



Dipartimento di Impresa e Management

Cattedra di Storia dell'Economia e dell'Impresa

Una nuova forma di moneta: i Bitcoin
Concetto ed evoluzione di un fenomeno incerto

Relatore

Prof. Amedeo Lepore

Candidato

Carlandrea Peparini
Matricola 199341

ANNO ACCADEMICO 2017/2018

Indice

INTRODUZIONE	2
1 LA MONETA INDIPENDENTE	4
1.1 Caratteri e valore innovativo delle criptovalute	4
1.2 L'evoluzione del Bitcoin nel contesto dei nuovi mercati	10
1.3 La quarta rivoluzione industriale e l'evoluzione dei mercati monetari	15
2 LA STRUTTURA TECNOLOGICA DEL BITCOIN	22
2.1 L'innovazione della tecnologia Blockchain	22
2.2 Le applicazioni legate alle cripto-valute	27
2.3 Anonimato, Smart Contract e Digital Wallet	30
3 BITCOIN: UNA NUOVA FORMA DI SPECULAZIONE O UN'ESIGENZA REALE DELL'ECONOMIA?	35
3.1 Sviluppi futuri del Bitcoin	35
3.2 Mercati finanziari, innovazione e Bitcoin	41
3.3 Applicazioni non monetarie del protocollo	45
CONCLUSIONI	49
BIBLIOGRAFIA	51

Introduzione

Viviamo indubbiamente in una realtà di forti cambiamenti, gli enormi passi compiuti dallo sviluppo tecnologico stanno radicalmente cambiando il paradigma che fino ad oggi ha sorretto il nostro sistema economico e finanziario. I benefici che la tecnologia sta portando sono innegabili, anche se non tutti concordano sulla loro completa bontà. Infatti, se da un lato l'automatizzazione della produzione si sta espandendo sempre di più, consentendo di raggiungere livelli di produttività non possibili prima, dall'altro lato sta riducendo i posti di lavoro drasticamente.

La grande crisi finanziaria del decennio scorso ha influito nell'evoluzione e nella creazione di molti aspetti della nostra odierna quotidianità. Si è trattato, infatti, di un evento di così grande importanza che ha impresso nelle persone una vasta sfiducia nelle istituzioni, comportando la spinta a cercare delle innovazioni. Non è un caso che la stragrande maggioranza di ciò che è stato considerato come un caposaldo di un sistema, venga improvvisamente rivoluzionato. E' in questo contesto che nasce una delle invenzioni più discusse e studiate degli ultimi anni, parlo della cripto-valuta più famosa sul mercato: il Bitcoin.

Satoshi Nakamoto, ancora rimasto anonimo, è considerato colui che ha creato la prima valuta virtuale al mondo. Satoshi fu ispirato da un articolo del 1998 scritto da Wei Dai che, nella sua visione, immaginava un sistema "in cui pseudonomi intracciabili [...] (potessero) cooperare in modo maggiormente efficiente...", Wei Dai sognava un sistema in cui vi fosse la possibilità di avere un metodo di scambio senza però ricorrere a degli intermediari. Per questa ragione si crede che da questa visione Satoshi fu ispirato nell'ideare il Bitcoin, che a differenza dalle normali "*fiat currency*"¹ il cui valore è determinato dalla legge e le banconote sono sottoscritte dallo stato, i bitcoin non sono collegati con nessun'altra valuta, per questo il loro valore è determinato semplicemente dalla domanda e dall'offerta.

Benché per molti si tratti ancora di un'invenzione, nonostante la comparsa dei bitcoin sul mercato risalga a circa dieci anni fa, questa innovazione si va diffondendo in un numero sempre maggiore di aree del mondo in un sempre maggior numero di aree geografiche del globo. Per questo e per una serie di altri motivi molti studiosi stanno infatti rivalutando l'opera del premio Nobel per l'economia F. Hayek² del 1976, in cui afferma: "il governo dovrebbe essere privato del suo monopolio nell'emettere moneta, aprendo (il mercato) a più affascinanti visioni teoretiche, e mostrare la

¹ Le valute fiat, sono qualsiasi tipo di valuta a corso legale, designata e pianificata da un'autorità centrale, come ad esempio il dollaro o l'euro. European Central Bank (ECB), Virtual Currency Schemes *5 (Oct 2012), online at <http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

² Denationalization of Money-The Argument Refined: An Analysis of the Theory and Practice of Concurrent Currencies, p. 7.

possibilità di accordi che non sono mai stati considerati”. La convinzione di Hayek è che una moneta staccata dallo stato, lasciando libera competizione agli individui di creare le cosiddette “valute private”, fosse l’unico modo di creare un sistema monetario sano.

Sin dalla sua prima apparizione, questa nuova moneta è stata in grado di far parlare di sé, costringendo esperti ed istituzioni a discutere, ed in alcuni casi rivalutare, l’idea classica di moneta e la sua funzione. Obiettivo di questa tesi è analizzare alcune delle più importanti caratteristiche dei bitcoin, come la decentralizzazione, l’anonimato, la sua tecnologia e le sue possibili future applicazioni al di fuori dell’ambito monetario. Farò un appunto, inoltre, sul contesto storico in cui il Bitcoin si inserisce, quella che molti definiscono la Quarta Rivoluzione industriale.

Lo scritto si divide in tre capitoli, il primo capitolo parlerà delle caratteristiche generali del Bitcoin, delle sue possibili evoluzioni come moneta ed introdurremo il contesto di Quarta rivoluzione industriale. Il secondo capitolo, invece, tratterà più nello specifico della tecnologia su cui si appoggia il Bitcoin, il sistema Blockchain. Ed infine il terzo capitolo tratterà dei futuri risvolti che potrà avere la cripto-valuta.

CAPITOLO I

1 La moneta indipendente

1.1 Caratteri e valore innovativo delle criptovalute

Il concetto del Bitcoin è ravvisabile nell'idea di sfidare il sistema dominante, "liberare il sistema dei pagamenti elettronici dalla necessità di passare attraverso il sistema bancario, permettendo lo scambio di moneta tra utenti, senza ritardi e senza oneri" (M. Amato, L. Fantacci, 2016).

Il Bitcoin, o abbreviato BTC, sin dal suo esordio nel 2009, è emerso come la cripto-valuta di maggiore successo ad oggi. Molte ne sono apparse, tra le altre: QQ, una cripto-valuta cinese; M-PESA usata in Kenia per convertire minuti di chiamate telefoniche in soldi; o i Tem usati a Volos una città portuale greca. Tuttavia a molti sfugge cosa sia esattamente il bitcoin. Le definizioni date sono moltissime e soprattutto variegate, mi sembra giusto per iniziare riportare le più significative. Satoshi Nakamoto³, suo ideatore, ha semplicemente e sinteticamente definito il Bitcoin come: "un sistema elettronico di pagamento peer-to-peer"⁴. Nicholas A. Plassaras⁵, lo definisce così: "Concettualmente, il Bitcoin è due cose in una, per prima cosa è una moneta digitale, quindi non ha una fisica controparte a corso legale. Secondo, il Bitcoin è ciò che Friedrich A. Hayek ha descritto come una "valuta privata"⁶ creata per combattere i monopoli dei governi sull'offerta di moneta". In *Research and Challenges on Bitcoin Anonymity*⁷, si delinea come: "una valuta virtuale online basata sulla crittografia di una chiave pubblica". Infine sempre Massimo Amato e Luca Fantacci, parlano di: "un sistema di pagamento estremamente innovativo e potenzialmente molto efficace, associato ad un sistema monetario antiquato e molto pericoloso".

