola una moneta che gli abitanti decisero di adottare: una pietra calcarea di forma circolare con un buco al centro. Tanto più grande era la "moneta di pietra" quanto più grande era il suo valore, (una pietra dell'isola di Yap di circa 2,5 metri di diametro è oggi in mostra nel museo della Banca del Canada, ad Ottawa, Ontario)[3].

La quantità di questa pietra, in principio, era piuttosto scarsa perché nell'isola non c'erano miniere o cave da

cui poter attingerne. Allo scopo di ottenerne ancora si organizzarono spedizioni, e i cercatori, non contenti di recarsi nella vicina isola di Palau, si spinsero fino a Guam (a Nord Est di Yap, nelle isole Marianne), dove questa materia prima era assai più reperibile. Guam dista quattrocento miglia di mare, e si narra che queste acque fossero sempre tempestose. Molti canotti, ritornando con il loro pesante carico, si perdevano e non era raro il caso che su molte imbarcazioni partite per Guam, soltanto una rientrasse in porto. Il valore della pietra era mantenuto elevato non solo dai pericoli che s'incontravano e dalle difficoltà che si dovevano superare per possederla, ma anche

dall'impossibilità di qualsiasi contraffazione, poiché a Yap non si trovava l'agognata specie di roccia. Non vi era dunque nulla di intrinsecamente prezioso nella pietra di Palau: essa aveva valore per gli indigeni di Yap perché era difficile a trovarsi e perché veniva accettata come valuta di scambio. Il possesso era dimostrato con delle incisioni su ogni singola pietra e tutti sapevano a chi appartenesse. Il passaggio della proprietà era segnato sulla pietra con l'incisione del nome del nuovo proprietario e, considerate le dimensioni, era pressoché impossibile rubarla o utilizzarla altrove, anche perché, al di fuori dell'isola, nessuno avrebbe accettato quella enorme pietra

come corrispettivo. Anche nell'isola di Yap non c'erano intermediari e il possesso era scritto direttamente sulle monete, la garanzia del possesso non passava per la fiducia, c'era maggiore trasparenza, chiunque poteva venire a conoscenza del nome del proprietario, verificando personalmente l'incisione.

In conclusione, possiamo affermare che se non ci fosse stato il concetto di fiducia alla base del sistema bancario nel suo complesso (banche di investimento, agenzie di rating, società di gestione del risparmio, ecc...) essa stessa non avrebbe potuto essere tradita e forse non ci saremmo imbattuti nella più grande crisi mondiale dagli anni trenta ad oggi.

2.2 La prima criptovaluta: il Bitcoin.

Nel primo capitolo abbiamo ripercorso le fasi storiche dell'evoluzione della moneta e dei mercati finanziari per comprendere l'ambiente in cui nasce e, muove i primi passi, l'idea di affrancamento e distacco dal sistema finanziario "fiduciario".

In realtà, già dagli anni ottanta, David Chaum, un informatico e crittografo americano, iniziò ad approfondire tematiche relative all'anonimato nelle transazioni nel suo *paper* "*Blind Signature for Untraceable Payments*"[4], partendo

dalla considerazione che la privacy e la tutela delle informazioni sensibili sono alla base della libertà, soprattutto in ambito finanziario. Chaum acquisì notorietà per lo sviluppo di *Ecash*, un'applicazione di pagamento elettronico che curava l'anonimato dell'utente. Queste idee tecniche di miglioramento della privacy di Chaum, insieme all'uso diffuso di tecnologie crittografiche avanzate, furono la base tecnica dell'ideologia del movimento Cypherpunk, anch'esso, iniziato alla fine degli anni ottanta, che aveva individuato in queste visioni la strada per il cambiamento sociale e politico.

Nel 1993, Eric Hughes, pubblica il "*Il Manifesto di Cypherpunk*"[5] nel

quale esprime con chiarezza i princìpi di questo movimento e annuncia la creazione di software gratuiti da utilizzare, per la massima tutela della privacy, che consentivano di limitare o estendere la visibilità del proprio operato (messaggi, email, trasferimento di moneta).

Se analizziamo più attentamente, con l'evoluzione tecnologica e l'utilizzo dei *device* nella vita quotidiana di ognuno, tutto o quasi tutto, è tracciato o quantomeno tracciabile a differenza del passato. Questo enorme potenziale informativo può essere un enorme vantaggio per essere analizzato e utilizzato a servizio di tutti ma, nel contempo potrebbe usato in maniera

“fraudolenta” e non eticamente corretta, violando i princìpi di legge che tutelano gli utenti dall’utilizzo improprio dei dati sensibili.

Un caso emblematico che possiamo citare è quanto accaduto nell’aprile 2018 con Cambridge Analytica che raccolse dati sensibili di oltre 80 milioni di utenti di Facebook, senza il loro consenso, e successivamente, questo enorme potenziale fu utilizzato da diversi politici, tra i quali anche Donald Trump, per "ottimizzare" le campagne elettorali.

Il 9 gennaio 2009 in una mailing list dedicata agli studi sulle applicazioni "*peer-2-peer*" e alla crittografia, fu annunciata, con questo messaggio[6], la

nascita e il rilascio della prima versione del protocollo Bitcoin:

"Annuncio la prima versione di Bitcoin, un nuovo sistema di denaro elettronico, che utilizza una rete peer-to-peer per evitare la doppia spesa. È completamente decentralizzato, senza server o autorità centrali. Vedi bitcoin.org per gli screenshot. e i link per scaricare: Si collega automaticamente ad altri nodi, se è possibile mantenere un nodo in esecuzione che accetta connessioni in entrata, aiuterai davvero molto la rete. Porta 8333 sul tuo firewall deve essere aperta per ricevere le connessioni in entrata. Il software è ancora alfa e sperimentale. Non c'è garanzia e lo

stato del sistema dovrà essere riavviato ad un certo punto se diventa necessario, anche se ho fatto tutto il possibile per integrare estensibilità e versatilità. Puoi ottenere monete facendo in modo che qualcuno te le invii o accendi Opzioni-> Genera monete per eseguire un nodo e generare blocchi. La difficoltà del proof-of-work è incredibilmente bassa per iniziare, quindi all'inizio, un tipico PC sarà in grado di generare monete in poche ore. Diventerà molto più difficile quando la competizione farà aumentare la difficoltà regolata automaticamente. Le monete generate devono aspettare 120 blocchi per maturare prima di poter essere spese. Ci sono due modi

per inviare denaro. Se il destinatario è online, tu puoi inserire il suo indirizzo IP, si connetterà per ottenere una nuova chiave pubblica e potrai inviare la transazione con i commenti. Se il destinatario non è online, è possibile inviare al suo indirizzo Bitcoin, che è un hash della chiave pubblica e riceverà la transazione la prima volta che si connette e dopo che sarà caricato il blocco su cui è scritta la transazione. Questo metodo ha lo svantaggio che nessuna informazione di commento viene inviata e si può perdere un po' di privacy se si utilizza l'indirizzo più volte, ma è un'alternativa utile se entrambi gli utenti non possono essere online allo

stesso tempo o il destinatario non può ricevere connessioni in entrata. La circolazione totale sarà di 21.000.000 di monete. Saranno distribuite ai nodi collegati quando faranno nuovi blocchi, l'importo della ricompensa sarà dimezzato ogni 4 anni. I Primi 4 anni: 10.500.000 monete, successivi 4 anni: 5.250.000 monete, successivi 4 anni: 2.625.000 monete, successivi 4 anni: 1.312.500 monete, eccetera... Quando l'importo massimo sarò raggiunto, il sistema potrà supportare le spese di transazione se sarò necessario. Si basa sulla competizione del libero mercato, e probabilmente non ci sarà bisogno, saranno sempre i nodi disposti a elaborare le transazioni

gratuitamente. Satoshi Nakamoto".

L'autore reale del post è rimasto, fino a ora, sconosciuto, nonostante i massicci sforzi per individuarlo. Di lui si conosce solo lo pseudonimo: Satoshi Nakamoto, il misterioso nome che ha firmato il *paper* dell'idea originale e che ha portato avanti la prima fase dello sviluppo del programma fino alla sua maturazione. Le teorie sulla vera identità di Satoshi Nakamoto sono numerose.

Secondo il Premio Nobel, Robert Shiller, uno dei motivi del successo del Bitcoin è il mistero che aleggia sulla figura del suo creatore.

In giapponese "Satoshi" significa "un pensiero chiaro, veloce e saggio", "Naka" può significare "medium, dentro

o relazione", "Moto" può significare "origine" o "fondamento". Molti giornalisti si sono appassionati alla ricerca del volto o dei volti che si celano dietro lo pseudonimo Satoshi Nakamoto. Anche Netflix, importante azienda americana operante nella produzione e distribuzione on-demand di film, serie televisive e altri contenuti d'intrattenimento, ha pensato bene di produrre un documentario *"Banking on Bitcoin"* per approfondire la prima criptovaluta, la sua blockchain e cercare di far luce sulla vera identità di Satoshi.

