

Dipartimento di Economia e Finanza

**CATTEDRA DI DIRITTO DEI MERCATI E DEGLI
INTERMEDIARI FINANZIARI CORSO PROGREDITO (c.p.)**

TESI DI LAUREA MAGISTRALE

**Andamento e sviluppo delle criptovalute nei
mercati finanziari**

RELATORE

Prof. Mirella Pellegrini

CANDIDATO

Francesco Esposito

Matricola 682861

CORRELATORE

Prof. Paola Lucantoni

Anno accademico 2017/2018

INTRODUZIONE

Negli ultimi anni l'economia mondiale, specialmente grazie all'evoluzione tecnologica ed informatica, ha visto sempre maggiori cambiamenti, ma soprattutto numerosi strumenti che sono andati ad aggiungersi al già molto complesso mondo finanziario.

Un' importantissima novità da poter prendere in considerazione riguarda una rivoluzione dei generali sistemi di pagamento: l'utilizzo delle "criptovalute".

La nascita di queste valute digitali è da collocarsi ufficialmente all'anno 2009, quando un ragazzo di cui, ad oggi, è conosciuto solo lo pseudonimo, *Satoshi Nakamoto*, presenta per la prima volta la criptovaluta più famosa ma soprattutto più importante per capitalizzazione e non solo, il *Bitcoin*.

Il motivo principale della creazione del cosiddetto "oro digitale" è da ricondursi al desiderio di *Nakamoto* di creare uno strumento di pagamento che si discostasse da un sistema che si era rivelato fallimentare; infatti, la pubblicazione del *white paper* che introduceva il *Bitcoin* avvenne solo poche settimane dopo il crollo della quarta banca d'investimento più grossa degli Stati Uniti, la *Lehman Brothers*.

Da allora in avanti le valute virtuali si sono ritagliate via via sempre maggiore spazio tra gli strumenti finanziari, catturando sempre maggiore interesse da parte degli investitori e delle istituzioni, sia per le funzioni che le stesse svolgono, sia per la portata rivoluzionaria in ambito socio-economico.

L'elaborato mira ad analizzare in maniera dettagliata le caratteristiche e gli eventi più importanti del *Bitcoin* ed in generale dell'intero sistema di criptomonete, mediante uno studio descrittivo ed analitico, suddividendo lo scritto in 3 capitoli principali.

Nel primo capitolo si valuteranno le cause e gli eventi che hanno portato alla creazione del *Bitcoin* e quindi delle "*Altcoins*", si studieranno le loro caratteristiche principali, facendo inoltre una breve panoramica sull'impatto sociale, politico ed economico delle stesse.

Nei successivi 2 capitoli ci si soffermerà sui numerosi punti di forza e di debolezza delle valute digitali che da anni ormai dividono la critica della dottrina economica, considerando i fattori principali della fortissima instabilità finanziaria, che da anni causa frequenti ed intensi rialzi e ribassi delle *criptocurrencies*, generando non poco scetticismo e diffidenza da parte degli investitori.

Si valuterà inoltre l'andamento delle più importanti criptovalute insieme al *Bitcoin* negli ultimi anni, con uno sguardo rivolto ai fenomeni economici che hanno accompagnato le stesse; da tali analisi, ne verrà fuori una correlazione molto accentuata tra il *Btc* e le *altcoins*, che verrà mostrata in maniera analitica.

Per concludere, si faranno delle brevi osservazioni sull'impatto che l'incertezza della politica economica può avere sull'andamento del Bitcoin e se quest'ultimo, in determinate situazioni che saranno riportate, possa essere utilizzato anche come uno strumento di copertura.

Indice

Capitolo 1 - Introduzione alle criptomonete	1
1.1 Cosa si intende per criptovaluta?.....	1
1.2 Le origini	2
1.2.1 Chi è <i>mister Bitcoin</i> ?	5
1.2.2 (Segue) <i>La Blockchain</i>	5
1.2.3 Considerazioni sulla <i>Blockchain</i> e possibili futuri utilizzi	9
1.2.4 Cosa sono le <i>ICO</i>	11
1.2.5 <i>Mining</i>	13
1.3 Valutazione dell’impatto sociale, politico ed economico.....	14
1.4 Altre principali criptovalute.....	17
1.4.1 (Segue) <i>ETHEREUM</i>	19
1.4.2 (Segue) <i>RIPPLE</i>	21
1.4.3 (Segue) <i>LITECOIN</i> : argento digitale	22
1.4.4 (Segue) <i>BITCOIN CASH (BCH)</i>	24
1.4.5 (Segue) <i>Altcoins</i> minori	25
Capitolo 2 - Riflessioni e andamento nei mercati	28
2.1 Principali punti di debolezza e critiche del <i>Bitcoin</i> e delle altre <i>Cryptocurrencies</i>	28
2.1.1 (Segue) Eccesso di volatilità.....	29
2.1.2 (Segue) Possibilità di usi illeciti	30
2.1.3 (Segue) Non è altro che una bolla speculativa!	33
2.1.4 (Segue) L’emissione di <i>Bitcoin</i>	37
2.1.5 (Segue) Assenza di tutele legali e contrattuali	39
2.1.6 (Segue) Rischio informatico	41
2.1.7 (Segue) Incertezza sul trattamento fiscale	45
2.1.8 (Segue) Altre considerazioni	46
2.2 Principali punti di forza	47
2.2.1 (Segue) Decentralizzazione	47
2.2.2 (Segue) Contenimento dell’inflazione	49
2.2.3 (Segue) Riduzione delle spese di transazione	51
2.2.4 (Segue) Trasparenza e Anonimato.....	53
2.3 Una breve analisi sulle criptovalute.....	54
2.3.1 La performance del <i>Btc</i>	55
2.3.2 Principali cause della bolla	62

2.3.3 Principali cause del <i>Bust</i>	64
2.3.4 Andamento delle <i>Altcoins</i> nel 2018.....	66
Capitolo 3 - Ultime analisi	68
3.1 <i>Performance</i> delle principali <i>altcoins</i> nel 2018.....	68
3.2 Correlazione tra <i>Bitcoin</i> e le principali <i>Altcoins</i>	76
3.3 Volatilità delle criptovalute	79
3.3.1 Un nuovo strumento: le <i>Stablecoins</i>	79
3.3.2 Studio della volatilità.....	81
3.3.3 Modelli <i>ARCH</i> e <i>GARCH</i>	84
3.3.4 Risultati dello studio.....	86
Conclusioni	87
Bibliografia	89
Sitografia	90

Capitolo 1 - Introduzione alle criptomonete

1.1 Cosa si intende per criptovaluta?

“Le criptovalute sono uno strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta.” (Treccani,2018)

Questa è una semplice definizione che viene data dal vocabolario italiano Treccani al concetto che andrò ad analizzare, quello delle criptovalute, ovvero delle valute digitali; paradossalmente, nonostante il rilevante impatto che queste ultime hanno avuto nella sfera economica e non solo, non vi è ancora una definizione ufficiale al momento, anche se è probabilmente soltanto questione di tempo, dato che, dopo diversi anni, si sta attribuendo finalmente una forma giuridica adeguata al fenomeno, come si vedrà in seguito.

Volendo utilizzare un’idea meno “formale”, si possono considerare come uno strumento di scambio paragonabile alle classiche monete quali Euro, Dollaro, Sterlina etc, ma che sono state programmate con l’intento principale di scambiare informazioni digitali attraverso un processo basato sulla Crittografia.¹

La finalità della Crittografia risiede nel fatto che solo i destinatari delle informazioni siano in grado di leggere le stesse, evitando dunque che terzi soggetti riescano ad accedervi; questa si basa su determinati algoritmi spesso molto complessi e controlla l’ingresso delle varie criptovalute nel sistema attraverso un processo definito “*mining*”, di cui si parlerà in seguito.

Ai giorni d’oggi c’è sempre meno disinformazione a riguardo, in virtù della loro rilevanza all’interno dei mercati, della crescita economica di questo mondo digitale e dei numerosi eventi che, nel tempo, hanno riguardato *Bitcoin* e le altre criptovalute; eppure, non tutti sono a conoscenza delle numerose sfaccettature che contraddistinguono le più importanti *criptocurrencies*, la loro capitalizzazione di mercato e le differenti tecnologie che sono alla base delle stesse

¹ Cfr. “Che cosa sono le criptovalute”, www.mercati24.it , 29 Gennaio 2019

La più importante delle *criptocurrencies* è sicuramente il *Bitcoin*, valuta digitale che è salita alla ribalta ma che stenta fortemente ad affermarsi come un reale mezzo di pagamento.²

1.2 Le origini

Figura 1: Fonte *Bitcoin.org*, *white paper* di *Satoshi Nakamoto*

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As

Un primo esordio del concetto di criptovaluta affonda le proprie radici nel ben remoto 1982, con la pubblicazione di un articolo di *David Chaum*,³ intitolato “*Blind Signature for Untraceable Payments*”, nel quale veniva introdotto un nuovo concetto, il concetto di “firme cieche”, ovvero le “*blind signatures*”, una sorta di firma digitale che viene apposta sul messaggio prima che quest’ultimo venga aperto e letto.

Il medesimo autore sottolineava le implicazioni pratiche di questo progetto nel settore dei pagamenti, che possono esprimersi senza la necessità di un controllo delle autorità e con l’adozione di forme anonime attraverso l’impiego di pseudonimi.

² Cfr. GENNAI A., “Cosa sono e come funzionano le criptovalute”, *Il Sole 24 ore*, 1 Ottobre 2018

³ *David Chaum* è un crittografo, fondatore della *DigiCash Inc* nel 1989 e famoso per aver sviluppato *l’e-cash* negli inizi degli anni ‘90, un’applicazione *web cash* con lo scopo di preservare l’anonimato dell’utente che ne fa uso, cosa che sarà ripresa qualche anno più tardi da *Satoshi Nakamoto* nella presentazione della sua criptovaluta.

Qualche anno più tardi, precisamente nel 1988, *David Chaum* pubblicava un *paper* intitolato “*The Dining cryptographers problem: unconditional sender and recipient untraceability*”, nel quale per la prima volta si parlava dei concetti di “chiave pubblica” e “chiave privata”.

Sebbene il progetto di *Chaum* non ebbe una vera e propria realizzazione pratica, catturò comunque gli interessi del movimento *Cyberpunk*, un gruppo di attivisti che vedevano nelle tecnologie informatiche e nella *cibernetica* strumenti utili per il cambiamento radicale nella società, che nel 1994 lo inserirono nel manifesto dei Cripto – Anarchici.

In buona sostanza, gli anarchici del manifesto individuaronò nel sistema di crittografia e cifratura ideato da *Chaum*, uno strumento che potenzialmente poteva rivelarsi utile alla loro lotta al potere sovrano.

Basandosi sulle idee di *Chaum*, *Wei Dai*, un esponente del gruppo *cyberpunk*, giunse ad una concreta idea di criptovaluta, e proponeva un sistema di interscambio di valore e stipulazione di contratti, che si basavano sull’uso di una moneta digitale che garantiva l’anonimato; la moneta in questione è denominata “*b-money*”.

Wei Dai proponeva due protocolli nel suo trattato di presentazione di questo sistema di pagamento anonimo e distribuito.

Nel primo protocollo veniva presentato l’utilizzo di un *proof of work*, inteso come strumento per creare moneta online.

Wei Dai riconosceva la presenza di un eventuale contratto con un ente terzo, con il fine di prevenire perdite.

Nel secondo protocollo spiegava come i partecipanti della rete potevano verificare che il proprio importo non fosse stato soggetto a inflazione.

Definiva inoltre le linee di partecipazione alla rete affermando che una somma di denaro era un requisito fondamentale per diventare *server* della rete, ma poteva essere perso se il *server* stesso si rivelava “disonesto”.

Tuttavia, anche se furono notevoli i progressi dell’*Information Technology*, il meccanismo teorizzato faceva attrito con l’impossibilità di una sua implementazione pratica funzionale.

Il problema riguardava infatti il fenomeno della *double spending*, ovvero il processo che consentiva di duplicare lo stesso gettone e spenderlo più volte.⁴

Dunque, per la nascita ufficiale delle Criptovalute bisogna attendere fino all’anno 2008, precisamente il 18 agosto, con la registrazione di *bitcoin.org* su “*anonymousspeech.com*” e , nell’ottobre dello stesso anno, vi fu la pubblicazione *online* di un *white paper* che trattava l’argomento, considerando

⁴ Cfr. AYOUBI M. , “Dalle radici di *Bitcoin* alla sua nascita”, www.StayUpgrated.it, 16 Gennaio 2018

anche la già citata crittografia; tale documento, denominato “*Bitcoin A peer- to-peer electronic cash system*”, conteneva tutti i dettagli tecnici della criptovaluta che, ad oggi, è ritenuta la più importante (e non solo per capitalizzazione), ma, soprattutto, proponeva per la prima volta l’idea di non tracciare la moneta, bensì le transazioni.

In questo modo, con la tracciabilità delle transazioni, viene posto un freno al fenomeno della “*double spending*”,⁵ garantendo maggiore fiducia al sistema in quanto, impedendo la “doppia spesa”, ovvero che gli stessi *Bitcoin* venissero utilizzati per transazioni differenti, non è possibile creare moneta dal nulla.

Il 3 Gennaio 2009 avviene il lancio ufficiale del *Bitcoin* nel mercato; viene infatti posto in essere il primo blocco di 50 *BTC*, il *Genesis block*, detto anche blocco zero, contenente una frase che recita il titolo di un articolo sulla *frontpage* del “*Financial Times*”: “*Chancellor on brink of second bailout for banks*”.⁶

A tale titolo sono stati attribuiti 2 significati: innanzitutto, si vuole andare a definire il giorno in cui è stato creato questo blocco, dato che contiene le informazioni di questo articolo uscito in quella data; il secondo è molto rilevante, in quanto in quel periodo ci si trovava nel pieno della crisi economica mondiale e si valutava un possibile secondo aiuto alle banche mediante l’applicazione del “*quantitative easing*.”⁷

Uno degli scopi fondamentali di tale invenzione era proprio quello di prendere le distanze da un sistema che si era rivelato fallimentare, causando ingenti danni economici agli investitori ma anche ai piccoli risparmiatori.⁸

Paradossalmente, a 10 anni ormai di distanza da tale pubblicazione, non è ancora nota l’identità del padre del *Bitcoin*; infatti l’autore di quello che è definito come il “Protocollo *Bitcoin*” si è firmato sotto lo pseudonimo *Satoshi Nakamoto*.

⁵ Il cosiddetto *double-spending* non è altro che il problema che potrebbe verificarsi nel momento in cui qualcuno fosse in grado di spendere più volte lo stesso *token*.

Il protocollo di *Bitcoin* è stato creato in modo che sia impossibile spendere due volte lo stesso *token* senza violarlo.

⁶ Cfr. BOHME R. , CHRISTIN N. , EDELMAN B. , Moore T: , “*Bitcoin: Economics, Technology, and Governance*”, *Journal of Economic Perspectives*, 20 Luglio 2015

⁷ *Q.e.* sta per alleggerimento quantitativo, ovvero l’ acquisto di titoli di Stato o di altro tipo dalle banche in modo da emettere maggiore liquidità, incentivare i prestiti bancari e far crescere l’inflazione.

Tra gli svantaggi di tale operazione va citata la svalutazione della moneta.

⁸ Cfr. PAGLIARI E. , “10 anni di *Bitcoin*: le principali tappe della storia del re delle criptovalute”, www.cryptominando.it, 31 Ottobre 2018

1.2.1 Chi è *mister Bitcoin*?

Nel corso degli anni diverse sono state le ipotesi su chi potesse celarsi dietro a questo ormai celebre personaggio ma, nonostante l'impegno delle autorità di numerosi paesi del mondo, nessuno è in grado di poter dire ne chi sia il creatore di tale strumento, ne chi muove i fili del sistema valutario digitale. Nel 2014 una giornalista di nome *Leah McGrath* scrisse, sulla rivista "*Newsweek*", di aver scoperto, erroneamente, l'identità di questo personaggio segreto, ma la persona interessata negò qualsiasi coinvolgimento; anche nel 2015, quando si affermò che il vero creatore fosse un imprenditore australiano di nome *Craig Wright*, si pensava di aver risolto tale mistero, anche per via delle dichiarazioni dell'uomo, che pubblicò *online* un *post* che diceva "*Satoshi è morto, ma siamo solo all'inizio*".

Poi, in avanti, l'uomo non sarà in grado di dimostrarlo producendo le prove crittografiche della sua identità e per via di una serie di incongruenze.⁹

Ad oggi vi sono solo alcune idee sull'identità e sul luogo in cui potrebbe trovarsi tale figura; grazie a delle attente analisi di *Stefan Thomas*, programmatore svizzero e membro della comunità *Bitcoin*, dagli orari di pubblicazione di ogni *post* di *network* firmato *Nakamoto*, se ne deduce che fosse americano per via di una totale assenza di pubblicazioni dalle ore 5 alle ore 11 di mattina (orario di *Greenwich*).

L'unica certezza che si ha a riguardo, oltre al fatto che *Bitcoin* ha avuto il merito di fare da apripista nel settore e che è stato proprio grazie all'impegno dei creatori della valuta che, successivamente, sempre più monete virtuali sono diventate famose ed adottate in tutto il mondo, è che sarà molto complesso risolvere questo enigma, anche perché si sostiene che tale *Nakamoto* sia in possesso di circa 1 milioni di *Bitcoin*, situazione che probabilmente potrebbe metterlo troppo in esposizione.

1.2.2 (Segue) La *Blockchain*

Tale sistema poneva le proprie basi e le proprie radici nella rivoluzionaria e ormai famosa *Blockchain*, che è, probabilmente, l'elemento più costruttivo ed innovativo presente in tale contesto.

Il sistema *blockchain* si struttura su un'organizzazione molto complessa basata su una serie di blocchi che archiviano una serie di transazioni validate e correlate da una Marca Temporale (*Timestamp*).

⁹ Cfr. PLATEROTI A. , " Da *Nakamoto* a *Wright*: chi si cela dietro l'inventore", Il Sole 24 ore, 24 Febbraio 2017

Tale *Timestamp* garantisce sicurezza al modello, in quanto impedisce che le operazioni, una volta eseguite, vengano annullate o modificate.

La Marca Temporale consente inoltre di associare una data e un'ora certe e legalmente valide a un documento informatico, attribuendo una validazione temporale che può essere opponibile a terzi. Ogni blocco include l'*hash* (una funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) che identifica il blocco in modo univoco e che permette il collegamento con il blocco precedente tramite identificazione dello stesso.

La tecnologia permette inoltre la creazione di archivi condivisi, ottenendo un'articolata rete informatica in cui le numerose e differenti transazioni sono custodite tramite un *database* decentralizzato in cui figureranno anche gli importi delle stesse e gli pseudonimi di chi le compiono; questa meticolosa struttura diviene quindi difficilmente violabile, potendo apportare modifiche, in una fase successiva alla transazione, soltanto tramite il consenso della controparte.¹⁰

Viene a crearsi dunque un registro digitale unico che baserà la propria operatività sui numerosissimi nodi di tale organizzazione e sarà consultabile da tutti, garantendo quindi rilevante trasparenza e tracciabilità.

La *blockchain* può essere quindi considerata una tecnologia che appartiene alla categoria delle tecnologie *Distributed Ledger*, *DLT*, che possono essere definite come un insieme di sistemi concettualmente caratterizzati dal fatto di fare riferimento a un registro distribuito, governato in modo da consentire l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete.

Qualunque transazione, ovvero i dati che la rappresentano, è sottoposta ad un meccanismo di firma a doppia chiave asimmetrica che, pur non dotata di certificati rilasciati da certificatori accreditati (la *blockchain* prevede appunto il superamento di organismi certificatori centralizzati), funziona con un meccanismo simile a quello della firma digitale. Le *DLT* prevedono l'utilizzo di algoritmi crittografici che abilitano l'utente all'utilizzo del sistema, mettendogli a disposizione una chiave pubblica ed una privata che viene usata per sottoscrivere le transazioni o per attivare gli *smart contract* o altri servizi collegati alla *blockchain*.

Gli *smart contract* hanno il compito di verificare l'avverarsi di determinate condizioni e di autoeseguire in automatico azioni (o dare disposizione affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate.

In altre parole lo *Smart Contract* è basato su un codice che "legge" sia le clausole che sono state concordate, sia le condizioni operative nelle quali devono verificarsi le condizioni concordate e si

¹⁰ Cfr. GENNAI A. , "Investire sulla *Blockchain*", Sole 24 ore – Plus 24, 28 Maggio 2018

autoesegue automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.¹¹

Le *DLT* prevedono pertanto un meccanismo di validazione, a sua volta distribuito, basato sul concetto di consenso, vale a dire su meccanismi che governano anche questo tipo di partecipazione dei nodi.

Le modalità di gestione del consenso, unitamente alle logiche di impostazione del registro, rappresentano due fra i principali punti qualificanti della carta d'identità delle tecnologie *Distributed ledger*.¹²

Molto importante è il concetto di *Proof of work (Pow)*, che esisteva già prima del *Bitcoin* ed è forse tra le più grandi idee alla base del *white paper* di *Nakamoto*, perché realizza un consenso senza fiducia e distribuito.

Un sistema di consenso affidabile e distribuito significa che se si desidera inviare e / o ricevere denaro da qualcuno non è necessario affidarsi a servizi di terzi, a differenza di quando si utilizzano i metodi di pagamento tradizionali, dove è necessario servirsi di una terza parte per impostare la transazione. Questa manterrà poi il proprio registro privato che memorizza la cronologia delle transazioni e i saldi di ciascun *account*.

Con *Bitcoin* e poche altre valute digitali, ognuno ha una copia del libro mastro, quindi nessuno deve affidarsi a terze parti, perché chiunque può verificare direttamente le informazioni scritte.

Proof-of-Work, o *PoW*, è l'algoritmo di consenso originale in una rete *Blockchain*.

In *Blockchain*, questo algoritmo viene utilizzato per confermare le transazioni e produrre nuovi blocchi alla catena.

Con *Pow*, i minatori competono l'uno contro l'altro per completare le transazioni sulla rete e vengono premiati.

Un libro mastro decentralizzato raccoglie tutte le transazioni in blocchi; tuttavia, è necessario prestare molta attenzione per confermare le transazioni e organizzare i blocchi.

Il *Proof of stake* è un modo diverso per convalidare le transazioni e ottenere il consenso distribuito. È ancora un algoritmo e lo scopo è lo stesso del *proof of work*, ma il processo per raggiungere l'obiettivo è abbastanza diverso.

A differenza del *proof of work*, dove l'algoritmo premia i minatori che risolvono problemi matematici con l'obiettivo di convalidare le transazioni e creare nuovi blocchi, con il *proof of stake*, il creatore di

¹¹ Cfr. BELLINI M. , “*Smart Contracts*: che cosa sono, come funzionano quali sono gli ambiti applicativi”, www.Blockchain4innovation.it, 28 Dicembre 2018

¹² Cfr. BELLINI M. , “*Blockchain*: cos'è, come funziona e gli ambiti applicativi in Italia”, www.Blockchain4innovation.it, 10 Febbraio 2019

un nuovo blocco viene scelto in modo deterministico, a seconda della sua ricchezza, definita anche come "*stake*".

Inoltre, tutte le valute digitali sono state create in precedenza all'inizio e il loro numero non cambia mai.

Ciò significa che nel sistema *PoS* non vi è alcun premio di blocco, quindi i minatori accettano le commissioni di transazione.¹³

Altro fattore determinante è quello che garantisce la non duplicabilità delle informazioni, mediante una tecnica complessa che permette la creazione di blocchi crittografati concatenati tra di loro tramite chiavi crittografate immutabili.

A dimostrazione della sicurezza e della inviolabilità di tale organizzazione tecnologica, va detto che dal 2009 ad oggi, infatti, sono stati compiuti innumerevoli tentativi di violazione della *blockchain*, ma nessuno ci è mai riuscito; la *blockchain* è pubblica e quindi chiunque può avervi accesso, ma è inviolabile proprio per il fatto che è distribuita in una quantità enorme di computer e quindi non ci sarebbe un unico *server* da modificare, ma una cifra elevatissima.

Si basa dunque su una rete chiamata *P2P*.¹⁴

La *blockchain* è la sintesi di 5 concetti fondamentali:

- 1) Trasparenza
- 2) Sicurezza
- 3) Immutabilità
- 4) Decentralizzazione
- 5) Consenso

Partendo da questi principi, la *blockchain* è diventata la declinazione in digitale di un nuovo concetto di *Trust*.

Per queste ragioni alcuni ritengono che la *blockchain* possa assumere anche un valore per certi aspetti di tipo "politico", come piattaforma che consente lo sviluppo e la concretizzazione di una nuova forma di democrazia, realmente distribuita e in grado di garantire a tutti la possibilità di verificare, di "controllare", di disporre di una totale trasparenza sugli atti e sulle decisioni, che vengono registrati in archivi immutabili e condivisi che hanno caratteristica di essere inalterabili, immutabili e dunque immuni da corruzione.

La *blockchain* inoltre viene spesso associata al concetto di moneta virtuale e di *digital payment*.

¹³ Cfr. CAVALLI S. , "Proof of Work vs Proof of Stake", www.Cryptominando.it, 2 Febbraio 2018

¹⁴ Un sistema *P2P* "*peer to peer*" è una rete composta da tanti computer aventi la stessa rilevanza; non vi è un *software* centrale.

In realtà essa ha un grande valore sia nella straordinaria esperienza *Bitcoin*, sia come piattaforma per la gestione di transazioni e scambi di informazioni e dati anche in settori completamente diversi e lontani dal *finance* e dal *payment*.¹⁵

1.2.3 Considerazioni sulla *Blockchain* e possibili futuri utilizzi

Questo sistema ha successivamente riscosso numerosi consensi, essendo ad oggi uno dei punti di maggiore forza e causa di successo delle criptovalute; infatti Piermattia Menon, analista di *Consultique*, spiega: “ *ci sono numerose aziende che stanno investendo in progetti sulla Blockchain, come Daimler, che ha emesso un bond tramite Blockchain, o Carrefour, che sta implementando una Blockchain per la gestione della supply chain.*

Anche il Nasdaq ha manifestato l'intenzione di creare un segmento di mercato gestito tramite Blockchain.”

Jamie Dimon, Ceo di JP Morgan, noto critico del Bitcoin, durante la conferenza Axios tenutasi a Los Angeles in concomitanza dei 10 anni dalla pubblicazione del famoso white paper di Satoshi Nakamoto, ha dichiarato che, a differenza del Bitcoin, ritenuto dallo stesso poco più che una mera frode ed un qualcosa di assolutamente non paragonabile alla moneta fiat, la Blockchain è un qualcosa di reale, una tecnologia che tornerà molto utile anche in futuro.

Infatti, attualmente rappresenta una tecnologia chiave per la *roadmap* della banca e la sua piattaforma di pagamento basata su *blockchain* è stata estesa a molteplici banche.

L'occasione per fare il punto su quel “grande laboratorio a cielo aperto” che è oggi la *Blockchain* è rappresentato dal primo convegno dell'Osservatorio *Blockchain & Distributed Ledger* della *School of Management* del Politecnico di Milano.

Il convegno conclude il lavoro del tavolo di lavoro *Blockchain & Distributed Ledger* e nello stesso tempo è anche il momento di inizio del nuovo Osservatorio, in collaborazione con il DEIB, il Dipartimento di Elettronica Informazione e Bioingegneria del Politecnico di Milano.

Siamo davanti a una “bestia da domare”, per usare l'espressione efficace di Nicolò Romani di SIA o a una “innovazione senza limiti“, come dichiara con entusiasmo Marta Piekarska di Hyperledger.

¹⁵ Cfr. BELLINI M. , “*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*”, cit.

Entrambe le affermazioni sono valide per descrivere cos'è e dove ci porta la *Blockchain*, ma ci sono non pochi “nodi” da sciogliere affinché le aziende e le Pubbliche Amministrazioni possano effettivamente e compiutamente sfruttarla.

La spinta più importante arriva dal campo *finance* che con 172 progetti è il motore di sviluppo più importante e che copre ben 172 dei 331 progetti censiti, vale a dire il 59% del mercato.

Seguono a distanza settori come *Government* con il 9% dei progetti, logistica con il 7,2%, *utility* con il 3,9%, per arrivare all'*agrifood* con il 3%, ad assicurazioni, *healthcare*, trasporto aereo e media, con quote variabili dall'1 al 3% (dati aggiornati ad aprile 2018); se poi si guarda al numero delle banche centrali (29) che si sono attivate su progetti *Blockchain*, si può dire che la prima fase della contrapposizione e della “paura” tra *Blockchain* e Istituti di credito è ampiamente superata.¹⁶

Importante è inoltre considerare che c'è anche la *Blockchain* all'interno del lungo *iter* che ha contribuito alla Legge di bilancio 2019 approvata dal Senato tramite una serie di interventi; in tale documento, infatti, sono presenti diverse disposizioni aventi finalità di promuovere e sviluppare ulteriormente tale tecnologia.

Si prevede che la corsa globale alla regolamentazione del settore vedrà dunque un primo punto d'arrivo, ma per una sostanziale adozione ed un impatto concreto sulla vita quotidiana sarà decisivo soprattutto oltrepassare i rischi legati alla fluttuazione delle criptovalute.

Come è ben noto, le notevoli fluttuazioni del mercato delle criptovalute hanno indebolito la fiducia degli investitori e abbiamo assistito al generale ridimensionamento del settore del *cripto-trading*.

Con l'inizio di questo nuovo anno è giunto il momento per la *blockchain* di oltrepassare definitivamente la concezione di tecnologia al centro delle valute virtuali e di superare lo scetticismo sulla volatilità.

In realtà, le tecnologie di registri distribuiti (*Distributed Ledger Technologies* o DLT) possono avere numerose applicazioni che sono completamente slegate dalle criptovalute, in quanto offrono un approccio totalmente diverso per archiviare informazioni, svolgere funzioni ed eseguire transazioni, il tutto creando legami fiduciari innovativi, saldi ed efficaci; si prevede quindi che, con il tempo, l'utilizzo di questo rivoluzionario sistema sarà sempre più frequente, anche perchè le applicazioni basate sulla *blockchain* possono effettivamente ridurre i costi di intermediazione tra le parti coinvolte nelle transazioni e consentire lo scambio di valori *peer-to-peer* in grado di responsabilizzare ed emancipare i consumatori, superando i modelli tradizionali di controllo centralizzato e migliorando i

¹⁶ Cfr. BELLINI M. , “Osservatorio *Blockchain* 2018: crescono del 73% i progetti e si afferma un nuovo rapporto con le *cryptocurrency*”, www.Blockchain4innovation.it, 18 Aprile 2018

servizi in una vasta gamma di settori chiave, come l'energia, la sanità, i servizi finanziari, la gestione della *supply chain*, i trasporti, l'istruzione e i servizi pubblici.¹⁷

Non sorprende dunque l'attuale sfida legislativa globale, in cui i paesi di tutto il mondo competono per cogliere le opportunità offerte dalle *DLT*, tenendo però in considerazione che le opportunità comportano dei rischi, legati sia a limiti tecnici derivanti dalle asimmetrie informative, sia a comportamenti fraudolenti e attività illegali, perpetrate attraverso le *blockchain* non autorizzate per l'evasione, l'elusione fiscale e il riciclaggio di denaro sporco, ma dei vari aspetti positivi e negativi di tale tecnologia ed in generale delle criptovalute se ne parlerà in maniera più approfondita nel secondo capitolo.

1.2.4 Cosa sono le *ICO*

Una *ICO* (*Initial Coin Offering*) è un'offerta iniziale di una moneta che verrà emessa in futuro.

Tramite una raccolta di fondi le aziende, o più precisamente le *Start-up*, consentono il finanziamento del progetto a diversi investitori, dando in cambio dei *Token*, utilizzabili come il resto delle criptovalute non appena sarà ultimato il progetto.¹⁸

Questi *Token* si distinguono in 2 categorie:

- *Utility token*
- *Securities token*

Gli *utility token* forniscono agli utenti l'accesso a un prodotto o servizio e, poiché l'offerta totale è fissa, gli *utility token* possono aumentare di prezzo nel tempo se la domanda per il prodotto o il servizio aumenta.

Con il termine inglese "*securities*" ci si riferisce ad una classificazione ampia di qualsiasi tipo di bene negoziabile.

Attraverso le *ICO*, gli investitori hanno accesso a una vasta gamma di *securities*, che vanno dalle *coin* riscattabili per i metalli preziosi alle *coin* sostenute da immobili.

Inoltre permette agli azionisti di assumere un ruolo più attivo nel governo societario dal momento che il voto può essere condotto in modo trasparente attraverso la *blockchain*.¹⁹

Con tale strategia l'azienda trova un modo intelligente per finanziare lo sviluppo del proprio piano.