Concretamente i Bitcoin sono file all'interno di computer, molto simili a messaggi di testo o musica in formato mp3, possono essere benissimo distrutti o persi, esattamente come il denaro contante. Possono essere conservati sia nei pc sia nei server online. Si possono spendere sia per beni sia per servizi, anche se spenderli vuol dire in realtà trasferirli da un utente ad un altro. "I bitcoin sono la

³ Si tratta dello pseudonimo che apparse sul paper di presentazione del Bitcoin, su una mailing list, il mistero ancora si cela, anche se le ipotesi sulla vera identità ormai ricadono su tre nomi: Finney, Szabo e Wright, i tre più stretti collaboratori del progetto Bitcoin.

⁴ Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 pp. 1

⁵ Nicholas A. Plassaras, *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, *Chicago Journal of International Law*: Vol. 14: No. 1, Article 12, 2013.

⁶ Valuta ideata da singoli individui, e non dalle istituzioni.

⁷ Jordi Herrera Joancomartí, *Research and Challenges on Bitcoin Anonymity*, University of Barcelona, 2014.

prima forma di contante digitale. “Unisce in sé i vantaggi della moneta elettronica e del contante”, stando a come affermano i due maggiori esperti sui Bitcoin italiani⁸.

Tra le principali caratteristiche risulta la sua robustezza di sistema, fattore dovuto alla tecnologia che vi è dietro: la tecnologia Blockchain, un database digitale pubblico reso stabile da validazioni crittografiche. Un'altra importante proprietà, responsabile del suo successo, è stata la decentralizzazione. Nessun ente pubblico governativo, infatti, è mai stato coinvolto in transazioni con dei bitcoin. Le interazioni che vi possono essere tra la moneta digitale e le altre valute non sono regolate da nessuna legge, e tutti gli aspetti del bitcoin sono controllati esclusivamente dai suoi utenti. La cripto-valuta opera, inoltre, usando un sistema peer-to-peer⁹ e la crittografia per mantenere l'anonimato¹⁰ nelle transazioni. Il software di questa tecnologia è di tipo “open source”, permettendo a tutti gli utenti di visionare i codici e capire come funziona il sistema.

Alcuni caratteri peculiari che abbiamo qui discusso, potrebbero permettere a questa nuova tecnologia di diffondersi come nuova moneta globale.

In ambito Europeo è interessante la posizione della BCE¹¹ che, nonostante approfondisca funzioni e sviluppi dei bitcoin e delle altre cripto-valute, ritiene che le monete virtuali, poiché prive di un apparato normativo che ne stabilisca le funzioni di mezzi di adempimento delle obbligazioni, non possono essere considerate come moneta. C'è comunque una piccola eccezione, nel senso che possono essere considerate valide ma solo nell'accezione di moneta contrattuale, quindi negli scambi nel momento in cui le due parti si siano già accordate al riguardo. G. Lemme, commenta questa posizione, definendola: “estremamente conservatrice nell'uso della parola moneta”¹². E' possibile, infatti, notare come la BCE affermi in modo molto determinato che: “le monete scritturali, e i bank money in euro o in euro elettronici non sono valute a corso legale. Non importa che queste forme siano largamente accettate per qualsiasi genere di pagamento”¹³. Ormai però la distinzione tra moneta fisica e moneta elettronica è un tema di discussione superato, e da tempo, in dipendenza del contesto la moneta elettronica ha la possibilità di adempire alle obbligazioni pecuniarie esattamente come la moneta fisica. Il problema principale della dottrina è, arrivati a questo punto, quello di stabilire entro quali limiti il Bitcoin sia in grado di assolvere alle obbligazioni. Un'altra domanda su cui gli esperti

⁸ M. Amato, L. Fantacci, Per un pugno di Bitcoin, università Bocconi, 2016.

⁹ Peer-to-peer: rete locale in cui i computer collegati hanno gli stessi diritti di tutti gli altri di accesso alle risorse comuni.

¹⁰ Wei Dai, B-Money (1998), online at <http://weidai.com/bmoney.txt>

¹¹ BCE, Virtual currency schemes – a further analysis, Febbraio 2015

¹² G. Lemme, S. Peluso, Criptomoneta e distacco dalla moneta legale: il caso bitcoin, dottrina e giurisprudenza commentata, Estratto dal n. 11, 2016.

¹³ Vedi nota 11.

si interrogano è sulla possibilità in cui il Bitcoin divenendo una cripto-valuta piuttosto diffusa possa divenire sostituta delle attuali valute.¹⁴

Gli economisti tipicamente definiscono una moneta, secondo tre caratteristiche fondamentali: mezzo di scambio, unità di conto e riserva di valore.

- Mezzo di scambio:

E' la fondamentale funzione che una moneta, per essere tale, deve assolvere. La moneta deve riuscire a fungere da strumento di pagamento nelle compravendite di beni e servizi, o come corrispettivo in altri ambiti commerciali. Uno degli aspetti che comporta l'adozione dei bitcoin o delle valute digitali in generale è il bassissimo costo delle transazioni, nonché altri benefici offerti dal Bitcoin come ad esempio l'anonimato e la trasparenza delle transazioni. Basti, infatti, pensare che in una normale transazione tra Bitcoin, il peso sul valore totale dello scambio è di circa l'1%¹⁵ (al massimo), rispetto al 2-5%¹⁶ delle canoniche transazioni con valute a corso legale; ciò grazie alla disintermediazione. G. Lemme aggiunge anche che: "Convenienza e velocità costituiscono senz'altro elementi a favore di Bitcoin rispetto alle valute standard." Anche lo studioso D. Yermack, che risulta essere uno degli esponenti più scettici nei confronti della criptovaluta che abbiamo preso in considerazione, nel paper *Is Bitcoin a Real currency?*, afferma: "i Bitcoin soddisfano sempre di più il primo dei tre criteri, poiché un sempre maggior numero di professionisti come commercianti, specialmente nel mercato online, appaiono concordi nell'accettare questi come forme di pagamento".

Quindi si può concludere che, sotto questo primo aspetto, il bitcoin assolva la funzione primaria richiesta ad una moneta, e con almeno due aspetti evolutivi: maggiore velocità e costi ridotti delle transazioni.

Plassaras¹⁷ rafforza ulteriormente il concetto attribuendo al Bitcoin l'aggettivo di "mezzo superiore di scambio", infatti: "le valute digitali [...] permettono agli individui di commerciare con un altro senza preoccuparsi di dove sia l'uno e l'altro e senza che questi si conoscano. Mentre lo stesso potrebbe essere detto di altri sistemi di pagamento elettronici come *PayPal*, le monete digitali sono uniche nel senso che oltrepassano i costi di transazione dovute al cambio di valuta. Nella visione dell'utente fare questo cambio implica un'ulteriore step prima di completare la transazione."