Alla fine, il cerchio si stringe ragionevolmente, attorno a tre nomi: Hal Finney, Nick Szabo e Craig Steven Wright. I primi due fanno parte dei

Cypherpunk. Hal Finney, geniale crittografo scomparso nel 2014, fu una delle prime persone a lavorare con Satoshi e partecipò alla prima transazione Bitcoin di sempre. Nick Szabo, già inventore del Bit Gold, precursore del Bitcoin, e infine Craig Steven Wright, imprenditore australiano che si era proclamato il papà dei Bitcoin nel 2016 portando diverse prove che avvaloravano la sua tesi, per poi ritrattare subito dopo la sua dichiarazione. Ad oggi, il nome che si cela dietro lo pseudonimo Satoshi Nakamoto risulta ancora un mistero irrisolto.

Il *paper* originale, firmato da Nakamoto, intitolato "*Bitcoin: A Peer-*

to-Peer Electronic Cash System"[7], è considerato una pietra miliare per gli addetti ai lavori nel mondo delle criptovalute, in esso viene descritta una struttura concepita per trasferire il denaro digitale senza dover ricorrere al coinvolgimento di servizi centralizzati o istituzioni finanziarie, risolvendo per la prima volta il problema del *double spending* (tentativo fraudolento di inviare a più destinatari la medesima quantità di denaro).

Il Bitcoin, creato da Satoshi Nakamoto, è gestibile utilizzando un software open source che può essere scaricato da chiunque lo desideri, con lo scopo principale di restituire ai legittimi proprietari, senza dover passare da terze

parti, la gestione del proprio denaro (bitcoin). Per fare questo si devono possedere le chiavi private dei rispettivi *wallet* (portafoglio), garantire che il denaro che si sta inviando sia davvero in tuo possesso e che non si duplichino le transazioni evitando così l'invio, della stessa quantità di denaro, a più persone, ma soprattutto curare la sicurezza dei dati decentralizzando e "ridondando", su tutti i nodi della rete Bitcoin, la blockchain.

La prima versione di Bitcoin rilasciata all'inizio del 2009, fu concepita come naturale evoluzione di un concetto già esistente: il Bit Gold, che era stato descritto per la prima volta poco più di un decennio prima, nel

1998, da Nick Zsabo[8].

Come già detto, non è un caso che la nascita di questa moneta arrivi proprio nel periodo forse più difficile della grande crisi economico-finanziaria degli ultimi vent'anni, apertasi nel 2008 negli Stati Uniti con la crisi dei mutui subprime, in un momento in cui la fiducia nelle banche e negli organi centrali di controllo finanziario era ai minimi termini, in tutto il mondo.

Il sistema ideato da Satoshi Nakamoto, come da lui stesso annunciato, prevede la generazione programmata di circa 21 milioni di monete (bitcoin) entro l'anno 2140.

Ogni bitcoin è divisibile in 100milioni di sottoparti, dette *satoshi*,

raggruppate in insiemi intermedi di millibitcoin (un millesimo di bitcoin) e microbitcoin (un milionesimo di bitcoin). Evidentemente, all'aumentare del valore di cambio, i sottomultipli bitcoin acquistano sempre maggior rilevanza.

Il 22 maggio del 2010 Laszlo Hanyecz, uno dei primi sviluppatori del progetto, acquistò due pizze da asporto alla pizzeria Papa John's di Jacksonville (FL) per 10.000 bitcoin[9], equivalenti a quel tempo a circa $25. Da allora il 22 maggio si celebra il Bitcoin Pizza Day. Oggi, per ricomprare le due famose pizze sarebbero sufficienti 357.000 satoshi ovvero 0,00357 bitcoin.

Il protocollo Bitcoin ha già previsto

una propria politica monetaria "deflattiva", che fissa "rigidamente" l'immissione di nuova moneta nel mercato, attraverso una regola chiamata *reward halving*[10], che a cadenza programmata, ogni 210.000 blocchi, pari circa ad un quadriennio, dimezza la ricompensa prevista per i *miners* e quindi diminuisce gradatamente il "conio" di nuova moneta. Così facendo, la rigidità dell'offerta programmata, non solo mantiene molto bassa la quantità di nuova moneta, ma in maniera decrescente, questa tende ad azzerarsi.

La rappresentazione della curva d'immissione di nuova moneta nel mercato è esemplificata dal grafico[11] sottostante (Figura nr. 1), che

rappresenta su l'asse delle ascisse gli anni di produzione dei bitcoin (2009-2033) e sull'asse delle ordinate i bitcoin che vengono assegnati (e prodotti) per il completamento di un singolo blocco.

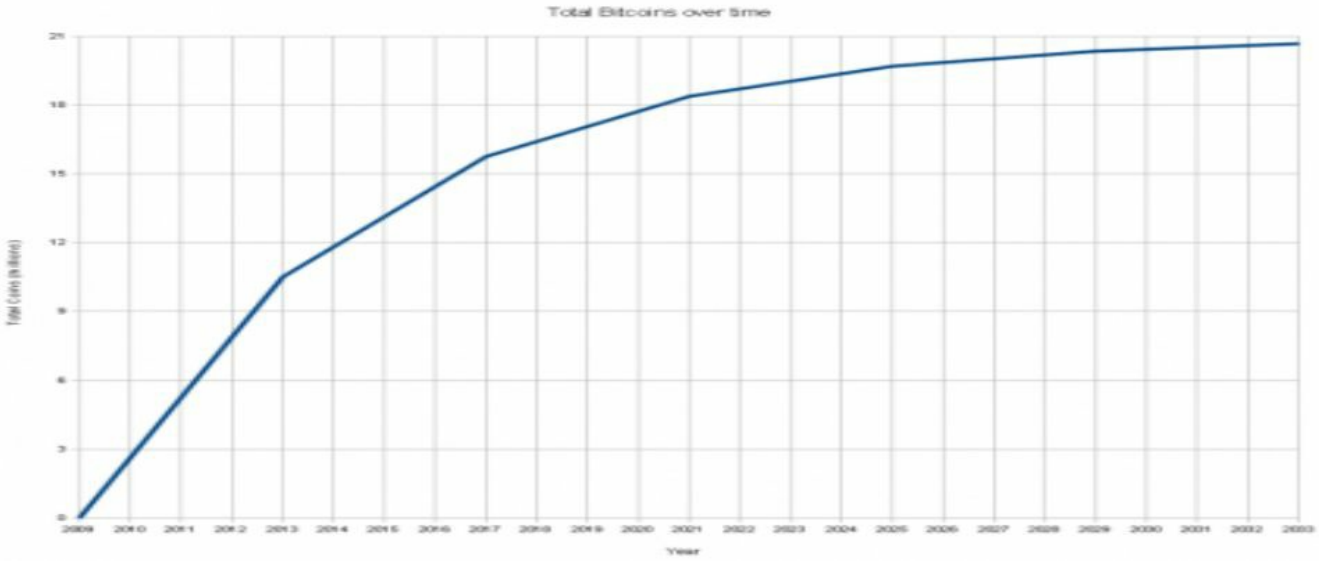


Figura nr. 1

Il numero totale di bitcoin tende asintoticamente al limite di 21 milioni. Come previsto da Satoshi Nakamoto: *"Saranno distribuite ai nodi collegati quando faranno nuovi blocchi, l'importo della ricompensa sarà*

dimezzato ogni 4 anni. I Primi 4 anni: 10.500.000 monete, successivi 4 anni: 5.250.000 monete, successivi 4 anni: 2.625.000 monete, successivi 4 anni: 1.312.500 monete, eccetera... Quando l'importo massimo sarò raggiunto, il sistema potrà supportare le spese di transazione se sarò necessario. Si basa sulla competizione del libero mercato, e probabilmente non ci sarà bisogno, saranno sempre i nodi disposti a elaborare le transazioni gratuitamente".

Notiamo come, all'avvicinarsi della data dell'ultimo periodo di immissione di nuova moneta ed ipotizzando che la domanda di Bitcoin crescerà più che proporzionalmente rispetto all'offerta, i

Bitcoin probabilmente subiranno una deflazione nel valore (cioè un aumento del valore reale) dovuta alla scarsità di nuova moneta. Analizzando l'andamento del valore di Bitcoin dal 2009 (vedi tabella 1) ad oggi, la tesi esposta è verificabile.