¹⁷ Cfr. RICCI T. , "*Blockchain*, che si prevede nel 2019: prospettive e sfide", www.Digital360.it, 17 Gennaio 2019

¹⁸ Cfr. DI NICOLA E. , "*Cosa sono le Ico*", www.BlogBitcoin.it, 20 Novembre 2017

¹⁹ Cfr. PORTA M. , "*Equity, Securities ed Utility token: quali sono le differenze?*", www.cryptominando.it, 26 Febbraio 2018

Tale “Offerta iniziale di moneta” è un termine utilizzato in analogia con il lessico di Borsa, dove con “*Initial Public Offering*” (*IPO*) si intende un'offerta al pubblico di azioni di una società che intende quotarsi per la prima volta su un mercato regolamentato; ma con due differenze importanti:

- 1) a differenza delle *IPO*, le “*Initial Coin Offerings*” non sono regolamentate.
- 2) chi investe in una *ICO*, non ottiene in cambio “azioni”, ma, come già detto, quelli che nel gergo delle criptovalute si chiamano dei *tokens*, ossia le singole unità della nuova criptomoneta che viene lanciata.

Questa recente tipologia di “operazione di mercato” viene considerata una invenzione di un tale *J.R. Willet*, che nel gennaio del 2013 pubblicò sul *forum BitCoin Talk* un *White Paper* in cui presentava una nuova idea: dei “protocolli che forniranno fondi iniziali,” scriveva, “per assumere gli sviluppatori per scrivere il *software* che implementa i nuovi livelli di protocollo, ricompensando economicamente i primi utilizzatori del nuovo protocolli”.²⁰

Tra le caratteristiche chiave delle *ICO* troviamo la possibilità di partecipare ad un progetto, ad una *DAO* (Organizzazione Autonoma Decentrata) o ad un sistema economico; non sempre, però, possedere dei *token* emessi da una *start-up* in fase di raccolta di capitale, dà all’investitore il diritto di prendere decisioni sul progetto, ma è un’opzione possibile.

La maggioranza delle *ICO* prevede la creazione di un numero definito di monete o *token* prima della vendita, inoltre i prezzi delle *ICO* di solito sono stabiliti dai creatori del sistema, progetto o *DAO* in questione.

Le raccolte di fondi possono essere più di una, e le criptovalute possono incrementare il loro valore fino alla data di rilascio.

I primi investitori avranno verosimilmente maggiori vantaggi inclusi nei loro *token*, come incentivi. Per quelle società che raccolgono capitale attraverso le *ICO*, i vantaggi sono molteplici.

Primo fra tutti, il fatto di non essere sottoposti a tassazione, cosa che invece avviene con le *IPO*.

Secondo punto a favore è che le vendite di *token* sono dirette e gli investitori basano le proprie decisioni sul contenuto dei progetti preparati dalla stessa società.²¹

Ovviamente, a tali operazioni sono connessi anche dei rischi: non va infatti dimenticato che il collocamento di nuove azioni in borsa è soggetto a precise regole di supervisione regolamentare che tutelano gli investitori, mentre nel mercato delle criptovalute non esiste una regolamentazione che tuteli i partecipanti alla *ICO*, che possono quindi ritrovarsi con l’investimento azzerato e senza possibilità di rivalersi su alcuno.

²⁰ Cfr. MALTESE F. , “*Ico come funzionano*”, *www.Trendonline.com* , 2019

²¹ Cfr. PROVENZANI F. , “*Ico: cos’è e come funziona l’offerta iniziale di valuta in criptovalute*”, *www.money.it* , 29 Marzo 2018

Ci si trova quindi in una situazione potenzialmente pericolosa, in quanto vi sono società con la possibilità di ottenere capitali anche in assenza di un prodotto concreto, e, se queste dovessero fallire o non produrre alcun valore, non vi sarà alcuna *chance* di rivalsa per gli investitori.

1.2.5 Mining

Il “*mining*”, o anche “*data mining*”, è il processo fondamentale ed imprescindibile che è alla base della produzione dei *Bitcoin*, che opera mantenendo la rete stabile e sicura.

Volendo dare per iniziare un’idea molto semplice, con il *Bitcoin mining* si va a risolvere, mediante il proprio *hardware*, dei problemi matematici o degli algoritmi, con la finalità di ottenere in cambio un certo numero di *Btc*, con dei “minatori” di *Bitcoin* che dovranno approvare le transazioni, in modo da poter tenere al sicuro il *network*.

Il *mining* è dunque quel processo in cui si aggiungono le registrazioni delle transazioni al registro contabile pubblico, ovvero la *blockchain*, trovando “minerale algoritmico” e ottenendo dei *token*; si può considerare come il centro dati dei *Bitcoin*, ad eccezione del fatto che è stato progettato per essere totalmente decentralizzato, con minatori che operano in tutte le nazioni senza che nessun individuo abbia il controllo della rete.

Il proposito primario del processo di *mining* è di permettere ai nodi della rete *Bitcoin* di raggiungere un consenso sicuro e a prova di manomissione.

Mining è pure il processo attraverso il quale i *Bitcoin* vengono immessi nel sistema: ai cosiddetti minatori vengono pagate delle *fee* come “sussidio” delle nuove monete create.

Questo serve per due propositi: distribuire nuove monete in maniera decentralizzata ed aggiungere sicurezza al sistema.

Si dice “minare” *Bitcoin* perchè il processo per ottenerli ricorda il lavoro delle miniere: richiede l’estrazione e crea lentamente nuova valuta, un pò come in passato si faceva con l’oro o altri metalli preziosi.²²

Vi sono 3 metodi di partecipazione all’attività di *mining*:

- **SOLO MINING**: l’attività di *mining* è svolta in maniera individuale, allo scopo di ottenere maggiori ricompense. L’elevata competitività attuale del *mining* richiede per questa specifica alternativa degli importanti investimenti in potenza computazionale.

²² Cfr. BERRETTI A. , “*Blockchain e mining, ecco come funziona: dietro le quinte della tecnologia*”, www.AgendaDigitale.it, 6 Giugno 2018

Maggiore è la potenza di cui si dispone, maggiore è la probabilità di risolvere dei blocchi e ottenere dei profitti. Il *solo-mining* tuttavia non garantisce flussi di cassa continui, e può trascorre molto tempo tra un'entrata e l'altra.

- *POOL-MINING*: in questo altro caso si svolge invece tale attività collettivamente, unendosi ad una *mining pool*, in cui più soggetti mettono a disposizione la propria potenza di calcolo e si suddividono i profitti proporzionalmente al contributo fornito. Il *pool-mining* permette di partecipare al *mining* anche se non si dispone di un'elevata capacità di calcolo, necessaria invece per il *solo-mining*. Generalmente questa seconda alternativa garantisce flussi di entrate di bitcoin minori ma continui.

-*CLOUD-MINING*: è possibile partecipare all'attività di *mining* senza possedere materialmente i dispositivi *hardware* necessari, eliminando i problemi relativi alla manutenzione e alla collocazione fisica di tali apparecchiature. Attraverso il *cloudmining* è possibile prendere a noleggio un determinato ammontare di potenza computazionale e far propri i profitti, in cambio di un canone di locazione.²³

Ovviamente i *server* necessari per compiere tali operazioni, oltre ad avere un determinato costo di acquisto, comportano un consumo di corrente davvero non indifferente, per via del fatto che lavorano per ben 24 ore al giorno, 7 giorni su 7, a cui vanno aggiunte delle spese necessarie a non causare surriscaldamenti dei computer (rischio verso il quale sono fortemente esposti per via della intensa attività) ; infatti le più grandi centrali che si occupano di *mining* si stanno spostando sempre di più in paesi con minori costi della manodopera e dell'elettricità , come l'Europa dell'est o la Cina.

Va detto però che tale mercato sta divenendo sempre meno conveniente e, forse, meno concorrenziale, a causa del continuo aumento dei costi connessi a tali attrezzature e della sempre maggiore riduzione di bitcoin ottenibile mediante tale processo.²⁴

1.3 Valutazione dell'impatto sociale, politico ed economico

Per iniziare a valutare l'impatto che le criptovalute ed, in modo particolare, il *Bitcoin*, hanno avuto all'interno del mondo economico ed in generale, va ripreso il motivo per cui tale strumento è stato creato.

²³ Cfr. KING R. , “How to mine Bitcoin: the complete guide”, www.BitDegree.it, 8 Agosto 2018

²⁴ Cfr. MURALI J. , “A new coinage: can Bitcoin, the global online digital currency, be the precursor of a new monetary system?”, *Economic and Political weekly*, 21 Settembre 2013

Come già detto, la nascita dello stesso è datata 2008, anno contraddistinto dalla famosa crisi che ha fortemente scosso il sistema economico globale e che ha messo in dubbio il sistema operativo bancario, la politica monetaria e non solo.

Tale periodo ha creato quindi forti tensioni ma soprattutto sempre maggiore diffidenza da parte di alcuni soggetti nei confronti delle Banche Centrali; tra questi vanno inclusi gli sviluppatori ed i sostenitori del Bitcoin, che volevano creare un'alternativa ad un sistema economico che si era rivelato molto fragile e che consentiva alle banche di curare maggiormente i proprio interessi, a discapito di una funzione pubblica sempre meno efficiente.

Si è quindi cercato uno strumento che andasse oltre determinati punti che si erano rivelati fallimentari o almeno opinabili, come la scarsa circolazione di moneta e dunque carenza di liquidità.

Emblematico è il caso del *Quantitative Easing* di Mario Draghi, che non ha prodotto gli effetti desiderati, a causa di un sistema bancario capace di contrastare e spesso invalidare le politiche espansive della BCE.

In effetti, nonostante i finanziamenti avessero tassi quasi prossimi allo zero e per quantità potenzialmente illimitate, le banche non hanno trasformato questo denaro disponibile in finanziamenti all'economia reale e allo sviluppo.

Sfruttando uno scenario del genere, *Nakamoto* e i suoi seguaci affrontano tale patologia del sistema tramite un modello opposto a quello in vigore, la cui intima ragione trova la sua massima espressione nell'idea di gestione dell'offerta di moneta.

La "cura" *Bitcoin* è tanto semplice quanto drastica: se il sistema bancario si rivela incapace di trasmettere le politiche monetarie, tanto vale impostare l'emissione di valuta secondo un sentiero predeterminato, bloccandone la quantità massima ad un ammontare fisso.

Questa cosiddetta scarsità artificiale di moneta è infatti essenziale al conseguimento della stabilità del potere di acquisto, evitando pericolose svalutazioni della moneta digitale dovute ad un'eccessiva emissione – creazione.

In buona sostanza, nessuno può influire sulla generazione di nuova moneta, trasformandosi in un'entità esogena all'esperienza umana.

Si tratta di una visione non esente da critiche; in particolar modo ci si chiede se il privare del tutto la politica monetaria di uno strumento importante quale la creazione monetaria possa essere una soluzione efficace.

Attraverso la decentralizzazione, *Bitcoin* mira a rendere l'offerta di moneta indipendente dal fattore umano e, di conseguenza, indipendente dal rischio di errori che esso porta con sé.

I *Bitcoiner* in concreto pensano che solo la tecnologia possa svolgere un ruolo così delicato come quello della creazione di moneta.

A tal proposito, talvolta *Bitcoin* è definito un sistema *trust-less*, privo di fiducia: dal protocollo *Bitcoin* invero si può leggere: “Ciò che serve è un sistema di pagamento elettronico basato su prove crittografiche, invece che sulla fiducia, che consenta a soggetti consenzienti di negoziare direttamente tra loro senza la necessità di un garante terzo”.

L’idea dunque è quella di fondare un’economia che sia in grado di fare a meno della fiducia, in nome della maggior libertà degli individui ed in forza di un protocollo informatico immutabile.

Bitcoin diffonde su diversi fronti il suo progetto di costruire una vita sociale che prescindendo completamente dall’elemento fiducia, aspetto che non tocca soltanto le banche commerciali e le autorità monetarie, ma anche le istituzioni, gli organismi di supporto, sino ad arrivare alle persone comuni. Tuttavia, con *Bitcoin*, piuttosto che ad una generica mancanza di fiducia, si assiste ad un trasferimento di questa. Si parla di trasferimento di fiducia dall’uomo, nel nostro caso l’autorità di garanzia, che nell’ottica di *Bitcoin* non è ormai più affidabile, alle leggi della matematica e dell’informatica, ossia alla crittografia e agli algoritmi che stanno alla base della rete *Bitcoin*.

Di contro, la rivoluzione, che comporterebbe l’adozione generalizzata della moneta digitale crittografata, conserva talvolta il germe di una strumentalizzazione populista e demagogica.²⁵

Dopo 10 anni di distanza possiamo affermare che le criptovalute, e soprattutto il *Bitcoin*, dopo un’iniziale fase di avversione e timore verso qualcosa di nuovo e sconosciuto, si stanno ritagliando uno spazio sempre maggiore, facendo diminuire progressivamente anche il numero di soggetti scettici.

Anche in generale il sistema di digitalizzazione che è stato proposto dalle criptovalute si sta ritagliando un proprio ruolo e sta facendo venire meno il notevole scetticismo dei primi anni; scetticismo del sistema bancario, e non solo, dovuto principalmente dalle preoccupazioni in materia di frode, ma ad oggi le banche stanno studiando come sfruttare la tecnologia per velocizzare i sistemi di liquidazione di *back-office* e liberare ingenti capitali legati al *trading* sui mercati globali.

Sei delle più grosse banche mondiali hanno deciso di lanciare insieme un progetto per creare una nuova forma di denaro digitale. Come riportato dal “*Financial Times*”, *Barclays*, *Credit Suisse*, *Canadian Imperial Bank of Commerce*, *HSBC*, *MUFG* e *State Street* si sono unite per lavorare al progetto “*Utility Settlement Coin*” creato dalla svizzera *UBS* per rendere più efficienti i mercati finanziari. Un programma che adesso punta ad aprire un tavolo di discussione con le banche centrali per il rafforzamento della *data privacy* per implementare nuovi sistemi di protezione *cyber security*.

La “*utility settlement coin*”, sviluppata da *Clearmatics Technologies*, mira a permettere ai gruppi finanziari di fare pagamenti o acquistare dei titoli, senza aspettare che i trasferimenti di denaro

²⁵ Cfr. AUGELLO V. , “l’impatto sociale ed economico dell’ideologia *bitcoin*”, www.ValuteVirtuali.it, 22 Novembre 2018

tradizionali siano completati. Le società potrebbero invece utilizzare monete digitali direttamente convertibili in denaro presso le banche centrali, riducendo il tempo, il costo e il capitale richiesti nelle fasi *post-trading*.²⁶ Le criptovalute sono, ormai, addirittura riconosciute a livello europeo, tramite una legge chiamata direttiva europea n. 156 del 19/06/2018 facente riferimento alla direttiva EU 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018;²⁷ essa modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e le direttive 2009/138/CE e 2013/36/UE.

Con l'atto legislativo l'UE definisce per la prima volta le criptovalute, che vengono considerate come: “una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo *status* giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente”.

Con questa direttiva l'Europa vuole fare una distinzione tra le monete complementari, utilizzate per esempio in una città o in una regione, e tra un numero limitato di utenti, e le cosiddette valute virtuali, che secondo la direttiva non devono essere considerate in modo uguale.

Si vuole quindi limitare la possibilità di utilizzare le criptomonete per il conseguimento di finalità criminali; la direttiva introduce formalmente la figura del portafoglio digitale, il *wallet*, che in buona sostanza è un prestatore di servizi, cioè un “soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali”. I singoli Stati membri dell'Unione Europea dovranno applicarla e recepirla entro la data ultima del 10 gennaio 2020; “Coloro che offrono i servizi tra cui delle attività consistenti nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale e i prestatori di servizi di portafoglio digitale, non sono soggetti all'obbligo dell'Unione di individuare le attività sospette”.²⁸

1.4 Altre principali criptovalute

Quando si parla di monete digitali, viene data sempre maggiore attenzione al *Bitcoin*, essendo questo il primo per capitalizzazione e, come già detto, per anzianità.

²⁶ Cfr. GOBBI M. , “Chi investe in *bitcoin* e *blockchain*”, *www.Area-Business.net*, 2016

²⁷ Cfr. Gazzetta ufficiale dell'Unione europea, “DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO”, Direttive, 30 maggio 2018

²⁸ Cfr. “Regolamentazione Criptovalute: l'Europa le regola ufficialmente”, *www.Lcriptovalute.org*, 31 Agosto 2018

Va detto però che il mondo delle criptovalute, in questo decennio, è andato ad allargarsi sempre di più, con la nascita di moltissimi strumenti digitali diversi tra di loro; ad oggi, infatti, se ne contano più di 1000 diverse tra loro, che prendono, tutte, il nome di “*Altcoins*”.

Le *Altcoins* sono le criptovalute alternative realizzate dopo il successo di *Bitcoin*, e che allo stesso *Bitcoin*, spesso e volentieri, pretendono di andarsi a sostituire sfruttando, e correggendo, eventuali problematiche riscontrate.

Non tutte le *Altcoins* sfruttano la tecnologia *peer-to-peer* e talvolta possono richiedere un processo di *mining* ai fini della validazione delle relative transazioni.

Il mondo delle *Altcoins* si è sviluppato in maniera notevole negli ultimi anni e, pertanto, al netto della nota definizione di valute digitali alternative al *Bitcoin*, è davvero difficile andarle a studiare come categoria.

Lo studio delle *Altcoins* potrebbe inoltre essere utile per tre ordini di motivi:

- 1) Maggiore margine di sviluppo a livello tecnologico rispetto al *Bitcoin*;
- 2) Prezzo di mercato decisamente più basso;²⁹
- 3) Possibilità di studiare le nuove *altcoins* dalla loro “nascita”: si può verificare lo sviluppo, passo dopo passo, senza l’ansia di entrare troppo tardi sul mercato.³⁰

Volendo fare un’analisi delle altre valute digitali che in questi anni si sono ritagliate uno spazio sempre maggiore, va premesso che sono, comunque, molto distanti dal *Bitcoin*, che resta in assoluto il *leader* di mercato in tutta la categoria delle monete digitali, vantando elementi chiave come una maggiore sicurezza, identità del marchio maggiormente riconoscibile ed uno sviluppo più attivo e razionale.

L’idea della grande maggioranza degli analisti è che il divario tra *Bitcoin* e le altre criptovalute si allargherà ancora di più nel tempo; c’è da aggiungere, inoltre, che la *performance* di tutte le altre monete è fortemente correlata con quella del *Bitcoin*.

Dopo aver fatto tali considerazioni, consideriamo le altre migliori criptovalute degli ultimi anni.

²⁹ C’è da dire però che il *Bitcoin* è anche acquistabile in un’unità di misura inferiore chiamata “*Satoshi*”, equivalente a 0,00000001 *Bitcoin*.

³⁰ Cfr. FERRO, “*Altcoin: cosa sono e perché è importante conoscerle*”, www.tecnologi.net, 13 Febbraio 2018

1.4.1 (Segue) *ETHEREUM*

Ethereum nasce nel 2013 per opera di *Vitalik Buterin*, uno sviluppatore di origini russe, cresciuto in Canada, che univa la competenza di programmatore a quello di ricercatore nell'ambito delle criptovalute.

Buterin si appoggiò ad una operazione di *crowdfunding*³¹ durante il 2014 e fu nella condizione di completare *Ethereum* l'anno successivo quando divenne pubblico e accessibile online.³²

Non è un caso se ad oggi è tra le prime monete digitali per capitalizzazione e si è ormai affermata in parte come una vera e propria alternativa al discorso bitcoin, già dall'inizio del 2016, periodo particolarmente importante per il rilancio delle criptovalute.

Ethereum è una piattaforma decentralizzata di tipo computazionale con lo scopo di produrre e pubblicare dei contratti intelligenti definiti "*smart contracts*", aventi la finalità di gestire diversi servizi in maniera sicura e pubblica; la stessa viene quindi "remunerata" attraverso scambi basati su una *cryptocurrency* calcolata in *Ether*.³³

Inoltre è importante precisare che può essere adottata da chiunque e gestisce i contratti in maniera intelligente, avendo a disposizione un archivio immutabile e condiviso di tutte le operazioni attuate nel corso del tempo.

Progettata per essere adattabile e flessibile e per creare facilmente nuove applicazioni, *Ethereum* è inoltre una *Programmable Blockchain* che non si limita a mettere a disposizione operazioni predefinite e standardizzate, ma permette agli utenti di creare le proprie "*operations*".

Di fatto è una *Blockchain platform* che permette di dare vita a diverse tipologie di applicazioni *Blockchain* decentralizzate non necessariamente limitate alle sole *cryptocurrencies*.

Nel 2016 *Ethereum* è stata divisa in due diverse *Blockchain*: *Ethereum Foundation* ed *Ethereum Classic*.

La prima è un'organizzazione che ha come obiettivo la gestione di tutte le attività di sviluppo, di ricerca e di supporto della piattaforma *Ethereum*, che è stata caratterizzata da una serie di prototipi e di azioni di sviluppo finanziati e gestiti da *Ethereum Foundation* sulla base del concetto e progetto di *Proof of Concept*, fino al lancio del progetto *Frontier network* allo scopo di migliorare sicurezza e usabilità.

³¹ Il "*Crowdfunding*" è un fenomeno attraverso il quale un promotore di un'iniziativa richiede ad un pubblico indistinto tramite una piattaforma somme di denaro necessarie a sostenere il progetto esposto (*funding*)

³² Cfr. Il fatto Quotidiano, 6 ottobre 2016.

³³ *Ether* risulta essere, da una parte, la potenza elaborativa necessaria per produrre i contratti e, dall'altra, la criptovaluta che permette di "pagare" per la realizzazione dei contratti stessi; è dunque un *token* che viene trattato come *cryptocurrency exchanges*.

Tra le varie iniziative va segnalato il progetto *Olympic* che aveva tra l'altro lo scopo di mettere alla prova con uno “*Stress Test*” le performance e i limiti della rete *Ethereum Blockchain*.

Con il progetto *Olympic* arriva poi il già citato *Frontier network*.

Accanto a *Homestead* è attivo il progetto *Metropolis*, finalizzato a semplificare l'utilizzo della *Ethereum Virtual Machine* e permettere agli sviluppatori di agire con maggiore flessibilità e velocità. *Ethereum Classic* è invece il frutto di una importante divisione nel nucleo originario di *Ethereum* a livello di *Ethereum Foundation*.

In particolare è costituito dai membri *Ethereum* che hanno deciso di dare vita ad una “nuova” versione, distaccandosi dalle linee di sviluppo di *Ethereum Foundation*.

Ethereum Classic è un *network* che resta compatibile con la tecnologia *Ethereum*, ma con una serie di servizi pensati per aumentare la sicurezza; questa è basata sullo sviluppo di una *blockchain* non-*hackerabile* e ha sviluppato una strategia di emissione dei *tokens* in proporzione allo sviluppo della rete nel corso del tempo, allo scopo di limitare i rischi di deflazione della criptovaluta.

Nello specifico va ricordato che *ETC* (*Ethereum Classic* ha come nome in codice appunto *ETC*) è un *token* digitale basato sulla piattaforma *Blockchain* di *Ethereum Classic*.

Inoltre vi sono una serie di nuove opportunità per i *miners*, in quanto la potenza di calcolo necessaria per “risolvere i problemi” e “sbloccare” i nodi della *blockchain* può essere inferiore a quella tradizionalmente necessaria per la piattaforma *Ethereum*.

Dal punto di vista del valore di mercato *l'ETC* riflette il volume di transazioni che vengono operate nel mercato e viene stabilito dalle operazioni che si svolgono sui principali siti di *exchange*.

Vi è una chiara motivazione alla base di questa “scissione”, per questo è opportuno conoscere la vicenda the *DAO*.

La *DAO* (*Decentralized autonomous organization*) è un'organizzazione creata su *Blockchain Ethereum* e caratterizzata dal fatto di essere una organizzazione senza una sede, senza una personalità giuridica, senza figure chiaramente identificabili come amministratori, quindi una sede virtuale.

La finalità principale era quella di raccogliere capitali da investire su progetti che venivano previamente valutati da un comitato e poi posti in votazione.

Il progetto ebbe un grande successo e nel giro di pochi mesi gli organizzatori di *The DAO* riuscirono a raccogliere circa 150 milioni di dollari.

Ma il 18 giugno 2016 venne violato l'indirizzo in cui erano allocati gli *ETH* ricevuti dall'organizzazione ed in poche ore furono persi circa 70 milioni di dollari.

La vicenda diede luogo a una serie di discussioni e confronti e portò alla fine ad una scissione della *Blockchain Ethereum* ed alla creazione di due nuove *blockchain* (oggi suddivise, appunto, in *Ethereum classic* ed *Ethereum Foundation*).³⁴

1.4.2 (Segue) *RIPPLE*

Di diritto tra le criptovalute più sorprendenti e particolari, *Ripple*, oltre ad avere una capitalizzazione tra le più alte del mercato delle valute digitali, è sicuramente tra quelle che negli ultimi anni si è messa più in mostra agli occhi degli investitori e non solo.

Fin dal 2013, anno della creazione del *Ripple*, l'intenzione è stata sin da subito quella di ritagliarsi sempre più spazio tra le grandi criptovalute fino ad allora presenti.

Ovviamente, come già accade per tutte le nuove criptovalute, anche il valore dei *Ripple* non si basa sulla circolazione di alcuna moneta fisica, ma viene stabilito direttamente dai rapporti monetari che si possono scambiare solamente *online*.

Questa rappresenta un'interessante criptovaluta basata su un protocollo creato da *OpenCoin*, fondata da *Chris Larsen* e *Jed McCaleb*; importante era la volontà di eliminare svantaggi e difficoltà legate all'utilizzo del *Bitcoin* e si è avuto un sistema basato sul trasferimento di fondi in tempo reale mediante un protocollo gestito dalla società stessa chiamato *Ripple Transaction Protocol*.

Grazie a questo è stato possibile facilitare gli scambi e le transazioni in denaro che avvengono tra gli utenti della rete.

Ripple è sia il nome della criptovaluta digitale (*XRP*), sia del *network* dove la valuta viene trasferita, infatti viene usato anche per cambiare moneta; ad esempio si possono effettuare cambi tra Sterlina ed Euro senza dover affidarsi ad un intermediario come una banca centralizzata per farlo.

Le transazioni di denaro in differenti valute vengono inoltre registrate su un database sicuro, il *Ripple Consensus Ledger (RCL)*.³⁵

Un punto che lo distingue dalle altre principali valute virtuali è sicuramente quello che, a differenza di queste ultime che utilizzano sistemi decentralizzati, *Ripple* ha un *network* centrale, servendosi di una piattaforma "*open source*", in quanto ogni sviluppatore può dare il proprio contributo con interventi ed eventuali modifiche.

³⁴ Cfr. Bellini M. , "Che cos'è e quali sono gli ambiti applicativi di *Ethereum*", www.Blockchain4innovation.it, 30 Agosto 2017

³⁵ Cfr. "*Ripple*: la guida completa alla valuta digitale atipica", www.criptovaluta.it

Un altro elemento di forte diversità risiede nel fatto che le monete vengono rilasciate a coloro che “donano” le capacità computazionali dei propri comparti *hardware*, dissociandosi quindi dall’attività di *mining*.

Inoltre il *Ripple*, a differenza del *Bitcoin*, non è solo una criptomoneta, ma una rete dove portare a termine transazioni fra varie valute, senza commissioni e senza oscillazioni del dollaro.

Con *Ripple*, la velocità della transazione è ampiamente superiore rispetto al *Bitcoin*: un intervallo di tempo compreso tra 2 e 5 secondi contro 10 minuti.

Il *Bitcoin*, poi, è in grado di tracciare esclusivamente i movimenti *BTC*, mentre il *Ripple* può tracciare ogni *asset* e quindi qualunque valuta.

Per concludere, va detto che per i *Ripple* è prevista un’emissione di 100 miliardi, mentre per i *Bitcoin* di 21 milioni.³⁶

Si tratta quindi di un prodotto dove le banche possono incontrare la domanda per pagamenti globali più veloci, a basso costo e *on-demand* per qualsiasi tipologia e quantitativo di pagamento.

Il risultato è che quindi attraverso questa tecnologia è possibile ottenere nuove opportunità d’investimento, costi di processazione più bassi ed un’esperienza per il consumatore complessivamente migliore.

Attraverso l’utilizzo di *Ripple*, la banca può quindi ottenere nuovi clienti ed aumentare i propri profitti attraverso prodotti e servizi differenziati.

Ripple può inoltre diminuire i costi di *back office* della banca attraverso quindi un processo per consentire i pagamenti internazionali.

Secondo gli esperti delle criptovalute, l’aumento sostenuto nel prezzo di *Ripple* è stato principalmente dovuto proprio al grande interessamento da parte delle banche, che stanno investendo e credendo sempre di più in questo *network*/criptovaluta.

Il *business* per l’invio e la ricezione dei pagamenti è un mercato che vale ben 500 miliardi di dollari l’anno e *Ripple* sta ottenendo molti accordi di *partnership* con moltissime banche di primo livello.

1.4.3 (Segue) *LITECOIN*: argento digitale

Litecoin è una criptovaluta a tutti gli effetti nata il 7 Ottobre 2011 grazie all’idea di un ex dipendente di *Google* di nome *Charlie Lee*, il quale non ha affatto nascosto di essersi ispirato al *Bitcoin*;

³⁶ Cfr. GAGLIARDUCCI C. , “*Ripple*: cos’è, come funziona e quali differenze con il *Bitcoin*?”, www.money.it , 23 Maggio 2017

l'obiettivo era quello di creare qualcosa che fosse argento (*LTC*) in un mercato dove il *Bitcoin* era oro.

Si ha quindi a che fare con una valuta digitale *peer-to-peer* che consente pagamenti istantanei quasi a costo zero a favore di un destinatario, ovunque esso si trovi, e si basa su un sistema *open source* completamente indipendente dal controllo di qualsiasi autorità centrale; il *Litecoin* è, dunque, un consolidato mezzo di scambio complementare al *Bitcoin*.

Si è cercato di migliorare *Bitcoin* limitando la sua vulnerabilità e aggiungendo un livello di sicurezza maggiore alla rete: ciò è stato fatto con il lancio della versione 0.8.5.1 di *Litecoin* nel 2013.

Verso la fine dello stesso anno il team di sviluppo ha rilasciato la versione 0.8.6.1 che ha ridotto di 20 volte le spese di transazione, migliorando ulteriormente il sistema di sicurezza.³⁷

Per quanto riguarda l'attività di *mining*, *Litecoin* ha una differenza molto particolare rispetto al *Bitcoin*. Quest'ultimo utilizza l'algoritmo di *hash* SHA-256, che comporta un aumento esponenziale del livello di difficoltà di *mining* per i *Bitcoin*.

Litecoin, invece, utilizza *scrypt*, che incorpora l'algoritmo SHA-256, ma i suoi calcoli sono molto più serializzati rispetto a quelli del SHA-256 di *Bitcoin*.

Scrypt privilegia grandi quantità di RAM ad alta velocità, piuttosto che la sola potenza di elaborazione, e necessita di più risorse; è inoltre riconosciuto come il miglior deterrente per attacchi e *brute force* al *network*, ma l'*hardware* per l'estrazione richiesto da *scrypt* è anche più costoso.

Anche la rete *Litecoin* è programmata per produrre un ammontare predeterminato di unità, infatti è prevista approssimativamente una quantità di monete virtuali pari circa al quadruplo rispetto a *Bitcoin*, ovvero circa 84 milioni di *Litecoin*; la *blockchain* di *Litecoin* elabora però un blocco ogni 2,5 minuti, rispetto ai 10 minuti di *Bitcoin*, il che consente una conferma delle transazioni circa 4 volte più veloce.³⁸ Per contro, un tempo così ristretto ha aumentato le dimensioni del *Litecoin blockchain* ed il numero dei blocchi orfani. Alla luce di tutte le sue peculiarità e della sua utilità, *Litecoin* è cresciuta tantissimo nel corso degli anni, diventando una delle valute digitali avente maggiore seguito e raggiungendo crescite di valore altissime, con l'apice del successo datato 17 Dicembre 2017; in tale giorno, vi fu la vendita dei propri *assets* digitali da parte proprio del suo creatore, *Charlie Lee*.

Tale azione ovviamente generò enorme sfiducia ed incertezza verso gli investitori e possessori dell'argento digitale, generando un violento e continuo calo del valore di tale strumento che, allora, era arrivato a superare la soglia dei 350 dollari. (ad oggi il prezzo di un *LTC* si aggira attorno ai 30 dollari, Gennaio 2019)

³⁷ Cfr. "*Litecoin*", www.NGC.it, 24 Gennaio 2018

³⁸ Cfr. GAGLIARDUCCI C. , "*Litecoin: cos'è, come funziona e le differenze con Bitcoin*", www.money.it , 6 Ottobre 2017

1.4.4 (Segue) BITCOIN CASH (BCH)

Bitcoin Cash è una criptovaluta molto recente, nata infatti il 1 Agosto 2017 da una “*hard fork*”³⁹ di *Btc*, con la finalità principale di risolvere il “*problem scaling*”, dovuto dal fatto che il *Bitcoin* originale riesce a produrre un numero di transazioni non molto elevato in un determinato arco di tempo (circa 7 scambi al secondo); con il *Bitcoin Cash* si va ad aumentare tale frequenza e dunque a risolvere tale problema, passando da un numero di blocchi di 1 *Mb* ad un limite di ben 8 *Mb*, e ciò rende per molti il *BCH* una moneta transazionale migliore dell’oro digitale.⁴⁰

C’è da dire che quello del *problem scaling* è un problema dovuto principalmente alla popolarità sempre crescente del *Btc*; infatti è stata raggiunta una soglia di utenti che ha portato ad un sovraccarico della rete ad un accumulo i blocchi, incrementando esponenzialmente i tempi di transazione.