¹⁴ Le cripto-monete hanno maggior attitudine rispetto alle monete complementari di assumere funzione monetaria vera e propria, teoria riscontrabile nell'opera di H. OLIPHANT, *The theory of money in the law of commercial instruments*, in *Yale Law Journal*, 1920, pp. 606 segg.

¹⁵ Vedi nota 12.

¹⁶ Vedi nota 12.

¹⁷ Vedi nota 3.

Per contro su questo aspetto di mezzo di scambio, non si può dimenticare che, non essendo una valuta a corso legale come l'euro o il dollaro, la possibilità di essere usata dipende solamente dalla volontà delle parti, ma legalmente, ancora, nessuno è obbligato a doverla accettare come metodo di pagamento. E' quindi opinione comune che sia proprio uno di questi tratti a rallentare la sua diffusione; inoltre va considerata anche la difficoltà per i più di entrare in possesso di Bitcoin (G. Lemme).

Questo della difficoltà, però, a mio avviso, è un fattore legato al tempo, potrebbe essere superato nel futuro, come è avvenuto per la moneta elettronica.

Un aspetto di complessità, è, infine, il livello di conoscenza dei sistemi informatici; infatti, il sistema Bitcoin si regge su strutture di codici molto complesse, che solo pochi programmatori sono in grado di implementare. Ma anche questo fattore è molto legato al tempo: in un primo momento potrebbe sembrare una barriera all'entrata, ma potrebbe essere superata come altre difficoltà tecniche; e la tempistica potrebbe sorprendere. Infatti la velocità di adozione della tecnologie (anche complesse) negli ultimi decenni ha fatto registrare una significativa accelerazione.

Quello che potrebbe essere considerato un limite importante dai mercati finanziari, è il fatto che il numero di Bitcoin in circolazione è noto e tutti i Bitcoin vivono all'interno della Blockchain. In sostanza non è possibile possedere Bitcoin al di fuori della Blockchain, si possono possedere solo indirizzi elettronici che danno il diritto a "spendere" o "ottenere". Non è, infatti, possibile creare una riserva frazionaria dentro questa struttura (G: Lemme). Questo sistema limita molto la struttura economica dei Bitcoin, poiché nessun ente esterno potrà mai dare o prendere a prestito Bitcoin a tasso zero, creandoli dal nulla. Ma questo aspetto potrebbe essere valutato già come ulteriore rispetto all'essenza della funzione "mezzo di scambio".

- Unità di conto:

Per poter sostenere una sufficiente unità di conto, una valuta deve fornire un'intuitiva misura del suo valore. Un Bitcoin potrebbe essere valutato in base alla sua difficoltà e complessità nel crearlo, o per usare termini tecnici per "estrarlo".

Plassaras ricorda che, allo stato attuale della tecnologia, la produzione dei Bitcoin dovrebbe terminare intorno al 2025 e che la difficoltà nel produrne nuovi potrebbe renderli rari e ricercati come l'oro.

Passando, però, ad aspetti meno teorici, Lemme prende in considerazione due aspetti per i quali la valuta virtuale si differenzia non poco dalle valute standard, ovvero divisibilità e volatilità di prezzo.

Divisibilità: possiamo dire che la divisibilità di Bitcoin è praticamente infinita, infatti ricordiamo che le valute a corso legale sono divisibili fino a due cifre decimali, mentre il Bitcoin un numero che va

fino ad n^8 , l'ultimo decimale prende il nome dal suo ideatore, si chiama infatti "Satoshi". Questa caratteristica potrebbe facilmente portare un utilizzatore poco esperto alla confusione, ed oltre questo, potrebbe risultare ancora più difficile determinare il vero valore. Ma come per altri casi tempo ed uso potrebbero consentire di superare questi problemi.

Nel breve periodo, la volatilità dei prezzi del Bitcoin è stata alta, a tal punto che sul sito stesso della cripto-valuta si consiglia di non investire soldi di cui si potrebbe necessitare, poiché i Bitcoin attualmente sono considerati come un investimento molto rischioso¹⁸. Questo fatto impatta, non indifferentemente, sulla prestazione di Bitcoin come unità di conto. Yermack nel suo scritto¹⁹, infatti, commenta: "la valuta presenta usuali e sostanziali cambi di volatilità, questo tende a minare qualsiasi tipo di ruolo per i Bitcoin come unità di valore". In conseguenza proprio di questa peculiarità i commercianti che fanno uso dei Bitcoin, sono costretti ad adeguare spesso ed in fretta i prezzi onde evitare che venga intaccata la loro competitività. E', infatti, considerata una grande esternalità negativa per quei commercianti che vendano i propri prodotti in Bitcoin, ma acquistino le materie prime in valute standard. In seguito alle forti variazioni di prezzo e tassi d'interesse che caratterizzano la criptovaluta, molti studiosi sono scettici su una sua reale affermazione nell'economia reale, ad esempio Brian P. Hanley, in *The False Premises and Promises of Bitcoin*, afferma: "E' impossibile immaginare che il commercio possa mai essere talmente robusto da traslare in bitcoin o centi-satoshi visto le alte volatilità dei tassi. Nessun giocatore razionale li userebbe per degli scopi d'acquisto".

In conclusione, su questo aspetto di unità di conto, il bitcoin tecnicamente è in grado di assolvere la funzione, ma manca al momento della "credibilità o diffusione" che ne calmierino la volatilità.

- Riserva di valore:

Il fatto che la moneta mantenga il proprio valore nel tempo, permette agli operatori di accumulare e mantenere ricchezza, questa caratteristica permette anche agli strumenti di pagamento di essere fruibili, poiché in quanto l'uso di uno strumento di pagamento presuppone proprio il fatto che la temporanea detenzione non faccia perdere potere d'acquisto.

Plassaras considera il bitcoin molto positivamente sotto questo aspetto: "l'indipendenza delle valute digitali dalla diretta influenza politica, rende queste ancora superiori, poiché loro posseggono una maggiore riserva di valore". Le valute tradizionali sono spesso accettate come riserva di valore poiché sostenute dai governi, che danno un senso di legittimità e stabilità agli occhi degli utenti. Ma se il governo decidesse di inflazionare la propria moneta, nel nome di una più grande politica economica,

¹⁸ Fonte: bitcoin.org

¹⁹ Yermack D., Is Bitcoin a Real Currency?, NBER Working Paper No. 19747, 2013.

il benessere dei propri individui nella forma di moneta diminuirebbe. Le valute elettroniche, invece, potrebbero rispondere alle forze del mercato. Conseguentemente i sostenitori delle valute digitali avrebbero un forte incentivo a mantenere la moneta stabile.

Un netto vantaggio che il Bitcoin possiede è quello di non appartenere a nessun governo, o istituzione, non è soggetto quindi ad inflazione e nemmeno soggetta alle politiche monetarie del caso. Le uniche variazioni a livello monetario intervengono finché i “*miner*”²⁰ continueranno ad investire per poter sbloccare nuovi Bitcoin, l’investimento di tutte queste risorse però richiede un continuo apprezzamento della moneta affinché ci sia un interesse economico. Ciò ha portato nel periodo 2009-2011 all’accumulazione da parte di alcuni utenti, invece che nell’uso, questa tendenza si è invertita dal 2011 in poi.