ANNO	VALORE MAX 1 BITCOIN	VARIAZIONE %
2009	$ 0,07	
2010	$ 0,39	457,14%
2011	$ 6,00	1438,46%
2012	$ 13,00	116,67%
2013	$ 900,00	6823,08%
2014	$ 320,00	-64,44%
2015	$ 450,00	40,63%
2016	$ 1.000,00	122,22%
2017	$ 19.000,00	1800,00%
2018	$ 7.000,00	-63,16%

Tabella 1

È difficile dimensionare il fenomeno

“Bitcoin”, esistono numerose variabili che possono condizionarne l’evoluzione. I cosiddetti “poteri forti” come Banche, Governi, Media tradizionali e Social Media, potrebbero avere molto interesse ad arginare questo fenomeno, ma con molta probabilità, il valore di Bitcoin è destinato a salire ancora molto, perché è una rivoluzione che parte dal basso, troppo frammentata e decentralizzata per essere fermata. Ad avvalorare quest’idea c’è un altro elemento molto interessante che emerge, si tratta della strettissima correlazione che esiste tra il prezzo del Bitcoin e la sua Capitalizzazione. Analizzando i grafici degli andamenti, del prezzo e della capitalizzazione di Bitcoin, espressi in

USD (Figura nr. 2 e 3) ci accorgiamo che, pur essendo due indicatori di natura completamente differente, relativamente alle loro dinamiche interne: il prezzo è determinato esclusivamente dalla ricerca dell'equilibrio tra domanda e offerta; la capitalizzazione è invece, la quantità di valuta fiat che viene immessa nel mercato del Bitcoin, sono praticamente sovrapponibili.

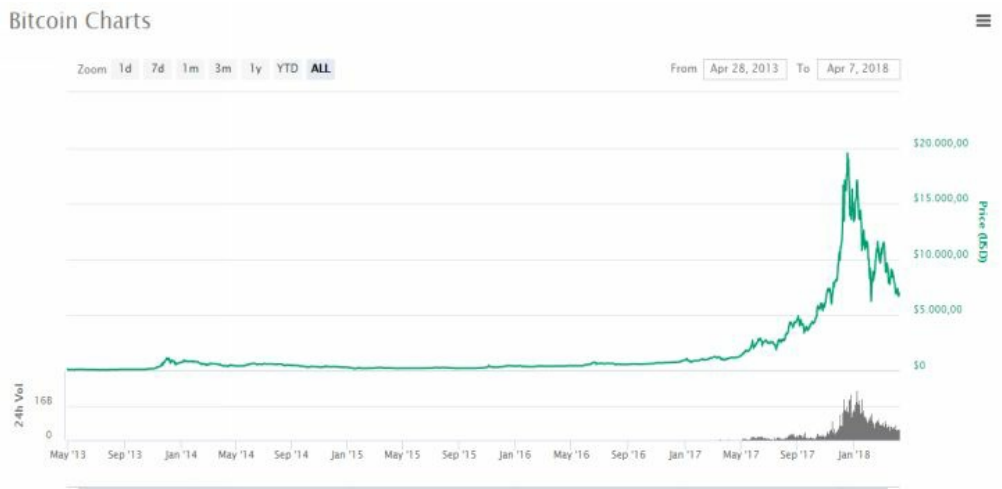


Figura nr. 2

(= prezzo in USD del Bitcoin)

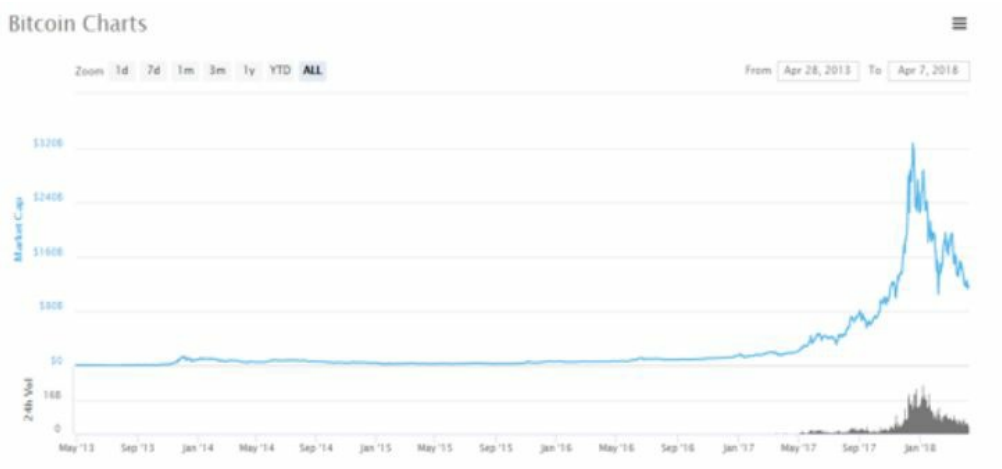


Figura nr. 3

 (= capitalizzazione in USD del Bitcoin)

Questa “sovrapponibilità” evidenzia come il Bitcoin sia recepito dal mercato. Esso sta assumendo, maggiormente in questa fase, la funzione della moneta come “riserva di valore” più che moneta come “mezzo di scambio” (gettando uno sguardo, all’intero pianeta, assistiamo anche al suo utilizzo localizzato come moneta commerciale). In Italia abbiamo un esempio molto interessante di come il Bitcoin sia entrato nella vita di ogni giorno.

Il caso in questione è la città di Rovereto, in Trentino, un comune di 40mila cittadini. Un gruppo di

sviluppatori informatici insieme ad alcuni imprenditori hanno avviato una startup “Inbitcoin”, che promuove la diffusione del bitcoin. All'inizio sono partiti da un bar e via via si è diffuso l’utilizzo di questa moneta digitale, tra i metodi di pagamento quotidiani. Oggi, a Rovereto si può pagare con bitcoin il dentista, la pizza, fare benzina o pagare la carne dal macellaio. Questo, possiamo affermare che è il primo germoglio italiano della nuova rivoluzione finanziaria appena iniziata.

Proviamo a fare un po’ di conti. Si stima che il mercato azionario in senso ampio ad oggi ammonti a circa 70 *trillions dollars* e il valore del denaro mondiale circolante ammonti a circa 80

trillions dollars, che sommati tra loro fanno 150.000 miliardi di dollari. La *Market Capitalization*[12] di tutto il mercato delle criptovalute ammonta a circa 263 miliardi di dollari, pari quindi allo 0,17% della capitalizzazione mondiale. Il bitcoin con la sua *Market Capitalization* di 119 miliardi di dollari, ha una *dominance* sul mercato delle cripto, di circa il 45,1%.

Questi numeri fanno riflettere. Ipotizzando che nei prossimi 5/10 anni il mercato delle criptovalute raggiunga, anche solo, il 2% del mercato mondiale, quindi dei 150.000 miliardi di dollari, vorrebbe dire che la capitalizzazione totale arriverebbe 3.000 miliardi di dollari, e anche abbassando la

dominance di Bitcoin al 32,88%, minimo storico toccato il 14 gennaio 2018, vorrebbe dire che il valore del bitcoin, il quale avrà raggiunto una *Total Supply*[13] di circa 18.375.000 *coins*[14], sarebbe matematicamente di circa 54.000 dollari contro l'attuale valore di 7.000 dollari.

2.3 Gli algoritmi crittografici, il mining e la generazione di monete POW, POS

A questo punto, andiamo a spiegare nel dettaglio, come avviene la produzione dei bitcoin e come il sistema ideato da Nakamoto possa essere definito come *"A stroke of genius - a monetary system governed by a computer algorithm"* (Un colpo di genio – un sistema monetario gestito da un algoritmo informatico)[15] e scopriremo quanto disarmante sia la semplicità del meccanismo sottostante, che non trascura in alcun modo la sicurezza.

Il protocollo della blockchain di Bitcoin consente di trasferire i Bitcoin da un utente a un altro, senza dover passare da un server centrale, ma avvalendosi di diversi "nodi", che mantengono aggiornato il "ledger", cioè il libro mastro nel quale sono scritte tutte le transazioni (vedi figura 1).

Per eseguire il trasferimento, per prima cosa è necessario creare un *wallet,* all'interno della blockchain di Bitcoin. È possibile utilizzare diversi servizi per la creazione di un wallet e scegliere tra diverse tipologie: desktop wallet, hardware wallet, paper wallet, web wallet e wallet per smartphone. Ognuno di essi presenta contemporaneamente dei vantaggi e

degli svantaggi.

Da un punto di vista di sicurezza informatica, sembrerebbe che gli hardware wallet consentano di garantire un alto livello di sicurezza perché mantengono le proprie criptovalute, in questo caso i bitcoin, *"off line"*, tutelandoli quindi dai rischi della rete, ma d'altro canto non sono immuni dai danneggiamenti meccanici o da smarrimenti.