La situazione è totalmente sfuggita di mano nel maggio del 2017, quando alcuni utenti segnalavano di aver dovuto attendere fino a quattro giorni per ricevere la conferma di avvenuto scambio.

Gli utenti possono accelerare il processo di conferma pagando spese di transazione più alte, ma tale approccio rese il *Bitcoin* inutilizzabile come metodo di pagamento, specialmente per acquisti di piccola taglia.

Dopo la suddivisione, tutti i possessori di *Bitcoin* hanno ricevuto la medesima quantità di *token Bitcoin Cash* e la nuova criptovaluta venne velocemente adottata dagli investitori, divenendo, dopo appena un giorno, la terza criptovaluta per capitalizzazione di mercato, dietro *Bitcoin* e *Ethereum*.

Tuttavia molti esprimono dei dubbi su questa criptovaluta a causa del fatto che non si ha una reale e completa decentralizzazione.

Infatti non è gestita da una *community* aperta di sviluppatori, ma da un gruppo ristretto e chiuso di persone, e ciò ne rende di fatto possibile il controllo.

Da un lato quindi ci sono gli sviluppatori di *BCH* che sostengono che sarà una vera e propria alternativa al *BTC* originale, tanto da poter addirittura arrivare a sostituirlo.

Dall’altro, invece, c’è la *community* originale degli sviluppatori di *Bitcoin* che sostiene che *BCH* non sia, e non sarà mai, *Bitcoin*.

³⁹ Una “*hard fork*” è l’unica modalità esistente di aggiornamento del *Bitcoin*, che consiste nella creazione di una nuova *Blockchain* con differenti regole tramite una suddivisione della rete da parte degli sviluppatori; fino al momento della divisione, la versione originale e quella più recente avranno la medesima *Blockchain*, dopodichè opereranno in maniera assolutamente indipendente.

⁴⁰ Cfr. “Cos’è il *Bitcoin Cash*?”, www.CointelegraphItalia.it

Per gli utilizzatori comuni, o almeno una buona parte di essi, probabilmente *BCH* risulta una moneta transazionale migliore di *BTC* (seppure non ottima), fin tanto che *BTC* non risolverà i problemi di *scaling*.⁴¹

Incredibile è stata la performance altamente negativa del *BCH* nel 2018; come è stato detto, subito dopo la sua nascita, il *Bitcoin Cash* si è immediatamente imposto nel mercato come una tra le criptovalute più interessanti ma soprattutto più utilizzate, con un prezzo esponenzialmente crescente. Dopo la fase di fortissimo rialzo, nel 2018 si è assistito ad un frequente e violento declino che ha portato tale strumento digitale a perdere nel giro di 12 mesi più del 95%, un valore che riflette una delle peggiori prestazioni registrate dalle criptovalute ai primi dieci posti in termini di capitalizzazione.

1.4.5 (Segue) *Altcoins* minori

Vi sono numerosissime *Altcoins* di capitalizzazione inferiore rispetto alle principali per il quale si prevedono ruoli di primo piano all'interno della propria categoria per via delle loro caratteristiche, delle novità o in alcuni casi dei loro miglioramenti.

Da citare è sicuramente *Monero (XRM)*, creata nel 2014 con il nome di *BitMonero*, derivante da *Bit* (come in Bitcoin) e *Monero* (traducibile come “moneta”), la cui caratteristica principale si fonda sulla *privacy*.

Altre tematiche fondamentali sono la scalabilità ed il decentramento.⁴²

Si tratta di una moneta digitale di tipo *opensource* che adopera il medesimo sistema *proof-of-work* di Bitcoin, al fine di evitare la doppia spesa e di mettere in sicurezza il *network*.

Nel gennaio 2017, è stato poi adottato l'algoritmo *Ring Confidential Transaction*, che ha rafforzato la *privacy* in favore degli utenti.

Rispetto al *Bitcoin*, *Monero* è programmato per un numero minore di monete emesse, ovvero, 18,4 milioni, che si esauriranno entro otto anni.

Tutto funziona mediante l'algoritmo di firma ad anelli, che ha introdotto uno strato di sicurezza in più, proprio perché non permette di far vedere l'ammontare di una transazione ad una persona terza. *Monero* si caratterizza anche per la sua alta scalabilità; non prevede al suo interno una dimensione massima per la dimensione dei blocchi come il *Bitcoin* che ha il limite ad 1 *Mb*.

⁴¹ Cfr. CAVICCHIOLI M. , “Cos’è il *Bitcoin cash (BCH)*?”, www.ilBitcoin.it, 12 Novembre 2017

⁴² Cfr. TORCHIANI G. , “*Altcoin*: cosa sono e come funzionano le criptovalute sorelle del Bitcoin”, www.Digital4Trade.it, 2 Febbraio 2018

Il sistema però prevede al contempo un meccanismo di penalizzazione, al fine di evitare che si verifichi un aumento dei blocchi eccessivo.

Infine, via via che il suo utilizzo aumenterà nel tempo, le commissioni per transazione diminuiranno; mentre di contro le commissioni per le transazioni totali andranno incrementandosi.⁴³

Un'altra moneta alternativa molto importante è il *Dash*, nata nel 2015 e chiamata inizialmente *Xcoin*. Questa si propone come un'alternativa avente l'intenzione di migliorare le principali caratteristiche dei *Bitcoin* dovunque sia possibile ed andando ad aggiungere anche alcune novità.

I *Dash coin*, inoltre, sono considerate come vero e proprio contante digitale in quanto vi è la possibilità di accedere a pagamenti istantanei e questo permette il trasferimento di denaro digitale da qualunque parte del mondo su conti diversi in una manciata di secondi.

Utilizzano inoltre una rete *open source peer to peer* più sicura e più veloce.

Per quanto riguarda la sicurezza del *Dash*, sono state introdotte delle misure preventive come i *MasterNodes*. Questi sono sistemi *proof of service* che proteggono e migliorano la moneta digitale.

Il *Dash* funziona comunque su due livelli: i già citati *MasterNodes* e il tradizionale *mining*.

Questo tipo di rete non è soggetta ad alcun tipo di controllo da nessun ente governativo, quindi gli scambi di valuta sono del tutto privi di controlli, ma questo non significa che siano monete illegali o non sicure.⁴⁴

Il padrone del conto in ogni caso è unico e nessuno può avere accesso alle sue credenziali.

Clamorosa la crescita che ha visto tale strumento nel 2017 partire da una base di 11 dollari arrivando, alla fine dello stesso anno, a valerne più di 350, registrando una crescita di circa il 3000%, con una capitalizzazione di mercato superiore ad 1,5 miliardi di Dollari.⁴⁵

Va citato, infine, un'altra importante *Altcoin*, l'*Eos*, nata soltanto a metà 2017 e divenuta in poco tempo la quinta piattaforma per capitalizzazione.

La stessa moneta si basa su un nuovo tipo di *blockchain* che supporta grandi volumi di transazioni al secondo e non prevede commissioni.

La piattaforma *EOS* nasce per offrire servizi già pronti come *database* o autenticazione e per semplificare lo sviluppo di nuove *App*.

Il progetto non riguarda quindi una semplice moneta digitale, ma va ben oltre; presenta quindi delle similitudini con *Ethereum*, che, come abbiamo visto, offre anche la possibilità di produrre *smart contracts*.

⁴³ Cfr. "Monero (XMR): cos'è e come fare trading", www.tradingonline.com, 2018

⁴⁴ Cfr. BELLINI M. , "Cos'è Dash (DASH), valore di mercato e ambiti applicativi", www.Blockchain4innovation.it, 21 Agosto 2018

⁴⁵ Cfr. PROVENZANI F. , "Dash: cos'è e come comprare la criptovaluta rivale del Bitcoin", www.money.it, 11 Dicembre 2017

La *blockchain* di *EOS* è capace di garantire alle applicazioni decentralizzate *scaling* verticale e orizzontale con una latenza minima.

Tra le caratteristiche principali di questa innovativa criptovaluta, troviamo un ottimo sistema di sicurezza in grado di bloccare le transazioni in caso di furto.

Alla base di *EOS* c'è un solido team guidato dal *CEO Daniel Larimer*, già rinomato per aver ideato il concetto di *DAO* e dell'algoritmo di consenso *Delegated Proof of Stake (DPoS)* utilizzato proprio da *EOS*.

Il "*Delegated Proof of Stake*", evoluzione del *PoS*, è maggiormente robusto e sicuro.

Per consenso, si intende l'approvazione di una transazione della *blockchain*, bloccando di contro quelle non valide.

L'algoritmo *DPoS* è diviso in 2 parti:

- il processo di elezione, che assicura il controllo ai possessori della criptovaluta
- la programmazione della produzione

A differenza degli altri algoritmi, il *DPoS* è in grado di funzionare pure quando la maggior parte dei produttori fallisce. Durante questo processo, la *community* può votare e decidere con chi rimpiazzare i produttori falliti. *EOS* non è minabile ed esistono 1 miliardo di *token*.

I fondi incassati dalla vendita di *EOS* sono gestiti dalla piattaforma tramite uno *smart contract* elaborato sulla piattaforma di *Ethereum*. Sono quindi 3 le caratteristiche principali di tale criptovaluta:

-La scalabilità: è la quantità di transazioni che la piattaforma riesce a supportare.

EOS progetta di poter confermare le transazioni in meno di 10 secondi, così da evitare le congestioni del sistema.

-La flessibilità: consiste nella possibilità di poter bloccare l'operazione nel caso in cui si verificasse un errore. Se per esempio l'indirizzo del destinatario fosse sbagliato, il denaro digitale inviato non verrebbe perso, ma grazie alla reversibilità tornerebbe al mittente, che potrà effettuare nuovamente la transazione senza intoppi.

-L'usabilità: è la possibilità per tutti, anche coloro che non dispongono di una conoscenza informatica avanzata, di poter capire come funziona questa piattaforma, è ritenuta infatti più semplice di *Ethereum*.⁴⁶

⁴⁶ Cfr. GATTI M. , "Eos è già nel futuro: ecco cos'è e come funziona", www.CryptoMinando.it , 2 Febbraio 2018.

Capitolo 2 - Riflessioni e andamento nei mercati

2.1 Principali punti di debolezza e critiche del *Bitcoin* e delle altre *Cryptocurrencies*

A dispetto delle tante novità ed innovazioni che le varie criptovalute, in maniera particolare il *Bitcoin*, hanno presentato all'intero universo economico, bisogna riconoscere che vi sono anche diversi punti opinabili che hanno portato le stesse ad esser viste spesso con diffidenza.

È importante premettere comunque che, dopo una fase di forte scetticismo verso questo nuovo strumento che era ancora tutto da esplorare, con il passare del tempo vi è stata una sempre maggiore approvazione ed avvicinamento verso tale realtà; ad oggi, infatti, oltre ad esserci un maggiore utilizzo delle valute digitali e delle tecnologie che le contraddistinguono, va rimarcato come il numero di criptovalute sia aumentato in maniera esponenziale, proprio a certificazione di come questo venga visto da molti come un discreto mercato in cui poter operare.

Si sono espressi a riguardo anche organismi di grande rilievo, come Banca D'Italia, che nel 2015 ha stipulato un elenco in cui vennero presentati i principali punti deboli e problemi connessi alle criptovalute,⁴⁷ unitamente ad organizzazioni quali l'Autorità europea degli strumenti finanziari e dei mercati *ESMA* (*European Securities and Markets Authority*), l'Autorità bancaria europea *EBA* (*European Banking Authority*) e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali *EIOPA* (*European Insurance and Occupational Pensions Authority*).⁴⁸

Le tre Autorità in esame⁴⁹ ritengono preoccupante il crescere del numero dei risparmiatori che acquista criptovalute, spesso con l'aspettativa di vederne continuamente aumentare il valore, senza tuttavia essere in alcun modo consapevoli dell'alto rischio di perdere il denaro investito, in quanto sorge un problema di tutela del consumatore stesso.

⁴⁷ Cfr. Banca D'Italia, "avvertenza sull'utilizzo delle cosiddette valute virtuali", 30 Gennaio 2015

⁴⁸ Cfr. Consob, "ESMA, EBA ed EIOPA avvertono i consumatori circa i rischi delle criptovalute", 9 Marzo 2018

⁴⁹ EBA, ESMA e EIOPA sono 3 autorità di vigilanza europea. La prima è l'autorità bancaria europea ed ha il compito di supervisionare e mantenere la stabilità finanziaria tramite determinati compiti. L'ESMA corrisponde all'autorità europea degli strumenti finanziari e dei mercati ed agisce a tutela degli investitori e del corretto funzionamento dei mercati. Infine l'EIOPA è l'autorità europea delle assicurazioni e delle pensioni aziendali e professionali e il suo ruolo è quello di contribuire alla protezione degli assicurati e degli iscritti e beneficiari dei sistemi pensionistici.

2.1.1 (Segue) Eccesso di volatilità

Con ogni probabilità è il punto più dolente e maggiormente criticato; del resto, come dar torto a chi afferma che tali strumenti, almeno per ora, non possano svolgere altra funzione oltre a quella connessa all'attività di mera speculazione, come Mario Draghi, che sostiene che *“una moneta dovrebbe anche essere una riserva di valore, in modo tale che si possa essere sicuri di poter acquistare più o meno lo stesso quantitativo di cose oggi, domani o il prossimo anno”*.⁵⁰

Questo avviene anche a causa dei meccanismi di formazione dei prezzi (talora opachi) e dall'assenza di un'autorità centrale in grado di intervenire per stabilizzarne il valore.

Tale circostanza può comportare perdite anche di rilevante entità in caso di detenzione di valuta virtuale.

Probabilmente, solo con prezzi che presenteranno maggiore stabilità, più persone inizieranno ad utilizzare i *Bitcoin* come mezzo di pagamento; negli ultimi mesi, peraltro, le transazioni richiedono più tempo e sono divenute più costose, dunque alla volatilità va ad aggiungersi il fatto che usare i *Bitcoin* per pagamenti di poca entità è divenuto meno conveniente.

La tecnologia alla base di questi strumenti è però ancora giovane, motivo per cui non è detto che questi problemi non si possano risolvere in futuro, favorendo le transazioni commerciali in *Bitcoin* ed altre valute digitali.

Molto chiaro a riguardo è il pensiero di Luca Fantacci, docente di Storia e istituzioni del sistema finanziario alla Bocconi, che afferma: *“Il white paper di Satoshi Nakamoto prometteva una moneta elettronica senza intermediari non basata sulla fiducia, un contante digitale. Questa promessa non è stata mantenuta: nei suoi primi 10 anni, Bitcoin è stato usato più come oggetto di speculazione che come moneta. Nel futuro prossimo potrebbe diventare un mezzo di pagamento non al dettaglio, bensì all'ingrosso, cioè uno strumento di regolamento all'interno di sistemi di compensazione, come l'oro nel commercio internazionale”*.⁵¹

La loro volatilità li rende inadatti ad essere usati come valuta e come mezzo di pagamento, in quanto caratterizzate spesso da oscillazioni violente che comportano la variazione di valore in un lasso di tempo anche molto breve.

Volendo citare un caso particolare per rendere meglio il concetto, consideriamo la prima transazione con *Bitcoin* nel 2011: allora, ignorando ovviamente l'esplosione che tale valuta digitale avrebbe avuto

⁵⁰ Cfr. LOPS V. , “5 motivi per cui il *Bitcoin* è un asset rischioso”, Il Sole 24 ore, 14 Febbraio 2018

⁵¹ Cfr. SOLDAVINI P. , “tra speculazione e rivoluzione:10 anni in altalena con i *Bitcoin*”, Il sole 24 ore, 31 Ottobre 2018

nel giro di pochi anni, furono acquistate 2 pizze per 10mila *Btc*, che oggi varrebbero una cifra intorno ai 60 milioni di dollari!

Questo lascia immaginare quanto, per via della forte volatilità che contraddistingue tali criptovalute, possa essere poco conveniente effettuare pagamenti con le stesse.

Ciononostante vi sono state diverse società ad aprire le proprie porte alle monete digitali, anche se qualcuna si è dovuta ricredere con il passare del tempo.

Stripe dal 2015 ha accettato la possibilità di utilizzare il *Bitcoin* come strumento di regolamento delle proprie vendite.

Da quel momento in poi, gradualmente in tutto il mondo, tutti i commercianti che utilizzavano la piattaforma di *Stripe*, hanno iniziato ad accettare pagamenti in *Bitcoin*: una mossa strategica piuttosto apprezzata, che poteva promuovere la diffusione su larga scala dell'oro digitale come mezzo di pagamento universalmente accettato dal grande pubblico.

Quei positivi auspici sono, però, stati evidentemente traditi.

Le attenzioni crescenti nei confronti di questa criptovaluta, e il forte sviluppo della sua capitalizzazione, non hanno infatti coinciso con la ricerca di una maggiore efficienza tecnica ed economica.

Ne è risultato quindi un utilizzo della *blockchain* più farraginoso, con tempi di validazione troppo lunghi, e commissioni ancora troppo elevate per poter rendere i pagamenti in *Bitcoin* un reale mezzo in grado di competere con altre forme di regolamento più tradizionali, facendo sì che *Stripe* non accettasse più pagamenti in valuta digitale.

Un'altra delle forti cause di tale decisione fu l'alta volatilità di tale strumento, che portò spesso a situazioni paradossali che vedevano operazioni errate in controvalore, poiché nell'arco di tempo che intercorre tra l'avvenuta transazione e la sua validazione, le fluttuazioni del prezzo della criptovaluta sono state in grado di determinare un importo differente rispetto al prezzo di pagamento.⁵²

2.1.2 (*Segue*) Possibilità di usi illeciti

Sicuramente anche questo aspetto non può assolutamente essere ignorato, in quanto, nel corso degli anni, vi sono stati diversi episodi in cui sono state registrate numerose operazioni mediante criptovalute per il sostenimento di fini illeciti, come ad esempio il riciclaggio di denaro.⁵³

⁵² Cfr. “*E-commerce: conviene accettare pagamenti in criptovalute? Stripe dice no a Bitcoin*”, www.wildseo.it, 3 Aprile 2018

⁵³ Cfr. Banca D'Italia, “avvertenza sull'utilizzo delle cosiddette valute virtuali”, cit.

In particolare, le cause più valide che favoriscono tali finalità risiedono nella natura stessa di strumenti come il *Bitcoin*; infatti, la maggior difficoltà nel tracciamento dettata dall'anonimità di chi compie delle transazioni e l'assenza di un organismo centrale aiutano non poco.

Incredibile come, tramite numerose indagini di Banca d'Italia, è stato scoperto che anche organizzazioni criminali come 'ndrangheta e camorra stanno probabilmente utilizzando le criptomonete per il perseguimento di finalità illecite, come quella di rimettere in circolazione i soldi "sporchi".

Il quotidiano "L'Espresso" parla addirittura di un "criptopizzo", una vera e propria estorsione informatica ispirata all'attività praticata dai mafiosi ed applicata online.

Lo stesso ha indagato intorno al lato oscuro della criptovalute, frequentato da criminali di ogni risma, inclusi pedofili, truffatori e mafiosi, appunto, che già da due anni fanno transazioni di *Bitcoin* con l'obiettivo di ripulire il denaro sporco dei traffici di droga, di truffe, estorsioni e usura.

Si sostiene che già da quattro anni i clan di camorra hanno scommesso sul conio virtuale.

Le recenti informative degli investigatori dell'UIF⁵⁴ indicano con precisione le "segnalazioni di operazioni sospette", in cui compaiono i nomi di personaggi dal notevole *pedigree* criminale.

In particolare uomini e donne vicini alla camorra napoletana, clan di Napoli e alcuni della zona di Caserta, area sotto il dominio del famigerato clan dei Casalesi.

Nel 2015 i personaggi legati alla camorra napoletana monitorati dall'UIF hanno investito all'incirca un milione di euro secondo delle indagini; oggi, quello sporco malloppo di *Bitcoin*, acquistati a poco meno di 500 euro cadauno, è diventato un'importante massa di milioni, dunque si ha a che fare con del denaro che non solo è stato ripulito, ma che addirittura è anche aumentato notevolmente.

"Riciclare attraverso l'acquisto di Bitcoin? È il fenomeno a cui stiamo assistendo. E non mi stupirei se anche le organizzazioni mafiose lo stessero facendo", spiega Taverna, direttore tecnico principale della polizia postale, la massima autorità di *intelligence* per il contrasto dei delitti sul *web*, che aggiunge un dettaglio: *"Il più delle volte avviene con la complicità degli exchanges, le società che cambiano valute correnti in virtuali"*.

Il motivo di questa ambiguità sta nel fatto che queste *holding* offrono una gamma variegata di servizi finanziari anonimi. *"Il problema è che spesso mischiano più Bitcoin provenienti da più indirizzi e permettono di convertirli con altre criptovalute. A quel punto le poche tracce svaniscono e risulta impossibile ricostruirne il tragitto. È un servizio che gli exchanges dichiarano lecito, tuttavia molte volte li rende complici di chi vuole ripulire il denaro sporco"*, osserva l'investigatore.

⁵⁴ UIF: Unità di Informazione Finanziaria per l'Italia

Sembra incredibile, ma queste società non hanno alcun obbligo antiriciclaggio.⁵⁵

Un'altra ricerca, condotta da Sean Foley (Università di Sidney), Jonathan R. Karlsen (University of Technology Sydney), e Talis J. Putnins (Stockholm School of Economics di Riga), evidenzia come circa il 40% delle transazioni di *Bitcoin* sia potenzialmente associabile ad attività di tipo illecito come finanziamenti dei gruppi terroristici, strumenti per il riciclaggio di denaro o per eludere i controlli fiscali.

Negli ultimi mesi si sono però scontrate numerose opinioni contrastanti a riguardo, con tesi che vanno invece a sminuire l'ipotesi di un così forte utilizzo delle criptovalute per finalità meramente illegali.

La Stampa, ad esempio, sostiene che, malgrado i numerosi allarmi che sono stati lanciati nel tempo, i numeri legati a tali attività non sono così elevati come molti sostengono e vanno ridimensionati.

Premettendo comunque che i dati a disposizione non sono molti e soprattutto non sono certi e concreti, in uno scenario incerto ed in continua evoluzione, viene sostenuto che le paure maggiori sono legate a molte criptovalute che offrono un maggior grado di anonimato rispetto al *Bitcoin*, poichè quest'ultimo genererebbe un problema di identità, nel senso che le transazioni possono essere ricondotte ai loro autori a meno di non intraprendere molti passaggi.

Insomma non è un mezzo semplice per la raccolta fondi in ambito terroristico, a differenza di altre valute digitali.

Secondo uno studio fatto in collaborazione tra una nota società che fa indagini su criptovalute, *Elliptic*, e il *Centre on Sanctions of Illicit Financing*, che si occupa di terrorismo, criminalità, corruzione e riciclaggio, gran parte del flusso di transazioni illecite proveniva dai mercati neri della droga, come (l'ormai defunto) *AlphaBay*.⁵⁶

Inoltre, secondo la ricerca, buona parte di quelle transazioni illecite sarebbero passate attraverso servizi di conversione europei.

Come dire: l'Europa non ne esce benissimo.

Ma il dato dipende probabilmente dal periodo esaminato, fra 2013 e 2016.

Negli ultimi anni infatti le maglie dei controlli si sono fatte più strette sul Vecchio Continente.

“Ultimamente i servizi di cambio europei, gli exchange, sono migliorati”, riconosce Fanusie, direttore del *Center on Sanctions and Illicit Finance*.

⁵⁵ Cfr. TIZIAN G. , “I *Bitcoin* piacciono anche alla mafia: così ‘ndrangheta e camorra riciclano denaro” , L'Espresso, 24 Gennaio 2018

⁵⁶ *AlphaBay* è stato uno dei più importanti *black market* del *Dark Web*, in cui venivano trattati strumenti come armi, documenti falsi, strumenti chimici, droga o qualsiasi tipo di servizi illegali.

Tale sito è stato ufficialmente chiuso il 4 Luglio 2017 con la successiva scoperta di oltre 350mila scambi illegali ed il giorno successivo, in Thailandia, è stato arrestato Alexandre Cazes, 26enne Canadese, tra gli utenti a capo della piattaforma, suicidatosi pochi giorni dopo in carcere.

Come già detto in precedenza, l'Europa si sta muovendo molto su questo terreno.⁵⁷

Non a caso il tema della regolazione del mercato in esame è un argomento molto caldo e tramite l'emanazione della direttiva 2018/843 del Parlamento Europeo e del Consiglio è stato fatto un gran passo in avanti, in quanto l'Europa riconoscerà ufficialmente le monete digitali, come hanno già fatto paesi come il Giappone, dove le criptomonete sono considerate come un'alternativa alla valuta tradizionale emessa dalle autorità.

Anche la *Duma* (il Parlamento della Russia) esaminerà un nuovo progetto di legge sulla regolamentazione delle attività finanziarie digitali, tra cui le *criptocurrencies*; lo ha annunciato il capo della Commissione della *Duma* sui mercati finanziari, *Anatoly Aksakov*, durante una conferenza stampa, affermando di aver presentato un disegno di legge alla fine di Dicembre e prevedendo importanti cambiamenti già nel mese di Febbraio del 2019.⁵⁸

Addirittura, lo scorso anno, Mosca ha confermato il via libera di *Vladimir Putin* allo studio di uno speciale “*criptorublo*”. A premere per il “*Bitcoin* russo” pare sia stato in particolare *Sergei Glazev*, consulente economico del Cremlino, che in un recente incontro con *Putin* ha sottolineato come il *criptorublo* permetterebbe a Mosca di saldare i pagamenti con le controparti in tutto il mondo dimenticando le sanzioni.⁵⁹

L'obiettivo di questa regolamentazione va ricercato nella necessità di aumentare la sicurezza e la tracciabilità delle monete digitali, attraverso l'obbligo del riconoscimento e dell'utilizzo, con la finalità di tutelare gli interessi degli investitori.

2.1.3 (*Segue*) Non è altro che una bolla speculativa!

Altro tema fortemente valido è, senza alcun dubbio, il timore che numerosi investitori, spesso anche di un certo calibro, nutrono nei confronti di tali strumenti; sono stati diversi, infatti, i casi in cui delle affermazioni degli stessi hanno causato discese, anche violente, delle *criptocurrencies*.

Difficile potersi prontamente sbilanciare a riguardo, in quanto, nonostante i risultati pazzeschi che sono stati raggiunti negli ultimi anni, non si può certamente ignorare la forte discesa che li ha visti come protagonisti negli ultimi 12 mesi.

⁵⁷ Cfr. FREDIANI C. , “*Bitcoin* e riciclaggio: tutto quello che sappiamo”, www.LaStampaItalia.it, 6 Febbraio 2018

⁵⁸ Cfr. CAVICCHIOLI M. , “Russia: progetto di legge per la regolamentazione crypto entro due mesi”, www.TheCryptonomist.it, 14 Gennaio 2019

⁵⁹ Cfr. MARRO E. , “*Putin* studia un «criptorublo» per aggirare le sanzioni occidentali”, *Il Sole 24 Ore*, 2 Gennaio 2018

Tale fenomeno, infatti, non ha fatto altro che alimentare critiche, scetticismi ed anche un pò di paura, mediante numerosi accostamenti alle bolle speculative degli anni passati.

Una “bolla speculativa” consiste in una particolare situazione del mercato azionario, caratterizzata da un’eccessiva euforia degli investitori, causata da una marcata sopravvalutazione di un’azienda, di un mercato o di una qualunque cosa che possa essere oggetto di investimento.

Quando un prodotto finanziario è sopravvalutato diventerà anche più richiesto, il che gonfierà ulteriormente la sua valutazione.

Il fenomeno delle bolle speculative rappresenta un esempio di come i mercati finanziari, spesso, si muovano seguendo dinamiche irrazionali, tant’è che è possibile definire le bolle come anomalie legate a fattori psicologici.

Il desiderio di un guadagno facile, assieme all’ondata di entusiasmo collettivo, fa sì che l’investitore tenda ad agire impulsivamente.

Ogni bolla finanziaria ha origine da uno spostamento di massa dell’interesse verso un particolare oggetto di investimento all’interno del mercato.

Un elemento chiave, inoltre, sono i tassi di interesse, dato che questo tipo di operazione è caratterizzata da un’elevata leva finanziaria; avviene, infatti, che gli investitori prendano in prestito denaro, mossi dalla convinzione di trovarsi davanti ad un guadagno sicuro e facile.

Quest’ultimo aspetto è il principale motivo per cui lo scoppio di una grossa bolla può portare una crisi sistemica del sistema economico-finanziario.

L’eccesso di liquidità presente nel mercato, grazie ai bassi tassi di interesse, contribuisce a gonfiare gli *asset*, finendo per ingrandire la bolla.⁶⁰

Tra i “big” del mercato mondiale c’è chi, come il premio Nobel *Nouriel Roubini*, sostiene che “*il Bitcoin inizia a sembrare come un dinosauro in via di estinzione*”, o chi, come Mario Draghi, è ancora più drastico, affermando che “*il Bitcoin è la combinazione di una bolla, uno schema Ponzi⁶¹ ed un disastro ambientale*”.

Addirittura anche veri e propri mostri sacri della finanza e degli investimenti, come *Warren Buffett*, *George Soros* o *Jamie Dimon*, amministratore delegato della *JP Morgan*, si inseriscono di prepotenza nella categoria degli scettici, con affermazioni spesso anche forti e che non hanno fatto certamente bene alle criptovalute.

⁶⁰ Cfr, SANNINO A. , “Le bolle speculative”, *www.StartingFinance.it*, 2017

⁶¹ Lo schema Ponzi è un modello economico di vendita, ideato dall’Italiano immigrato negli Stati Uniti Carlo Ponzi, che spesso si cela dietro operazioni commerciali apparentemente sicure, ma che in realtà, si rivelano fortemente dannose per tutti gli investitori.

Il punto di forza di tale piano è, oltre ad una meticolosa organizzazione, la promessa di investimenti sicuri con alti rendimenti.

Vi sono stati anche diversi accostamenti delle valute digitali con la bolla dei Tulipani del 1637, considerata come la prima grande crisi finanziaria nella storia del capitalismo, causata anch'essa da finalità puramente speculative e quella delle *dot-com*.

L'analogia con la prima bolla viene pensata poiché anche in quel caso (nei Paesi Bassi) la domanda di uno strumento, quali i bulbi di Tulipano, raggiunse un picco così alto da causare in breve tempi prezzi enormi, in realtà causati esclusivamente dalla speculazione.

Il bulbo di Tulipano diventò quindi il quarto principale prodotto di esportazione dei Paesi Bassi, fino a perdere, in un lasso di tempo molto breve, tutto il suo valore, facendo scomparire per moltissime persone somme ingenti di denaro da un giorno all'altro, con centinaia di olandesi, inclusi facoltosi uomini di affari, che caddero in rovina finanziaria.⁶²

Va detto però che non sembra del tutto appropriato paragonare le due cose, non perché si vuole escludere l'ipotesi di una bolla speculativa alla base del *Bitcoin*, ma perché c'è una fondamentale differenza riguardante il valore intrinseco dei 2 beni che non consente di ritenere corretto questo accostamento.

Infatti la bolla dei tulipani riguardava il valore dei bulbi di tulipano, ovvero una merce dal valore intrinseco piuttosto basso, che però scatenò una vera e propria corsa all'acquisto speculativo.

Con un'analisi superficiale anche il *Bitcoin* (che non ha valore intrinseco) potrebbe fare la stessa fine, ma non può sfuggire una differenza sostanziale: chi acquistava bulbi di tulipano si impossessava di un bene fisico non particolarmente scarso, facilmente replicabile, e dal valore intrinseco molto basso, pagandolo prezzi spropositati gonfiati dalla bolla speculativa.

Chi invece acquista *token BTC* acquista un mezzo di scambio virtuale relativamente raro, non replicabile, senza valore intrinseco, ma sempre e comunque utilizzabile come mezzo di scambio, il cui valore è semplicemente quello che il mercato gli dà.⁶³

Per quanto riguarda la famosa e più recente bolla delle *Dot-com*, alla fine degli anni novanta vi fu un rapido aumento del valore delle aziende operanti nell'ambito di internet e dell'informatica.

Il periodo fu segnato dalla fondazione (e successivi fallimenti) di numerose piccole aziende con lo scopo sociale di svolgere attività nel settore legato a Internet e più in generale nel settore informatico e generalmente chiamata *Dot-com*; erano compagnie scarsamente capitalizzate, di piccole dimensioni (in molti casi con un solo azionista fondatore), molto esposte in un settore fortemente sovrastimato.