Volendo trarre delle conclusioni sul valore innovativo e tecnico del bitcoin in confronto con le fiat currencies, abbiamo annoverato diversi aspetti innovativi:

- buon potenziale come mezzo di scambio, meno costoso e più rapido di valute tradizionali, sebbene dipendente da capacità e conoscenze tecnologiche piuttosto avanzate
- ottima risposta sull’aspetto divisibilità
- buon potenziale come riserva di valore, da taluni ritenuta superiore a quella delle valute tradizionali, per via della relativa estraneità a andamenti politici.

Sono, invece, da considerare con prudenza i seguenti aspetti:

- volatilità dei prezzi
- capacità come riserva di valore (legata alla volatilità dei prezzi), che a sua volta è anche legata però alla ridotta circolazione.

Comunque passi avanti nel riconoscere il Bitcoin come valuta se ne stanno facendo. Infatti è stato decretato dalla Corte di Giustizia UE, con la sentenza 22.10.15 (in causa C-264/14, Skatteverket c/ David Hedqvist), che “le operazioni relative a valute non tradizionali, vale a dire diverse dalle monete con valore liberatorio in uno o più paesi, costituiscono operazioni finanziarie, in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento”.

²⁰ Coloro che prestano la propria potenza computazionale per estrarre bitcoin dai nuovi blocchi generati dalla Blockchain.

1.2 L'evoluzione del Bitcoin nel contesto dei nuovi mercati

Dal loro primo rilascio nel gennaio del 2009 i Bitcoin hanno acquisito sempre più piede nell'economia reale; la valuta è accettata per pagamenti in molti siti come Wordpress.com, Reddit e molti altri. Ritengo infatti che il crescente numero di utenti sia stato influenzato dai vantaggi che il cyberspace comporta ed ha inoltre aiutato la diminuzione della fiducia nel sistema bancario.

Nonostante la sua forte innovatività, il bitcoin, infatti, non nasce dal nulla, ma prende spunto dai pensieri della scuola austriaca di Hayek, si discosta dal pensiero di Keynes, critica aspramente le fiat money. Tutte riflessioni che, messe insieme, sintetizzano il perché il Bitcoin sia una via alternativa.

Non è affatto un caso, infatti, che Nakamoto dica: "Ciò che occorre è un sistema di pagamento elettronico basato su una verifica crittografica anziché sulla fiducia". E' per questo genere di assunti che il Bitcoin ha intenzione di differenziarsi ed allontanarsi da ogni forma di moneta fiduciaria passata e attuale. Non è nemmeno casuale il fatto che l'inizio dell'era Bitcoin, coincida esattamente con uno dei peggiori periodi finanziari della storia (cfr. crisi finanziaria 2007-2008), in cui la sfiducia nei confronti del sistema si estendeva dalle grandi organizzazioni, come le banche centrali, passando per la rappresentanza politica, fino ad arrivare a sfere della vita civile.

Nell'agosto del 2008, appare per la prima volta il dominio bitcoin.org, anche se la presentazione ufficiale arriva con la pubblicazione del proprio paper di introduzione, firmato con lo pseudonimo di Satoshi Nakamoto, con titolo: "Bitcoin a peer-to-peer electronic cash system". Nel paper si introduce al fatto che il bitcoin sarà un sistema trasparente, decentralizzato ed anonimo, ideale per far fronte alle nuove esigenze di un mercato appena uscito da una delle peggiori crisi dell'ultimo secolo. Colpisce la decisione dell'autore nell'imporre un tetto massimo di bitcoin in circolazione di 21 milioni di bitcoin, che secondo gli esperti verrà raggiunto nel 2025 circa.

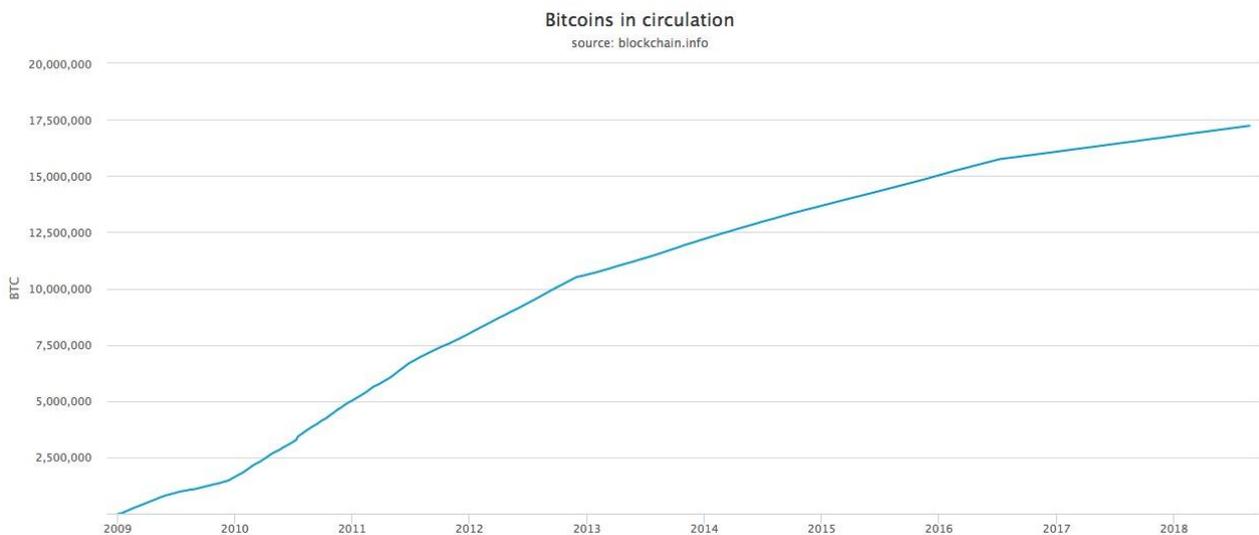
Nonostante la registrazione del dominio e la pubblicazione del paper i primi bitcoin furono generati, però, nel 2009, come dimostrazione della funzionalità del sistema. Inizialmente i bitcoin circolarono solamente tra volontari e tecno-fanatici. La prima transazione avvenne il 3 gennaio 2009 quando gli sviluppatori comprarono una pizza per 10.000 bitcoin, ma il pagamento non avvenne direttamente in bitcoin, ma attraverso una terza piattaforma che li convertì in dollari.

Non così lentamente tra gli investitori e il mondo della finanza in generale il nome bitcoin iniziava sempre di più ad attrarre utenti, a tal punto che verso la fine del 2009 i bitcoin furono quotati alla New Liberty Standards con un cambio con il dollari di 1,309.

In seguito alla quotazione, la fama della cripto-valuta continuava a crescere in modo esponenziale, attirando alcune delle piattaforme di cambi, come Mt Gox ad iniziare a trattare bitcoin, fornendo inoltre consulenze, statistiche ed altre informazioni fondamentali per gli utenti.