Figura 1

Il wallet Bitcoin è generato attraverso l'applicazione della crittografia asimmetrica. Partendo da una stringa arbitraria, generalmente composta da una serie alfanumerica di

512 caratteri o da una *passphrase* di 12-20 parole, si ottengono una chiave pubblica e una chiave privata, da qui l'asimmetria della crittografia.

Nella figura 2, possiamo vedere l'esempio di un wallet di bitcoin.

Il Bitcoin address o *the public key*, è la chiave utilizzata per indirizzare le transazioni, e lo vediamo identificato con la seguente stringa alfanumerica: 12UToZvQKJZdXDkttfoCV9YZEW23Q

Questa serie di numeri e lettere sarà quella che troveremo scritta e visibile a tutti nei blocchi della blockchain di Bitcoin in ogni transazione effettuata, sia in entrata che in uscita, da questo wallet.

Attraverso l'*explorer* della blockchain di Bitcoin al sito

https://blockchain.info/ chiunque può consultare tutti i blocchi e quindi tutte le transazioni in essi contenuti, dal primo movimento del 2009 fino ad oggi. Per tutelare la privacy e/o l'anonimato, principio ispiratore del Bitcoin, è prevista la possibilità di creare "n" bitcoin address, essendo questi gratuiti e immediatamente calcolabili.

La Private key invece, è l'altra faccia della stessa medaglia, generata dall'applicazione dell'algoritmo crittografico asimmetrico, (nella figura 2 la riscontriamo con il seguente codice: L4k5upMvxi44gZi8z1mz6m6TLjLm94FJ

Questa stringa alfanumerica dovrà rimanere segreta e ben custodita. Solo con questa si potranno "firmare" le

transazioni, ma soprattutto senza di essa non sarà più possibile gestire il proprio wallet e quindi si perderebbe tutto il suo contenuto.

Figura 2

Una volta in possesso di un wallet è possibile eseguire una prima transazione, da un wallet che già presenta un saldo attivo di bitcoin da trasferire, verso il wallet creato.

Quando s'inserisce la transazione, oltre alla quantità di bitcoin da trasferire, è necessario impostare anche

la quantità di bitcoin destinati alla *fee* (commissione) messa a disposizione, per chi poi scriverà la transazione nella blockchain.

È in questa fase che entra in gioco il *"Mining"*. Il Mining è il modulo utilizzato dal sistema bitcoin, e dalle criptovalute in generale che adottano la Proof of Work, per emettere nuova moneta.

Affinché la transazione venga convalidata, questa dovrà essere inserita in un blocco e il blocco per essere aggiunto alla blockchain, dovrà, a sua volta, essere "chiuso".

Per la chiusura del blocco è necessario calcolare un codice valido, chiamato *"hash"*, che è il risultato

dell'applicazione dell'algoritmo SHA-256[16] ai seguenti dati del blocco in questione:

1- Numero progressivo del blocco; Nonce[17];
2- Transazioni e/o dati scritti nel blocco;
3- Hash del blocco precedente.

L'algoritmo SHA-256 presenta due importanti caratteristiche che lo rendono adatto alla blockchain di Bitcoin: in primo luogo perché restituisce sempre, partendo da una stringa di lunghezza arbitraria, una stringa di lunghezza definita di 256 bit; in secondo luogo è una funzione irreversibile, pertanto non è possibile risalire alla stringa di

lunghezza arbitraria di partenza dal risultato ottenuto.

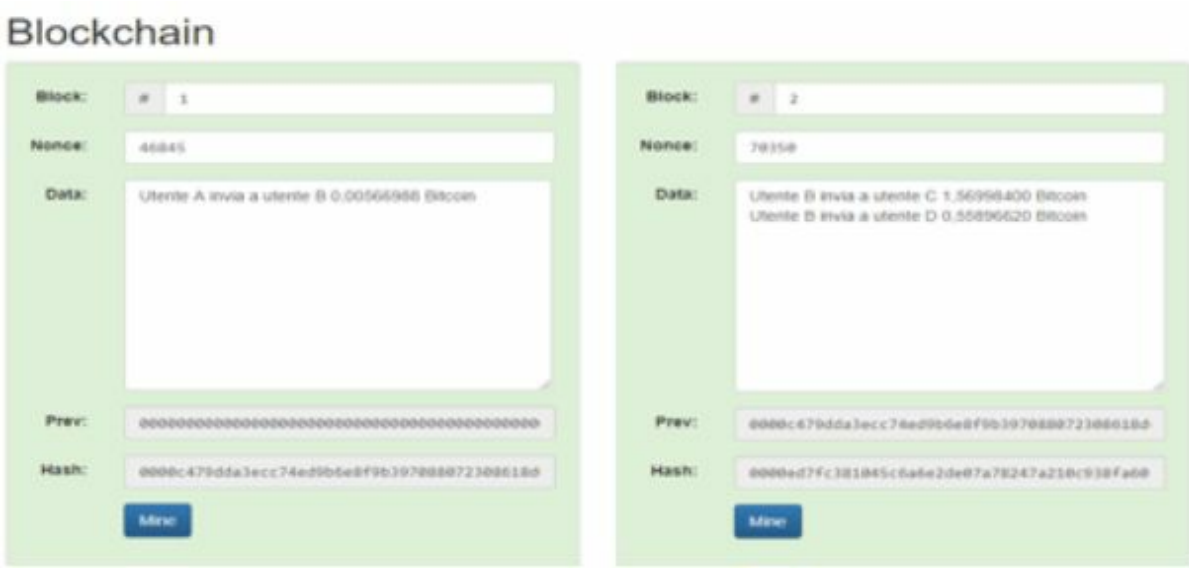


Fig.3

Nella figura 3 possiamo vedere un esempio di un pezzo di blockchain composta da 2 blocchi: blocco nr. 1 e blocco nr 2.

L'operazione di "chiusura" di un blocco con il calcolo dell'hash valido comprendente l'hash del blocco precedente, ciò sostanzialmente, impedisce qualsiasi possibilità di

modifica futura, perché, evidentemente, ogni variazione a un blocco qualsiasi, causerebbe l'invalidazione di tutti i blocchi a seguire.

Quanto sopra descritto, però non rende ancora sicura e immutabile la Blockchain perché gli Hash non corretti possono evidenziare la non validità del blocco, ma non possono impedire che ciò accada. Qual è allora il meccanismo che rende immutabile le transazioni di Bitcoin?

Come già detto la Blockchain è un *ledger* condiviso e custodito da una pluralità di nodi di una rete informatica *peer to peer* (P2P)[18] che si aggiorna automaticamente, questo significa che se una copia della Blockchain viene

contraffatta, molto semplicemente quella copia, non essendo valida, sarà "ignorata" da tutta la rete di Bitcoin.

Pertanto, affinché un tentativo di contraffazione vada in porto, è necessario che "il contraffattore" modifichi contemporaneamente il 50% + 1 delle copie della Blockchain di Bitcoin di tutta la rete informatica, quindi, in teoria, sarebbe possibile contraffare la blockchain, ma praticamente è irrealizzabile.

La parola *mining* deriva dal verbo *to mine,* in italiano minare-estrarre, nasce dall'assimilazione con i ricercatori di oro. I soggetti, economici e non, che si organizzano per calcolare e chiudere il blocco della blockchain sono infatti

chiamati *miners*.

Per procedere alla chiusura e alla validazione dei blocchi, i *miners*, devono assolvere in primo luogo alla funzione di controllo delle transazioni proposte, scartando quelle "ingannevoli" (sventando i tentativi di *double spending)*, che propongono trasferimento di fondi superiore al saldo presente nel *wallet* e successivamente, con l'imposizione del loro "sigillo", ovvero l'*hash* valido del blocco, garantiscono la sopravvivenza della rete.

In sostanza, dopo che ogni *miner* ha selezionato le transazioni (a discrezione del *miner* scegliere le transazioni da inserire nel proprio blocco, in base

anche alle *fees* messe a disposizione dal mittente), queste vengono controllate, organizzate nel blocco e ciò avvia una vera e propria gara tra tutti i *miners* della rete, per trovare il *nonce* e quindi sigillare il blocco con l'*hash* valido.

Quando un *miner* trova finalmente un *nonce* per validare il blocco, lo divulga immediatamente nella rete Bitcoin assieme al suo blocco, affinché tutti gli altri *miners* possano anch'essi calcolarne l'Hash per la verifica del *nonce*. Questa verifica è un'operazione svolta automaticamente dai *softwares* che ciascun miner utilizza per il mining, è importante sottolineare che non vi è alcun intervento umano.

A questo punto, appena il 50% + 1

dei *miners* avrà verificato la validità del *nonce* proposto, tutti gli ordini di pagamento presenti in quel blocco diventeranno transazioni "confermate" e il blocco appena chiuso verrà acquisito da tutti i nodi della rete ed aggiunto alla loro copia della Blockchain.