Una serie di eventi lasciava presagire un andamento di mercato sempre migliore, come l'aumento della fiducia degli investitori o l'incremento dei prezzi delle azioni, ma, tra il 2000 ed il 2001 ci si

⁶² Cfr. Consob, "la bolla dei tulipani", Educazione finanziaria, le crisi finanziarie

⁶³ Cfr. CAVICCHIOLI M., "Ecco perché è sbagliato associare la bolla dei Tulipani al Bitcoin", www.ilBitcoin.it, 3 Dicembre 2017

rese conto di trovarsi dinanzi ad una bolla finanziaria a tutti gli effetti, con forti precipitazioni del valore dei titoli ed il fallimento di diverse società.⁶⁴

Anche in questo caso non è però pienamente corretto associare le 2 fasi economiche per determinati motivi: innanzitutto dopo lo scoppio della bolla delle *dot-com*, il *Nasdaq Composite index* ha continuato a crollare, senza sosta, fino a tornare ad una quota pari a quella pre-bolla (1.172,060), come del resto ci si aspetta che accada quando si innesca una bolla finanziaria.

Invece, dopo il raggiungimento dei massimi storici di fine 2017, il prezzo di *Bitcoin* sembra essersi stabilizzato dopo un periodo di forti perdite, a differenza di quanto avvenuto nel primo caso.

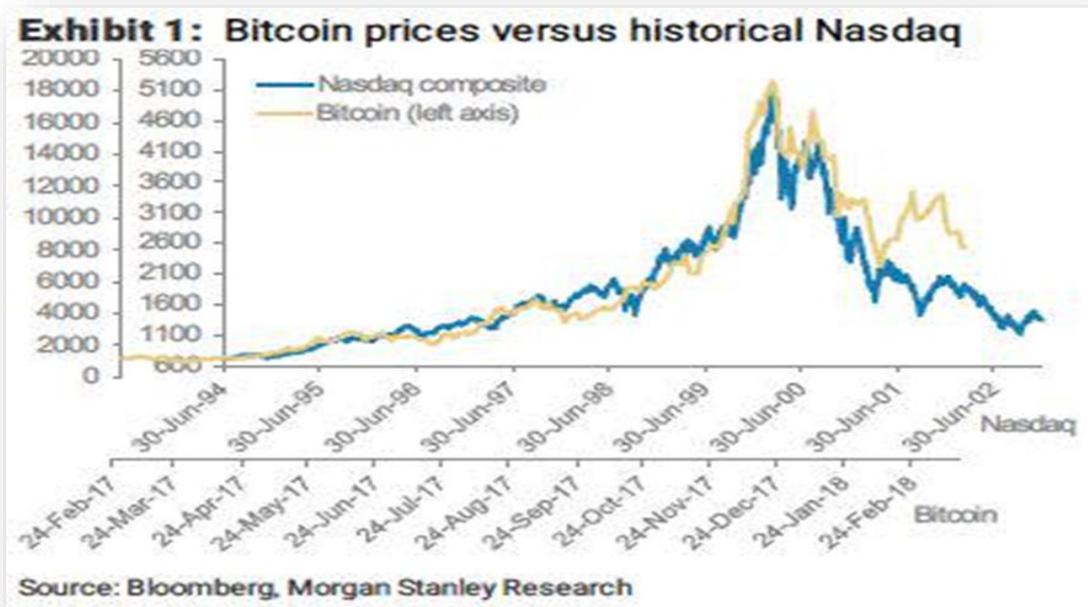
La seconda differenza è che prima dell'innescarsi della bolla delle *dot-com*, il *Nasdaq Composite index* era in costante crescita, anno su anno: 4 anni di crescita che lo hanno portato da 755 a 2.505.

Invece *Bitcoin* negli anni precedenti al 2017 era rimasto sostanzialmente fermo, passando da 754 dollari di inizio 2014 a 951 di fine 2016.

La terza è l'incremento annuale durante la bolla: il *Nasdaq Composite index* nel 1999 è passato da 2.505 a 4.696, con un incremento inferiore al 100%.

Invece *Bitcoin* nel 2017 è passato da 959 dollari a 14.297, con un incremento di quasi il 1.400%.⁶⁵

Figura 2: Fonte *Bloomberg*, prezzo del *Btc* rispetto al *Nasdaq* negli anni della crisi.



⁶⁴ Cfr. Consob, "La bolla delle C.D. Dotcom", Educazione finanziaria, Le crisi finanziarie

⁶⁵ Cfr. CAVICCHIOLI M., "La bolla di Bitcoin non è come quella delle Dot-Com", www.ilBitcoin.it, 18 Settembre 2018

2.1.4 (Segue) L'emissione di *Bitcoin*

L'aspetto relativo all'attività di *Mining* è comunque da dover valutare con scrupolosità per quanto riguarda determinati aspetti.

Innanzitutto, bisogna partire dal presupposto che, come già detto in precedenza, il *Mining* è il sistema attraverso il quale ogni transazione viene verificata e aggiunta all'interno del pubblico registro distribuito conosciuto come *blockchain*, ma è anche il processo che rende possibile l'emissione dei nuovi *coins* fino al raggiungimento di 21 milioni di *token*.

Sebbene il *mining* sia un'attività libera, che chiunque può svolgere, la complessità dei calcoli che stanno alla base della creazione di un *Bitcoin* può essere affrontata solo da chi possiede degli *hardware* specializzati.

Di conseguenza, è necessario interrogarsi sulla buona fede e l'affidabilità dei minatori – il cui numero risulta essere comunque circoscritto – nello svolgere le funzioni di gestione e controllo.

I maggiori timori riguardano cioè il fatto che la maggior parte dei *Bitcoin* potrebbe essere posseduta da un piccolo gruppo che li promuove e che questa esclusività possa essere appannaggio di interessi poco leciti, e, in effetti, non sarebbe del tutto da escludere tale ipotesi in un mercato in cui (la Storia insegna) è possibile attendere sempre nuove sorprese.

Negli ultimi tempi si sono accesi anche i riflettori degli ambientalisti: la produzione e lo scambio dei *coin* divora energia, tanto da poter far aumentare di due gradi la temperatura media globale.

Paradossalmente, però, il vero problema, o quantomeno il più concreto, è quello relativo agli elevatissimi consumi sostenuti per poter svolgere tali attività di creazione di moneta virtuale.

La rete *Bitcoin* può essere attualmente stimata con un consumo di almeno 2,55 *gigawatt* di elettricità, e potenzialmente più di 7 *gigawatt* in futuro, paragonabili a paesi come l'Irlanda (3,1 *gigawatt*) e l'Austria (8,2 *gigawatt*).

I modelli economici ci dicono inoltre che il consumo energetico di *Bitcoin* tenderà ad aumentare sempre di più con il passare del tempo.⁶⁶

L'elettricità impiegata nel *mining* di *Bitcoin* è quindi tra i maggiori temi che circondano il mondo delle criptovalute e si colloca di diritto tra i più preoccupanti.

L'energia necessaria non è poca, poichè vengono richiesti grandi quantità di calcoli *hash* per processare le transazioni finanziarie; secondo alcuni studi, infatti, il consumo energetico relativo a tali attività si aggira intorno allo 0,30% del consumo mondiale totale, un valore che probabilmente tenderà ad aumentare in breve tempo raggiungendo lo 0,50% della domanda mondiale di consumo.

⁶⁶ Cfr. PICANO F. , “Un’analisi sul grande consumo di energia per il minino di *Bitcoin*”, www.Bioterra.it, 20 Giugno 2018

Si tratta di valori macroscopici; basta pensare, infatti, che si sta raggiungendo il consumo energetico annuale dell' Austria, un paese di quasi 9 milioni di abitanti.

Questa previsione preoccupante è opera dell'economista esperto di finanza *Alex de Vries*, che ha affermato: “*la maggior parte delle persone sono scioccate dal fatto che Bitcoin possa usare tanta energia. Penso che sia una reazione appropriata.*”

Mezzo punto percentuale dell'energia mondiale è una quantità enorme, soprattutto per un sistema che in realtà viene utilizzato solo per fare speculazione.”

Questo pensiero lo ha portato a non essere molto amato tra gli investitori *online*, che percepiscono le affermazioni come un attacco ingiusto a *Bitcoin*.

Va detto, tuttavia, che lo stesso *de Vries* è il primo a riconoscere che le sue stime non sono ancora qualificabili come dati certi.

Può essere impossibile conoscere l'esatto consumo energetico della rete *Bitcoin*, ma i limiti superiori e inferiori del suo consumo energetico possono essere comunque calcolati in modo affidabile utilizzando modelli economici. Migliorare l'accuratezza di questi modelli, tuttavia, richiede un sacco di informazioni che semplicemente al momento non sono disponibili nello spazio ancora in gran parte non regolamentato delle criptovalute, ha detto *de Vries*.

Lo stesso ritiene che, in futuro, sarà possibile ottenere informazioni più dettagliate sul consumo energetico di *Bitcoin* mediante una certa cooperazione tra i vari Paesi, che dovrebbero andare a segnalare delle attività di *mining* che superano una certa dimensione, come già deciso in Russia a partire dal 2018.

Al momento ci sono poche soluzioni per impedire a *Bitcoin* di consumare più elettricità.

I più ottimisti sul futuro dei *Bitcoin*, prevedendo un forte aumento di valore degli stessi, ritengono che i livelli di energia consumata dal sistema cresceranno ancora di più in quanto sarebbe più redditizio che mai estrarre *Bitcoin*.

Invece, coloro che considerano che l'economia di *Bitcoin* stia soltanto attraversando una fase di bolla, prevedono un conseguente crollo della domanda di energia elettrica.

Sono anche al vaglio soluzioni tecniche come *Lightning Network*, che elaborerebbe le transazioni al di fuori della *blockchain* principale di *Bitcoin* e quindi abbatterebbe in modo significativo il costo dell'energia per transazioni di tali strumenti.

Un'altra alternativa è quella di utilizzare l'energia eolica e altre forme di energia pulita per il *mining* di *Bitcoin*.⁶⁷

⁶⁷ Cfr. OBERHAUS D. , “Il consumo energetico di *Bitcoin* è la prossima emergenza ambientale”, www.Motherboard.it, 21 Maggio 2018

2.1.5 (*Segue*) Assenza di tutele legali e contrattuali

L'acquisto, lo scambio e l'utilizzo di valute virtuali non sono assistiti da tutele legali e/o contrattuali analoghe a quelle che accompagnano le operazioni in valuta legale; le transazioni in valuta virtuale sono generalmente irreversibili, spesso non sono supportate da un contratto né da procedure di reclamo e le controparti sono anonime; in ogni caso, la mancanza di definizioni, di *standard* legali e di obblighi informativi renderebbe difficile provare in giudizio di aver subito un danno ingiusto.

E' possibile che l'utilizzo o la conversione di valute virtuali siano soggetti a costi e commissioni non chiaramente indicati.⁶⁸

Le transazioni in *Bitcoin* una volta eseguite non possono inoltre essere in alcun modo contestate.

A causa dell'assenza di strumenti di risoluzione delle controversie a tutela delle parti, le transazioni in *Bitcoin* comportano pertanto sempre un certo livello di rischio a carico degli utenti, seppure mitigato dall'immunità dal controllo statale e all'eventuale confisca da parte di un'autorità centrale.

La correzione di una transazione errata, che si tratti di inadempimento di contratto o di frode, è possibile solo attraverso un accordo volontario delle parti coinvolte nello scambio.

Questi fattori non possono che avere un forte effetto sfavorevole sull'uso di *Bitcoin* rispetto a quello delle valute *standard*, in particolare considerando la categoria degli operatori dei mercati finanziari avversi al rischio.⁶⁹

A rendere la tutela dell'investitore ancora più complicata si aggiunga la frequente difficoltà ad individuare il soggetto intermediario, oltre al territorio e la giurisdizione di riferimento, dove poter intervenire a tutela dei propri interessi ove lesi.

Al momento non ci sono ricette pronte a prevenire i "mali" delle criptovalute né tanto meno a curarli, tuttavia è possibile fissare dei principi che l'investitore intenzionato ad investire in criptovalute attraverso portali detti *exchanger*, deve seguire.

Qualche criterio ci viene fornito dall'unica sentenza italiana e da alcune delibere Consob che ci aiutano a comprendere quando ci possa essere una competenza delle autorità italiane ad intervenire e quali strumenti legali azionare.

Il Tribunale di Verona con la sentenza n. 195 del 2017, ha stabilito la "nullità" del contratto intercorso fra un utente italiano ed una piattaforma facente capo ad una società italiana che aveva corrisposto valuta avente corso legale in cambio di Bitcoin e quindi la restituzione della somma investita.

⁶⁸ Cfr. Banca D'Italia, "avvertenza sull'utilizzo delle cosiddette valute virtuali", cit.

⁶⁹ Cfr. LEMME G. e PELUSO S., Criptomoneta e distacco dalla moneta legale: il caso *Bitcoin*, in Riv. dir. banc., dirittobancario.it, 43, 2016

Il giudice accogliendo le domande dell'utente ha accertato che aveva agito da consumatore e l'attività svolta dal portale era stata condotta in violazione degli obblighi legali di forma e di informativa precontrattuale previsti agli art. 67-*duodecies* del Codice del Consumo.⁷⁰

Il Tribunale ha ritenuto che al rapporto conclusosi *on-line* si applicassero le norme relative alla fornitura dei servizi finanziari ai consumatori italiani nelle operazioni di cambio di valuta in corso contro unità di criptovaluta e in particolare le previsioni relative alla commercializzazione a distanza di servizi finanziari ai consumatori.

Queste prevedono che il consumatore ha diritto a ricevere tutta una serie di informazioni, prima che lo stesso sia vincolato da un contratto a distanza o da un'offerta.

Ad esempio l'identità, anche geografica, del fornitore e del suo rappresentante; l'identità del professionista e della veste in cui esso agisce nei confronti del consumatore; l'iscrizione del fornitore in un registro commerciale o analogo pubblico registro, come pure l'assoggettamento e gli eventuali estremi dell'autorizzazione amministrativa necessaria per le attività così svolte; le principali caratteristiche del servizio finanziario offertogli; il meccanismo di formazione del prezzo, in senso lato; il rapporto con strumenti che implicano particolari rischi dovuti a loro specifiche caratteristiche o alle operazioni da effettuare, o il cui prezzo dipenda dalle fluttuazioni dei mercati finanziari su cui il fornitore non esercita alcuna influenza; i rimedi che gli sono attribuiti dall'ordinamento; lo Stato membro o gli Stati membri sulla cui legislazione il fornitore si basa per instaurare rapporti con il consumatore prima della conclusione del contratto a distanza.

La decisione di Verona è inequivocabile: gli *exchanger* forniscono servizi finanziari: devono inderogabilmente rispettare gli obblighi informativi precontrattuali verso l'investitore/consumatore che ha diritto di pretenderli.

Nel caso in cui la piattaforma facesse capo ad un soggetto straniero, l'applicazione del diritto italiano non è scontata, potendo ricorrere solo in determinate situazione ed a certe condizioni.

Come emerge ad esempio da due delibere Consob (n 19968/2017 e 2027/2017), i siti redatti in lingua italiana rappresentano elementi "inequivocabili" circa il fatto che l'offerta di investimenti sia rivolta al pubblico residente in Italia con la conseguenza che al ricorrere di certe condizioni anche i soggetti stranieri sono assoggettabili alla legge italiana.

In particolare alle disposizioni del Testo Unico della Finanza (TUF).

La Consob ha chiaramente stabilito che i "pacchetti di estrazione di criptovalute" hanno la natura di "prodotto finanziario sub specie di investimento di natura finanziaria" lì dove implicino la

⁷⁰ Art. 67-*duodecies* del Cod. del Consumo: Diritto di recesso

compresenza di un impiego di capitale, un'aspettativa di rendimento di natura finanziaria, l'assunzione di un rischio connesso all'impiego di capitale.

Ebbene, davanti a questo tipo di prodotti finanziari, venduti in termini standardizzati e uniformi, si profila quindi un'ipotesi di un'offerta al pubblico definita nell'art. 1, comma 1, lett. t del TUF con conseguente obbligo preventivo di pubblicazione di un prospetto informativo a tutela dell'investitore. Inoltre “prima della pubblicazione del prospetto è vietata la diffusione di qualsiasi annuncio pubblicitario riguardante offerte al pubblico di prodotti finanziari diversi dagli strumenti finanziari comunitari”.

In conclusione, la prima buona norma da seguire è la prudenza: l'investitore deve richiedere tutte le informazioni necessarie ad individuare i soggetti emittenti e soprattutto la tipologia delle criptovalute che si intendono acquistare.

Solamente partendo da qui si può da subito disegnare il perimetro della tutela legale.⁷¹

2.1.6 (*Segue*) Rischio informatico

Un altro rischio nell'investimento in criptovalute e *Bitcoin* risiede nei possibili attacchi *hacker* a danno dell'investitore, unitamente a possibili malfunzionamenti tecnologici che potrebbero bloccare il proprio portafoglio; inoltre, in caso di smarrimento della *password* del portafoglio elettronico, la perdita potrebbe essere permanente, non essendoci autorità centrali che registrano le *password* o ne emettono altre sostitutive.⁷²

Il rischio nella detenzione di *Bitcoin* è dovuto al fatto che non c'è nessuna forma di assicurazione che permetta di assorbire in qualche misura l'eventuale perdita, sebbene molti di questi istituti che ne gestiscono gli scambi agiscono come fossero vere e proprie banche virtuali.

Quest'intera situazione rappresenta un chiaro limite, avendo a che fare con società esposte a rischi di perdite ingenti senza nessun tipo di garanzia offerta.⁷³

Per agire mediante operazioni fraudolente, gli *hacker* devono controllare la maggior parte della rete, mediante il controllo del 51% (almeno) nella rete di *Bitcoin*, in modo tale da poter approvare determinati blocchi scartando quelli generati dagli altri.

In questo modo “salta” il concetto di rete decentralizzata ed i *miners* potranno avere il totale controllo del *network*.

⁷¹ Cfr. PRISCO M. , “*Bitcoin* e criptovalute, quali garanzie legali per chi investe” , www.Digital360group.com, 8 Febbraio 2018

⁷² Cfr. Banca D'Italia, “avvertenza sull'utilizzo delle cosiddette valute virtuali”, cit.

⁷³ Cfr. BIENNA M. , “*Bitcoin* e attacchi *hacker*: problemi di sicurezza irrisolvibili?” , www.money.it, 29 Agosto 2016

Tutte le criptovalute sfruttano il concetto di *Ledger* distribuito per rendere il sistema *trustless* ed evitare che un solo ente centrale possa controllare le transazioni ed il *network*.

Il registro, ovvero la *blockchain*, è distribuito su una serie di nodi, fra cui i *masternodes*.

La *blockchain* viene però “creata” dai minatori, che si occupano di raccogliere le transazioni dal *network*, validarle e sigillarle nei blocchi della catena.

Ovviamente per svolgere tale operazione, come già detto in precedenza, ricevono una remunerazione derivante dal premio per blocco e dalle spese di commissione del *network*.

In una rete che utilizza l’algoritmo di consenso *PoW (Proof-of-Work)*, per aggiungere un nuovo blocco, i minatori devono, in parole povere, eseguire una serie di algoritmi crittografici per dimostrare di aver svolto il proprio lavoro. Il primo minatore che trova la soluzione corretta, ha l’opportunità di creare un nuovo blocco ed ottenere una ricompensa adeguata.

Maggiore è la potenza computazionale a disposizione del minatore, maggiori sono le probabilità di trovare la soluzione giusta più velocemente degli altri, e dunque di ottenere una retribuzione.

Quando il minatore trova la soluzione corretta, essa viene propagata ai partecipanti del *network*, che dopo una verifica, aggiungono alla *blockchain* il nuovo blocco validato.

Il vincolo chiave per effettuare un attacco del 51% è quello di possedere la maggioranza della potenza di mining della rete, per ottenerne il controllo.

Se il minatore o la *pool* di *mining* controllano più della metà dell’*hashrate* totale, allora hanno la capacità di controllare completamente la rete e possono quindi aggiungere nuovi blocchi, manipolare le operazioni bidirezionali e rifiutarsi di confermare le nuove transazioni.

Inoltre, l’attacco del 51% può consentire ai malintenzionati di eseguire il *double spending*, ovvero spendere più volte la stessa moneta.

Un’operazione che non deve assolutamente verificarsi in una criptovaluta, visto che la renderebbe praticamente inutilizzabile.

Tuttavia, la parte attaccante non può modificare le informazioni nei blocchi già creati o generare nuove monete.

Va notato che le criptovalute in cui l’algoritmo di consenso è basato sul *PoS (Proof-of-Stake)*, sono difficilmente soggette ad attacchi del 51%.

Infatti, in tale algoritmo, i validatori contribuiscono a mantenere le capacità operative del *network* in base alla quantità di criptovalute che possiedono (*stake*), dunque non viene considerata la potenza di calcolo.

Di conseguenza, qualsiasi tentativo di attacco in questo sistema diventa poco redditizio.

Nella maggior parte dei casi, tali tipi di attacchi vengono eseguiti sulle criptovalute più recenti, in quanto non è necessario possedere potenze di mining estremamente elevate.⁷⁴

Vi sono stati negli anni diversi casi di operazioni fraudolente da parte degli *hacker*, con risultati, a volte, davvero devastanti; come il caso avvenuto lo scorso anno in Giappone, quando abbiamo assistito al più grande furto relativo alle criptovalute della storia.

Coincheck, una delle maggiori piattaforme giapponesi, sospese improvvisamente le contrattazioni su *Bitcoin* e bloccò il ritiro dei fondi da parte dei clienti apparentemente senza alcun motivo.

Poi in serata annunciò di aver subito un furto di circa 500 milioni di *Nem*⁷⁵, per un controvalore di circa 58 miliardi di *yen*, poco più di 530 milioni di dollari, dai *wallet* custoditi presso la piattaforma. Le voci sul maxifurto erano circolate già nella stessa mattinata a Tokyo e avevano contribuito a indebolire le quotazioni, con il *Bitcoin* scivolato a quota 10.500 dollari e il *Nem* che cedeva il 15% dopo il congelamento dei conti da parte dell'*exchange* che aveva lasciato presagire una situazione ben peggiore.⁷⁶

La perdita è stata una conseguenza diretta di un attacco *hacker* alla piattaforma di scambio delle monete digitali *Nem*, avvenuta nelle prime ore di venerdì, e scoperto solo nel pomeriggio, otto ore dopo l'incidente.

Le monete erano custodite in quello che viene comunemente chiamato *hot wallet*, un archivio di valuta digitale connesso a *internet* per poter effettuare spese in modo rapido e agevole.

Precedentemente, il non invidiabile "primato" apparteneva ad *Mt. Gox*, altra piattaforma per lo scambio di criptovalute, in Cina.

Tale *exchange* gestiva, fino al 2014, quasi il 70% di tutte le transazioni di *Bitcoin* nel mondo; fino al 7 Febbraio dello stesso anno, quando bloccò definitivamente tutti i ritiri di *Bitcoin*.

Qualche giorno dopo comunicò alla stampa di avere dei problemi nel *software* nel proprio sito, e che, fino a quando non avrebbero risolto il *bug*, l'opzione di ritiro non sarebbe stata disponibile.

Il 24 Febbraio, vennero sospese anche tutte le operazioni di *trading*, e, successivamente, venne annunciato al mondo la notizia che la compagnia era insolvente a causa di un furto di oltre 744.408 *Bitcoin*, per un valore allora pari a circa 450 milioni di dollari.⁷⁷

⁷⁴ Cfr. PAGLIARI E. , "Attacco del 51%: ecco cosa significa e le conseguenze, www.Cryptominando.it, 22 Aprile 2018

⁷⁵ *Nem* è una criptovaluta creata nel sol levante il 1 Marzo 2015.

Meno nota di alcune, ma tra le prime 20 per capitalizzazione.

⁷⁶ Cfr. "In Giappone il più grande furto di criptovalute della storia: rubati 500 milioni di dollari in *Nem*" , Il Sole 24 ore, 26 Gennaio 2018

⁷⁷ Cfr. SESANA J. , "Il furto su *Coincheck*, niente a che vedere con *Mt. Gox*", www.Ngc.it, 27 Gennaio 2018

Va detto però che, con il valore attuale dei *Bitcoin*, il furto avrebbe un valore stimato di diversi miliardi di dollari.⁷⁸

Anche nel nostro territorio recentemente è stato registrato un episodio simile, con il fallimento di *Bitgrail*, *exchange* italiano per criptovalute, che un anno fa venne proiettato alla ribalta delle cronache del criptomondo per un ammanco di circa 150 milioni di dollari.

Questa piattaforma non permetteva la conversione in valuta a corso legale se non passando attraverso una specifica criptovaluta, il *Nano*.

Iniziata come ditta individuale, poi è passata in gestione ad una srl nel Gennaio 2018.

Un mese dopo, la società ha denunciato ammanchi per 17 milioni di *Nano*, per poi cessare la propria attività, anche a seguito della tempestiva richiesta di sequestro di criptovaluta da parte della Procura della Repubblica di Firenze, ottenuta dal Tribunale fallimentare.

Agli atti sono stati sequestrati alla società circa 2.345 *Bitcoin* e 4 milioni di *Nano* per circa 36 milioni di euro e all'amministratore Francesco Firano circa 170 *Bitcoin* e oltre 500.000 euro.

Vi è da specificare, però, che non è ancora nota con certezza la causa di questa situazione.

Nella migliore delle ipotesi, si tratterà di semplice negligenza da parte della piattaforma; nella peggiore e più probabile ipotesi, si tratta di un furto a tutti gli effetti.⁷⁹

Clamorosa, infine, l'indagine dell'*Anti-Money Laundering*, (Antiriciclaggio); sono stati stimati circa un miliardo di dollari connessi a furti di criptovalute, un dato mai così alto ed in fortissima crescita rispetto agli anni precedenti.

Secondo la stessa indagine, soltanto nella prima metà del 2018, ci sono stati più furti dell'intero anno precedente.

Dunque, nonostante la continua evoluzione e la maggiore attenzione che si ha in questo mondo informatico così complesso e articolato, non si è ancora in grado di prevenire eventuali furti informatici; da qui se ne ricava che le accuse e lo scetticismo di Banca d'Italia e molti altri personaggi che condannano tali strumenti, non sono del tutto infondate.

⁷⁸ Cfr. SCIALÒ L. , "Su *Coincheck* il più grande furto di criptovalute della storia: ecco cosa è successo", www.Webeconomia.com, 5 Febbraio 2018

⁷⁹ Cfr. CAPACCIOLI S. e SOLDAVINI P. , "Fallisce *Bitgrail*, la piattaforma Italiana per le criptovalute", *Il Sole24ore*, 26 Gennaio 2019

2.1.7 (*Segue*) Incertezza sul trattamento fiscale

La natura decentralizzata delle rete di valute virtuali e l'assenza di regolamentazione fanno sì che il trattamento fiscale delle valute virtuali possa presentare incertezze e lacune, a cominciare dall'individuazione dello Stato beneficiario, dando vita a implicazioni imprevedibili per i soggetti coinvolti.⁸⁰

Per quanto le criptovalute esistano ormai da circa un decennio, solo la loro recente “esplosione”, sia in termini di utilizzo che di valore, ha posto una serie di interrogativi sia in capo agli utilizzatori (giustamente timorosi delle “attenzioni” del fisco) che della stessa amministrazione finanziaria.

Con la risoluzione n.72/E/2016, l'Agenzia delle Entrate ha chiarito il trattamento fiscale, sia ai fini di Iva che ai fini delle imposte dirette (Ires e Irap), applicabile alle operazioni connesse alle monete virtuali.⁸¹

Per quanto riguarda il trattamento tributario in Italia possiamo già giungere a delle conclusioni sotto il profilo delle imposte dirette.

Nel caso degli *exchanger*, la commissione di cambio dovrebbe basarsi sulle regole fiscali proprie del reddito d'impresa; ai fini Iva, poi, si dovrebbe ritenere che l'operazione di cessione del bene finito venga assoggettata ad imposta.

In via generale la posizione del *miner* è quella tipica di ciascun residente nel territorio dello Stato che decida di prestare il proprio servizio per ottenere in cambio uno specifico corrispettivo.

Per quanto riguarda il trattamento fiscale applicabile invece alle operazioni connesse alle criptovalute, ci si basa su quanto affermato dalla Corte di Giustizia Europea nella sentenza del 22 ottobre 2015, causa C-264/14.

In tale occasione, agli effetti dell'Iva, la Corte Europea ha riconosciuto che le operazioni che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale e viceversa, costituiscono prestazioni di servizi a titolo oneroso.

In assenza di una specifica normativa applicabile al sistema delle valute virtuali, la predetta sentenza costituisce necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile alle monete virtuali.

In particolare, nella sentenza viene chiarito che tali prestazioni: “costituiscono operazioni finanziarie, in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento

⁸⁰ Cfr. Banca D'Italia, “avvertenza sull'utilizzo delle cosiddette valute virtuali”, cit.

⁸¹ Cfr. PELLEGRINI M. , DI PERNA F. , “*Cryptocurrency (and Bitcoin), a new challenge for the regulator*”, 19 Marzo 2018.

alternativo ai mezzi di pagamento legali e non abbiano altre finalità, oltre a quella di un mezzo di pagamento.”

In sintonia con quanto sostenuto dalla Corte, l'Amministrazione finanziaria sostiene che:

-l'attività di intermediazione di valute virtuali costituisce un'attività rilevante, oltre agli effetti dell'Iva, anche dell'Ires e dell'Irap.

-l'attività è soggetta agli obblighi di adeguata verifica della clientela, di registrazione e di segnalazione all'Unità di Informazione Finanziaria (UIF) previsti dal D.lgs.n 231/2007.

Quanto agli utilizzatori, i guadagni di tipo speculativo dovrebbero essere dichiarati come reddito di capitale.

L'art 67 del Testo Unico delle Imposte sui redditi (TUIR), al fine di non attrarre a tassazione fattispecie di guadagno non significative, al comma 1 prevede che: “La tassazione delle plusvalenze derivanti dalla cessione di valute provenienti da depositi e conti correnti si ha solo nel caso in cui la giacenza in valuta nei depositi e conti correnti complessivamente sia superiore ad euro 51.645.69 per almeno 7 giorni lavorativi continui nel periodo d'imposta in cui la plusvalenza è stata registrata.”

Per quanto concerne la base imponibile, in base a quanto previsto dall'art. 68 del DPR n.917/86, questa sarà pari alla differenza tra il costo di acquisto ed il corrispettivo di vendita.

Eventuali minusvalenze sono deducibili dai redditi della stessa natura ed il differenziale positivo delle plusvalenze e minusvalenze dovrebbe essere soggetto ad una ritenuta del 26%.⁸²

2.1.8 (*Segue*) Altre considerazioni

Oltre ai già citati principali punti deboli delle criptovalute, ne sono stati messi alla luce altri, probabilmente di minor rilevanza, dalla critica generale.

Tra questi, vanno presi in seria considerazione quelli presentati dalle tre Autorità di vigilanza europea, ovvero *EBA*, *ESMA*, *EIOPA*. Le stesse affermano infatti che chi acquista valuta virtuale deve essere consapevole del rischio di poter perdere gran parte del denaro investito, se non addirittura di perderlo completamente, e il consumatore che acquista criptovalute o prodotti finanziari con esposizione diretta alle criptovalute si espone a una quantità di rischi, dovuti in particolare ai seguenti fattori:

-nessuna opzione di uscita: decidendo di acquistare criptovaluta, ci si espone al rischio di non poterla negoziare né scambiare con valute convenzionali quali l'euro per lunghi periodi, con possibilità di conseguenti perdite.

⁸² Cfr. MIGLIORINI F. , “Bitcoin e Criptovalute: tassazione delle monete virtuali”, www.Fiscomania.it, 5 Dicembre 2018

-non trasparenza dei prezzi: i processi di formazione dei prezzi delle criptovalute spesso non sono trasparenti. Vi è pertanto un elevato rischio che in sede di compravendita di criptovalute i prezzi non siano equi né accurati.

-interruzioni dell'operatività: su alcune piattaforme per la negoziazione di criptovaluta si sono manifestati gravi inconvenienti, quali interruzioni dell'operatività, che hanno impedito ai consumatori di acquistare e vendere criptovaluta nel momento che ritenevano opportuno, esponendoli a perdite dovute alle fluttuazioni di prezzo delle criptovalute da essi detenute nel periodo di interruzione dell'operatività.

-informazioni fuorvianti: le informazioni fornite ai consumatori intenzionati ad acquistare criptovaluta, quand'anche rese disponibili, sono nella maggioranza dei casi incomplete e di difficile comprensione e non rivelano in modo efficace i rischi insiti nelle criptovalute: tali informazioni possono pertanto risultare fuorvianti.

-inadeguatezza delle criptovalute per la maggioranza degli impieghi, compresi investimenti e piani pensionistici: l'elevata volatilità delle valute virtuali, l'incertezza del loro futuro e l'inaffidabilità delle piattaforme di negoziazione e dei *provider* di portafogli digitali le rende inadeguate per la maggioranza dei consumatori, compresi quelli con orizzonti d'investimento a breve termine e, in particolare, quelli che si pongono obiettivi a lungo termine quali il risparmio pensionistico.⁸³

2.2 Principali punti di forza

Dopo aver considerato i (numerosi) aspetti negativi e fortemente criticati, passiamo adesso a descrivere i principali punti di forza di tali strumenti, che hanno permesso al *Bitcoin* e alle criptovalute di affermarsi con successo in breve tempo e che hanno portato diverse novità all'interno dei mercati economici.