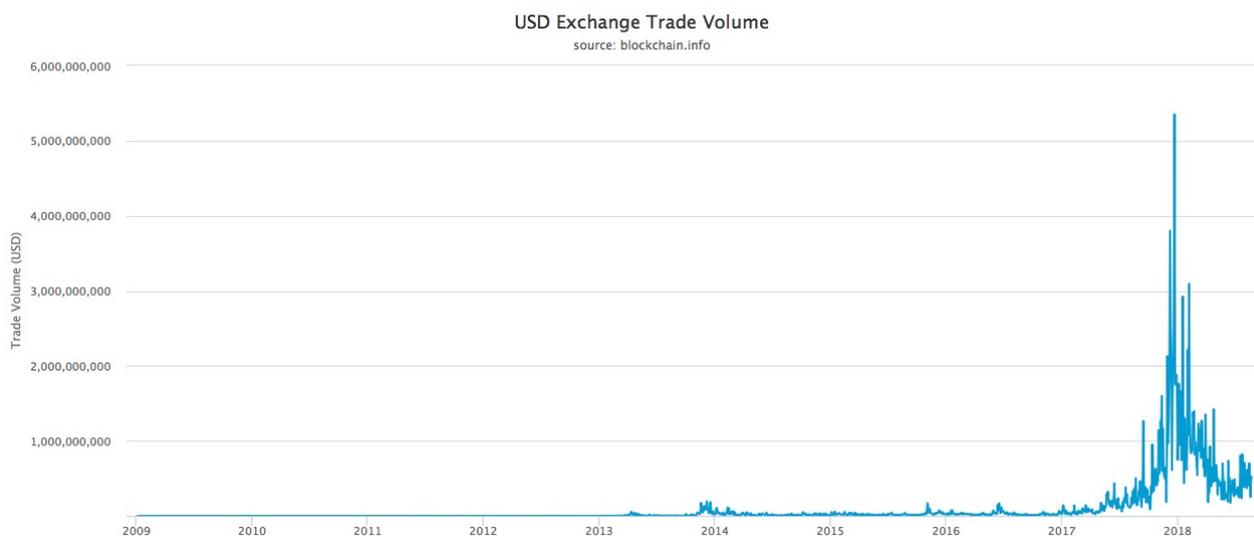
Di seguito ho riportato nella tabella 1 il trend di bitcoin in circolazione, dalla loro creazione, fino ad oggi. Osservando il grafico è facilmente ravvisabile come già a soli due anni dalla loro comparsa, quindi nel 2011, fossero in circolazione già 5 milioni di unità di bitcoin, questo trend si è tenuto in costante crescita fino ad arrivare ai 17.500.000 in circolazione nel 2018.

Tabella 1, fonte: blockchain.info



Ma non sono gli unici dati degni di nota. E' importante, infatti, notare come siano cambiati nel corso di questi dieci anni la quantità di volumi scambiati sul mercato. In questo caso, però, i primi segni rilevanti risalgono al 2014, come è possibile notare dalla tabella 2, da quel momento la crescita non ha subito particolari cambiamenti, fino a raggiungere dei picchi senza eguali nel 2018, apice fino ad ora della sua popolarità, arrivando a toccare gli oltre 5 miliardi di dollari in volumi di scambio.

Tabella 2, fonte: blockchain.info



La terza tabella infine mostra come i bitcoin siano stati soggetti a forti speculazioni, soprattutto nell'anno corrente, se quindi nel 2009 avevano un valore di 1,309 dollari, nel dicembre del 2017 la cripto-valuta ha rivoluzionato i mercati finanziari toccando un valore di circa 19.000 dollari per unità.

Tabella 3, fonte: blockchain.info



Tutti questi dati facilitano la comprensione di come il bitcoin si inserisca nei mercati monetari attuali. Poiché la struttura di questa moneta implica un possesso assoluto ed esclusivo, come l'oro d'altronde, non è utilizzabile al di fuori dell'ambito monetario. Per questo motivo Gavin Andresen ha affermato:

“This is better gold than gold” (Greenberg 2011)²¹. Spieghiamoci meglio, si tratta di un oro migliore dell’oro, per il fatto che è moneta allo stato puro, è completamente di proprietà e non produce passività finanziarie²². Tutto il suo valore è dato dal suo valore di scambio, F. von Hayek, in uno dei suoi scritti introdusse il concetto di: “moneyness”, traducibile in italiano con “moneità” che l’economista intese come massima qualità di moneta, viste le caratteristiche appartenenti al bitcoin è possibile affermare che questo sia ciò che meglio rappresenta il concetto di Hayek. M. Amato e L. Fantacci a tale proposito aggiungono: “Il bitcoin potrebbe essere considerato il bene privato per eccellenza: può essere ceduto in cambio di qualsiasi altro bene privato in una relazione binaria di scambio”.

Fatto molto peculiare d’altronde è che gran parte del pensiero dietro questa cripto-valuta, risiede nell’idea che un uomo possessore di bitcoin sia “individuo assoluto”, cioè libero da qualsiasi legame che “lo ecceda o lo trascenda”. A proposito di questa conclamata libertà dell’individuo prende forma e si sviluppa tra i sostenitori del Bitcoin il concetto di “capitalismo distribuito”, cioè un capitalismo fondato “sull’idea che ognuno può commerciare e scambiare; o, in poche parole che ognuno “può diventare un capitalista indipendente” (Kostakis, Giotitsas)²³.

Fino ad ora si nota come il punto di maggiore forza nel pensiero bitcoiniano sia la libertà che comporta il sostegno di questo nuovo piano monetario, appoggiando inoltre una scissione da qualsiasi tipo di sistema economico esistente. Tutti bisogni derivati da una sfiducia dell’attuale organizzazione economica.

Seguendo ancora questo filone, infatti, gli autori del libro Amato e Fantacci, delineano un interessante carattere della moneta: “Bitcoin è disegnato su una idea di natura. Che l’economia sia il mercato, e che il mercato sia questo mercato, in cui anche la moneta è al contempo una merce tra le altre e un potere di comando tra tutte le merci”. Si percepisce quindi che il sistema del Bitcoin possa fare a meno di rapporti umani, come ad esempio la fiducia, per dare luogo a rapporti commerciali tra individui, “ma di un quadro di certezza procedurale”. Si tratta di una chiara critica al concetto di mercato degli istituzionalisti, che a loro volta definiscono il mercato come: “un costruito istituzionale che presuppone la legge” (M. Amato, L. Fantacci). Al contrario, nella cripto-economia si afferma: “Aldilà del fatto che si vedono segnali dell’emergere di strutture di governo in Bitcoin, si può anche vedere come la sua logica segue le regole delle altre valute. E’ il codice a comandare invece delle banche centrali [...] ma su internet il codice è legge, ovvero vi è un politica intrinseca in ogni pezzo di software. [...] (nel mondo reale) la legge assicura la credibilità dei contratti, difende i diritti di

²¹ Greenberg A., Crypto Currency, <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#2bd6f317353e>

²² Si parla di passività finanziarie quando l’impresa contabilizza delle passività correnti che ritiene di poter estinguere nell’esercizio corrente.

²³ Kostakis V., Giotitsas D., the (a)political economy of bitcoin, Triple, 2014.

proprietà e regola la circolazione monetaria. [...] Viceversa nel mondo digitale è il codice ad assumere questo ruolo e a stabilire cosa gli utenti possono o non possono fare. Perciò Bitcoin, in quanto frammento di software, incorpora le idee tratte da una certa visione politica” (Kostakis, Giotitsas 2014). La fede riposta in Bitcoin è quella che sia possibile una ricreazione informatica dell’economia, e che tale mondo così ricreato non possa che essere migliore.