Il *nonce*, associato alle transazioni del blocco, è la cosiddetta *Proof of work (Pow)*, ovvero la prova del lavoro svolto dal *miner*. Ogni 10 minuti circa, si ripete questa corsa alla ricerca del *nonce*, e il vincitore si aggiudica la *reward* prevista.

Per trovare l'*hash*, i *miners* hanno bisogno di notevole capacità di calcolo chiamata appunto *hashing power*. I soggetti economici che si organizzano

con capitali e macchinari per fare *mining* sono incentivati dal ritorno economico che deriva dalla chiusura del blocco.

Il protocollo Bitcoin prevede che la chiusura di ogni blocco avvenga ogni 10 minuti circa, per regolamentare questa tempistica, il protocollo impone delle condizioni alla validità dell'hash e la misura di quanto sia difficile trovare l'hash corretto, viene chiamata: *difficulty*. Nel grafico riportato nella figura 4, possiamo riscontrare come sia aumentata in maniera esponenziale la *difficulty* per minare il Bitcoin, nell'ultimo biennio.

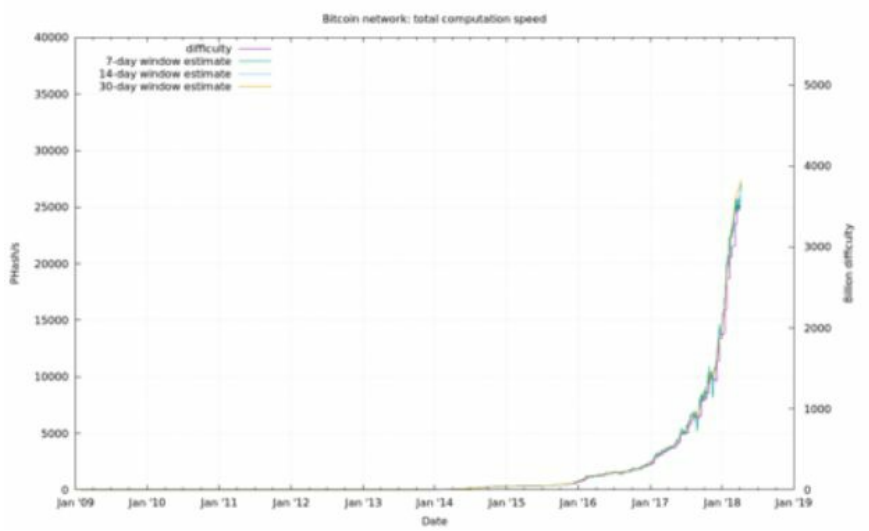


Fig. 4

Ad oggi il protocollo di Bitcoin prevede, per ogni blocco chiuso, una ricompensa di 12,5 Bitcoin nuovi di conio, più tutte le *f e e s* messe a disposizione dalle transazioni scelte ed inserite nel blocco, che saranno trasferite dai singoli *wallet* dei mittenti al *wallet* del *miner*. Tradotto in termini economici, al valore odierno di un Bitcoin, pari a circa $ 7.000,00, la sola ricompensa della *Proo-of-Work*

ammonta a circa $ 87.500,00, più tutte le commissioni previste nel blocco.

L'aumento del valore di Bitcoin che rende, pertanto, sempre più interessante l'attività di mining, ha determinato, come si vede dal precedente grafico (Figura nr. 4), l'aumento esponenziale della difficulty, consequenzialmente è aumentata la quantità di energia necessaria per alimentare gli hardware calcolatori. Per questo molti operatori economici nel campo del mining scelgono paesi come la Cina, l'Europa dell'Est, la Russia, Stati Uniti e Canada, per installare le cosiddette *mining farm*, dove l'energia costa poco e le temperature climatiche sono basse e favoriscono il raffreddamento dei

macchinari.

Alcuni team di sviluppatori hanno studiato metodi alternativi alla Proo-of-Work, e alcune criptovalute stanno già adottando sistemi quali la Proof-of-Stake o la Proof-of-interest che non richiedono lo svolgimento di "lavoro reale" ma i reward sono legati alla relazione con le criptovalute.

La Proof of Stake (Pos), (prova di possesso), dà più probabilità di ricevere i reward previsti dal protocollo, in relazione alla quantità di moneta posseduta. Il mining, quindi, si limita all'attività di controllo e conferma delle transazioni.

La *Proof of Interest* (Poi) (prova di interesse) oltre alla quantità posseduta,

prende in considerazione anche il numero di transazioni che il possessore esegue, quindi l'interesse mostrato verso l'utilizzo di quella criptovaluta.

Capitolo 3

IL CRIPTO CAPITALISMO – LE INITIAL COIN OFFERING I.C.O.

3.1 Gli smartcontracts e il criptocapitalismo

Assunto che la blockchain porta in sé tutta una serie di vantaggi in termini di sicurezza, trasparenza, decentralizzazione, gli *Smart contract* sono una naturale applicazione evolutiva di tale protocollo.

Al ricorrere di una condizione informaticamente verificabile, il sistema esegue automaticamente un'azione prestabilita *self-enforcement*[19]. Invero, già dal 1996 con l'introduzione dello standard *Electronic Data Interchange*[20], un protocollo standardizzato che consente lo scambio digitale automatico in ambito amministrativo, commerciale e logistico, sono stati introdotti dei contratti di

natura digitale. Per esempio, nel web advertising è possibile stipulare contratti il cui corrispettivo è legato al numero di visualizzazioni o al numero di click realizzati dagli utenti, il conteggio e il pagamento sono automatizzati dal software di gestione. Anche nel Booking on line e nell'e-commerce le fasi del contratto si svolgono completamente on line.

Tecnicamente, gli smart contract funzionano con il paradigma *"If - Then"* per cui è possibile inserire tutte le condizioni contrattuali previste, anche le ipotesi di risoluzione nel caso in cui non si verifichino le condizioni sospensive. È anche possibile inserire condizioni relative scadenze o eventi specifici tratti

da fonti pubbliche, sempre che questi siano informaticamente verificabili in maniera univoca.

Gli sviluppatori informatici cercano soluzioni tecniche per l'applicazione e l'utilizzo degli smart contract nella vita di tutti i giorni. A tale scopo lo *smart contract management* rappresenta un passo in avanti, proponendo forme di gestione dinamica finalizzate dalla modellazione dei contracts, alla singola fattispecie contrattuale. Lo sviluppo di queste tipologie di contratti si basa essenzialmente sulla sicurezza tecnologica della blockchain, sulla sua massima flessibilità e adattabilità, sulla trasparenza dei codici. Il campo di applicazione della contrattazione smart è

particolarmente ampio, a partire dai semplici pagamenti, sino all'esecuzione delle clausole penali, o alle clausole di tutela nei contratti dei consumatori.

Financhè il Consiglio Nazionale del Notariato Italia sta valutando e studiando la possibilità di adottare la blockchain per la registrazione dei trasferimenti immobiliari.

L'evoluzione prevista dagli smart contracts, con l'utilizzo della blockchain è un ambito giuridico che è ancora in maggior parte da definire, ma che *de jure condendo* si rivela particolarmente affascinante e promettente. Gli esperti di diritto studiano la *regulatory compliance* per una corretta coniugazione di questa evoluzione

tecnologica, con il rispetto degli ordinamenti giuridici e tutelando i diritti degli attori contrattuali.

Dal punto di vista giuridico, solleva non poche perplessità, la possibilità intrinseca della blockchain di operare utilizzando pseudonimi. Questa condizione di anonimato rende anche possibile la conclusione di contratti con contenuti illeciti. Proprio perché manca la possibilità sanzionatoria dei fatti illeciti.

Ad oggi, alcune tra le migliori piattaforme di blockchain per scrivere i propri smart contracts sono Ethereum e Dragonchain.

ETHEREUM

Ethereum è una piattaforma blockchain del Web 3.0 nata per la creazione e pubblicazione peer-to-peer di contratti intelligenti utilizzando principalmente come linguaggio di programmazione: Solidity

DRAGONCHAIN

Dragonchain è una piattaforma di blockchain di tipo commerciale che si rivolge soprattutto alle imprese. Nata in seno alla Disney corporation, consente di sviluppare, tra le altre funzionalità, anche gli smartcontracts con l'utilizzo di linguaggi di programmazione più comuni e diffusi come Java, Python, Node, C++.

3.2 Cosa sono le initial Coin Offering (ICO)

Una delle applicazioni più importanti degli Smart contract è stato l'utilizzo per l e *Initial Coin Offering* (ICO). Analogamente alle *Initial Public Offering* del mondo azionario, le ICO sono una forma di finanziamento utilizzata dalle start up, attraverso l'offerta di token della criptovaluta collegata alla *business idea,* in cambio di contributi volontari utili alla nascita e allo sviluppo del programma proposto.