2.2.1 (Segue) Decentralizzazione

Molto probabilmente, la decentralizzazione è il principale elemento di successo e di innovazione del mondo digitale connesso al *Bitcoin* (insieme alla tecnologia *Blockchain* di cui si è già parlato).

⁸³ Cfr. Consob, “*ESMA, EBA ed EIOPA avvertono i consumatori circa i rischi delle criptovalute*”, 9 Marzo 2018.

A detta di molti, come lo sviluppatore *Jimmy Song*, questa è l'elemento chiave che giustifica la notevole differenza tra il *Bitcoin* e le altre criptovalute che non godono di tale proprietà; infatti, secondo alcune indagini, si registra un valore di *altcoins* che non si basa su un sistema decentralizzato superiore all'80%.⁸⁴

Bitcoin è stata la prima criptovaluta decentralizzata ad esser mai stata realizzata.

La differenza fondamentale con le valute tradizionali è l'emissione, in quanto non interviene nessuna banca centrale, nessuna approvazione governativa o finanziaria; *Bitcoin* vive sui propri utenti sfruttando i protocolli *peer-to-peer*.

Con il nuovo sistema *Bitcoin*, come precedentemente detto, non vi è alcun intermediario che si siede fra le controparti e verifica il pagamento e la sicurezza dello stesso; per tale ragione, il crescere progressivo delle monete digitali decentralizzate pone inevitabilmente domande sul futuro ruolo della Banca Centrale nel mondo dei pagamenti.

Un'organizzazione decentralizzata non ha bisogno di Autorità centrali, ma è governata da protocolli di approvazione delle transazioni, con regole chiare e partecipazione diretta.

In tale sistema ogni nodo del *network* ha la stessa importanza, non esistendo un'entità centrale che ne regola e garantisce il funzionamento ed il suo grande vantaggio risiede proprio nel fatto che nessuno possa "comandare *Bitcoin*"; nessuno può alterarlo o modificarlo, a differenza delle monete fiat, che sono gestite da un centro di potere.⁸⁵

Si sostiene che le Banche Centrali abbiano timore e stiano prendendo in considerazione la "minaccia *Bitcoin*".

Nonostante attualmente il valore complessivo di *Bitcoin* immessi nelle economie è di gran lunga inferiore rispetto a quello delle monete e banconote, l'impatto della moneta digitale non è stato preso alla leggera.

La BIS (Banca per i Regolamenti Internazionali) ha affermato come le criptovalute rappresentino "un'ipotetica sfida per le banche centrali, non attraverso la sostituzione della stessa con qualche altro tipo di corpo centrale, ma soprattutto perché ne riduce le funzioni e, in casi estremi, può eliminare la necessità di un corpo centrale interamente".

Inoltre, tutto il panorama finanziario è stato pressoché sconvolto da questa innovazione: secondo una stima del *World Economic Forum*, entro il 2025 più del 10% del Pil mondiale riguarderà attività registrate attraverso la tecnologia con protocolli *Blockchain*.

⁸⁴ Cfr. SUBERG W. , "Jimmy Song: la decentralizzazione è la chiave dietro al successo del *Bitcoin* sulle *altcoin*", www.Cointelegraph.com, 1 Gennaio 2019

⁸⁵ Cfr. CAVICCHIOLI M. , "La decentralizzazione, questa sconosciuta", www.IlBitcoin.it, 5 Ottobre 2018

Se i *test* dovessero essere promettenti, si giungerà forse all'ambizioso progetto della Norvegia: digitalizzare in maniera totale il contante, rendendo le transizioni criptate, anonime e sempre più sicure.⁸⁶

2.2.2 (Segue) Contenimento dell'inflazione

Come già detto in precedenza, riferendoci ancora al *Bitcoin*, è stato progettato da *Satoshi Nakamoto* un limite alle monete digitali che negli anni verranno messe in circolazione, ovvero 21 milioni.

Questo limite non è però rispettato da tutte le altre criptovalute; ad esempio, vi sono *altcoins* come *Ethereum*, per le quali non è previsto alcun limite di produzioni, ed altre come *Ripple* e *Litecoins* che hanno, rispettivamente, un limite di circa 100 miliardi ed 84 milioni.

Vi è un determinato vantaggio all'interno di una emissione limitata di criptovalute; infatti, mediante tale strategia, si va a contrastare l'inflazione che spesso va ad indebolire il potere di acquisto delle famiglie.

Dunque, stabilendo un "*Max Supply*", *Nakamoto* ha creato una moneta deflazionistica e destinata ad apprezzarsi nel tempo proprio per la sua rarità, come l'oro.⁸⁷

L'iperinflazione è avvenuta 57 volte dalla fine della prima guerra mondiale, affliggendo diversi miliardi di persone.

In effetti, questa è una forma di disastro economico unico per la moneta di stato. Non c'è mai stato un esempio di iperinflazione quando le economie utilizzavano monete basate su oro o argento.

Il denaro di stato è relativamente economico da produrre, il che significa che i governi in crisi sono molto felici di produrlo, generando quindi tale fenomeno.

Sebbene la maggior parte dei paesi non abbia subito l'iperinflazione, quasi tutti hanno sperimentato una significativa svalutazione della propria moneta per periodi prolungati. Tra il 1960 e il 2015, ad esempio, l'offerta di moneta in tutti i paesi è aumentata in media del 32 percento all'anno.⁸⁸

Ci sono alcuni paesi nel mondo in cui l'inflazione è davvero un grosso problema.

Il primo è il Venezuela. 30 milioni di abitanti, ed un'iperinflazione che sta provocando danni serissimi alla propria valuta, essendo la più alta mai verificatasi in questo secolo.

⁸⁶ Cfr. PIPARO P. , "*Bitcoin: la prima moneta digitale decentralizzata*", www.Startingfinance.it, 12 Gennaio 2017

⁸⁷ Cfr. DAL PRÀ M. , "*Bitcoin: perché 21 milioni?*", www.Finanzaonline.it, 26 Febbraio 2018

⁸⁸ Cfr. AMMOUS S. , "*The problem Bitcoin solves*", www.TheSpectator.com, 10 Novembre 2018.

Un altro paese in cui l'inflazione è molto elevata, seppur ancora sotto controllo, è l'Argentina: 43 milioni di abitanti e 30% di inflazione.

Anche in Turchia l'inflazione è elevata, perchè nel 2018 è salita fino al 16%. E la Turchia ha 80 milioni di abitanti.

Ci sono problemi di inflazione anche in Iran: 77 milioni di abitanti e un'inflazione in ascesa, sopra il 10%.

Prendendo in considerazione anche solo questi 4 paesi, stiamo parlando di 230 milioni di persone, circa, che hanno problemi con l'inflazione della loro moneta.

Ebbene, a costoro non conviene tenere i risparmi in valuta locale.

Solitamente cambiano la valuta locale in valuta estera più solida (come il dollaro), e tengono i risparmi in valuta estera, ma ciò non è sempre semplice. Infatti, come accade ad esempio in Venezuela o in Iran, in questi paesi sarebbe proibito “esportare capitali” all'estero acquistando valuta di altri Stati, USA in primis.

Quindi i cittadini di quei paesi sono sempre alla ricerca di alternative.

I dati degli ultimi mesi dimostrano chiaramente che un numero sempre crescente, soprattutto di turchi ed argentini, stia cambiando la valuta locale in criptovalute, e in particolare in *Bitcoin*.

Certo, il valore dei *Bitcoin* può anche scendere, ma non a causa dell'inflazione e quindi mai per un eccesso di liquidità (che è solitamente la causa principale di inflazione).

Pertanto quello che sta succedendo al *Bolivar* venezuelano, o alla *Lira* turca, o al *Peso* argentino, o al *Riyal* iraniano, non può accadere a *Bitcoin*, che segue una dinamica differente.

Questo sta spingendo quindi a convertire i propri risparmi da valuta locale inflattiva, che perde inevitabilmente valore nel corso dei mesi, in valute più stabili ed in criptovalute deflative.⁸⁹

Negli ultimi anni anche in Sudafrica è registrato un maggiore utilizzo di valute digitali a causa di problemi connessi all'inflazione, con l'apertura di almeno 15 nuove sedi di *trading* negli ultimi mesi.

Per quanto riguarda il sistema fiscale del paese, il *South African Revenue Service* (SARS) ha pubblicato le linee guida relative a come gestirà le criptovalute. Le ha definite “attività immateriali” in contrapposizione alla “moneta”, ai fini dell'imposta sul reddito o dell'imposta sulle plusvalenze.

Ciò significa che tutte le entrate relative alle criptovalute nel paese devono essere dichiarate e la responsabilità ricade sul contribuente, dal momento che l'inadempienza probabilmente comporterà multe e interessi associati. Secondo il servizio delle entrate, le tasse sono applicabili sia alle operazioni di *mining* che alle operazioni di scambio di criptomonete.

⁸⁹ Cfr. CAVICCHIOLI M. , “Fate attenzione all'inflazione”, www.ilBitcoin.it, 1 Settembre 2018.

Anche in tale contesto, essendoci una rilevante percentuale inflazionistica che colpisce i vari paesi, criptovalute come *Bitcoin* o *Litecoin* sono visti da molti come strumenti che consentono la protezione dei propri risparmi dall'inflazione.

Per concludere, va detto che, posizionandosi come alternativa al denaro fiduciario, mantenendo la sua indipendenza dagli organi economici di ciascun paese, ogni criptovaluta costituisce sia un rischio che un'opportunità. Ciò dipenderà dall'uso che viene fatto.

Anche se la capacità di investimento è inferiore, le criptomonete possono essere un'alternativa economica per le persone affinché non perdano i propri risparmi e offrire una sicurezza economica che non troveranno nella propria moneta nazionale e nel sistema bancario, ma, allo stesso tempo, potrebbero causare danni anche più gravi per via della forte volatilità che da sempre le contraddistingue.

2.2.3 (*Segue*) Riduzione delle spese di transazione

Uno dei vantaggi dell'utilizzo della *blockchain* è che si suppone che effettui transazioni più economiche rispetto all'utilizzo di altri metodi di pagamento convenzionali.

Va detto, però, che non si può parlare di costi di commissione fissi, in quanto anche questi, così come le criptovalute, variano in base a determinati fattori.

Si può precisare che il loro costo dipende principalmente da 3 aspetti fondamentali:

- Spazio occupato dalla transazione
- Numero di transazioni sulla rete
- Valore della valuta

Le commissioni sono direttamente proporzionali alla risorsa che utilizzano ed alla moneta con cui si pagano e, non essendo fisse, appunto, potrebbero in determinati momenti salire di valore.

A causa della popolarità del *Bitcoin* nel 2017, vi è stato infatti un aumento della congestione della rete e successivamente il costo medio delle transazioni è salito alle stelle.

Dalla fine di dicembre dello stesso anno, queste tasse sono state in costante calo, qualcosa che è stato accolto favorevolmente dagli utenti *Bitcoin* e non solo.

Il motivo principale per cui le tasse si sono drasticamente ridotte è dovuto al numero di transazioni divenuto inferiore.

Oggi in media una transazione ha commissioni pari a 0,0001 *Bitcoin*; ma alcuni *wallet* danno la possibilità di impostare il costo della commissione. In questo modo, in caso di transazioni particolarmente importanti, si ha la possibilità di raddoppiare o triplicare il costo della commissione per far processare più velocemente la transazione.

Uno dei più grandi vantaggi nell'utilizzo di *Bitcoin* e molte altre criptovalute sta nel fatto che la commissione è la stessa, a prescindere dal luogo in cui verrà effettuata la transazione; questo non è generalmente vero nel mondo bancario attuale.

C'è da fare però una valutazione: le spese di transazione, specie durante i periodi in cui la rete è sotto stress, aumentano con il conseguente aumento delle *fees*.

Tuttavia, stando ai dati della *Bank of America*, le spese di commissione per un bonifico internazionale possono essere fino ad un centinaio di volte più costose rispetto alle *fee* per una transazioni *Bitcoin*. Innanzitutto, effettuare un bonifico internazionale ha un costo che dipende sia dalla propria banca che dall'importo da transare. Tuttavia, parlando delle banche europee, le spese per un bonifico internazionale possono variare da 10 ad anche 50 euro, in base alla banca e allo Stato.

Inoltre, alcune banche applicano limiti massimi a tali operazioni, oltre le quali occorre pagare ulteriori spese di commissione in base al capitale trasferito oppure utilizzare altri metodi di pagamento.

Tornando all'esempio ed ai dati della *BoA*, un bonifico internazionale costa circa 45 Dollari per transazione. Ad oggi, la commissione media di transazione è di circa 0,46 Dollari per *Bitcoin* (secondo i dati di *Bitinfocharts.com*).

Tutte le transazioni della *Bank of America* vengono elaborate attraverso la rete di trasferimento di denaro della *Federal Reserve*, denominata *FedWire*. Quest'ultima addebita una commissione di elaborazione massima di 82 centesimi di dollaro per l'utilizzo della rete. Tale tariffa fa sì che il margine per le transazioni della *Bank of America* sia superiore al 98%.

Le commissioni *FedWire* sono stimate in base alle dimensioni delle singole transazioni e al volume totale dei pagamenti. Può essere applicato anche uno sconto aggiuntivo – “*incentive fee*” – per trasferimenti superiori al 60% del volume storico di riferimento di un cliente.

Le banche degli Stati Uniti possono quindi arrivare a pagare solamente 0,32 \$ di commissioni per transazioni superiori a 90.000 \$. Ma, almeno in base alle cifre disponibili pubblicamente, le commissioni dei clienti non beneficiano di questo sconto.

Al contrario, una transazione *Bitcoin* del valore di 90.000 \$ avrebbe un costo di soli 75 centesimi, secondo i dati di *Earn.com*, che mostra le tariffe raccomandate in satoshi per *byte*.

Per concludere, vanno elogiate anche le tempistiche. Mentre per un bonifico, infatti, possono servire anche 4-5 giorni (fino a 10 per certi stati), con *Bitcoin* sono necessarie poche decine di minuti o al più qualche ora.⁹⁰

⁹⁰ Cfr. PORTA M. , “*Fee di Bitcoin e bonifico internazionale: il confronto sui costi*”, www.CryptoMinando.it, 21 Settembre 2018

2.2.4 (Segue) Trasparenza e Anonimato

Con l'utilizzo di *Bitcoin* in nessun modo, teoricamente, dovrebbe essere possibile determinare a chi appartenga un determinato indirizzo; l'unico riferimento disponibile è semplicemente uno pseudonimo.

Ciononostante, la *Blockchain* è completamente trasparente, pertanto sarà possibile conoscere tutta la storia finanziaria di un determinato indirizzo, pur non sapendo a chi appartiene, e degli indirizzi correlati, costruendo dei veri e propri “*cluster*” di operazioni.

Gli indirizzi non contengono informazioni riguardo ai loro proprietari e consistono in sequenze casuali di caratteri e cifre molto lunghe. Tuttavia, una volta che questi vengono utilizzati, sono corrotti dalla storia di tutte le transazioni in cui sono coinvolti e tutti possono vedere il bilancio e le transazioni di ogni indirizzo.

Gli utenti possono avere un numero discrezionale di indirizzi, non essendoci un limite previsto.

Il sistema dei *Bitcoin*, insomma, sposa trasparenza e anonimato rendendo limpidi i trasferimenti, ma celando ogni riferimento che possa ricondurre la criptovalute ai legittimi possessori.

Con i dati *Bitcoin*, condivisi da nodi su una rete *peer-to-peer* senza indirizzi *IP*, anche le origini dei nodi sono anonime. L'uso di un libro mastro pubblico può essere utile per verificare che le transazioni mantengano l'integrità e la riservatezza (attraverso la pseudonimia), ma questo non significa necessariamente che *Bitcoin* sia anonimo e privato.

Infatti, questo non sempre garantisce il pieno anonimato, poiché l'analisi della *blockchain* pubblica può collegare insieme diversi indirizzi. Se, quindi, anche uno solo degli indirizzi è collegato a un'identità reale, tutti possono esserlo.

Inoltre, la condizione di anonimato permane fintanto che non venga utilizzato un *Exchange* o un servizio soggetto agli adempimenti di tipo “*Know Your Customer*”.

A seguito della quarta Direttiva dell'UE (n.2015/849) in materia di antiriciclaggio, infatti, chi fornisce il servizio di compravendita di criptovalute, deve richiedere ai clienti dei documenti identificativi. Possiamo dire quindi che un sistema, anonimo e trasparente come la *Blockchain*, resta tale fintanto che non si utilizzano piattaforme soggette a normativa.

Esistono però dei siti, chiamati *Mixer*, che consentono di costruire transazioni “offuscanti”.

Il comportamento è quello di aggregare più transazioni, di utenti diversi, all'interno di un'unica transazione, “mescolando le tracce” dei movimenti di *Bitcoin* collegati agli indirizzi. Non sarà dunque possibile, a partire da tale transazione, se ben costruita, evincere chi stia inviando *Bitcoin*, e dove.

Utilizzando più *wallet*, o dei *wallet* che permettano il “*multiaccounting*”, è possibile tenere segregati i fondi in indirizzi diversi, che non si incontreranno mai, e non saranno dunque “*clusterizzabili*”.

Questo ha dei pro e dei contro, sul fronte dell'usabilità, ma è una delle rivoluzioni del *Bitcoin*: l'utente, adesso, può scegliere quale livello di *privacy* desidera ottenere e, se lo desidera, prendere tutti gli accorgimenti del caso per mantenerla.

Sono diversi, inoltre, i team di criptovalute che lavorano sul miglioramento dell'anonimato nelle transazioni. Ad oggi, con *ZCash* e *Monero*, ad esempio, si può già ottenere un livello di anonimato maggiore di quanto offra il *Bitcoin*.⁹¹

Ci si aspettano molti miglioramenti in futuro, in ambito di *privacy* del *Bitcoin*; l'anonimato è infatti una promessa importante di *Btc* che, sgravato dagli impedimenti, rappresenta uno strumento per la trasformazione degli affari e della finanza.

Soprattutto perché, senza il giusto grado di anonimato, si lascerebbe una traccia completa delle informazioni finanziarie individuali pubblicamente disponibile, per sempre.

In definitiva, va specificato che vi sono anche tanti altri piccoli vantaggi, come l'irreversibilità delle transazioni o il fatto che non c'è bisogno di essere degli esperti del settore informatico per potere operare nell'ambito delle criptovalute, ma resta l'idea che non è affatto semplice poter dare un giudizio oggettivo in merito alla bontà di tali strumenti digitali, anche dopo aver considerato i punti fondamentali degli stessi.

Anzi, proprio per via della moltitudine di elementi caratterizzanti, sostengo che possano essere degli strumenti utili o meno in base al tipo di investitore, alle sue idee e al suo modo di voler operare nel mercato.

2.3 Una breve analisi sulle criptovalute

Dopo aver introdotto la nascita, l'espansione e i vari punti critici del *Bitcoin* e delle altre criptovalute, diviene molto interessante andare ad analizzare l'andamento di queste monete digitali negli anni, considerando gli eventi più importanti e le cause principali dei numerosi “*boom e bust*”.

⁹¹ Cfr. DOTTA G. , “Il *Bitcoin* e l'anonimato”, www.webnews.it, 2018

2.3.1 La performance del *Btc*

Iniziamo tale analisi ripercorrendo la storia dell'oro digitale, il padre di tutte le criptovalute, create principalmente grazie al successo del *Btc* e spesso per correggerlo e migliorarlo.

Come già detto, il *Bitcoin* nasce nel 31 ottobre 2008, ma solo l'anno successivo *Nakamoto* presenterà al mondo intero il “*genesis block*”, il primo blocco della catena che ancora oggi lega tutte le transazioni, ottenendo come ricompensa 50 *Btc*.

La primissima quotazione del *Bitcoin* risale al 5 ottobre del 2009, quando il sito *New Liberty Standard* pubblica la sua prima quotazione: con un dollaro era possibile acquistare oltre 1300 *Bitcoin*.

La criptovaluta, a quel tempo, valeva neanche un decimo di *pence*; un valore a dir poco incredibile, se si pensa che in meno di un decennio il prezzo di un singolo *token* arriverà poi a sfiorare anche i 20mila dollari di valore.

Nell'anno successivo il prezzo più alto è stato di 0,39 dollari ma, il 17 Luglio, si registra un evento molto importante: la nascita di *Mt. Gox* a Tokio, che diventerà *l'exchange* più importante, arrivando a gestire oltre il 70% di tutte le transazioni di *Bitcoin* nel mondo.

Si deve attendere fino al 9 Febbraio 2011 per vedere il valore di un *token* toccare la quota di 1 dollaro, superandolo; la performance del *Bitcoin* in quegli ultimi 6 mesi fu del 1000% circa.

Il primo *flash crash* si registra però il 19 Giugno dello stesso anno, quando un attacco *hacker* blocca *Mt. Gox*, provocando un *bust* del *Bitcoin*, che in breve tempo dal valore di 17,5 dollari arriva a valerne 0,01.

Figura 3: Fonte *Coinmarketcap*, andamento dei primi anni di *Bitcoin* tra il 2010 ed il 2011



Nel Giugno del 2012 si registra la nascita di un'altra importantissima piattaforma, chiamata *Coinbase*, con sede a *San Francisco* in *California* e che sarà tra le più utilizzate.

Successivamente vi sarà un forte rialzo di valore; il 28 Marzo 2013, infatti, per la prima volta, la capitalizzazione del *Btc* supererà il miliardo di dollari, con il prezzo di un singolo *token* che, nel giro di pochi mesi, aumenta dai 100 dollari del 2 Aprile ai 1000 del 29 Novembre, sostenuto prevalentemente dagli acquisti di criptomonete dei cittadini Cinesi.

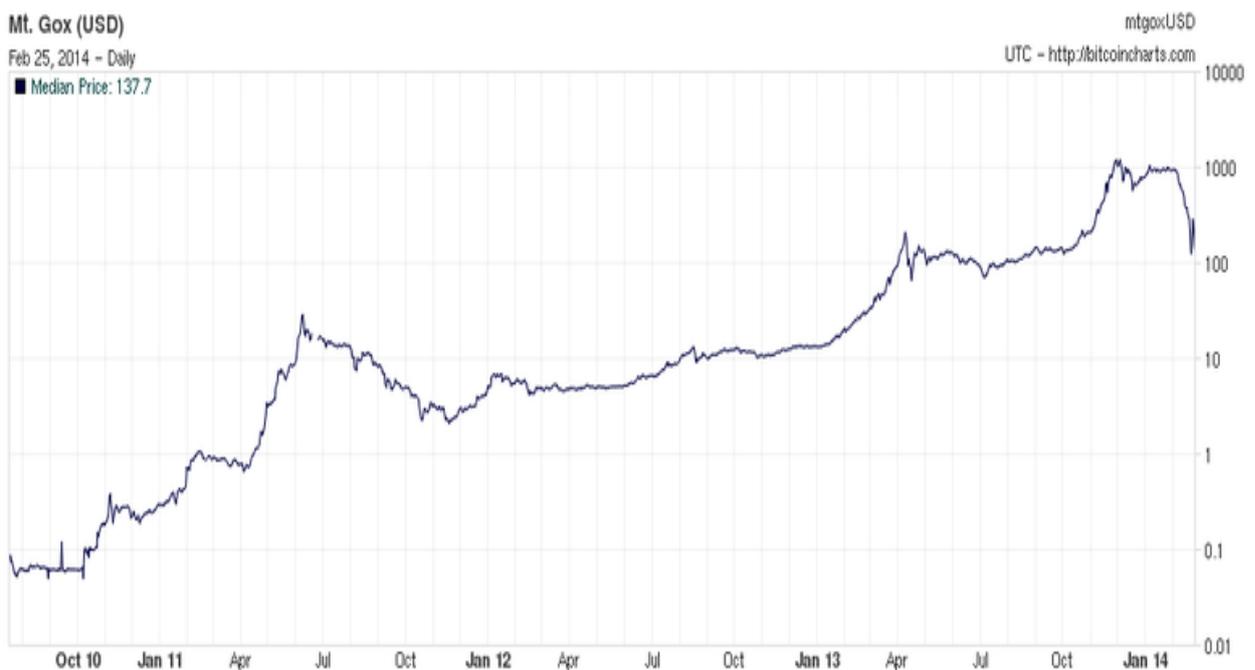
La fiducia degli investitori stava aumentando sempre di più e la voglia di investire, abbinata ad un mercato privo di controlli, porta però al primo importante *crack*.

Il 5 dicembre 2013, infatti, la Banca Centrale Cinese proibisce alle aziende nazionali di accettare pagamenti in *Bitcoin*, affermando che qualsiasi operazione di compravendita con *Bitcoin* verrà da quel momento considerata illegale.

Un dato assolutamente rilevante considerando che in quel preciso momento l'80% delle transazioni venivano effettuate all'interno della Repubblica Popolare Cinese.

Nella figura 4 è rappresentato l'andamento del *Bitcoin* nei suoi primi anni, fino ad arrivare al 2014.

Figura 4: Fonte *Bitcoincharts*, primi anni del *Bitcoin*



Inoltre, il 19 Gennaio dell'anno seguente, *Alibaba* cancella i prezzi in *Bitcoin* dal proprio portale *e-commerce*, facendo perdere alla moneta virtuale il suo principale mercato mondiale.

Un altro evento assolutamente dannoso per l'andamento economico della criptovaluta avviene il 24 febbraio 2014: il maggiore *exchange* di *Bitcoin* al mondo, *Mt. Gox*, dichiara bancarotta dopo aver subito un attacco *hacker*, nel corso del quale spariscono 750 mila *Bitcoin* dei clienti e 100 mila della società. *Mt.Gox* aveva già subito attacchi *hacker* in precedenza, ma quest'ultimo risultava fatale, decretando la sua chiusura definitiva. Fra le cause del declino di *Bitcoin*, il *Guardian* citò i guai giudiziari che hanno riguardato, oltre ad *Mt. Gox*, anche *Charlie Shem*, fondatore e capo di un'associazione che promuoveva l'utilizzo di *Bitcoin* e di un mercato online per convertirli, arrestato e accusato di «aver convertito un milione di dollari in *Bitcoin* per reati legati al traffico di narcotici», oltre a una serie di attacchi informatici e furti subiti in primavera da alcuni utenti.⁹²

Figura 5: Fonte *Coinmarketcap*, caduta del *Btc* dopo la bancarotta di *Mt. Gox*



Come possiamo vedere nella figura 5, la fiducia su *Bitcoin* cala drasticamente dopo questi avvenimenti, portando il prezzo a perdere l'80% dai massimi toccati nell'anno precedente.

⁹² Cfr. "Il complicato 2014 di *Bitcoin*", www.IIPost.it, 18 Dicembre 2014

Dopo un lento ma costante viaggio di ritorno nell'interesse comune della gente, *Bitcoin* ha recuperato terreno in modo impressionante nel 2017, raggiungendo un massimo di 1.000 \$ a gennaio e poi crescendo ulteriormente fino a 3.000 \$ a luglio 2017, grazie anche al fatto che ad Aprile il Giappone legalizzava il *Bitcoin* come metodo di pagamento.

Figura 6: Fonte *Coinmarketcap*, la grande ripresa del 2017



Nel mese di Settembre, si avrà un ulteriore crollo, dovuto principalmente a questi fattori:

- Il 3 Settembre la Cina proibisce alle aziende di finanziarsi tramite offerte iniziali di valute.
- Il 15 Settembre il governo Cinese chiude inoltre tutti gli *exchanges* di criptovalute.⁹³

In più, nello stesso mese, vi sono stati degli attacchi dell'ad di *JP Morgan*, *Jamie Dimon*, che ha definito il *Bitcoin* come una vera e propria truffa.

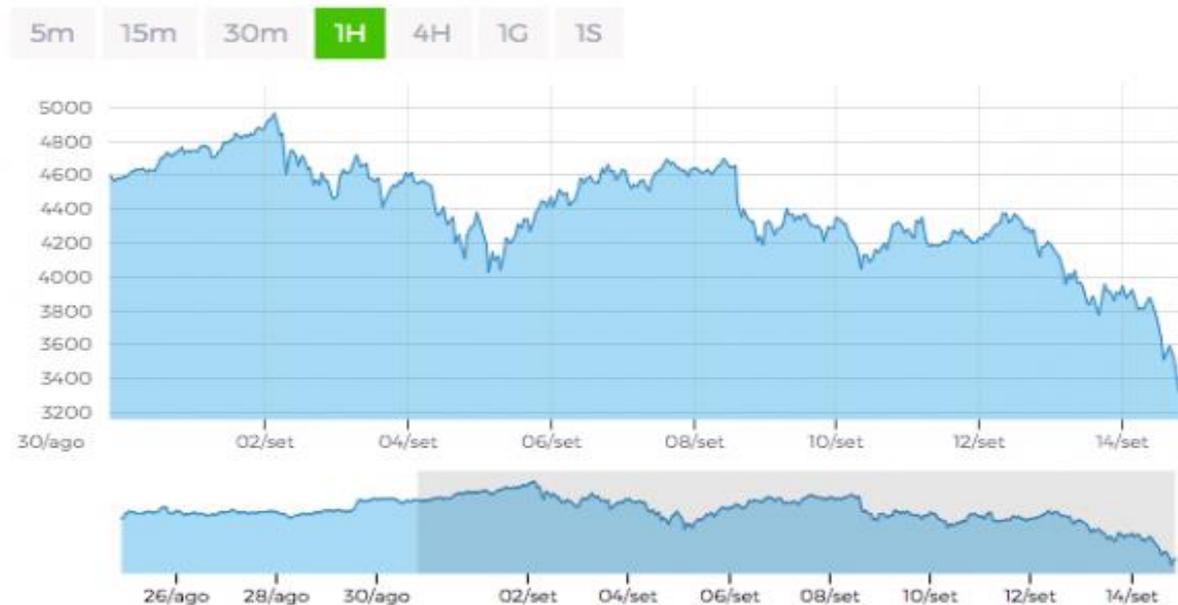
Tali avvenimenti hanno causato una "correzione" del 37%, vale a dire una perdita della capitalizzazione pari circa a 27 miliardi di dollari, come si evince dalla figura 6.⁹⁴

⁹³ Cfr. Ufficio studi *Money.it*, "*Bitcoin*, dieci anni dalla nascita della rivoluzionaria criptovaluta", www.Money.it, 29 Ottobre 2018

⁹⁴ Cfr. PROVENZANI F. , "I motivi del crollo del *Bitcoin*", www.Money.it, 14 Settembre 2017

Figura 7: Fonte *Coinmarketcap*, correzione nel mese di Settembre, la fase che precederà il più grande boom di *Btc*

Quotazione e grafico in tempo reale



Nonostante questa breve fase, c'è stata una crescita massima dei prezzi durante gli ultimi due mesi dell'anno, dove dai minimi segnati del 13 novembre a 5.605 dollari, la valuta digitale ha registrato un + 248,10% di progresso fino ai top assoluti registrati il 18 dicembre. Proprio in questa fase di forte *momentum* rialzista il fenomeno del *Bitcoin* è stato trattato da tutti i principali media ed ha attirato sempre di più i piccoli investitori.

Le quotazioni della regina delle valute digitali sono incredibilmente passate dai valori minimi registrati a 752,46 dollari del 12 gennaio 2017 ad un massimo assoluto toccato lo stesso anno a 19.511 dollari il 18 dicembre 2017, una performance stratosferica pari a 2492,96%.⁹⁵

Nel frattempo, l'11 dicembre 2017 prendevano vita i contratti *futures* al *Cboe* di Chicago.⁹⁶

È una notizia molto importante: per la prima volta titoli relativi ai *Bitcoin* vengono scambiati su un mercato ufficiale e regolato.

⁹⁵ Cfr. Ufficio studi *Money.it*, "Bitcoin: inizio e fine di una bolla speculativa", www.Money.it, 10 Dicembre 2018

⁹⁶ *Chicago Board Options Exchange (CBOE)* è la più importante borsa del mondo per la negoziazione di opzioni. Opera sotto il controllo della *Security and Exchange Commission (SEC)*. Istituita nel 1973, è stata la prima borsa a offrire contratti standardizzati di opzioni, prima solo su azioni, dal 1983 anche su indici azionari

Per molti è un importante segnale di “sdoganamento” per i *Bitcoin*.

La possibilità di scambiare *futures* sui *Bitcoin* significa che sarà possibile scommettere sul loro valore nel prossimo futuro su un mercato regolamentato (la *CBOE*, appunto). Gli investitori potranno cercare di assicurarsi contro una eventuale diminuzione nel prezzo dei *Bitcoin*, ma potranno anche scommettere per guadagnare dalla fluttuazione del loro prezzo.

Non è necessario possedere *Bitcoin* per acquistare *futures* basati sul loro valore. Soltanto i *futures* legati al prezzo dei *Bitcoin* saranno scambiati alla borsa di Chicago; i *Bitcoin* sono scambiati mediante un altro sistema. La decisione di permettere lo scambio di *futures* basati sui *Bitcoin* è stata presa dallo *US Commodities and Futures Trading Commission*, l’ente del governo statunitense che si occupa di regolare questo tipo strumenti finanziari.