E’ stata proprio questa fede, riposta in questa nuova tecnologia, che ha influenzato l’esponenziale sviluppo senza freni e senza controlli del Bitcoin ed in generale delle altre cripto-valute. Secondo molti esperti si tratta, però, di una delle più recenti crescite finanziarie incontrollate, che rischia, come già successo una decina di anni fa, di trasformarsi in un’altra grande bolla finanziaria.

Attualmente i Bitcoin in circolazione valgono circa 97 miliardi di dollari, mentre la diffusione della cripto-valuta, come già accennato, sta crescendo sempre più. Questa enorme e diversificata massa monetaria, priva di una regolazione, rischia di essere il prossimo capitolo di altre bolle speculative, se non si interviene per tempo a stabilire meccanismi di garanzia e di controllo. Nonostante i chiari rischi che si potrebbero prospettare, si riconoscono anche dei vantaggi, come afferma Christine Lagarde: “Proprio come alcune tecnologie emerse nell’era delle dot.com hanno trasformato le nostre vite, le risorse crittografiche potrebbero avere un impatto significativo sul modo in cui risparmiamo, investiamo e paghiamo i nostri conti”²⁴. Non possiamo di certo definire Lagarde una completa sostenitrice di questo sistema, infatti la responsabile del FMI ha esposto le proprie titubanze sulla natura decentralizzata ed anonima della tecnologia Bitcoin, includendo nelle proprie paure l’aumento di finanziamenti al terrorismo, metodi di riciclaggio di denaro, ed una maggiore facilitazione all’acquisto di droghe e armi su Internet.

Ad ogni modo nessuno ha mai proposto l’idea di bloccare il processo di innovazione, sarebbe una soluzione poco lungimirante, dal momento che la digitalizzazione rappresenta importanti meccanismi per ridurre i costi di transazione e migliorare la competitività dell’economia internazionale. Non a caso la tecnologia Blockchain non mira ad effettuare transazioni, ma punta all’obiettivo di azzerare i costi amministrativi legati alle operazioni di trasporto. Ma affinché questo potenziale non si tramuti in altro, conterà ancora di più la regolazione e la tutela dell’interesse collettivo, che dovranno inevitabilmente assumere forme nuove, meno burocratiche ma comunque efficaci per evitare manovre speculative che possono poi soffocare lo sviluppo.

²⁴ Fonte: <https://www.borsainside.com/criptovalute/67654-il-fondo-monetario-internazionale-spinge-le-quotazioni-di-bitcoin/>

1.3 La quarta rivoluzione industriale e l'evoluzione dei mercati monetari

“Il termine rivoluzione denota un cambiamento repentino e radicale. Nel corso della storia le rivoluzioni hanno avuto luogo quando le tecnologie e le nuove modalità di concepire il mondo hanno dato il via a profondi mutamenti nei sistemi economici e nelle strutture sociali”.²⁵

E' esattamente quello che sta accadendo alla nostra società, con il continuo avanzamento delle tecnologie, si sta modificando il paradigma sociale che noi tutti conosciamo, rendendo le connessioni molto più diffuse e dirette, migliorando tecniche produttive e il nostro modo di vivere.

Fino ad ora il genere umano ha vissuto tre rivoluzioni industriali, ognuna di queste ha apportato dei significativi cambiamenti all'interno del costruito sociale ed economico. La prima, avvenuta in Inghilterra tra gli anni 1760 e 1840, segnò il passaggio dal lavoro manuale a quello meccanico, con l'invenzione del telaio a vapore e delle ferrovie. La seconda, che risale al periodo tra la fine dell'800 ed i primi del '900, in cui dal lavoro meccanico si passò alla produzione di massa, ricordiamo l'epoca del fordismo e del taylorismo. Infine la terza, iniziata durante gli anni '60 del XX sec. e conclusasi verso gli inizi degli anni 2000, ricordata come la rivoluzione digitale, per via della diffusione dei personal computer, di internet e dei sistemi informatici.

E' opinione diffusa che stiamo affrontando un periodo di ulteriore svolta, la cosiddetta Quarta rivoluzione industriale, in cui possiamo riscontrare caratteri di differenziazione netti rispetto alle scorse rivoluzioni. Klauss Schwab, la connota così:

- 1) velocità di diffusione. Responsabile di questa velocità è il fatto che il sistema sia sempre più interconnesso ed eterogeneo.
- 2) la portata e l'intensità, le nuove tecnologie infatti creano nuovi paradigmi economici e sociali, che ridefiniscono chi siamo e cosa facciamo
- 3) l'impatto sui sistemi; questo aspetto riguarda la trasformazione di interi sistemi: paesi, aziende, settori e società.

A ben vedere ciascuna delle precedenti rivoluzioni ha avuto un impatto forte rispetto ai punti 2 e 3, quindi è rifatto il primo aspetto, l'elevata velocità di diffusione e la predisposizione di un mondo globalizzato che la recepisce così omogeneamente, che la rendono così pervasiva e potente.

In generale il carattere innovativo di questa nuova rivoluzione risiede in un maggior uso di internet, un notevole utilizzo della robotica nella produzione e nel trasporto umano, uso sempre più diffuso di forme di apprendimento automatizzate e dell'integrazione dell'intelligenza artificiale.

²⁵ Schwab Klaus, La quarta rivoluzione industriale, FrancoAngeli edizioni, 2016.

Molte aziende o organizzazioni si sono focalizzate su quali potrebbero essere le tecnologie e le innovazioni che potranno essere predominanti all'interno di questa Quarta Rivoluzione Industriale. I campi in cui queste prenderanno piede sono sostanzialmente tre: sfera fisica, sfera digitale e sfera biologica.

I cosiddetti “megatrend” o i “driver del cambiamento”, per quanto riguarda la sfera fisica le innovazioni sono rappresentate da: veicoli autonomi, stampa 3d, robotica avanzata e utilizzo nuovi materiali. Per quanto concerne la sfera digitale troviamo, sensori sempre più sofisticati, utilizzo di tecnologie come quella blockchain e lo sviluppo di piattaforme per la *sharing economy*. Tutte queste innovazioni si sviluppano nell'ambito dell'*iot* (internet of things), cioè il rapporto che intercorre tra cose ed individui realizzato grazie alle connessioni. Infine elenco alcune delle innovazioni del campo biologico, come: sequenziamento del DNA, applicazioni delle nanotecnologie, mappatura dei geni e via dicendo.

Nonostante per i più questo genere di innovazioni possa rappresentare un punto di svolta, molti ancora restano scettici sui loro utilizzi. Il dibattito infatti è tra due scuole di pensiero, da un lato i tecnopessimisti, che ritengono che ormai i benefici tecnologici degli ultimi anni abbiano esaurito la propria utilità, e che quindi questo periodo si svilupperà senza alcun significativo cambiamento, dall'altro lato ci sono i tecno-ottimisti, che al contrario sono fiduciosi dell'attuabilità di queste innovazioni, rendendo possibile un incremento del benessere sociale ed economico.