Nello specifico smart-contract, sono indicate tutte le condizioni economiche, le tempistiche delle prestazioni e anche

la previsione di restituzione del contributo versato nel caso di non raggiungimento della soglia minima per l'avvio dell'investimento chiamato *soft-cap*. Il codice informatico con cui è scritto lo smart-contract è pubblico e chiunque può analizzarlo prima di decidere se contribuire.

Analizzare la bontà di una ICO non è cosa semplice. Molti piccoli investitori, allettati dalla possibilità di facili guadagni, hanno contribuito a progetti che non hanno mai visto la luce. Ad oggi, non esistono garanzie per gli investitori, l'investimento fatto potrebbe svanire nel nulla. Per queste ragioni il rischio d'investimento nelle ICO è veramente molto elevato, ma d'altro

canto, quando il progetto è solido e il team di lavoro riesce a portarlo alla luce e a realizzare quanto previsto, i risultati possono essere veramente interessanti. Prendiamo l'esempio di Ethereum: dopo una fase di sviluppo avviata dai fondatori Vitalik Buterin e Gavin Wood, nel 2014 fu lanciata la loro ICO, che offriva gli Ether (la coin minata della blockchain di Ethereum) in cambio di contributi per lo sviluppo del progetto. Raccolsero $ 18.400.000,00 circa e distribuirono circa ETH 60.100.000,00, l'investimento medio per ogni ETH fu pertanto di $ 0,30. A gennaio 2018 la quotazione di ETH giunse al suo massimo storico di $ 1.390,00 (il 463.233,00% di ROI in 4

anni). In questo caso, l'investimento in ICO diede ottimi risultati.

La strada giusta per investire in maniera sana nelle ICO è, sicuramente, approcciarsi a esse non prescindendo dall'approfondire: *money managment*, conoscenza tecnica, approfondimento dei progetti attraverso i cosiddetti *White Paper*; l'analisi dei *Bussines Model;* lo studio dei *Business Plan,* la *Road Map* del progetto e la conoscenza del *team,* compresi gli *Advisors* che propongono e supportano il progetto.

Il 2017, per le *Initial Coin Offering* è stato davvero importante soprattutto per la mole di capitali che sono stati captati, a livello internazionale.

Si stima che nel solo 2017 si siano

raccolti circa 1,25 miliardi di dollari.

Nel secondo semestre 2017, le prime quattro startup italiane in termini di somme raccolte grazie alle ICO (Eidoo, Aidcoin, Friendz, Xriba), hanno raggiunto complessivamente la cifra di 70 milioni di dollari, eguagliando quasi la cifra che nel 2017 è stata investita dai Venture Capitalist tramite i canali tradizionali (Angel Investor, Crowdfunding, ecc.). Anche nel 2018 sembra che il trend sia in linea con l'anno precedente.

Eidoo, che è riuscita a raccogliere circa 28 milioni di dollari, ha creato una piattaforma per la gestione dell'intera filiera delle criptovalute: ICO, commercio di beni e servizi,

trasferimento e gestione di diverse criptovalute simultaneamente.

Aidcoin, con 15.8 milioni di dollari raccolti, è una piattaforma dedicata al mercato delle donazioni, che traccia, utilizzando la blockchain, l'impiego dei fondi raccolti in favore di associazioni non profit.

Friendz ha raccolto 12 milioni di dollari. L'idea è quella di permette a chi usa i social media (Facebook, Instagram, Snapchat, ecc.) di essere pagato dai grandi brand, e consentire alle grandi aziende di promuovere, direttamente agli utenti, specifici i propri prodotti.

Xriba ha superato i 15 milioni di dollari raccolti da grandi investitori. Essa punta alla gestione della tesoreria e

alla trasparenza degli investimenti, con un sistema di "cambio" delle cripto valute in valuta fiat, consentendo, quindi, il corretto posizionamento contabile degli asset nei bilanci aziendali.

Analizzando questi dati e il trend positivo delle ICO, potremmo azzardare a coniare un neologismo economico: il "Crypto Capitalismo", che potrebbe incorporare e assorbire tutti i canali fino ad ora utilizzati per il finanziamento di startup (Angel Investor, Crowdfunding, Venture Capitalist).

Chiaramente, affiancando a questo strumento una regolamentazione che certifichi la liceità dei contenuti dei progetti proposti, il riconoscimento

degli utenti/investitori e quindi la tracciabilità delle fonti di finanziamento e le legittime garanzie contro eventuali truffe.

Facendo un salto nel passato e tornando agli anni ’90, sembra di rivivere quei momenti d’incertezze causati dall’avvento di Internet e dalla cosiddetta *New Economy,* l’economia della nuova tecnologia, contro la *Old Ecomony,* legata ai tradizionali canali industriali manifatturieri. Quel periodo vide la nascita di grandi aziende come Google, Amazon, Ebay che ancor oggi esistono e che sono diventati i più grandi players internazionali dei rispettivi mercati, ma allo stesso tempo molte aziende dopo una grande crescita

dovuta all'euforia dei mercati, svanirono, assorbite dalle bolle speculative, la cosiddetta bolla del Dot.com.

3.3 La Regolamentazione e i risvolti monetari economico-politici

Il ricorso all'utilizzo delle ICO per finanziare le nuove imprese, come abbiamo visto nel 2017, ha registrato un utilizzo imponente, tanto da entrare tra i punti importanti da osservare nelle agende istituzionali di tutto il mondo.

Gli Stati Uniti d'America sono stati i primi a muoversi in tal senso. Il 25 luglio 2017 si registra il primo provvedimento della U.S. Security and Exchange Commission, il Report di investigazione n. 81207[21] relativo alle ICO e ad uno specifico caso: **The DAO**.

The DAO era una "*Decentralized*

Autonomous Organization", ossia un'organizzazione decentralizzata, creata su Blockchain Ethereum (tramite una serie di smart contracts correlati) con lo scopo di fornire un nuovo modello di business decentralizzato per il coordinamento d'imprese, sia commerciali che no-profit. La fase di finanziamento del progetto seguì tutti i passaggi delle ICO e furono raccolti circa 150 milioni di dollari. Nel giugno del 2016 emerse un *bug* nel codice del progetto e furono *hackerati* dal wallet che deteneva gli Ether raccolti, un quantitativo di Ether pari al valore di circa 70 milioni di dollari. A seguito di questo episodio la Security and Exchange Commission avviò

un'ispezione per verificare se le ICO e, nel caso specifico, la DAO avessero violato le leggi federali sui titoli. Il risultato di questa operazione fu divulgato con il Report d'investigazione n. 81207 del 25 luglio 2017.

Il primo passo della SEC fu quello di classificare la tipologia d'investimento proposto con l'ICO e verificare, quindi, la riconducibilità nell'ambito di applicazione della *Securities Law*[22]. A tal scopo la Sec fece riferimento al cosiddetto test Howey[23] che analizza nella sostanza, più che nella forma, il contratto di investimento proposto, e se quest'investimento in denaro, offre la ragionevole aspettativa di profitti derivanti da sforzi manageriali o

imprenditoriali di terzi.

Nel caso di specie la SEC ritenne che tutte le condizioni richieste dal "test" erano rispettate pertanto attribuì ai Token DAO la natura di strumenti finanziari e quindi sottoposti alla Seurities Law.

A seguito di questa vicenda Jay Clayton, chairman della SEC, pubblicò, il 12 novembre 2017, un *"Public Statement"*[24] che richiama all'attenzione dell'investitore tutti i documenti e gli avvertimenti per gli investimenti nel mondo della criptovalute già precedentemente pubblicati, confermando quanto emerso dal precedente report di luglio e aggiungendo una serie di avvertimenti

consigliando, alla fine del documento, di porsi "*Sample Questions for Investors Considering a Cryptocurrency or ICO Investment Opportunity*".[25].

Il Report n. 81207, pur non essendo una vera e propria regolamentazione, influenzò però la platea internazionale tanto che, da lì a poco, vennero pubblicati dalle varie autorità di controllo dei singoli paesi una serie di provvedimenti che avvertivano gli investitori, in criptovalute e ICO, delle azioni che ogni paese stava ponendo in essere in questo ambito di investimento.

Il 4 settembre 2017 la People's Bank of China[26] annunciò il divieto di Initial Coin Offering e sospese le attività di scambio di criptovalute sugli exchange.

Analogamente alla Cina, anche la Corea del Sud il 29 settembre 2017[27], annunciò uno stop alle ICO e alle criptovalute. Altri paesi, a seguire, divulgarono dei propri provvedimenti sulla scia delle indicazioni della SEC: il 24 agosto 2017 il Canadian Securities Administrators[28], il 28 settembre 2017 la Australian Securities ed Investment Commission [29]; il 5 settembre 2017 la Securities and future Commission di Hong Kong[30]; il 15 novembre 2017 la Banca Centrale di Singapore[31].