La commissione ha avvertito i potenziali investitori che i *futures* saranno probabilmente soggetti a forti variazioni e volatilità nel loro prezzo, e quindi sono da considerare uno strumento molto rischioso. La *Futures Industry Association*, l’associazione che raccoglie i principali operatori di mercato che si occupano di *futures*, ha criticato la decisione sostenendo che la commissione avrebbe dovuto valutare molto più seriamente i rischi questo strumento.⁹⁷ Dopo questo spropositato ed incredibile aumento di valore, il *Bitcoin* nel 2018 è andato incontro all’ennesimo violento ribasso della sua storia, con la perdita del 50% del suo valore soltanto in un mese; quest’anno, il 2018, è da molti considerato come quello dello scoppio della bolla *Bitcoin*.

Figura 8: Fonte *Bloomberg*, *BTC/USD*, grafico settimanale da Gennaio 2017 a Dicembre 2018



⁹⁷ Cfr. “Cosa sono questi *futures* sui *bitcoin*?”, www.IIPost.it, 11 Dicembre 2017

La figura 8 mostra in modo molto chiaro il crollo che c'è stato in un lasso di tempo molto breve. Come si evince dal grafico, il 2018 è stato un anno da dimenticare per la criptovaluta più importante, in quanto ha portato perdite superiori all'80% e quindi risultati estremamente negativi.

Oggi la quotazione sta oscillando da svariati mesi con una stabilità che risulta essere molto strana per un mercato finanziario che ci ha abituati a delle salite e discese da cardiopalma.

Alcuni esperti del settore affermano che si è tornati a una sorta di fase iniziale precedente al "boom". Tuttavia, l'opinione che sembra essere al momento più diffusa tra i personaggi di spicco del mondo *tech* e non solo è quella che si tratti di una bolla destinata a scoppiare. Potrebbe infatti venire a mancare la fiducia da parte delle persone, visto che il *Bitcoin*, come ogni criptovaluta che si rispetti, ha dimostrato di essere altamente volatile.⁹⁸

Ufficialmente nato una manciata di settimane dopo il fallimento di *Lehman Brothers*, il *Bitcoin* si proponeva come un sistema di pagamento alternativo alle monete tradizionali per permettere di chiudere in tutta sicurezza le transazioni online, senza l'intermediazione delle barcollanti banche ormai travolte dalla crisi.

Dieci anni dopo, si ritrova a essere il simbolo stesso della volatilità dei mercati e di strada ne ha fatta tantissima, non solo per l'impatto che ha avuto nel gotha della finanza internazionale.⁹⁹

Figura 9: Fonte *Coinmarketcap*, andamento del *Btc* negli ultimi 5 anni.



⁹⁸ Cfr. ZANETTIN A. , “L’andamento del *Bitcoin* negli ultimi 10 anni: bolla o moneta del futuro?”, www.everyeye.it, 31 Ottobre 2018

⁹⁹ Cfr. CAVALLI S. , “La storia che si ripete: i principali crolli del *Bitcoin (BTC)* dal 2009 ad oggi”, www.Cryptominando.it, 25 Novembre 2018

2.3.2 Principali cause della bolla

Tornando al *boom* improvviso che c'è stato nel 2017, va detto che lo stesso ha fatto nascere diverse idee che ne trovino una giustificazione. Una teoria che circola ormai da mesi e che è anche ritenuta attendibile da molti, vede come fonte di tale aumento di valore una vera e propria manipolazione di mercato. La stessa, afferma che il grande *sprint* del *Bitcoin* nel 2017 non era esclusivamente frutto di una crescente domanda da parte di chi non voleva perdere il treno di una corsa al rialzo che sembrava non fermarsi più. Ma sarebbe effetto, almeno per metà dei guadagni, di una grande manipolazione, incentrata attorno a *Bitfinex*, uno delle maggiori piattaforme globali di scambio per criptovalute, e al *Tether*, criptovaluta esistente dal 2015 e che funziona in un modo particolare, perché si basa sul dollaro americano: ogni unità di *USDT* vale, con un certo grado di approssimazione, un dollaro, e viene utilizzata soprattutto per facilitare le transazioni in criptovalute, che sono infatti più facili e veloci da trasferire da un sito di *exchange* a un altro se non passano da una valuta tradizionale.

La piattaforma, con sede alle Isole Vergini, è da sempre chiacchierata ed è finita sotto inchiesta della *Commodity Futures Trading Commission* proprio per la scarsa trasparenza e per i sospetti legati all'emissione di *Tether*, valuta che dovrebbe quindi essere garantita da analoga quantità di dollari. Uno studio di un ricercatore dell'Università del Texas, *Amin Shams*, sotto la guida di *John Griffin*, docente di finanza dell'Università, riportato dal *New York Times*, rinfocola le polemiche andando a esaminare nel dettaglio la relazione tra i movimenti del *Bitcoin* e l'emissione di *Tether*.

In sostanza i dati vanno a confermare sospetti circolati da tempo sul mercato. Dalla piattaforma di *Bitfinex* uscivano correnti di acquisto su *Bitcoin* e su altre criptovalute proprio nei momenti in cui le quotazioni languivano sugli altri *exchange*. Per muovere il mercato venivano usati i *Tether*.¹⁰⁰

La società che gestisce la criptovaluta ha sempre dichiarato inoltre di possedere un patrimonio in dollari equivalente ai *Tether* in circolazione, che oggi sono circa 2,5 miliardi. In molti hanno messo in dubbio però che questa riserva esista davvero, e la stessa società non ha infatti mai fornito prove per dimostrarlo.

Griffin ha analizzato i flussi di criptovalute in entrata e in uscita da *Bitfinex*. Ufficialmente *Bitfinex* è una società separata da *Tether*, ma in realtà si sa da tempo che hanno lo stesso *CEO*, *Jan Ludovicus van der Velde*, e gli stessi dirigenti. Per via di questo collegamento, una teoria che circola da tempo è che *Bitfinex* abbia creato *Tether* dal nulla, scambiandoli poi con *Bitcoin*: in questo modo avrebbe gonfiato il volume d'affari di *Bitcoin* (e di conseguenza il valore delle singole unità) con soldi che in

¹⁰⁰ Cfr. SOL P. , “Il *Bitcoin* record nel 2017? Frutto di una grande manipolazione”, Il Sole 24 ore, 14 Giugno 2018

realtà non esistevano. Dopo la diffusione di queste ricostruzioni, a Dicembre entrambe le società erano state indagate da un'apposita commissione del governo statunitense.

Ora *Griffin* dice di aver studiato le 87 ore in cui, tra marzo 2017 e marzo 2018, si sono verificati i maggiori acquisti di bitcoin con *Tether*, attraverso *Bitfinex* e pochi altri siti di *exchange*. I dati, che sono pubblici grazie alla *blockchain*, proverebbero la teoria della manipolazione. *Griffin* sostiene che gli acquisti di bitcoin analizzati rappresentino meno dell'1 per cento di quelli totali nel periodo studiato, ma da soli abbiano rappresentato almeno il 50 per cento dell'aumento di valore di *Bitcoin*. Secondo lo stesso *Griffin*, i dettagli ricorrenti di queste operazioni, tipo il numero di *Bitcoin* acquistati o il fatto che nei tre giorni precedenti a tutte queste operazioni erano state emesse larghe quantità di nuovi *Tether*, e che nell'ora precedente il valore dei *Bitcoin* fosse diminuito, escludono la possibilità che sia un fenomeno casuale. Il *pattern* sospetto si era interrotto dopo che *Tether* aveva smesso di emettere nuove unità a gennaio. Le operazioni erano riconducibili spesso a un ristretto e preciso gruppo di portafogli virtuali. Una manipolazione analoga, secondo *Griffin*, è stata portata avanti per mantenere stabile il valore di *Bitcoin* in alcuni momenti in cui era in calo.

Griffin ha basato le sue conclusioni sullo studio di milioni di operazioni, ma non ha prove concrete che *Bitfinex* abbia tramato in accordo con *Tether* per manipolare il mercato: e *van der Velde* ha negato qualsiasi coinvolgimento delle due società. Diversi esperti, come *Sarah Meiklejohn* della *University College London*, che è stata tra le prime a usare questo sistema di analisi, o *Philip Gradwell*, capo degli economisti a *Chainalysis*, una società che studia la *blockchain*, hanno detto che lo studio di *Griffin* è credibile. Lo stesso *Griffin*, poi, in passato aveva già scoperto un'importante manipolazione sui mercati finanziari tradizionali, e gestisce una società che si occupa di frodi sul mercato delle criptovalute. È possibile che queste nuove scoperte portino a nuove indagini, o che contribuiscano a quelle già in corso sulle due società.¹⁰¹

Lo studio sull'ipotesi di manipolazione del prezzo del *Bitcoin* ha lasciato l'amaro in bocca, ma ha soprattutto rinnovato l'invito ai regolatori a prendere tutte le misure necessarie a rendere il mercato un luogo veramente sicuro e libero in cui operare.¹⁰²

¹⁰¹ Cfr. GUEZ J. , “Il grande aumento di valore di *Bitcoin* dipese da una manipolazione del mercato?”, www.IIPost.it, 14 Giugno 2018

¹⁰² Cfr. GAGLIARDUCCI C. , “Il prezzo del *Bitcoin* è stato manipolato nel 2017: ecco come”, www.Money.it, 14 Giugno 2018

2.3.3 Principali cause del *Bust*

Come già detto, intorno al 20 Dicembre del 2017 è iniziata una fase di forte discesa.

Ovviamente, circolano diversi pareri ed idee relative alle principali cause che hanno portato il *Bitcoin* a perdere molti miliardi di capitalizzazione nel giro di poche settimane.

Una delle motivazioni principali di tale crollo è da attribuire alla stretta della *Sec (Securities and Exchange Commission)*, l'ente federale statunitense preposto alla vigilanza della borsa valori, alle *Ico*, per le quali è arrivata la prima condanna assoluta. Le *Ico* rivestono un ruolo importante all'interno del mondo della *blockchain* e delle criptovalute e la bocciatura della Consob americana rappresentava un paletto pesante da digerire per gli investitori, nonché un segnale negativo circa il futuro delle monete digitali.

Un'altra probabile causa è stata per molti "l'effetto Corea", causato dall'annuncio del ministro di giustizia sudcoreano di voler chiudere i siti di *exchange* del paese.

A tale dichiarazione seguì un *down* del 30% circa, essendo la Corea del Sud il terzo paese al mondo per volume d'affari in criptovalute. Anche se il governo lo ha di fatto smentito, dichiarando che si tratta solo di un'ipotesi e che i sudcoreani potrebbero sempre usare *exchange* stranieri, questo ha scatenato una piccola crisi di panico nei mercati, con molti investitori che per hanno iniziato a vendere, generando un "*panic selling*".¹⁰³

Anche dalla Cina sono giunte notizie non rassicuranti: Pechino ha infatti messo in atto una *escalation* di misure per non permettere ai cinesi di acquistare e vendere criptovalute.

Il vicegovernatore della *People's Bank of China*, *Pan Gongsheng*, ha affermato che le autorità locali avrebbero dovuto vietare anche tutte le piattaforme che offrono servizi di *trading* centralizzato sulle criptovalute, aggiungendo inoltre che sarebbero stati messi al bando tutti i siti nazionali e stranieri, le *app* mobili che forniscono servizi centralizzati per cinesi, piattaforme per servizi di pagamento in criptovalute e servizi che più in generale assistono gli utenti nello spostamento di fondi all'estero.

Insomma sono state prese misure per bloccare tutte le residue possibilità che i cittadini cinesi avevano di operare sulle criptovalute in un regime di inconvertibilità della valuta locale.

Le autorità locali hanno così chiuso le maggiori piattaforme per scambiare criptovalute bloccando di fatto l'operatività dei cinesi, frenati dalla impossibilità di conversione dello *yuan*.

La mossa di Pechino è attribuibile in prima battuta all'esigenza di mettere un freno al *trading* che si era trasformato in una modalità alla portata di tutti per esportare valuta. Con il risultato di accentuare la pressione anche sul cambio controllato e di mettere in difficoltà le autorità cinesi. Non è un caso

¹⁰³ Cfr. SPAGNUOLO E. , "*Bitcoin*, le 5+1 ragioni del crollo", *www.Wired.it*, 18 Gennaio 2018

che la stretta sia stata attuata alla vigilia di un delicato Congresso del Partito comunista che ha registrato gli equilibri del regime.¹⁰⁴

C'è stato anche chi ha ipotizzato per rassicurare gli investitori, erroneamente, che il mercato delle criptovalute attraversa un crollo ogni gennaio, e che quindi tali perdite fossero semplicemente fisiologiche.

Infatti, nel 2015 *Bitcoin* perse il 33 per cento, nel 2016 il 16 per cento, nel 2017 il 17 per cento, sempre intorno ai primi giorni di Gennaio e sempre nel giro di poche ore, anche se le moltissime cose cambiate nel settore negli ultimi mesi suggerivano di diffidare da chi riteneva il crollo un semplice fenomeno stagionale.¹⁰⁵

Oltre a diverse dichiarazioni di personaggi di rilievo, negli ultimi mesi un altro motivo ritenuto importante per la fase attraversata da *Bitcoin* è quello relativo ai continui rinvii della *SEC* in merito all'approvazione di un *Bitcoin Exchange Traded Fund (ETF)*.

Un *ETF* è una quota di un fondo indice quotato in borsa. I fondi indice sono fondi comuni di investimento aperti e indicizzati; cioè replicano fedelmente l'andamento di un indice azionario oppure obbligazionario, di un indice del mercato immobiliare, di indici settoriali o di panieri di azioni/obbligazioni. La caratteristica peculiare dei fondi indice è quella che viene chiamata gestione passiva. I gestori del fondo, cioè, non acquistano quello che vogliono. Ma tengono nel portafoglio del fondo gli stessi titoli che compongono l'indice di riferimento (*benchmark*) e nel medesimo peso percentuale.¹⁰⁶

Nel caso di *Bitcoin* quindi, si avrebbe un fondo che detiene *Bitcoin* e che vende azioni, le quali possono essere acquistate da potenziali clienti tramite il loro conto. Quindi l'idea è quella di accumulare un numero rilevanti di *Bitcoin*, e renderli simili a strumenti e prodotti finanziari scambiabili sui mercati in modo simile alle azioni.

In molti sostengono che i molteplici rinvii della *SEC* stiano contribuendo ad affossare il mercato delle criptovalute; infatti, giustificando la sua decisione con l'eccessiva volatilità del settore e con i possibili rischi da esso derivanti, la Commissione ha scelto di non dare il via libera allo strumento e di rigettare tutte le richieste avanzate in merito, almeno per il momento, nonostante nel corso degli ultimi mesi la domanda di *ETF* sul *Bitcoin* sia iniziata ad aumentare notevolmente.

Secondo gli esperti, potrebbe essere proprio il crescente interesse delle istituzioni finanziarie e delle grandi banche a spingere la Commissione verso l'approvazione dello strumento.

¹⁰⁴ Cfr. SOLDAVINI P. , “Ecco come e perché Cina e Corea del Sud dichiarano guerra al *Bitcoin*”, *Mercati & Finanza*, Il Sole 24 ore, 16 Gennaio 2018

¹⁰⁵ Cfr. “Il crollo di *Bitcoin* e delle criptovalute, spiegato”, www.ILPost.it, 17 Gennaio 2018

¹⁰⁶ Cfr. LEONELLI M. , “*ETF (Exchange Traded Fund)*: cosa sono e perché sono vantaggiosi”, www.Soldionline.it, 2018

Il via libera della SEC potrebbe inoltre determinare il tanto atteso rimbalzo delle quotazioni delle criptovalute, mentre secondo personaggi come *John Wu*, CEO di *SharesPost Digital Assets Group*, l'ok della Commissione darà al mercato la fiducia necessaria e una maggiore chiarezza sul fronte regolamentazione.¹⁰⁷

Tuttavia, recentemente, la decisione sulla domanda degli *ETF* è stata posticipata fino al 27 febbraio 2019.

2.3.4 Andamento delle *Altcoins* nel 2018

Dopo aver analizzato il sorprendente andamento pluriennale del *Btc*, soffermiamoci innanzitutto sulle migliori e peggiori *altcoins* nell'anno immediatamente successivo al grande *boom* del *Bitcoin* ed in generale delle *criptocurrencies*, l'anno che per molti ha messo a nudo i grandi problemi legati a questo mondo digitale.

Il 2018 è stato infatti un periodo davvero molto negativo per le criptovalute; dopo la *performance* notevole dell'anno precedente, l'intero mercato ha assaporato una serie di mesi in rosso, con le monete virtuali che sono state al centro di forti ribassi.

Con il passare del tempo alcuni analisti sostenevano che questa potesse essere solo una battuta d'arresto, altri che era solo l'inizio della discesa, altri ancora che le criptovalute erano finite e che si erano rilevate una bolla.

L'unica certezza oggi nota è che le criptovalute non sono fallite, ma si sono certamente ridimensionate.

Venuti meno i fasti della "criptomania", numerosi progetti sono sull'orlo della bancarotta, mentre altri stanno adottando misure drastiche, come il taglio del personale e la riorganizzazione.

Tutte le criptovalute, tranne rare eccezioni, sono calate nella capitalizzazione.

Tuttavia, alcune sono andate meglio di altre.

Andiamo quindi ad elencare alcune tra le migliori e peggiori *altcoins* in questi mesi profondamente negativi per questo tipo di mercato digitale, partendo dalle migliori prestazioni.¹⁰⁸

La migliore *performance* registrata in questo lasso di tempo è da attribuire ad *Odem (ODE)*, con un aumento del 197% della propria capitalizzazione di mercato.

¹⁰⁷ Cfr. GAGLIARDUCCI C. , "Criptovalute: cosa accadrebbe con l'approvazione dell'ETF su Bitcoin", *Economia e Finanza*, www.Money.it, 15 Ottobre 2018

¹⁰⁸ Tale analisi include esclusivamente le prime 100 criptovalute per capitalizzazione di mercato, escludendo *altcoins* di valore irrilevante o che siano state create da meno di 6 mesi.

Odem, lanciato nell'Aprile 2018, fa parte di una piattaforma *blockchain* che mira a cambiare il futuro dell'istruzione e delle certificazioni.

Secondo il sito *web* del progetto, la piattaforma sarà un luogo in cui studenti e rappresentanti degli studenti possono creare e richiedere servizi per programmi di istruzione.

Gli insegnanti e i fornitori di servizi educativi possono ricevere richieste per la realizzazione del programma e la fornitura dei servizi. Valutando la seconda migliore prestazione dell'anno appena trascorso, da attribuire a *Huobi Token (HT)*, si noterà che *Odem* è stata l'unica criptovaluta ad essere cresciuta in questo periodo, in quanto la seconda migliore criptovaluta ha registrato una perdita del 19%. Un risultato assurdo, considerando un campione oggetto di studio composto da ben 100 valute digitali, e che mostra come il mercato delle *altcoins* sia fortemente correlato con il *Bitcoin*, come si analizzerà nel capitolo 3. Il *Token* di *Huobi*, lanciato nel gennaio 2018, è la criptovaluta nativa di *exchange* meglio classificata in questo elenco; è stato inizialmente creato e distribuito ai membri *VIP* di *Huobi*, uno dei principali exchange di criptovalute in Cina, in risposta al *ban* delle *crypto* da parte della Cina e alla diminuzione dell'attività di trading. Tra le peggiori *performance*, invece, non si può non menzionare quella di *Bitcoin Cash*, la decima tra le peggiori per esattezza, con una perdita di capitalizzazione del 95,5% circa. Tale perdite hanno seguito una fase di fortissimo rialzo, che avevano permesso a *Bitcoin Cash* di imporsi molto presto nel mercato come una tra le criptovalute più interessanti ma soprattutto più utilizzate, come già detto nel 1 Capitolo. Il motivo principale di questo disastroso andamento è stato un *hard fork* contenzioso che ha diviso la *community*, causando una spaccatura al suo interno e generando forti perdite per tale criptovaluta. Incredibile però, come, con una perdita del genere, *Bch* sia soltanto la decima tra le peggiori *criptocurrencies*; vi sono, quindi, criptovalute andate anche peggio. Le peggiori tre, infatti, sono state *Aion* (-97,57%), *Qtum* (-97,36%) e *Bitcoin Private* (-97,26%).¹⁰⁹ Delle perdite clamorose, che rispecchiano il momento negativo per il mondo delle valute digitali ma soprattutto la forte volatilità che da sempre le contraddistingue e che, molto probabilmente, continuerà a farlo, considerando che solo pochi mesi fa erano nel loro momento migliore, sconvolgendo investitori, scettici ma, soprattutto, l'intero mercato mondiale.

Proprio per questo, però, non è possibile sbilanciarsi sull'andamento futuro delle stesse.

Si è pronosticato, infatti, che la maggior parte delle *altcoin* "andrà a zero"; in molti, me compreso, sostengono invece che, per via delle caratteristiche e dell'andamento storico di tali strumenti, da sempre caratterizzato, come visto, da frequenti e notevoli "up & down", le criptovalute si riprenderanno e torneranno ad avere valori molto più alti di quelli attuali, per la gioia di molti investitori.

¹⁰⁹ Cfr. BROGNA G. , "Le 10 peggiori e le 10 migliori criptovalute per *performance* nel 2018", www.Etherevolution.it, 27 Dicembre 2018

Capitolo 3 - Ultime analisi

Nel capitolo precedente, oltre ai vari pro e contro che contraddistinguono il mondo delle *criptocurrencies* da quello delle monete *fiat*, ci si è soffermati sull'analisi dell'andamento del *Bitcoin* in questi suoi primi 10 anni di vita all'interno del mercato; successivamente, sono state menzionate alcune tra le migliori e le peggiori *altcoins* per rendimento nel 2018, anno molto importante per queste tipologie di strumenti digitali, poiché ha mostrato per l'ennesima volta, semmai ce ne fosse bisogno, quanto le criptovalute fossero altamente volatili ed instabili.

Non sono però state ancora considerate alcune tra le più importanti *altcoins* per capitalizzazione.

In questo capitolo conclusivo, dunque, si farà una valutazione delle *performance* di criptovalute come *Ethereum*, *Ripple*, *Litecoin* e *Bitcoin Cash*, menzionando i principali fattori che hanno contribuito ad influenzare, complessivamente, l'andamento delle stesse.

Inoltre si andrà a valutare la correlazione che c'è tra il *Bitcoin* e le altre valute digitali, che, come si è già intuito nel capitolo precedente, è un fattore chiave di queste monete digitali e che causa spesso andamenti di mercato coerenti con quello del *Btc*.

Si andrà infine ad analizzare l'impatto che l'incertezza della politica economica potrebbe avere sul *Btc* ed i casi in cui quest'ultimo potrebbe fungere da elemento di copertura dal rischio di mercato.

3.1 *Performance* delle principali *altcoins* nel 2018

Dopo il grande *exploit* che ha visto il settore delle criptovalute crescere in maniera esponenziale in un lasso di tempo molto breve, ha fatto seguito un periodo di forte calo per lo stesso settore, con *Bitcoin* e le altre valute che non sono riuscite a riprendersi da questa fase di declino.

Sono state registrate perdite di miliardi di dollari in poche settimane, mediante un crollo economico giustificato da diverse ragioni, si pensi al crescente controllo regolamentare o alle iniziative prese dai giganti di *Internet* come *Google*, *Facebook* e *Twitter*, che non consentono più agli inserzionisti di creare pubblicità sulle criptovalute.¹¹⁰

Quasi tutte le criptovalute nel 2017 avevano infatti realizzato incredibili guadagni e i prezzi in aumento hanno creato un inevitabile ciclo di *feedback* positivi, attirando sempre più capitali nella rete. Sfortunatamente, nel momento in cui *Bitcoin* e le altre *criptocurrencies* hanno cominciato a

¹¹⁰ Cfr. GIAMBARRESI F. , “Criptovalute: *Bitcoin*, *Ethereum* e *Ripple* in caduta”, www.Webnews.it, 4 Aprile 2018

perdere terreno, questo mercato fortemente volatile ha portato a massicci disinvestimenti, con le diverse *criptocurrencies* che hanno conosciuto, fatta eccezione per pochi casi particolari come *Odem*, un unico andamento comune: quello del ribasso.

Questo effetto è generato principalmente dalla grande correlazione che esiste tra il *Btc* e tutto il resto delle principali criptovalute.

Tra le più importanti *altcoins* da considerare, si parte da *Ripple (XRP)*, che, specialmente a causa del calo maggiore di *Ethereum*, attualmente è la seconda criptovaluta per capitalizzazione nel mercato, alle spalle ovviamente del *Btc*.

Figura 10: Fonte *Coinmarketcap*, performance del *Ripple*



Come si può notare nel grafico, *Ripple*, come la maggior parte delle criptovalute, ha avuto un violento *exploit* nello stesso periodo del *Bitcoin*, per poi scendere di valore drasticamente.

In questo caso, si è passati dal punto massimo di capitalizzazione di circa 140 miliardi di dollari, con un prezzo per *token* fissato a circa 3,65 dollari, ad una capitalizzazione attuale di mercato pari a circa 13 miliardi di dollari, con un prezzo per *token* di circa 0,3 dollari.¹¹¹

¹¹¹ Dati al 02/02/2019 reperiti tramite la piattaforma www.Coinmarketcap.com

Buona parte degli esperti e degli analisti finanziari ritiene però che *Ripple*, per il 2019, raggiungerà nuovi massimi. Si sostiene che con l'attuale capitalizzazione di mercato, il margine di miglioramento è piuttosto interessante ed i *capital gain* davvero promettenti.

Il *CEO Brad Garlinghouse* ha lasciato intendere di essere comunque soddisfatto sulla *performance* di *Ripple* nel 2018, principalmente perchè la rete delle banche clienti di XRP è arrivata a circa 150 unità. Al di là della debolezza strutturale del 2018, quindi, *Ripple* sembra godere della fiducia degli investitori. Un evento che potrebbe avere un buon impatto su questa criptomoneta nel 2019 potrebbe essere la concretizzazione della *partnership* con *Apple*.¹¹²

Ripple riceve grandi consensi da parte degli utenti privati, ma anche dai principali intermediari creditizi e dalle banche di tutto il mondo.

Inoltre, molte istituzioni finanziarie utilizzano il protocollo *Ripple* per trasferire denaro da una parte all'altra del mondo.¹¹³

Discorso simile si può fare anche con *Ethereum*, in quanto anche per questa criptomoneta il 2018 è stato un anno da dimenticare, almeno dal punto di vista delle performance del prezzo; infatti *Ether*, il token nativo della *blockchain* di *Ethereum*, ha perso fino a circa il 94% dal suo massimo storico del gennaio 2018.

Nella classifica della capitalizzazione di mercato, *Ethereum* ha dovuto cedere, come già detto, la seconda posizione a *Ripple*, in particolare in occasione del duro *sell off* di novembre-dicembre.

Dal punto di vista dell'evoluzione tecnologica, anche nel 2018 il progetto ha continuato ad essere al centro dell'attenzione per le ricerche e per la pianificazione degli sviluppi futuri ma, nonostante le interessanti novità in divenire sul piano dello sviluppo, il prezzo di *Ether* ha continuato a scendere, evidentemente condizionato dal lungo “*bear market*”¹¹⁴ che ha interessato l'intera categoria di strumenti.

L'entusiasmo degli investitori che all'inizio dell'anno portarono *Ether* a volare oltre i 1400 dollari, oggi sembra un triste ricordo.

Il motivo principale del violento calo della stessa criptomoneta risiede probabilmente nella stretta connessione tra *Ethereum* e *ICO* che oggi sta pericolosamente stringendo il collo alle quotazioni; nella maggior parte dei casi, risulta infatti che gli emittenti di *ICO* non hanno rispettato i regolamenti, creando non pochi problemi per i numerosi investitori e risparmiatori.

¹¹² Cfr. “Previsioni *Ripple* 2019: possibile target tra 3 e 5 USD ma ottimisti vedono XRP a 20 USD”, www.Borsainside.com, 2 Gennaio 2019

¹¹³ Cfr. PACE F. , “Quotazione *Ripple* 2019: quali sono le previsioni degli esperti?”, www.Trendonline.com, 24 Gennaio 2019

¹¹⁴ Con il “*bear market*” si intende un mercato che tende al ribasso. Questo si contrappone al “*bull market*”, in cui si intende un mercato rialzista.

Questi progetti relativi alle *Initial Coin Offering* hanno infatti delle libertà che quasi nessun'altra azienda può permettersi, generando non pochi problemi, come le numerose frodi che sono state fatte nel tempo ai danni degli investitori.

Normalmente chi ottiene denaro mediante una raccolta di fondi pubblica, dovrebbe dichiarare pubblicamente cosa sta facendo e cosa intende fare con i fondi raccolti; tale trasparenza sembra mancare alle varie *ICO*, soprattutto per l'assenza di una chiara regolamentazione.¹¹⁵

Anche *Vitalik Buterin*, fondatore di *Ethereum*, ha fatto alcune osservazioni molto interessanti riguardo alle ultime *ICO*, in quanto egli ritiene che l'attuale tendenza delle vendite massive di gettoni sia insostenibile. Lo stesso *Buterin* al quotidiano finanziario *TheMarker* ha fatto queste dichiarazioni: “sarebbe un errore sottovalutare il valore delle *ICO* o dire che sono una cosa negativa.

Le ICO sono interessanti perché consentono la monetizzazione per progetti open source, cosa che spesso non avviene.

Quello che stiamo vedendo recentemente, però, è che la gente sta prendendo questa idea in maniera sbagliata e ci sono progetti che emettono una moneta esclusivamente per raccogliere denaro.

Molti progetti stanno raccogliendo più soldi di quello che sarebbero in grado di raccogliere nel mercato normale del Venture Capital e talvolta non vi è alcuna corrispondenza tra la necessità, l'utilità del progetto e la sua capacità di raccogliere fondi.

*Inoltre, questo mercato è ancora giovane e la gente ancora non sa come distinguere tra diversi progetti. Se molte *ICO* falliscono, questo è un rischio per il mercato (anche per lo stesso *Ethereum*).*

Dobbiamo evitare l'eccessiva pubblicizzazione di questi progetti.

Il modo per valutarli è principalmente valutare le persone che sono dietro al progetto.

*Purtroppo ci sono progetti che fanno dichiarazioni false pur di raccogliere denaro in *ICO*, ma, a lungo andare, il mercato deve trovare un modo per giudicare quali progetti hanno senso e quale sia il loro valore appropriato.”¹¹⁶*

La situazione relativa alle *ICO* rafforza ulteriormente le intenzioni della *SEC* di regolamentare la raccolta delle stesse e definire la terminologia corretta tra *token utility* e *security*.

Se venissero infatti approvate delle regole a protezione degli investitori dai progetti truffaldini nel mondo delle *ICO*, *Ethereum* potrebbe probabilmente rivendicare legittimità come la miglior piattaforma di *crowdfunding* per *ICO*.

¹¹⁵ Cfr. GATTI M. , “Mercato in altalena: le *ICO* hanno venduto oltre 100'000 *Ethereum (ETH)*. Le ultime dalla *SEC*.”, www.Cryptominando.it, 27 Novembre 2018

¹¹⁶ Cfr. MICHELI F. , “Il fondatore di *Ethereum*, *Vitalik Buterin* contro le *ICO*: sono una bolla”, www.criptovalute24.it , 2018

In attesa di possibili sviluppi, l'incertezza continuerà a prevalere ed influire sulla volatilità dei mercati crittografici, ma non è da escludere che un eventuale intervento legislativo possa far tornare *Ethereum* ai livelli economici di pochi mesi fa.

Figura 11: Fonte *Coinmarketcap*, performance di *Ethereum* nel 2018

Ethereum Charts



Non fanno eccezione, tra le più importanti criptomonete del mercato, il *Litecoin* ed il *Bitcoin cash*, seguendo sostanzialmente lo stesso livello di *performance* delle altre.

Analizzando la prima criptomoneta, va detto che anche per “l’argento digitale”, dopo aver toccato un massimo di circa 330 dollari alla fine del 2017, il 2018 è stato un anno da dimenticare, con le quotazioni che sono tornate agli stessi valori della prima metà del 2017, a circa 33 dollari.¹¹⁷

Tra le cause principali di questo brusco ridimensionamento che vanno ad aggiungersi, ovviamente, alla forte correlazione con il *Btc*, si ricorda la chiusura di *LitePay*, il recente sistema di pagamento con carta di debito alimentato in *LTC*, nel mese di Marzo, che ha causato in poche ore una perdita superiore al 15%.¹¹⁸

¹¹⁷ I dati sono stati aggiornati in data 02/02/2019 tramite la piattaforma *Coinmarketcap.com*

¹¹⁸ Cfr. “Con la chiusura di *LitePay*, *Litecoin* rileva un calo del 15% del valore”, www.Monetevirtualipro.it, 28 Marzo 2018

Quello tra la *Foundation* di *LTC* e *LitePay* si è delineato, infatti, come un rapporto particolarmente difficile negli ultimi periodi.