Schwab tiene una posizione critica: “ho l'impressione che i livelli richiesti di gestione e recepimento dei cambiamenti in atto siano ancora insoddisfacenti, se messi a confronto con la necessità di ripensare al nostro sistema economico, sociale e politico per governare correttamente la Quarta Rivoluzione Industriale”²⁶.

Indubbiamente rispetto agli anni passati le tecnologie e le innovazioni hanno la tendenza a diventare sempre più accessibili a chiunque, privati cittadini e non. A mio avviso Schwab mette in evidenza due punti critici importanti: primo punto, l'infrastruttura istituzionale essenziale è inadeguata per riuscire a condurre la diffusione dell'innovazione e minimizzare possibili disagi;

secondo punto manca una visione condivisa attraverso cui definire le opportunità e le sfide.

Proprio poiché queste innovazioni hanno il potenziale di riscrivere i manuali di storia ed economia, bisogna essere pronti a saper ristrutturare l'organizzazione sociale ed economica, sottolinea infatti che oltre alla velocità di diffusione sono impressionanti le economie di scala ottenute con

²⁶ Vedi nota 21.

automazione e altre innovazioni. Questo avrà un impatto impressionante sull'utilizzo e la redistribuzione del lavoro.

Basti pensare che nel 1990, a Detroit, le tre maggiori fabbriche della città davano lavoro a circa 1,2 milioni di persone, oggi Google, nella metà del tempo, ha raddoppiato il fatturato, dando lavoro soltanto a 140.000²⁷ persone.

Schwab osserva che, negli ultimi anni, molti tra i paesi maggiormente sviluppati, come ad esempio la Cina, abbiano registrato un calo della forza lavoro in confronto al PIL. Carl Benedikt Frey e Michael Osborne, che nel loro scritto "Technology at work"²⁸, hanno notato che circa la metà di questo declino può essere espresso dalla riduzione dei prezzi sui beni d'investimento, che a turno sono guidati dagli avanzamenti tecnologici dei sistemi informatici, portando le aziende a sostituire il lavoro con il capitale nella produzione.

Veniamo quindi a considerare aspetti finanziari correlati a questa rivoluzione: nel futuro le tecnologie digitali potranno sostituire sempre di più il capitale. Sarà sempre più semplice infatti codificare beni e servizi, e una volta codificati, questi potranno essere digitalizzati e replicati. Se un tempo la tendenza era quella di cercare "venture capital", ora non sarà più così, le aziende non avranno infatti più così bisogno di cercare capitale fisico, come un tempo facevano i giganti dell'economia. Basti pensare ai famosi social network, Whatsapp o Instagram, che non hanno avuto bisogno di grandi capitali per iniziare, né di un team così numeroso.

Mentre le tecnologie digitali si sostituiscono al lavoro, la richiesta di capitale decresce. Finora chi ha veramente beneficiato dei vantaggi dovuti alla digitalizzazione sono stati gli azionisti. Infatti, come accennavamo anche prima, le prime tre aziende della Silicon Valley, nonostante abbiano un numero decisamente contenuto di dipendenti, fatturano 1.09 trilioni di dollari, quindi visto questo favorevole rapporto, hanno una capitalizzazione e rendimenti molto elevati. Perciò le aziende che vorranno veramente emergere da questa rivoluzione saranno quelle che riusciranno ad offrire ai propri clienti innovazione.

Un'ulteriore chiave di cambiamento da osservare in questo XXI sec. sarà quella di cercare di includere nella crescita economica un nuovo sistema di tassazione. Infatti, visto che i costi stanno crollando e che con i sistemi informatici dirompenti è molto più semplice spostare i lavoratori per il globo, o farli addirittura restare a casa a lavorare, il sistema attuale di tassazione dimostra di non stare al passo con il cambiamento. Infatti, poiché i consumatori stanno beneficiando del declino dei prezzi

²⁷ Vedi nota 23.

²⁸ C. Benedikt F. M. Osborne, Technology at work, Citi GPS: Global Perspectives & Solutions, 2015, p. 7.

di molti prodotti e servizi, l'idea più condivisa è quella di spostare il carico delle tasse dal lavoro, e quindi dal reddito, al consumo. Secondo Thomas Piketty, le tasse potrebbero essere traslate dal lavoro alla ricchezza, infatti secondo l'esperto, il gap di ricchezza che si è andato a creare tra i possessori di capitali e lavoratori potrebbe essere combattuto con una tassa sulla ricchezza.

Le moderne aziende stanno automatizzando sempre di più il lavoro e sfruttando le nuove tecnologie, stanno rendendo i propri business sempre meno dipendenti dai capitali, persino i più tradizionali beni e servizi stanno diventando incredibilmente mobili. Diversi sondaggi hanno dimostrato che, oramai, le persone preferiscono impiegarsi autonomamente e non divenire dipendenti in altre aziende. Probabilmente questo è il nuovo trend lavorativo del futuro, in cui l'impiego autonomo sarà la nuova normalità. La sfida delle istituzioni quindi sarà quella di dover incentivare questo genere di business con un modello di tassazione che non ostacoli i nuovi imprenditori. Bisogna, però, ricordare che, se da un lato questa rivoluzione sta creando nuovi modelli di business e di aziende, dall'altro lato però sta lasciando indietro molti altri lavoratori, a causa della forte automatizzazione che stiamo vivendo. Secondo gli autori del paper il 47%²⁹ dei lavori negli USA è in grave pericolo. Una possibile soluzione a questo problema è la cosiddetta crescita inclusiva, cioè la capacità dei governi di saper reintrodurre i lavoratori, per gestire correttamente questa transizione andranno fatti molti più investimenti per implementare le skills dei lavoratori e prepararli al meglio per questo nuovo sistema.

Analizzando ora la produttività, negli ultimi anni si è assistito a come la crescita del PIL globale sia stata costantemente lenta, nonostante l'avanzamento tecnologico sia stato esponenziale. Molti riconducono questa tendenza al paradosso dell'odierna logica di non saper conciliare le alte tecnologie alle produzioni. In realtà il discorso da fare è ben diverso, non è l'economia che cresce lentamente nonostante gli ampi progressi tecnologici, ma, come afferma Hal Varian, capo economista di Google, gli attuali metodi di rilevazione dell'utilità non sono in grado di valutare i benefici che noi tutti quotidianamente traiamo dalle innovazioni, ad esempio prenotare un veicolo con il telefono, il cui valore economico viene ignorato da tutti poiché trattasi di un servizio erogato gratuitamente, come molti altri ad esempio.

E' sulla base di questo tipo di esempi che possiamo credere che la Quarta rivoluzione industriale riuscirà ad apportare migliorie sia i termini economici sia sociali. Infatti questa rivoluzione apre al mondo numerosi prospetti positivi, per esempio aumentando drasticamente la domanda di milioni di utenti, concedendogli al tempo stesso la possibilità di soddisfare questa domanda, favorendo un accesso più rapido e semplificato a beni e servizi e accompagnando una più facile interazione tra individui provenienti da tutto il globo.

²⁹ Vedi nota 26.