Altri organi di controllo, invece, come l'Autorità di Supervisione Finanziaria Svizzera[32], la Financial Service Agency del Giappone[33], e la Financial Conduct Authority del Regno

Unito[34] emisero provvedimenti ricordando ai soggetti promotori di applicare le leggi nazionali di regolamentazione dei valori mobiliari, a seconda della tipologia d'investimento proposto relativo al token di futura emissione.

Anche l'European Securities and Markets Authority (ESMA) il 13 novembre 2017[35] pubblicò parallelamente due comunicati, uno per gli investitori e uno per i soggetti promotori di ICO.

Alcuni paesi hanno annunciato la volontà di avviare la creazione della propria "criptovaluta" nazionale, come l'Estonia o la Russia con il "criptorublo". Più recentemente, a

febbraio 2018 il presidente del Venezuela, Nicolas Maduro ha avviato il Petro, la prima criptovaluta nazionale garantita dal petrolio, per aggirare le sanzioni imposte dagli Stati Uniti.

L'ESMA ha inserito la regolamentazione delle ICO nel supervisory convergence work programme,[36] all'interno delle financial innovation. Si procederà con l'analisi del mercato delle ICO per valutare in quali ipotesi sarà necessaria una regolamentazione del fenomeno[37].

Lo scorso dicembre, la Financial Condut Authority è tornata sul tema delle ICO con la pubblicazione del Feedback Statement in materia di Distributed Ledger Technology[38]. In particolare, la

FCA ha ribadito la natura speculativa dello strumento e la necessità di un'analisi caso per caso per individuarne la disciplina applicabile, programmando la raccolta di ulteriori informazioni ai fini di una valutazione sulla necessità o meno di una regolamentazione specifica.

Di recente, la Swiss Financial Market Regulatory Authority (FINMA) ha pubblicato delle linee guida relative alle richieste di chiarimenti in materia di ICO[39]. Il documento, non solo, indica agli utenti le modalità per formulare quesiti all'autorità, ma chiarisce anche i principi che la FINMA stessa applicherà nel rispondere a tali domande. In particolare, il documento fornisce una

panoramica delle categorie di token e un'indicazione delle caratteristiche al ricorrere delle quali i token sono classificabili quali titoli.

Alla luce dei provvedimenti emessi e del solco giuridico tracciato dalle autorità nazionali appare evidente che la normativa tenderà, in primo luogo a creare delle "classi" di Token emettibili con le ICO ed in questa fase se ne possono già identificare almeno quattro tipologie:

1. *payment token*, lo strumento non conferisce diritti verso controparti, ma nasce come esclusivo utilizzato di moneta digitale, destinato allo scambio;

2. *asset token*, questa tipologia di strumento conferisce un diritto verso il

soggetto emittente o verso terzi[40];

3. *utility token*, rientrano in questa tipologia gli strumenti che assegnano l'accesso a prodotti o servizi distribuiti tramite applicazioni digitali, ma che rappresentano al contempo una proprietà.

4. *security token,* in questo caso si parla di veri e propri investimenti di tipo finanziario (vedi il caso DAO prima esposto).

Appare evidente che sarà necessario analizzare ogni tipologia di token proposti ad ogni ICO per comprendere al meglio come classificare le ICO o le STO (Security Token Offer) in base allo strumento proposto e quindi a quale "classe" di strumento finanziario fare

riferimento, se non addirittura valutare la creazione di nuovi Cripto strumenti finanziari dedicati.

Durante l'incontro del G20[41] svoltosi in Argentina nel 2018, sono arrivati dei segnali d'attenzione all'evoluzione finanziaria legata alle criptovalute in senso generale.

L'approccio seguito è stato quello di assimilare il fenomeno delle criptovalute a degli asset, più che a delle valute vere e proprie. L'argomento all'ordine del giorno è stato infatti sui "*crypto-assets*", e alla fine è emerso un sostanziale atteggiamento positivo di tipo attendista, aprendo le porte a una discussione sulla regolamentazione condivisa, rimandando al 2019 eventuali

azioni. Quanto emerso dal G20 ha fugato, almeno per il momento, le preoccupazioni e i timori di molti, che si avviassero azioni di contrasto e chiusura sull'argomento.

In conclusione, si può affermare che fino ad oggi le autorità di vigilanza, pur allertando i potenziali investitori dei rischi in materia di ICO o STO, hanno privilegiato un atteggiamento di osservazione del fenomeno – anche in virtù della sua ampiezza, nonché dell'impossibilità di ricondurlo sotto un unico insieme – rimandando la regolazione a un momento successivo all'analisi.

Capitolo 4

CONCLUSIONI

Durante la scrittura di questo documento mi è tornato più volte in mente J. A. Schumpeter con le sue teorie

economiche “dinamiche” focalizzate sull’innovazione e sulla figura dell’Imprenditore, che per far crescere il proprio business, la propria impresa, è chiamato a essere in continua evoluzione e l’Innovatore nel mercato in cui opera.

Il misterioso Satoshi Nakamoto, lo associo a quell'Imprenditore di cui parla Schumpeter, con una grande visione, portatore d’innovazione e cambiamento, a cui tutti noi ci stiamo, piano piano, avvicinando.

Questa volta, l'idea rivoluzionaria e innovativa non si limita a essere destinata a un mercato specifico, a un’innovazione di processo o di prodotto o soltanto all’applicazione di

una *business idea*.

Questa tecnologia, la blockchain, è un fenomeno che ha una dimensione molto più profonda che coinvolge, non solo gli aspetti economici e finanziari, ma arriva a toccare aspetti socio-culturali.

La "cripto-rivoluzione" basata sulla blockchain, nasce da un'ideologia, dal desiderio e dalla voglia di restituire a ciascuno la titolarità dei diritti sui propri valori (beni, denaro ecc…) trasferibili, grazie a questa tecnologia, senza intermediazione alcuna, in trasparenza e sicurezza.

Si potrebbe cadere nell'errore di pensare che questa rivoluzione sia contro *l'Establishment* finanziaria,

contro i cosiddetti “Poteri forti”, ma credo invece che l’approccio corretto per valutare questo cambiamento sia quello di guardarlo con mente aperta. La crisi finanziaria del 2008 ci ha mostrato una condizione globale nella quale un numero esiguo di persone ha deciso per moltissimi, e non ha dato possibilità di scelta a molti ignari investitori, facendo pagare però a tutto il mondo, le conseguenze catastrofiche che ciò ha causato. Questa crisi, che coincide fatalmente con l'inizio della diffusione della blockchain e delle cripto valute, non si è limitata alla mera perdita di capitali, ma come abbiamo avuto modo di vedere prima, è arrivata a compromettere un intero sistema

"fiduciario".

Schumpeter parlava di "distruzione creatrice", che può essere accolta, osservata e utilizzata per ripartire e ricominciare la ricerca dei nuovi equilibri. Probabilmente, chi saprà cogliere gli aspetti positivi apportati dall'innovazione ne potrà anche trarre tanti benefici, chi invece si opporrà ottusamente, senza il dovuto approccio critico, probabilmente sarò travolto dalla naturale evoluzione e dovrà poi, obtorto collo, adeguarsi necessariamente alla nuova realtà.

Il futuro dipenderà dalle nostre scelte e, personalmente, mi auguro possa vederci in grado di cogliere quest'opportunità.

Mi sono chiesto: come applicare concretamente questa potenziale libertà di scelta? Guardando alle necessità degli italiani, la prima cosa che mi è venuta in mente è stata la possibilità di invertire il paradigma dell'imposizione fiscale.

Ad oggi, noi siamo costituzionalmente e giustamente chiamati a concorrere alla spesa pubblica in ragione della capacità contributiva di ciascuno.

Nell'attuale sistema, però, il singolo cittadino partecipa solo in maniera indiretta e "rappresentativa", cioè, ancora una volta, attraverso un intermediario, all'impiego delle somme raccolte, soprattutto a livello locale.

Ho visto nella blockchain una valida alternativa. Poniamo il caso in cui nella scuola dei tuoi figli i riscaldamenti siano guasti.

Ipotizziamo che il Comune, deputato ad eseguire i lavori di riparazione del guasto non abbia i soldi per risolvere il problema. Come fare?