A *Kenneth Asare*, *Ceo* di *LitePay*, è stato più volte richiesto di fornire ulteriori dettagli in merito allo stato del progetto, ma il *CEO*, oltre a non riuscire a dar certezze sulla validità dello stesso, ha spesso risposto richiedendo nuovi finanziamenti. Un dialogo non sufficiente a proseguire il rapporto, secondo la fondazione, che ha rifiutato di concedere ulteriori fondi a *LitePay* e che, successivamente, ha pubblicato un bollettino lunedì 26 marzo, nel quale si informava il pubblico della chiusura di *LitePay*, scusandosi per "non aver effettuato abbastanza pratiche di *due diligence*"¹¹⁹ prima di promuovere la società.¹²⁰

Figura 12: Fonte *Coinmarketcap*, andamento del *Litecoin* nel 2018

Litecoin Charts



La stessa situazione riguarda *Bitcoin Cash*, la criptomoneta nata recentemente da una *hard fork* di *Btc*. L'andamento ha seguito quello delle altre grandi criptovalute ma in maniera più intensa, in quanto *BCH*, attualmente quinta per capitalizzazione, ha subito un crollo molto violento del 95,5% circa, passando da una valutazione di quasi 5000 dollari del 20 Dicembre 2017, quando grazie al

¹¹⁹ Con "due diligence" si fa riferimento ad uno scrupoloso studio dei dati e delle possibili sfumature di un determinato progetto, con la finalità di valutarne la convenienza.

¹²⁰ Cfr. GAGLIARDUCCI C. , "Litecoin: tonfo del 14% in un solo giorno. Che succede?", *www.Money.it*, 27 Marzo 2018

debutto sulla piattaforma *Coinbase* la moneta registrò un +50% del proprio valore in sole 24 ore, ad una valutazione attuale di poco inferiore ai 120 dollari, come si può verificare dalla figura 4.¹²¹

Figura 13: Fonte *Coinmarkecap*, andamento del *BCH*

Bitcoin Cash Charts



Come già descritto, un evento che ha contribuito fortemente a tale situazione di ribasso è certamente quello relativo al *fork* di tale criptomoneta in data 15 Novembre.

Prima del *fork*, *Bitcoin Cash* aveva un prezzo di circa 500 dollari, salito a 530 nei giorni a ridosso del 15 novembre. Poi il 14 novembre è iniziato il crollo: prima è sceso a 480, poi in brevissimo tempo raggiunge il suo minimo storico di 75 dollari, come è evidenziato nella figura 5.

Insomma, a causa del *fork* ha perso gran parte del proprio valore.

Ma la cosa più importante è che ha perso valore anche rispetto a *BTC*. Infatti prima del *fork* 1 *BCH* valeva circa 0,085 *BTC* per poi, nel giro di un mese, crollare a 0,023 *BTC*.

¹²¹ Cfr. CAVICCHIOLI M., “Mentre Bitcoin scende, Bitcoin Cash sale”, www.IIBitcoin.it, 20 Dicembre 2017

In altre parole il *fork* di *BCH* ha fatto male un po' a tutte le criptovalute, ma soprattutto allo stesso *BCH*.

Il *fork* ha generato due criptovalute, *Bitcoin Cash ABC* e *Bitcoin Cash SV (Satoshi's Vision)*, ma ad oggi non è ancora certo quale delle due sarà considerata la vera erede di *BCH*.

Inoltre, tale scissione non è sembrata giustificata da uno scopo tecnico o da un indirizzo strategico, generando diffidenza ed incertezza per gli investitori: si sosteneva infatti che questo evento aveva ragioni diverse e aventi poco o nulla a che vedere con il mondo delle criptovalute.¹²²

In aggiunta, il *fork* ha dimostrato che dietro al progetto *Bitcoin Cash* ci sono in realtà due gruppi distinti, ovvero quello che appoggia *ABC* e quello che appoggia *SV*.

Tutto ciò è molto distante dalla “visione” originale di *Satoshi Nakamoto*, che creò una criptovaluta decentralizzata che non potesse essere controllata da nessuno.¹²³

Non sono mancate sul tema diverse riflessioni.

Pierangelo Soldavini de Il Sole 24, dichiara: “si ha la sensazione di assistere a una lite di famiglia, senza alcuna giustificazione precisa se non uno scontro di potere tra i creatori della nuova valuta.

Il risultato è che il valore del *BCH* si è più che dimezzato in una settimana, arrivando a quota 200 dollari, rispetto a 530 sette giorni fa.

Nel complesso quindi la *hard fork*, ha contribuito a rafforzare l'immagine di un mondo senza governance, decisamente opaco e in mano a pochi attori che ne possono determinare le evoluzioni”. Ciò sembrerebbe rafforzare la percezione di una totale mancanza di *governance*, che non farà altro che allontanare gli investitori più tradizionali e le istituzioni.¹²⁴

La cosa più importante che va sottolineata, però, è che il *fork* di *Bitcoin Cash* è da molti considerato come il *trigger event* che ha determinato il crollo delle quotazioni di tutto il mercato delle criptovalute; probabilmente tutti gli eventi e le contraddizioni emerse dall'*hard fork* di *Bch* hanno fortemente contribuito ad acuire le tensioni nel mercato, già provato dal *tether affaire*.

Inoltre la paura che in un prossimo futuro si possano verificare degli *hard fork* anche su altre *blockchain* che al momento sono rimaste indenni da tali problematiche, ha finito per destabilizzare ulteriormente l'ambiente.¹²⁵

¹²² Cfr. “*Bitcoin* perde il 30% a Novembre: crollo definitivo?”, www.OkForex.it, 20 Novembre 2018

¹²³ Cfr. CAVICCHIOLI M. , “*Bitcoin Cash* crolla a causa del *fork*”, www.IlBitcoin.it, 17 Novembre 2018

¹²⁴ Cfr. SOLDAVINI P. , “*Bitcoin* in caduta libera perde il 30% in una settimana: le tre ragioni del crollo”, *IlSole 24 ore*, 20 Novembre 2018

¹²⁵ Cfr. PALUSCI C. , “cosa ha determinato il crollo del *Bitcoin*?”, www.Investing.com, 6 Dicembre 2018

Figura 14: Fonte *Coinmarketcap*, crollo del *Bch* immediatamente dopo il *fork*

Bitcoin Cash Charts



3.2 Correlazione tra *Bitcoin* e le principali *Altcoins*

Come abbiamo appena visto, il crollo del *Btc* ha portato inevitabili perdite anche per le più importanti criptovalute presenti nel mercato, giustificando l'idea di una possibile correlazione tra esse.

Le principali *altcoins* hanno seguito, nel periodo di studio considerato, un andamento quasi all'unisono, seppure con intensità diverse.

Sono stati considerati per completezza anche gli eventi più importanti che hanno principalmente influenzato, in negativo, la *performance* delle criptomonete nel 2018.

Tali eventi sono stati sicuramente rilevanti e di un certo peso nel contesto che ha visto un crollo di tali strumenti ma, principalmente, la causa fondamentale di un quasi identico andamento di mercato della grandissima maggioranza delle *criptocurrencies* è la forte correlazione che c'è tra questi stessi strumenti ed il "market mover", ossia il *Bitcoin*.

Prima di iniziare un'analisi di tale argomento, definiamo in maniera molto semplice il concetto di correlazione.

La correlazione è una misura statistica del grado di corrispondenza di 2 o più variabili, che di norma viene espressa come un coefficiente che oscilla tra -1 e +1, a seconda del grado di correlazione.

Una correlazione positiva determina una forte dipendenza tra le variabili considerate, nel senso che, ad una variazione di una, seguirà la variazione dell'altra e, ovviamente, più il coefficiente è prossimo all'unità, maggiore sarà l'intensità della variazione; viceversa, in caso di correlazione negativa, si avrà un effetto completamente contrario.

Nel caso di un coefficiente di correlazione pari a 0, semplicemente non vi sarà alcuna relazione tra le variabili considerate.¹²⁶

$$\rho_{xy} = \frac{\sigma_{xy}}{\sigma_x \cdot \sigma_y}$$

Questa formula mostra che è possibile ottenere il coefficiente di correlazione tramite il rapporto tra la Covarianza di 2 variabili X ed Y, ed il prodotto delle Variazioni standard di entrambe.

Tale valore può anche essere espresso in questo modo:

$$\rho_{xy} = \frac{\sum(x - \bar{x})(y - \bar{y})}{\sqrt{\sum(x - \bar{x})^2 \sum(y - \bar{y})^2}}$$

Dove \bar{x} e \bar{y} sono i valori medi.¹²⁷

Tornando adesso alla correlazione che riguarda le criptomonete, uno studio rivela che la tendenza al ribasso del 2018 ha portato ad un aumento della correlazione stessa nei principali mercati. Secondo tale analisi, ben 10 delle 15 maggiori criptovalute per capitalizzazione di mercato mostrano una correlazione di prezzo superiore al 65%.¹²⁸

Per rendere meglio il concetto, ho stimato, mediante *Excel*, la correlazione che hanno alcune tra le maggiori criptomonete con il Bitcoin, ovvero *Ethereum*, *Ripple*, *Bitcoin Cash*, *Litecoin*, *Eos* e *Monero*.

L'orizzonte temporale scelto per tale analisi è il periodo che intercorre tra l'*exploit* delle stesse, ovvero Dicembre 2017, ad oggi.

¹²⁶ Cfr. CICCHITELLI G., D'URSO P., MINOZZO M., *Statistica: principi e metodi 3/Edizione*, Pearson

¹²⁷ Cfr. CICCHITELLI G., D'URSO P., MINOZZO M., *Statistica: principi e metodi 3/Edizione*, cit.

¹²⁸ Cfr. "Studio: le principali criptovalute mostrano una correlazione di prezzo elevata", www.Nanobitonline.it, 7 Gennaio 2019

I valori scelti sono quelli corrispondenti al prezzo di chiusura giornaliero del giorno 1 di ogni mese di una determinata criptovaluta e i dati storici sono stati raccolti tramite la piattaforma *Coinmarketcap*.

Tabella 1: Correlazione delle principali *altcoins* rispetto a *Btc*

DATA	BTC	ETH	XRP	BCH	LTC	EOS	XMR
01/02/2019	3487,95	107,61	0,308517	116,56	32,83	2,34	43,72
01/01/2019	3843,52	140,82	0,364771	164,85	31,98	2,66	48,37
01/12/2018	4214,67	118,64	0,372906	172,12	34,34	2,96	59,65
01/11/2018	6377,78	198,87	0,455722	424,09	50,27	5,28	103,88
01/10/2018	6589,62	230,77	0,576461	530,91	60,21	5,74	114,52
01/09/2018	7193,25	295,34	0,347721	615,31	65,95	6,64	120,97
01/08/2018	7624,91	420,75	0,445852	769,35	77,86	7,26	128,15
01/07/2018	6385,82	453,92	0,461358	739,42	80,24	8,13	129,77
01/06/2018	7541,45	580,04	0,623364	1002,92	119,92	12,31	157,54
01/05/2018	9119,01	673,61	0,841407	1351,28	148,49	18,95	240,26
01/04/2018	6844,23	379,61	0,485081	643,03	115,22	5,66	175,51
01/03/2018	10951	872,2	0,928347	1291,92	209,75	8,63	314,04
01/02/2018	9170,54	1036,79	0,96253	1274,35	142,30	10,21	240,96
01/01/2018	13657,2	772,64	2,39	2432,54	229,03	8,84	358,99
01/12/2017	10957,6	466,54	0,255699	1462,68	99	3,24	190,94
Correlazione	1	0,794	0,726	0,966	0,892	0,461	0,940

Come si può notare, i dati ottenuti certificano ciò che è stato detto fino ad ora: tra le varie criptovalute vi è una correlazione altissima.

È fondamentale però chiarire che la correlazione non è statica, ma tende a variare nel tempo: infatti, generalmente, la correlazione tra diverse classi di attività e mercati aumenta in periodi di elevata volatilità.¹²⁹

E' sempre fondamentale scegliere un determinato arco temporale su cui fare le proprie valutazioni e su cui basare le proprie scelte.¹³⁰

¹²⁹ Cfr. “4 Motivi per cui la questione della correlazione del mercato”, www.talkingofmoney.com

¹³⁰ Cfr. CAVALLI S. , “I legami tra *Bitcoin* e *Altcoins* ci sono: la Matrice di Correlazione”, www.CryptoMinando.it, 12 Luglio 2018

Infatti, spostando l'analisi su uno stesso orizzonte temporale ma prendendo come riferimento i dati giornalieri e non quelli mensili, come in questo caso, verranno risultati leggermente differenti, ma comunque rappresentativi di alta correlazione.

I risultati ottenuti sono i seguenti:

- Correlazione *BTC/ETH* = 0,89
- Correlazione *BTC/XRP* = 0,83
- Correlazione *BTC/BCH* = 0,92
- Correlazione *BTC/LTC* = 0,91
- Correlazione *BTC/EOS* = 0,71
- Correlazione *BTC/XMR* = 0,94

3.3 Volatilità delle criptovalute

Tra tutte le caratteristiche identificate in questo elaborato, la volatilità del prezzo è senza ombra di dubbio la differenza più grande che intercorre tra *Bitcoin* e le valute aventi corso legale, cito fra tutte Euro e Dollaro.

Le ormai abituali oscillazioni di prezzo delle *criptocurrencies* non stanno facendo altro che favorire l'ingresso nel *crypto market* di speculatori, intenzionati esclusivamente ad ottenere ricavi in breve tempo mediante un fortunato investimento, a sfavore della funzione di riserva di valore che le stesse criptovalute dovrebbero avere; questo problema rischia inoltre di ostacolare il futuro utilizzo globale delle valute digitali a favore delle monete legali.¹³¹

3.3.1 Un nuovo strumento: le *Stablecoins*

Proprio per far sì che l'intero mondo delle *criptocurrencies* non venisse considerato dalla maggior parte degli investitori esclusivamente come un semplice investimento speculativo, caratterizzato da forti rialzi o ribassi in tempistiche molto brevi, sono state prese diverse iniziative.

Tra le più importanti va incluso sicuramente il lancio delle *Stablecoins*.

¹³¹ Cfr. LEMME G. , PELUSO S. , “Criptomoneta e distacco dalla moneta legale: il caso *Bitcoin*”, cit.

Queste sono delle criptovalute, nate in tempi molto recenti, che vogliono eliminare uno dei maggiori problemi del settore, ovvero la volatilità del prezzo, garantendo al contempo un'operatività il più possibile simile a quella dei mercati tradizionali delle criptovalute, anche per eludere le stringenti normative che regolano l'attività bancaria.

Le *stablecoins* sono quindi degli *assets* che godono delle proprietà di riserva di valore e unità di conto, diversamente da tutte le altre criptomonete, e al pari della moneta legale, i cui valori economici sono completamente soggetti alla legge della domanda e dell'offerta.¹³²

Per poter soddisfare la caratteristica della *stability*, queste si legano ad altre risorse, come una valuta tradizionale o a una materia prima, senza comunque vincolarsi ad alcuna banca centrale; inoltre cercano di riprodurre la stabilità della valuta cartacea tradizionale, garantendo tutte le caratteristiche principali delle criptovalute, ovvero trasferimenti veloci, sicuri ed economici per i suoi utenti, che possono usufruirne ovunque nel mondo con una semplice connessione ad *internet*.¹³³

Esistono 3 tipologie di *stablecoin*: vediamo nel dettaglio quali sono e in cosa consistono.

Una prima tipologia è quella delle *stablecoins* collaterali in valuta *fiat*: questa si basa sul fatto che una certa quantità di moneta in corso legale, come il dollaro, venga depositata a garanzia dell'emissione delle criptovalute e le *stablecoins* siano emesse in proporzione uno a uno rispetto a tale moneta legale. Sebbene questo metodo sia solido, richiede la centralizzazione e l'affidarsi a un custode, che andrà controllato periodicamente da revisori. Il sistema può essere costoso, e anche uscire da una *stablecoin* con queste caratteristiche avrà un costo.

Nelle *stablecoins* di secondo tipo, il collaterale è invece sostenuto da altre criptovalute e non da dollari o oro. In questo modo tutto può restare sulla *blockchain* e non c'è bisogno di un'autorità centrale.

Il problema è che le criptovalute sono instabili, il che significa che le garanzie fluttueranno.

Per risolvere quindi questo problema la *stablecoin* viene sovra-garantita, mediante depositi maggiori del sottostante, per fare in modo che possa assorbire le fluttuazioni dei prezzi nel collaterale.

Tuttavia, in caso di un evento finanziario imprevedibile, a causa del quale la criptovaluta sottostante perderebbe tutto il suo valore, anche la *stablecoin* collasserebbe e le perdite sarebbero addirittura maggiori per via della sovra-garanzia.

Infine l'ultima famiglia di *stablecoin* è quella delle "non collateralizzate", cioè senza garanzie.

Queste si basano sulla fiducia e chi le acquista crede che il prezzo rimarrà fisso, senza che vi sia alcun tipo di arbitraggio dei mercati. In pratica la fornitura della moneta è dettata dal valore sul mercato della *stablecoin*. Se il prezzo supera un dollaro, l'offerta di moneta aumenta per riportarlo in basso, e quando il prezzo è inferiore a un dollaro, l'offerta diminuisce.

¹³² Cfr. COSCIA E. , "Stablecoins: cosa sono e come funzionano", www.Fintastico.com, 8 Giugno 2018

¹³³ Cfr. WARNER J. , "Cosa sono gli *Stablecoin* e come funzionano?", www.IgBank.it, Dicembre 2018

Questo tipo di meccanismo punta a creare una pressione al rialzo e al ribasso sul prezzo. Se, insomma, abbastanza persone credono che il sistema sopravviverà, questa convinzione porterà a un ciclo virtuoso che ne garantirà la sopravvivenza.¹³⁴

Volendo fare infine una panoramica di mercato, le *stablecoins* sono diventate maggiormente utilizzate nella seconda metà del 2018, rappresentando una proposta sempre più allettante, in particolare per gli investitori timorosi della volatilità dei prezzi delle criptovalute tradizionali, che mostrano una grande quantità di fluttuazioni anche per valutazioni *intra-day*.

Per avere un'idea dello stato dell'arte delle *stablecoins* può essere interessante il recente studio realizzato da *Blockchain.com*, da cui emerge che al momento dell'analisi erano presenti sul mercato 57 *stablecoins* di cui 23 (il 40%) già disponibili sul mercato e 34 (60%) in fase di pre-lancio.

Per il 66% delle *stablecoins* è il dollaro il collaterale di riferimento, per il resto sono utilizzate altre valute *fiat* (euro, yen), beni (oro) e inflazione.¹³⁵

Una *stablecoin* funzionante potrebbe davvero essere qualcosa di importante per il mercato delle criptovalute, ma, da un punto di vista rivolto ai profitti, al momento non ci sono molte ragioni per utilizzare una *stablecoin*, soprattutto nel lungo termine, principalmente per via dei bassi rendimenti. Esistono inoltre diversi problemi di fiducia relativi all'investimento in una *stablecoin*, come la credibilità di chi emette tali strumenti o la sicurezza della *blockchain* sottostante.¹³⁶

3.3.2 Studio della volatilità

È interessante notare che lo *status* di *Bitcoin* come una risorsa altamente volatile, è diventato un tema principale nella stampa finanziaria e nel mondo accademico; la stessa volatilità insita nel *Btc* e nel resto delle criptomonete è stata frequentemente anche oggetto di studi in cui venivano utilizzati diversi modelli economici per la valutazione della stessa.

Molti di questi studi hanno cercato di utilizzare modelli differenti, per tenere conto della persistenza della volatilità nel mercato *Bitcoin*, e la maggior parte degli stessi evidenziano una volatilità estrema e in molti casi superiore a quello delle azioni e dell'oro.

¹³⁴ Cfr. SPAGNUOLO E., “*Stablecoin: come funzionano gli “anti-bitcoin” con un prezzo stabile*”, www.Wired.it, 18 Luglio 2018

¹³⁵ Cfr. *Blockchain Team*, “*Shining light on The State of Stablecoins*”, www.Blockchain.com, 26 Settembre 2018

¹³⁶ Cfr. VILLANI F., “*Criptovalute e stablecoin: come orientarsi*”, www.Money.it, 10 Dicembre 2018

Un altro flusso di ricerca che continua ad attirare l'attenzione di studiosi ed esperti è la capacità di *Bitcoin* di diversificare/coprire il rischio di ribasso di attività finanziarie come azioni, obbligazioni e materie prime.

Uno studio sul tema è stato condotto da *Libing Fang* della *School of Management and Engineering, Nanjing, China*, *Elie Bouri* della *USEK Business School, Libano*, *Rangan Gupta* del *Department of Economics in Pretoria, Sudafrica*, e *David Roubaud* della *Montpellier Business School, Francia*, in un articolo pubblicato nella fine del 2018 e chiamato “*Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin?*”.¹³⁷

Con tale documento si valuta se la volatilità a lungo termine di *Bitcoin*, azioni, materie prime e obbligazioni sono influenzate dall'*Economic Policy Uncertainty (EPU)*, ossia l'incertezza della politica economica globale, e i risultati empirici forniranno prove a sostegno di questa ipotesi, tranne che nel caso di obbligazioni.

Questo paper parte dalla premessa che molti studi, basandosi sull'applicazione di modelli della famiglia *GARCH*, indicano che la volatilità di *Bitcoin* è alta e persistente e si trova ad essere maggiore rispetto ad altre attività, come le azioni o come molte *commodities*.

Bitcoin è inoltre una criptomoneta molto poco correlata con i beni convenzionali come azioni, obbligazioni, e materie prime.

Recentemente, *Demir et al.*¹³⁸ indicano che l'incertezza della politica economica può essere utilizzata per anticipare i rendimenti di *Bitcoin*, sostenendo che un aumento delle incertezze relative alla politica economica tende a far diminuire la fiducia degli investitori nel sistema finanziario globale e, di conseguenza, l'attrattiva di investimenti in *Bitcoin* aumenta.

Lo scopo di questo documento è, però, duplice. In primo luogo, come già detto, si esamina l'impatto dell'incertezza della politica economica sulla volatilità dei *Bitcoin*.

In secondo luogo, si considera se il potenziale impatto dell'incertezza delle politiche economiche sulle correlazioni tra *Bitcoin* e beni convenzionali comporti un miglioramento dell'efficacia della copertura *Bitcoin*.

Sul fronte metodologico, questo documento applica il modello *GARCH-MIDAS* di *Engle, Ghysels e Sohn* (2013) per indagare direttamente su come le volatilità a lungo termine di *Bitcoin* e le attività convenzionali sono influenzate dall'incertezza della politica economica globale, in quanto la volatilità

¹³⁷ Cfr. FANG L. , BOURI E. , GUPTA R. , ROUBAUD D. , “*Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin?*”, *International Review of Financial Analysis*, www.Elsevier.com, 2018

¹³⁸ *Et al.* è un'abbreviazione dell'espressione latina “*et alii*”, ovvero “e altri”.

condizionata viene stimata in maniera più efficace col modello *GARCH-MIDAS* piuttosto che col modello *GARCH*.

Si applica anche un altro modello, chiamato il *DCC-MIDAS* (Colacito, Engle, & Ghysels, 2011), per esaminare l'impatto dell'incertezza della politica monetaria sulla correlazione tra *Bitcoin* e le attività convenzionali in studio.

L'idea alla base del modello *DCC-MIDAS* è di decomporre la correlazione tra *Bitcoin* ed *assets* convenzionali in componenti a lunga e breve durata e combinare i rendimenti giornalieri di *Bitcoin* e le attività convenzionali con livelli mensili dell'indice *EPU*.

Permettendo che sia le correlazioni a lungo che a breve termine siano influenzate dall'*EPU*, possiamo anche fare deduzioni sull'efficacia di copertura di *Bitcoin* in base all'effetto di *EPU* su quelle correlazioni.

Il documento fornisce utili implicazioni agli investitori e ai professionisti contribuendo a migliorare l'efficacia dell'allocazione di risorse tra *Bitcoin* e diversi *assets*, a seconda dell'influenza dell'incertezza della politica economica.

Ciò è importante per la costruzione di portafogli diversificati e per la gestione dei rischi.

Ad esempio, i periodi di correlazione negativa tra i prezzi di *Bitcoin* e le attività finanziarie offrono l'opportunità di ottimizzare le strategie di portafoglio e di copertura condizionate dal fatto che il livello di incertezza sia alto, medio o basso. In effetti, la letteratura sostiene che un aumento dell'incertezza della politica economica può influenzare positivamente le materie prime, *bond* e *Btc* dato che questi tre beni possiedono alcune proprietà di copertura.

Basandosi su questa idea, l'effetto positivo dell'incertezza della politica economica sulla correlazione tra *Bitcoin-commodities* e *Bitcoin-bonds* implica che *Bitcoin* servirà come una copertura per le materie prime o per le obbligazioni quando il livello di incertezza è basso e quando la correlazione del *Btc* con *commodities* e obbligazioni è negativa.

Tuttavia, quando il livello di tale incertezza è alto, il *Bitcoin* potrebbe non servire come uno strumento di copertura.

Al contrario, dato che un aumento della medesima influisce negativamente sulle azioni, in questo caso *Bitcoin* servirà da copertura per le azioni stesse e quando la correlazione *Bitcoin-azioni* è negativa. Ma, come nel caso precedente, quando invece il livello di incertezza della politica economica è basso, *Bitcoin* non può servire come una buona copertura.

Questo studio utilizza dati giornalieri e mensili. I dati giornalieri sono espressi in *USD* e includono i livelli di chiusura di *Bitcoin*, azioni globali, materie prime e obbligazioni, misurati rispettivamente dall'indice di *Bitcoin Price* di *CoinDesk*, dall'indice *MSCI World Stock index*, dall'indice *S&P GSCI commodity* e dal *PIMCO Investment Grade*.

I dati del prezzo di *Bitcoin* sono raccolti da *coindesk.com*, mentre i dati di azioni, materie prime, e indici obbligazionari sono estratti da *DataStream*.

Per quanto riguarda i dati mensili, è incluso l'indice di incertezza della politica economica globale, il *GEPU*, *Global Economic Policy Uncertainty*.

L'indice *GEPU* è una media ponderata del PIL degli indici nazionali di incertezza della politica economica per 20 paesi: Australia, Brasile, Canada, Cile, Cina, Francia, Germania, Grecia, India, Irlanda, Italia, Giappone, Messico, Paesi Bassi, Russia, Corea del sud, Spagna, Svezia, Regno Unito e Stati Uniti.

Il periodo di campionamento inizia il 21 settembre 2010 e termina il 26 gennaio 2018.

Le analisi empiriche sono condotte con la serie *log-Return*, fatta eccezione per il *GEPU*, che viene utilizzato nella sua forma di livello grezzo, dato che è stazionario.

3.3.3 Modelli *ARCH* e *GARCH*

Il modello *ARCH*, acronimo di *AutoRegressive Conditional Heteroskedasticity*, ovvero modello autoregressivo con eteroschedasticità condizionata, viene usato per la specificazione di serie storiche caratterizzate da errori e permette di poter fare delle previsioni sui rendimenti futuri di attività finanziarie. Proposto nel 1982 da *R. Engle*,¹³⁹ questo è un modello adeguato alla descrizione del fenomeno empirico del *volatility clustering* secondo il quale periodi di elevata volatilità tendono a permanere e sono seguiti da periodi di relativa stabilità che a loro volta manifestano una certa persistenza.

Dal 1982 sono stati posti in essere diversi altri modelli basati sull'elaborato di *Engle*, tra cui il modello *GARCH* (*Generalised Autoregressive Conditional Heteroskedasticity*), sviluppato nel 1986 dall'economista Danese *Tim Peter Bollerslev*, consistente in un'estensione di tale modello.¹⁴⁰

Secondo tale modello generalizzato, la varianza del termine d'errore, in un dato momento t , dipende dal quadrato dei termini d'errore dei precedenti periodi.

Nella famiglia dei modelli *GARCH*, il più semplice ed utilizzato è il *GARCH* (1,1), in cui si assume una media pari a 0 ed una distribuzione normale (basata sui rendimenti passati).

Il modello *GARCH*(1,1) è definito nel modo seguente:

¹³⁹ *Robert Franklin Engle* è un economista americano che attualmente insegna alla *Stern School of Business* della *New York University*. Tramite i suoi studi relativi ai metodi di analisi delle serie storiche economiche con volatilità variabile nel tempo (*ARCH*), vinse il premio *Nobel* per l'economia nel 2003.

¹⁴⁰ Cfr. *Dizionario di Economia e Finanza* 2012, Treccani

$$\sigma_t^2 = \omega + \alpha \varepsilon_{t-1}^2 + \beta \sigma_{t-1}^2$$

Con $\omega > 0$, $\alpha, \beta \geq 0$ ¹⁴¹

ω , α e β sono posti non negativi per garantire la positività della varianza condizionata.

I termini ε_t sono la componente *ARCH*, mentre i termini σ sono la componente *GARCH*.

– σ_t^2 è la varianza condizionata (dei rendimenti passati) di ε_t

$$\text{Var}(y_t | \text{past}) = \sigma^2$$

Così c'è eteroschedasticità: una famiglia di variabili aleatorie $\{Y_i\}$ si dice eteroschedastica se le sue componenti non hanno tutte la stessa varianza e questo concetto di si contrappone a quello di omoschedasticità. ¹⁴²

- La media condizionata $E(y_t | \text{past})$ è assunta pari a 0. ¹⁴³

I modelli *GARCH* sono inoltre simmetrici, cioè non ci interessiamo del segno di ε_t .

Chiaramente questo non è un dettaglio da poco nel momento in cui vogliamo usare modelli di questo genere per studiare delle serie finanziarie, per le quali il segno è estremamente importante. ¹⁴⁴

Nel corso degli anni questi modelli sono stati sempre più utilizzati per la valutazione delle serie storiche e sono stati sempre in continua evoluzione, in quanto la dottrina economica ha presentato, nel tempo, numerose implementazioni degli stessi, come *EGARCH* (*Exponential GARCH*), *AGARCH* (*Asymmetric GARCH*) e *GARCH M* (*GARCH in Mean*).¹⁴⁵

Fanno parte di questa categoria anche i 2 modelli che sono stati considerati in questo studio, ovvero *GARCH-MIDAS* e *DCC-MIDAS*.

¹⁴¹ Cfr. TSAY, “*Analysis of Financial Time Series*”, *Financial Econometrics*

¹⁴² Cfr. LEORATO S. , *Dizionario di Economia e Finanza*, Treccani

¹⁴³ Cfr.S. TSAY, “*Analysis of Financial Time Series*”, cit.

¹⁴⁴ Cfr. BIANCHI L. , “*modelli ARCH e GARCH*”, www.unipi.it

¹⁴⁵ Cfr. DI STEFANO G. , “*Analisi delle serie storiche: modelli ARCH e GARCH*. Prof. M. Ferrara”, www.Docplayer.org, 2016

3.3.4 Risultati dello studio

Il modello *GARCH-MIDAS* è stato utilizzato per descrivere le volatilità a lungo termine di *Bitcoin*, *MSCI*, *S&P GSCI* e *PIMCO* in base alla *Realized Volatility*.¹⁴⁶

L'applicazione e lo sviluppo di tale modello dimostra che la volatilità a lungo termine di *Bitcoin*, azioni e materie prime è significativamente influenzata dall'incertezza delle politiche economiche, anche se l'effetto sulla volatilità a lunga durata di *Bitcoin* è diverso da altri asset (ad esempio, azioni). L'applicazione del *DCC-MIDAS* rivela invece che l'incertezza della politica economica ha un impatto negativo significativo sulla correlazione *Bitcoin-obbligazioni* e un impatto positivo sulle correlazioni *Bitcoin-equity* e *Bitcoin-commodities*, suggerendo una possibilità per *Bitcoin* di agire come una copertura in condizioni di incertezza economica specifiche.

Ulteriori analisi dimostrano che l'efficacia di copertura di *Bitcoin* sia per le azioni che per le obbligazioni è aumentata leggermente dopo aver considerato l'impatto dell'incertezza della politica economica.

Questi risultati aggiungono implicazioni utili per quanto riguarda le decisioni di investimento, strategie di copertura, e la creazione di politiche economiche.

Il fatto che la volatilità di *Bitcoin* sia influenzata dallo stato di incertezza economica suggerisce che gli investitori e gli operatori del mercato *Bitcoin* debbano sempre considerare il livello di incertezza della politica economica globale, pur facendo una decisione di investimento che coinvolga la volatilità dello stesso *Bitcoin*.

Pertanto, gli investitori possono utilizzare informazioni sullo stato di incertezza economica globale per migliorare le previsioni sull'andamento del *Bitcoin*. Questo potrebbe essere utile quando si fanno inferenze di gestione del rischio che comportano il potenziale lancio di contratti di opzioni su *Bitcoin* e *Bitcoin futures* che sono ora scambiati sul *CME Group* e il *CBOE*.

La prova dell'effetto debole dello stato di incertezza della politica economica sulla capacità di copertura di *Bitcoin* implica che gli investitori non possono migliorare sostanzialmente le prestazioni di copertura di *Bitcoin* in diverse condizioni di incertezza.¹⁴⁷

¹⁴⁶ Per *RV* si intende la somma dei rendimenti al quadrato. Questa è utile perché fornisce una misura relativamente accurata della volatilità.