Immaginiamo ora che, dopo le dovute pratiche amministrative la scuola o chi per lei, ottenga il solo nulla osta a eseguire i lavori, ma non i fondi per realizzarli. Dove e come recuperare i soldi? Qui entrerebbe in gioco la blockchain, attraverso una "donazione" dei cittadini contribuenti che desiderano ripristinare i riscaldamenti. In cambio, cittadini contribuenti che deciderebbero

di contribuire, riceverebbero dei "*payment stable token*" che potrebbero essere utilizzati per il pagamento delle imposte locali e/o nazionali o essere utilizzati per pagamenti presso negozi che, a loro volta, potrebbero utilizzare per il pagamento delle imposte locali e/o nazionali.

Evidentemente, tutto ciò potrebbe avvenire esclusivamente utilizzando le caratteristiche di trasparenza, sicurezza, immutabilità e decentralizzazione della blockchain, servendosi di uno specifico smartcontract, studiato ad hoc, che destinerebbe i fondi in quel progetto specifico e che regolamenterebbe tutti gli aspetti giuridici e le eventuali eccezioni o clausole.

Così facendo saremmo riusciti ad invertire il paradigma dell'imposizione fiscale: il cittadino-contribuente sceglierebbe di concorrere direttamente alla spesa pubblica, destinando il suo contributo a quel determinato progetto che egli ritiene più caro, di conseguenza avrebbe già pagato le imposte per la misura della "donazione" erogata a quel progetto.

In questo modo si otterrebbero, almeno, due grandi risultati. Primo: si restituirebbe al cittadino contribuente la capacità e la possibilità di esprimere direttamente la sua "Sovranità" sulla spesa pubblica. Secondo: il cittadino-contribuente avrebbe un riscontro diretto con ciò per cui ha pagato, ovvero la

spesa pubblica. Le imposte dovute non sarebbero percepite come soldi destinati a fondi per nutrire le casse comunali, ma come beneficio diretto alle proprie esigenze, per cui, nel nuovo ordine d'idee, e tornando al nostro esempio, se non pagherà le tasse, egli lascerà i propri figli al freddo, non avrà soltanto evaso il fisco.

Facendo leva sulla libertà/responsabilità si otterrebbe senz'altro una notevole diminuzione dell'evasione fiscale.

Questo esempio vuole far luce, solo, su uno dei tantissimi vantaggi che si potrebbero ottenere con l'applicazione intelligente della blockchain nella vita quotidiana.

Note

[1] Vocabolario Treccani: http://www.treccani.it/vocabolario/pecu

[2] Da "SAPERE" – Ulrico Hoepli Editore Anno III – Volume VI – n. 69 15 novembre 1937 – XVI LA MONETA DI PIETRA DELL'ISOLA DI YAP di Willard Price

[3] Da Wikiit.wikipedia.org/wiki/Rai_(moneta)

[4] Cit. David CHAUM, "Blind signatures for untraceable payments", in Advances in cryptology, Springer, 1983,

pp. 199-203.

[5] https://www.activism.net/cypherpunk/r

[6] http://satoshinakamoto.me/2009/01/09/bi v0-1-released/

[7] Cit. Satoshi NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, in https://bitcoin.org/bitcoin.pdf

[8] Cit. Nick Szabo https://en.wikipedia.org/wiki/Nick_Szab

[9] In realtà Hanyecz mise un annuncio su internet offrendo 10.000 bitcoin a chi gli avesse recapitato 2 pizze large al suo domicilio. Rispose una persona inglese

che andò a comprare le pizze e gliele recapitò.
[10]

Reward Halving consiste nel dimezzamento della ricompensa riservata ai miners per la chiusura di un blocco. Dalla nascita del Bitcoin ad oggi sono avvenuti 2 Reward Halving, che hanno dimezzato la ricompensa da 50 Bitcoin a 25 la prima volta il 28 novembre 2012 e da 25 Bitcoin a 12,5 il 9 luglio 2016 la seconda volta.

[11] http://www.tecnologiaecomunicazione-il-bitcoin/

[12] Fonte: https://coinmarketcap.com/ dell'8 aprile 2018

[13] Total Supply: è il saldo totale di monete esistenti in un determinate momento (meno tutte le monete verificatamente bruciate).

[14] Il coin è la moneta digitale di riferimento di una piattaforma blockchain. Ether per Ethereum, bitcoin per Bitcoin. Il token è invece un altro asset che si appoggia su una blockchain esistente che non hanno una propria blockchain e non possono quindi essere definiti "coin".

[15] Cit. David Andolfatto Vice President Federal Reserve Bank of St. Louis nel “Dialogue with the FED BeyondToday’s Financial Headlinedel 31/04/2014

[16] Con il termine SHA si indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA. La sigla SHA sta per Secure Hash Algorithm. SHA-256 produce un digest di 256 bit

[17] In crittografia il termine Nonce indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. Nonce deriva infatti dall'espressione inglese for the nonce, che significa appunto "per l'occasione".

[18] Si stima che la rete Bitcoin vanti la presenza di circa 50.000 nodi: oltre 10.000 sono presidiati dai miners e circa 40.000 si stimano essere presidiati da privati, chiunque con un PC collegato ad internet può custodire una copia sempre aggiornata della Blockchain e quindi essere un nodo della rete. Inoltre chiunque, scaricando il software apposito, può minare i bitcoin.

[19] Wei Dai, B-Money, 1998: "5. The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence

in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly." http://www.weidai.com/bmoney.txt

[20] Vedi: http://www.nist.gov/ e http://www.unece.org/info/ece-homepage.html

[21] Con il Report of Investigation n. 81207 del 25 luglio 2017, la U.S. Security and Exchange Commission ha statuito che la disciplina federale in materia di valori mobiliari è applicabile a offerte, vendite e scambi di diritti in "organizzazioni virtuali" (cfr. U.S. SEC press release

https://www.sec.gov/news/press-release/2017-131).

[22] L'apparato legislativo statunitense che regolamenta i valori mobiliari

[23] decisione della Corte Suprema statunitense del 1946 (caso SEC v. W. J. Howey Co)

[24] https://www.sec.gov/news/public statement/statement-clayton-2017-12-11

[25] Statement on Potentially Unlawful Promotion of Initial Coin Offerings and Other Investments by Celebrities and Others (Nov. 1, 2017), available at https://www.sec.gov/news/public-

statement/statement-potentially-unlawful-promotion-icos; Investor Alert: Public Companies Making ICO-Related Claims (Aug. 28, 2017), available at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_icorelatedclaims; Investor Bulletin: Initial Coin Offerings (July 25, 2017), available at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings; Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 7, 2014), available at https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-bitcoin-other-virtual-currency; Investor Alert: Ponzi

Schemes Using Virtual Currencies (July/23/2013),available at https://www.sec.gov/investor/alerts/ia_v

[26]
http://www.cbrc.gov.cn/chinese/newInde

[27]
http://www.fsc.go.kr/info/ntc_news_viev
[28]
http://www.osc.gov.on.ca/documents/en/Category4/csa_20170824_cryptocurrenc offerings.pdf

[29] https://www.asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#shares

[30] http://www.sfc.hk/web/EN/news-

and-announcements/policy-statements-and-announcements/statement-on-initial-coin-offerings.html

[31] http://www.mas.gov.sg/~/media/MAS

[32] https://www.finma.ch/en/documentatic guidance/#Order=4

[33] https://www.fsa.go.jp/policy/virtual_c

[34] https://www.fca.org.uk/news/statemen coin-offerings

[35] https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms

[36] ESMA, 2018 supervisory

convergence Work programme,7-febbraio-2018 (cfr. https://www.esma.europa.eu/sites/default/files/library/esma42-114-540_2018_supervisory_convergence_wo

[37] Da ultimo, il 12 febbraio 2018 le tre autorità di vigilanza europee (ESMA, EBA ed EIOPA) hanno emesso un comunicato collettivo in merito ai rischi correlati all'acquisto di valute virtuali. Le tre autorità hanno rimarcato come gli acquirenti ed i possessori di valute virtuali non siano tutelati perché tali prodotti non sono regolamentati al livello europeo (cfr. https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-

risks-in-buying-virtual-currencies).

[38] Financial Conduct Authority, Distributed Ledger Technology Feedback Statement on Discussion Paper 17/03, December 2017 (cfr. https://www.fca.org.uk/publication/feedb 04.pdf).

[39] FINMA, ICO Guidelines, 16 febbraio 2018 (cfr. https://www.finma.ch/en/news/2018/02/2 mm-ico-wegleitung/).

[40] Si tratta di diritti di varia natura: 1) diritti al pagamento, con l'assimilazione a valori mobiliari, strumenti finanziari e strumenti partecipativi al capitale di

rischio; 2) diritto al ricevimento di una prestazione di servizi o di un bene.

[41] Il G20 o Il Gruppo dei 20 è un forum dei ministri delle finanze e dei governatori delle banche centrali, creato nel 1999, e rappresenta i due terzi del commercio e della popolazione mondiale, oltre all'80% del PIL mondiale.