¹⁴⁷ Per lo svolgimento dei modelli si rimanda all'art. "Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin?", cit.

Conclusioni

Abbiamo visto come la creazione di *Bitcoin* abbia proposto un cambiamento radicale non solo nei sistemi di pagamento, mediante numerose procedure basate su caratteristiche differenti ed innovative, ma anche mediante una tecnologia che negli anni è stata sempre maggiormente considerata, e non solo nell'ambito delle criptovalute: la *Blockchain*.

Il *Bitcoin*, creato da un personaggio ignoto, identificatosi con lo pseudonimo *Satoshi Nakamoto*, aveva inizialmente la finalità principale di presentarsi come una valida alternativa ad un sistema che, in quegli anni, aveva fortemente deluso gli investitori, i piccoli risparmiatori e non solo.

Questa sfiducia nei confronti del sistema economico, portava quindi alla creazione di una caratteristica fino ad allora sconosciuta, ovvero la decentralizzazione.

Bitcoin si proponeva quindi come uno strumento indipendente da altre entità finanziarie, e, a differenza delle monete *fiat*, che sono gestite da un centro di potere, nessuno può alterarlo o modificarlo. Tuttavia, lo scenario creato da *Bitcoin* e dalle altre *criptocurrencies* comporta anche diversi rischi, di cui si è parlato in maniera approfondita nel secondo capitolo.

Tra i rischi più importanti, l'utilizzo delle criptomonete per il conseguimento di finalità illecite è sicuramente una chiara conseguenza all'anonimato che molti di questi strumenti garantiscono, ma non vanno trascurati altri problemi, come l'incertezza relativa al trattamento fiscale, il rischio informatico, l'assenza di tutele legali e l'eccessiva volatilità delle criptomonete.

Quest'ultimo è un tema su cui ho ritenuto importante soffermarmi maggiormente, studiando l'andamento di mercato del *Bitcoin* e di alcune tra le principali criptovalute per capitalizzazione, analizzando inoltre i principali avvenimenti che hanno causato una serie numerosa e spesso intensa di "up and down".

Proprio mediante tali analisi, è stato mostrato come le *altcoins* tendono a seguire l'andamento del "market mover", il *Bitcoin*, lasciando presagire una grande correlazione tra le varie valute digitali, dato confermato tramite un'analisi, ottenuta mediante il programma *Excel*, dei rendimenti mensili di alcune tra le principali criptovalute.

Si è discusso inoltre, basandosi su un paper di recente pubblicazione, di come l'incertezza della politica economica possa influenzare l'andamento del *Bitcoin*, affermando che un aumento delle incertezze relative alla politica economica tende a far diminuire la fiducia degli investitori nel sistema finanziario globale e, di conseguenza, l'attrattiva di investimenti in *Bitcoin* aumenta.

Inoltre, l'altro scopo di questo studio è rivolto a considerare se il potenziale impatto dell'incertezza delle politiche economiche sulle correlazioni tra *Bitcoin* e beni convenzionali comporti un miglioramento dell'efficacia della copertura *Bitcoin*.

Per concludere, ritengo che le criptovalute siano degli strumenti potenzialmente eccezionali, ma che difficilmente riusciranno a godere di una forte stabilità in un orizzonte temporale molto breve.

Un fattore fondamentale che caratterizza la volatilità delle stesse, risiede sicuramente nel fatto che il loro valore sia attribuito, principalmente, da parametri basati sulla legge della “domanda e dell’offerta”; dunque, a mio avviso, l’ampia categoria di critici certamente non aiuta le criptovalute a stabilizzarsi.¹⁴⁸

Sarebbero infatti necessari numerosi e radicali cambiamenti per far sì che gli investitori e le istituzioni siano meno diffidenti nei confronti di questi strumenti, partendo da giuste regolamentazioni a livello internazionale, che si occupino di tutelare gli investitori, in modo tale da creare un aumento di fiducia nel settore, incentivando gli investimenti.

A tal proposito va fatta un’osservazione, a mio avviso, molto rilevante: siamo, ad oggi, dinanzi ad una situazione molto particolare, in quanto ci si trova ad investire in un mercato ancora privo di una corposa e meticolosa regolamentazione, facendo venire meno un elemento fondamentale: la tutela dell’ investitore e dei risparmi.

Emblematica è la situazione che ha visto numerosi piccoli risparmiatori, molto poco informati e competenti, investire nelle criptovalute negli ultimi mesi del 2017, basando le proprie scelte esclusivamente sulle notizie quotidiane e su un desiderio di guadagno che, purtroppo, si è rilevato in breve tempo assolutamente controproducente.

E’ molto importante, quindi, evidenziare che le autorità finanziarie di vari Stati come Giappone, Usa e anche Stati Uniti e Europa, stanno cercando di intervenire su questo mercato fissando regole più severe a tutela degli investitori e soprattutto finalizzate a prevenire l'utilizzo delle criptovalute per scopi illegali.

Il 2019 potrebbe essere quindi un anno molto importante per l’evoluzione delle criptovalute, in quanto è previsto anche il *G20*, in cui, molto probabilmente, si arriverà a delle decisioni concrete sulla tematica *criptocurrencies*, relative ad argomenti riguardanti le *ICO*, come annunciato dal Vicepresidente del Parlamento Europeo *Valdis Dombrovskis*, o anche la tassazione e l’utilizzo delle criptovalute.¹⁴⁹

¹⁴⁸ Cfr. TAR A. , “Prezzo del Bitcoin, spiegato semplicemente”, www.Cointelegraph.com, 15 Gennaio 2018

¹⁴⁹ Cfr. LUGANO F. , “Il Parlamento Europeo introdurrà la regolamentazione per le ICO”, www.theCryptonomist.it, 19 Novembre 2018

Cfr. CAVICCHIOLI M. , “Il G20 regolerà l’utilizzo e la tassazione delle criptovalute”, www.theCryptonomist.it , 3 Dicembre 2018

Bibliografia

BOHME R. , CHRISTIN N. , EDELMAN B. , MOORE T. , “Bitcoin: Economics, Technology, and Governance”, *Journal of Economic Perspectives*, 20 Luglio 2015

BOURI E. , FANG L. , GUPTA R. , ROUBAUD D. , “Does global economic uncertainty matter for the volatility and hedging effectiveness of Bitcoin?”, *International Review of Financial Analysis*, www.elsevier.com, 2018

CAPACCIOLI S. e SOLDAVINI P. , “Fallisce Bitgrail, la piattaforma Italiana per le criptovalute”, *Il Sole24ore*, 26 Gennaio 2019

CICCHITELLI G. , D'URSO P. , MINOZZO M. , *Statistica: principi e metodi 3/Edizione*, Pearson

DI PERNA F. , PELLEGRINI M. , “Cryptocurrency (and Bitcoin), a new challenge for the regulator”, 19 Marzo 2018

LEMME G. e PELUSO S. , *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Riv. dir. banc.*, dirittobancario.it, 43, 2016

LEORATO S. , *Dizionario di Economia e Finanza*, Treccani

LOPS V. , “5 motivi per cui il Bitcoin è un asset rischioso”, *Il Sole 24 ore*, 14 Febbraio 2018

MARRO E. , “Putin studia un «criptorublo» per aggirare le sanzioni occidentali”, *Il Sole 24 Ore*, 2 Gennaio 2018

MURALI J. , “A new coinage: can Bitcoin, the global online digital currency, be the precursor of a new monetary system?”, *Economic and Political weekly*, 21 Settembre 2013

PLATEROTI A. , “Da Nakamoto a Wright: chi si cela dietro l’inventore”, *Il Sole 24 ore*, 24 Febbraio 2017

SOL P. , “Il Bitcoin record nel 2017? Frutto di una grande manipolazione”, *Il Sole 24 ore*, 14 Giugno 2018

SOLDAVINI P. , “tra speculazione e rivoluzione:10 anni in altalena con i Bitcoin”, *Il sole 24 ore*, 31 Ottobre 2018

TIZIAN G. , “I Bitcoin piacciono anche alla mafia: cosi ‘ndrangheta e camorra riciclano denaro” , *L’Espresso*, 24 Gennaio 2018

TSAY, “Analysis of Financial Time Series”, *Financial Econometrics*, Usa, 2005

Sitografia

www.agendadigitale.it

www.area-business.net

www.banca d'Italia.it

www.bioterra.it

www.bitdegree.it

www.blockchain.com

www.blockchain4innovation.it

www.borsainside.com

www.cointelegraph.com

www.cointelegraphItalia.it

www.consob.it

www.criptovaluta.it

www.criptovalute24.it

www.cryptominando.it

www.digital360group.com

www.digital4trade.it

www.docplayer.org

www.etherevolution.it

www.everyeye.it

www.finanzaonline.it

www.fiscomania.it

www.igbank.it

www.ilbitcoin.it

www.ilpost.it

www.ilsole24ore.it

www.investing.com

www.lastampaItalia.it

www.lecriptovalute.org

www.mercati24.it

www.money.it
www.motherboard.it
www.nanobitonline.it
www.ngc.it
www.okforex.it
www.publications.europa.eu
www.soldionline.it
www.startingfinance.it
www.stayupgraded.it
www.talkingofmoney.com
www.tecnologi.net
www.thecryptonomist.it
www.thespectator.com
www.tradingonline.com
www.trendonline.com
www.unipi.it
www.valutevirtuali.it
www.webeconomia.com
www.webnews.it
www.wildseo.it
www.wired.it

Riassunto

Nel corso del ventunesimo secolo, grazie ad una intensa rivoluzione tecnologica ed informatica, abbiamo assistito a numerosi cambiamenti nel settore economico-finanziario.

Uno tra i più importanti e rivoluzionari è sicuramente quello che ha proposto una modifica dei generali sistemi di pagamento, mediante la creazione delle “criptovalute”.

La più importante tra queste criptomonete è sicuramente il *Bitcoin*, nata con la finalità di creare una via di investimento alternativa, discostandosi da un sistema che non si era rivelato impeccabile in quel periodo; infatti, *Satoshi Nakamoto*, pseudonimo del creatore di *Bitcoin*, di cui ad oggi ancora non è nota l'identità, pubblicò il *white paper* contenente tutti i dettagli tecnici della stessa nel 2008, anno di forte crisi economica.

Non era un caso infatti che tale pubblicazione avvenne solo poche settimane dopo il fallimento di una delle più importanti banche di investimento degli Stati Uniti, ovvero la *Lehman Brothers*.

Per il lancio ufficiale del *Bitcoin* nel mercato bisogna attendere fino al 3 Gennaio 2009, quando viene creato il primo blocco di 50 *BTC*, detto *Genesis block*.

Il sistema di *Bitcoin* si basa su una tecnologia che nel tempo ha riscosso sempre maggiore successo e maggiori consensi, essendo spesso utilizzata anche in contesti estranei alle criptovalute e che, probabilmente ,è la vera chiave di successo del Bitcoin ed in generale delle valute digitali: la *Blockchain*.

Questa tecnologia è fondata su un'organizzazione molto articolata basata su una serie di blocchi, in cui sono archiviate numerose transazioni, validate e correlate da una Marca Temporale, detta *Timestamp*.

Tale Timestamp garantisce sicurezza al modello, in quanto impedisce che le operazioni, una volta eseguite, vengano annullate o modificate.

Inoltre, grazie alla Marca Temporale, viene attribuita una validazione temporale ai vari documenti informatici, rendendoli opponibili a terzi.

Questa tecnologia permette anche la creazione di archivi condivisi, ottenendo un'articolata rete informatica in cui le numerose e differenti transazioni sono custodite tramite un *database* decentralizzato in cui figureranno anche gli importi delle stesse e gli pseudonimi di chi le compiono; si ottiene quindi una meticolosa struttura difficilmente violabile, potendo apportare modifiche, in una fase successiva alla transazione, soltanto tramite il consenso della controparte.

Viene a crearsi dunque un registro digitale unico che baserà la propria operatività sui numerosissimi nodi di tale organizzazione e sarà consultabile da tutti, garantendo quindi rilevante trasparenza e tracciabilità.

Fondamentale è anche il concetto di *Proof of work (Pow)*, mediante il quale si realizza un consenso senza fiducia e distribuito in quanto, a differenza dei sistemi di pagamento tradizionali, non c'è bisogno di una terza persona per porre in essere una transazione con una controparte.

Vi è infatti un registro che memorizza la cronologia delle transazioni e i saldi di ciascun *account*.

Con *Bitcoin* e poche altre valute digitali, ognuno ha una copia del libro mastro, quindi nessuno deve affidarsi a terze parti, perché chiunque può verificare direttamente le informazioni scritte.

Altro elemento importante alla base di questa tecnologia è quello che garantisce la non duplicabilità delle informazioni, tramite la creazione di blocchi crittografati concatenati tra di loro tramite chiavi crittografate immutabili.

Dunque, per questi ed altri motivi, la tecnologia *Blockchain* può avere numerose applicazioni anche completamente indipendenti dalle criptovalute, poiché offrono un approccio fortemente innovativo per archiviare informazioni, svolgere funzioni ed eseguire transazioni.

Con *Bitcoin*, si assiste ad un trasferimento di fiducia dall'uomo, nel nostro caso l'autorità di garanzia, che nell'ottica di *Bitcoin* non è ormai più affidabile, alle leggi della matematica e dell'informatica, ossia alla crittografia e agli algoritmi che stanno alla base della rete *Bitcoin*.

Dal *white paper* di *Nakamoto* ad oggi possiamo affermare che le criptovalute, e soprattutto il *Bitcoin*, dopo un'iniziale fase di avversione e timore verso qualcosa di nuovo e sconosciuto, si stanno ritagliando uno spazio sempre maggiore nel mondo economico, essendo ormai riconosciute a livello europeo, tramite la direttiva europea n. 156 del 19/06/2018 facente riferimento alla direttiva EU 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018, in cui l'UE definisce per la prima volta le criptovalute stesse.

Dopo l'avvento del *Bitcoin*, abbiamo assistito negli anni alla creazione di numerosissime altre *criptocurrencies*, ognuna dotata di proprie caratteristiche e finalità.

Ad oggi nel mercato sono presenti più di 1000 "*Altcoins*", ossia tutte le criptomonete alternative al *Bitcoin*.

Il mondo delle *Altcoins* si è sviluppato in maniera notevole negli ultimi anni, ma va comunque detto che sono ancora molto distanti dal *Bitcoin*, che resta in assoluto il *leader* di mercato nella categoria delle criptomonete, vantando elementi chiave come una maggiore sicurezza, identità del marchio maggiormente riconoscibile ed uno sviluppo più attivo e razionale.

Tra le più importanti *altcoins* vanno incluse *Ethereum*, *Ripple*, *Litecoin* e *Bitcoin cash*.

Va però riconosciuto che, nonostante le tante novità ed innovazioni portate dal Bitcoin e dalle varie criptovalute all'intero universo economico, c'è ancora tanto timore verso le valute digitali per via di diversi punti opinabili delle stesse.

Innanzitutto, un problema molto importante è da ricondursi alla forte volatilità che da sempre caratterizza questi strumenti digitali e che spesso, in tempi molto brevi, ha causato improvvise perdite molto accentuate.

Tale caratteristica, oltre a non far considerare questi strumenti finanziari come una moneta avente riserva di valore, porta le criptovalute ad essere viste come uno strumento principalmente di tipo speculativo, facendo venir meno la caratteristica di moneta utilizzabile come mezzo di pagamento.

Un altro importante problema di cui si è discusso, è il possibile utilizzo delle criptovalute per il sostenimento di fini illeciti, in quanto, nel corso degli anni, vi sono stati diversi episodi in cui sono state registrate numerose situazioni di frode.

In particolare, le cause più valide che favoriscono tali finalità risiedono nella natura stessa di strumenti come il *Bitcoin*; infatti, la maggior difficoltà nel tracciamento dettata dall'anonimità di chi compie delle transazioni e l'assenza di un organismo centrale aiutano non poco.

Proprio per far fronte a questi problemi, l'Europa si sta muovendo molto, volendo creare una regolamentazione per le *criptocurrencies*, aumentando la sicurezza e la tracciabilità delle monete digitali attraverso l'obbligo del riconoscimento e dell'utilizzo, con la finalità di tutelare gli interessi degli investitori.

Altro tema fortemente valido è dato dal timore che molti investitori nutrono nei confronti di tali strumenti, per via di un andamento che lascia immaginare una situazione di ennesima bolla speculativa del mercato mondiale.

Numerosi sono stati, infatti, gli accostamenti delle criptovalute alle famose bolle "*dot-com*" e "dei Tulipani", principalmente a causa di *performance* economiche eccessivamente squilibrate e poco coerenti. Difficilmente si può valutare la veridicità di tali accostamenti, in quanto, nonostante i risultati pazzeschi che sono stati raggiunti negli ultimi anni, non si può certamente ignorare la forte discesa che li ha visti come protagonisti negli ultimi 12 mesi.

Va detto, però, che non sembra del tutto appropriato paragonare le *criptocurrencies* con questi 2 fenomeni; rispetto alla bolla dei Tulipani, infatti, c'è una fondamentale differenza riguardante il valore intrinseco dei 2 beni, essendo uno un bene tangibile ed avente valore intrinseco molto basso, rispetto alle criptovalute come il *Bitcoin* che sono un mezzo di scambio virtuale relativamente raro, non replicabile e senza valore intrinseco.

Rispetto invece alla bolla "*dot-com*", vi sono segnali di differente natura che lasciano immaginare che non è pienamente corretto associare le 2 fasi economiche, come il fatto che dopo lo scoppio della

bolla delle *dot-com*, il *Nasdaq Composite index* ha continuato a crollare, senza sosta, fino a tornare ad una quota pari a quella pre-bolla, cosa che invece non è avvenuta al *Bitcoin*; inoltre, i diversi andamenti economici che ci sono stati nel tempo tra *Nasdaq* e lo stesso *Bitcoin* sembrano confermare questa idea.

Tra gli altri aspetti da dover valutare, va menzionata l'attività di "*Mining*", ovvero l'attività mediante il quale si aggiungono le registrazioni delle transazioni al registro contabile pubblico, la *blockchain*, trovando "minerale algoritmico" e ottenendo dei *token*.

Il *Mining* è anche il processo attraverso il quale i *Bitcoin* vengono immessi nel sistema: ai cosiddetti minatori vengono pagate delle *fee* come "sussidio" delle nuove monete create.

Sebbene il *mining* sia un'attività libera, la complessità dei calcoli che stanno alla base della creazione di un *Bitcoin* può essere affrontata solo da chi possiede degli hardware specializzati.

Di conseguenza, è necessario interrogarsi sulla buona fede e l'affidabilità dei minatori, il cui numero risulta essere comunque circoscritto, nello svolgere le funzioni di gestione e controllo.

I maggiori timori riguardano cioè il fatto che la maggior parte dei *Bitcoin* potrebbe essere posseduta da un piccolo gruppo che li promuove e che questa esclusività possa essere appannaggio di interessi poco leciti. Inoltre, vanno ad aggiungersi a questo problema il fatto che la produzione e lo scambio dei *coin* divora così tanta energia da poter far aumentare di due gradi la temperatura media globale e che i consumi sostenuti per poter svolgere tali attività di creazione di moneta virtuale sono elevatissimi.

Va considerata anche l'assenza di tutele legali e contrattuali che, unita alla mancanza di definizioni, di *standard* legali e di obblighi informativi, rende molto difficile dimostrare ad una terza parte di aver subito un danno ingiusto.

Tali assenze comportano pertanto sempre un certo livello di rischio a carico degli investitori, in quanto una transazione errata è modificabile solo attraverso un accordo volontario delle parti coinvolte nello scambio.

A rendere la tutela dell'investitore ancora più complicata si aggiungono le difficoltà ad individuare il soggetto intermediario, oltre al territorio e la giurisdizione di riferimento, dove poter intervenire a tutela dei propri interessi ove lesi.

Un altro rischio insito nelle criptovalute e nel *Bitcoin* risiede nei possibili attacchi *hacker* a danno dell'investitore, insieme a potenziali malfunzionamenti tecnologici che potrebbero bloccare il proprio portafoglio; inoltre, in caso di smarrimento della *password* del portafoglio elettronico, la perdita potrebbe essere permanente, non essendoci né autorità centrali che registrano le *password* o ne emettono altre sostitutive, né alcun tipo di assicurazione.

Per agire mediante operazioni fraudolente, come il “*double spending*”, con cui si spende più volte la stessa moneta, gli *hacker* devono controllare la maggior parte della rete, mediante il controllo del 51% (almeno) nella rete di *Bitcoin*, in modo tale da poter approvare determinati blocchi scartando quelli generati dagli altri.

In questo modo “salta” il concetto di rete decentralizzata ed i *miners* potranno avere il totale controllo del *network*. Vi sono stati negli anni differenti situazioni di operazioni fraudolente da parte di *hacker*, con risultati, a volte, davvero devastanti, come il caso di *Coincheck*, una delle maggiori piattaforme giapponesi, Mt. *Gox* o *Bitgrail*, l'*exchange* Italiano per criptovalute.

La natura decentralizzata delle rete di valute virtuali e l'assenza di regolamentazione creano inoltre incertezze e lacune anche per quanto riguarda il trattamento fiscale, dando vita ad implicazioni imprevedibili per i soggetti coinvolti.

Oltre a questi problemi, vanno presi in considerazione quelli presentati dalle tre Autorità di vigilanza europea, ovvero EBA, ESMA, EIOPA:

- nessuna opzione di uscita
- non trasparenza dei prezzi
- interruzioni dell'operatività
- informazioni fuorvianti

Inoltre, le stesse affermano che chi acquista criptomonete deve essere consapevole del rischio di poter perdere gran parte del denaro investito, se non addirittura di perderlo completamente.

Dopo aver considerato i (numerosi) aspetti negativi e fortemente criticati, passiamo adesso a descrivere i principali punti di forza di tali strumenti, che hanno permesso al *Bitcoin* e alle criptovalute di affermarsi con successo in breve tempo e che hanno portato diverse novità all'interno dei mercati economici. Sicuramente la decentralizzazione è tra i principali fattori di successo dell'universo digitale connesso al *Bitcoin*.

Bitcoin è stata la prima criptovaluta decentralizzata ad esser mai stata realizzata.

La differenza fondamentale con le monete *fiat* è la modalità di emissione, in quanto non interviene nessuna banca centrale e non vi è nessuna approvazione governativa o finanziaria.

Essendoci inoltre indipendenza dalle Banche Centrali, ogni nodo del *network* ha la stessa importanza, non esistendo un'entità centrale che ne regola e garantisce il funzionamento ed il suo grande vantaggio risiede proprio nel fatto che nessuno possa “comandare *Bitcoin*”; nessuno può alterarlo o modificarlo, a differenza delle monete legali, che sono gestite da un centro di potere.

Un altro grande vantaggio consiste nel limite di *Bitcoin* che negli anni verranno messe in circolazione, ovvero 21 milioni. C'è un consistente vantaggio in una emissione limitata di criptovalute, in quanto così si va contrastare l'inflazione che spesso va ad indebolire il potere di acquisto delle famiglie.

Dunque, stabilendo un “*Max Supply*”, *Nakamoto* ha creato una moneta deflazionistica e destinata ad apprezzarsi nel tempo proprio per la sua rarità, come l’oro.

Questo sta spingendo paesi soggetti ad alta inflazione, come il Venezuela, l’Iran, la Turchia ed il Sudafrica, a convertire i propri risparmi in criptovalute deflative.

Uno dei vari vantaggi dell'utilizzo della *blockchain* è che si suppone che effettui transazioni più economiche rispetto all'utilizzo di altri metodi di pagamento convenzionali.

Il loro costo dipende principalmente da 3 aspetti fondamentali:

- Spazio occupato dalla transazione
- Numero di transazioni sulla rete
- Valore della valuta

Va detto, però, che le commissioni stesse sono direttamente proporzionali alla risorsa che utilizzano ed alla moneta con cui si pagano e, non essendo fisse, potrebbero in determinati momenti salire di valore. Vanno elogiate anche le tempistiche: infatti, mentre per un bonifico possono servire anche 4-5 giorni (fino a 10 per certi stati), con *Bitcoin* sono necessarie poche decine di minuti o al più qualche ora. Infine, va considerata la trasparenza che è alla base del sistema *Blockchain*.

Nonostante l’anonimato, la *Blockchain* è completamente trasparente; pertanto sarà possibile conoscere tutta la storia finanziaria di un determinato indirizzo, pur non sapendo a chi appartiene, e degli indirizzi correlati, costruendo dei veri e propri “*cluster*” di operazioni.

Il sistema dei *Bitcoin*, insomma, sposa trasparenza e anonimato rendendo limpidi i trasferimenti, ma celando ogni riferimento che possa ricondurre la criptovalute ai legittimi possessori.

E’ importante definire però che la condizione di pseudonimato permane fintanto che non venga utilizzato un *Exchange* o un servizio soggetto agli adempimenti di tipo “*Know Your Customer*”.

Infatti, a seguito della quarta Direttiva dell’UE (n.2015/849) in materia di antiriciclaggio, chi fornisce il servizio di compravendita di criptovalute deve richiedere ai clienti dei documenti identificativi.

In definitiva, va specificato che vi sono anche tanti altri piccoli vantaggi, come l’irreversibilità delle transazioni o il fatto che non c’è bisogno di essere degli esperti del settore informatico per potere operare nell’ambito delle criptovalute, ma resta l’idea che non è affatto semplice poter dare un giudizio oggettivo in merito alla bontà di tali strumenti digitali, anche dopo aver considerato i punti fondamentali degli stessi.

Anzi, proprio per via della moltitudine di elementi caratterizzanti, sostengo che possano essere degli strumenti utili o meno in base al tipo di investitore, alle sue idee e al suo modo di voler operare nel mercato.

Volendo, dopo aver introdotto ed analizzato i pro ed i contro delle criptovalute, soffermarsi sull’andamento negli anni del *Bitcoin*, quotato per la prima volta il 5 ottobre del 2009, si scopre che,

quando il sito *New Liberty Standard* pubblica la sua prima quotazione, con un dollaro era possibile acquistare oltre 1300 *Bitcoin*.

Vale a dire che, una criptovaluta che è arrivata recentemente a sfiorare i 20 mila dollari di valore, solo 10 anni fa valeva neanche un decimo di *pence*; un dato a dir poco incredibile, che lascia immaginare le potenzialità di questo strumento digitale.

Nel corso di questi 10 anni di *Bitcoin*, numerosi eventi hanno messo a nudo la fortissima volatilità che da sempre caratterizza questa criptovaluta, con una serie di “*up & down*” inattesi e spesso molto intensi. Il periodo più importante è sicuramente quello tra il 2017 ed il 2018, in quanto il *Btc*, dopo aver raggiunto il suo valore massimo storico di quasi 20 mila dollari nel Dicembre 2017, in brevissimo tempo è caduto in una forte fase di ribasso, perdendo numerosi miliardi di dollari di capitalizzazione. Vi sono diverse teorie rivolte alla giustificazione dell’improvviso *exploit* del 2017; tra le più attendibili va citata quella che vede come fonte di tale aumento di valore una vera e propria manipolazione di mercato.

La stessa, afferma che il grande *sprint* del *Bitcoin* nel 2017 non era esclusivamente frutto di una crescente domanda da parte di chi non voleva perdere il treno di una corsa al rialzo che sembrava non fermarsi più, ma sarebbe effetto, almeno per metà dei guadagni, di una grande manipolazione, incentrata attorno a *Bitfinex*, uno delle maggiori piattaforme globali di scambio per criptovalute, con sede alle Isole Vergini e al *Tether*, criptovaluta esistente dal 2015 e che funziona in un modo particolare, perché si basa sul dollaro americano: ogni unità di *USDT* vale, con un certo grado di approssimazione, un dollaro, e viene utilizzata soprattutto per facilitare le transazioni in criptovalute, che sono infatti più facili e veloci da trasferire da un sito di *exchange* a un altro se non passano da una valuta tradizionale.

La piattaforma è da sempre chiacchierata ed è finita sotto inchiesta proprio per la scarsa trasparenza e per i sospetti legati all’emissione di *Tether*, valuta che dovrebbe quindi essere garantita da analoga quantità di dollari.

Per quanto riguarda invece le cause del “*Bust*”, una delle motivazioni principali di tale crollo è da attribuire alla stretta della *Sec* (*Securities and Exchange Commission*), l’ente federale statunitense preposto alla vigilanza della borsa valori, alle *Ico*, per le quali è arrivata la prima condanna assoluta. Le *Ico* rivestono un ruolo importante all’interno del mondo della blockchain e delle criptovalute, in quanto permettono il finanziamento di determinati progetti; la bocciatura della Consob americana, dunque, rappresentava un paletto pesante da digerire per gli investitori, nonché un segnale negativo circa il futuro delle monete digitali.

Altre cause probabili sono state per molti “l’effetto Corea”, causato dall’annuncio del ministro di giustizia sudcoreano di voler chiudere i siti di *exchange* del paese, insieme alla decisione di Pechino

di mettere in atto una *escalation* di misure per non permettere ai cinesi di acquistare e vendere criptovalute.

Mediante una valutazione delle principali *Altcoins*, si nota un elemento fondamentale: il 2018 è stato un anno di ribasso per quasi tutte le criptovalute.

Alla base di ciò vi è, quindi, la grande correlazione che lega le criptovalute al “*Market maker*”, il *Bitcoin*.

In tabella sono mostrate le correlazioni con *Bitcoin* di alcune tra le più importanti criptovalute, in ordine: *Ethereum*, *Ripple*, *Bitcoin cash*, *Litecoin*, *Eos* e *Monero*.

Tabella 1: Correlazione delle principali *altcoins* rispetto a *Btc*

DATA	BTC	ETH	XRP	BCH	LTC	EOS	XMR
01/02/2019	3487,95	107,61	0,308517	116,56	32,83	2,34	43,72
01/01/2019	3843,52	140,82	0,364771	164,85	31,98	2,66	48,37
01/12/2018	4214,67	118,64	0,372906	172,12	34,34	2,96	59,65
01/11/2018	6377,78	198,87	0,455722	424,09	50,27	5,28	103,88
01/10/2018	6589,62	230,77	0,576461	530,91	60,21	5,74	114,52
01/09/2018	7193,25	295,34	0,347721	615,31	65,95	6,64	120,97
01/08/2018	7624,91	420,75	0,445852	769,35	77,86	7,26	128,15
01/07/2018	6385,82	453,92	0,461358	739,42	80,24	8,13	129,77
01/06/2018	7541,45	580,04	0,623364	1002,92	119,92	12,31	157,54
01/05/2018	9119,01	673,61	0,841407	1351,28	148,49	18,95	240,26
01/04/2018	6844,23	379,61	0,485081	643,03	115,22	5,66	175,51
01/03/2018	10951	872,2	0,928347	1291,92	209,75	8,63	314,04
01/02/2018	9170,54	1036,79	0,96253	1274,35	142,30	10,21	240,96
01/01/2018	13657,2	772,64	2,39	2432,54	229,03	8,84	358,99
01/12/2017	10957,6	466,54	0,255699	1462,68	99	3,24	190,94
Correlazione	1	0,794	0,726	0,966	0,892	0,461	0,940

Come si può notare, prendendo dei valori corrispondenti al prezzo di chiusura giornaliero del giorno 1 di ogni mese, si ottiene una correlazione molto alta, a conferma di un 2018 da incubo per le *criptocurrencies*.

Infine, è interessante notare che lo *status* di *Bitcoin* come una risorsa altamente volatile, è diventato un tema principale nella stampa finanziaria e nel mondo accademico; la stessa volatilità insita nel *Btc* e nel resto delle criptomonete è stata frequentemente anche oggetto di studi in cui venivano utilizzati diversi modelli economici per la valutazione della stessa.

Un recente studio sul tema valuta se la volatilità a lungo termine di *Bitcoin*, azioni, materie prime e obbligazioni sono influenzate dall'*Economic Policy Uncertainty (EPU)*, ossia l'incertezza della politica economica globale, e i risultati empirici forniranno prove a sostegno di questa ipotesi, tranne che nel caso di obbligazioni.

Inoltre, si considera se il potenziale impatto dell'incertezza delle politiche economiche sulle correlazioni tra *Bitcoin* e beni convenzionali comporti un miglioramento dell'efficacia della copertura *Bitcoin*.

I risultati sono che l'effetto positivo dell'incertezza della politica economica sulla correlazione tra *Bitcoin-commodities* e *Bitcoin-bonds* implica che *Bitcoin* servirà come una copertura per le materie prime o per le obbligazioni quando il livello di incertezza è basso e quando la correlazione del *Btc* con *commodities* e obbligazioni è negativa.

Tuttavia, quando il livello di tale incertezza è alto, il *Bitcoin* potrebbe non servire come uno strumento di copertura.

Al contrario, dato che un aumento della medesima influisce negativamente sulle azioni, in questo caso *Bitcoin* servirà da copertura per le azioni stesse e quando la correlazione *Bitcoin-azioni* è negativa. Ma, come nel caso precedente, quando invece il livello di incertezza della politica economica è basso, *Bitcoin* non può servire come una buona copertura.