Ovviamente i fattori di cambiamento sono tanti e diversi, le varie tecnologie aiuteranno a cambiare il modello di business ma le aziende dovranno essere pronte a sconfinare dai propri confini sia tecnologici che geografici. Vi sarà un cambiamento delle aspettative dei clienti, un miglioramento dei prodotti, la creazione di nuove partnership e la trasformazione dei modelli standard in modelli digitali.

La rivoluzione digitale sta promuovendo quindi degli approcci che cambieranno radicalmente il nostro modo di fare le cose. Inoltre il mercato come abbiamo visto sta volgendo i propri interessi verso una diversa composizione di domande e offerta di beni e servizi, a capo di tutto ciò c'è sicuramente un fattore: la velocità.

I mercati sono sempre più orientati ad avere una spiccata efficienza ed interconnessione tra tutto il globo, un mercato che necessita di un sistema snello e funzionante, che stabilisca sicurezza in coloro che vogliono utilizzarlo.

Tra i cosiddetti “driver del cambiamento” che abbiamo citato prima, vorrei focalizzarmi su alcuni che in particolare mi sembrano rispondere alle molte richieste di un mercato moderno: il sistema Blockchain e il Bitcoin.

Anche se già introdotto all'inizio del lavoro ricordiamo che il sistema Blockchain è un protocollo di sicurezza decentralizzato, una sorta di database pubblico, reso sicuro da codici crittografici. La tecnologia tende a creare un contesto di fiducia reciproca facendo sì che avvengano scambi tra individui che non si conoscono e che possano collaborare senza un intermediario. Al momento il miglior protocollo di sicurezza è il Bitcoin e gli scambi che avvengono tra utenti che utilizzano questa cripto-valuta vengono registrati nel sistema Blockchain, che come analizzerò più avanti ci si sta rendendo conto che questa struttura possa avere moltissime ulteriori capacità, gli esperti affermano che nel 2025 il 10%³⁰ del PIL globale risiederà all'interno di una Blockchain, o ancora che i governi a breve inizieranno a riscuotere le imposte tramite Blockchain e via dicendo. Tutti queste ulteriori applicazioni che escono dal campo monetario le tratterò più approfonditamente in seguito.

Le idee che sono osservabili dietro tutte queste nuove applicazioni nascono da una profonda sfiducia nei sistemi attuali. E' chiaro, infatti, che, in seguito alla crisi finanziaria dello scorso decennio, si sia sviluppata una generalizzata sfiducia nei confronti del sistema canonico finanziario. Questa sfiducia si estende dalle grandi organizzazioni, come le banche centrali, passando per la rappresentanza politica, fino ad arrivare a sfere della vita civile, ed è per questo che la domanda del mercato sta volgendo su altri aspetti che prima non venivano molto considerati. Ad esempio ora è richiesta una

³⁰ M. Amato, L. Fantacci, Per un pugno di Bitcoin, università Bocconi, 2016.

maggior trasparenza, un maggior coinvolgimento all'interno dell'azienda, anche una maggior libertà di utilizzo. Tutti questi aspetti stanno obbligando le imprese a rimodellare i propri business, ed in risposta a queste inclinazioni del mercato si stanno diffondendo innovazioni come quella del bitcoin.

Infatti, il tentativo del Bitcoin è quello di rispondere all'esigenza di un'economia che prescindendo dalla fiducia verso l'intermediario e riponga questa fiducia negli individui. Ma, per raggiungere una completa libertà individuale dal sistema, si necessita di un protocollo immutabile. Per questo motivo parliamo di un progetto sviluppato a livello globale. Ma come i bitcoin, negli anni '80, anche la globalizzazione fu definita come un mix di pratiche ed ideologie da soddisfare: "E' lontano il tempo delle differenze territoriali o nazionali [...] Le differenze dovute alla cultura, alle norme, alle strutture, sono vestigia del passato [...] La convergenza, tendenza di tutto e tutti a diventare come tutti, orienta il mercato come una comunità globale." (Levitt)³¹. Il bitcoin, come anche l'oro d'altro canto, è uno strumento concepito per non conoscere confini, una moneta che ha intenzione di essere caposaldo di un'economia caratterizzata dall'assenza di confini e "dalla messa in scacco dei poteri statali di controllo". In altri termini, il Bitcoin ricopre il sogno di una moneta commutativa, ossia libera da ogni istanza di giustizia distributiva. Carbone afferma: "In quanto moneta strettamente privatistica denuda le posizioni inconsistenti di tutti i sostenitori del libero mercato (monetaristi in primis) che incoerentemente difendono il monopolio statale sulla produzione monetaria"³². Dunque, il bitcoin è una moneta privata e globale, "pensata per un mondo in cui ogni forma di delimitazione appare come un baluardo artificiale destinato a essere spazzato via dalla potenza delle relazioni paritarie che non abbisognano di nessuna mediazione di un'istanza terza per potersi realizzare" (M. Amato, L. Fantacci).

E, se questo fosse un aspetto monetario di un possibile scenario futuro, il bitcoin potrebbe essere definito come uno strumento anch'esso rivoluzionario; persino un'arma o una leva monetaria di questa rivoluzione.

E' certo, quindi, che il Bitcoin si voglia imporre come obiettivo ultimo quello di diventare una moneta globale e rivoluzionaria, economicamente parlando.

Al momento è lontano dal poter sostituire le valute standard attuali, di sicuro con il progredire delle tecnologie e della rivoluzione industriale, queste carenze si assottiglieranno. Associandoci alla visione dei tecno-pessimisti citati sopra, è ravvisabile facilmente come questo schema economico sia attualmente limitato all'ambito del semplice scambio. Per spiegarci meglio riporterò l'esempio di

³¹ Levitt T., *The marketing imagination*, The Free Press, New York, 1983.

³² Carbone F., *Rivoluzione Bitcoin*, 2013.

una semplice situazione economica nella quale, in seguito al ricevimento di un corrispettivo in Bitcoin, un commerciante potrebbe preoccuparsi del fatto che nessun intermediario o ente si farà carico di controllare la significatività di quell'importo. E con significatività intendo in primis stabilità del valore reale, o per essere più tecnici, potere d'acquisto. Si ritorna quindi al punto debole di cui si diceva nel precedente capitolo 1.2.

CAPITOLO II

2 La struttura tecnologica del Bitcoin

2.1 L'innovazione della tecnologia Blockchain

“La Blockchain è un’incorruttibile libro contabile digitale che segna le transazioni economiche, programmata per registrare non solo le transazioni finanziarie ma virtualmente ogni valore esistente”³³.

Molto prima dell’avvento della tecnologia Blockchain, la moneta digitale era stata già pensata in modo che, attraverso l’utilizzo di un server centrale e automatizzato, si potesse ovviare al problema del *double-spending*³⁴, ossia di transazioni fraudolente.

David Chaum³⁵, considerato uno dei pionieri delle valute digitali e ispiratore del movimento dei Cypherpunk³⁶, nel suo scritto³⁷ del 1983 teorizzò quelle che poi sarebbero divenute le firme digitali. Egli sosteneva che, attraverso le firme crittate (che sono codici) e l’utilizzo di pseudonimi, si sarebbe potuto fare a meno di una terza parte che si incaricasse di accertare la bontà delle transazioni online: “il metodo innovativo prevede infatti che gli individui utilizzino differenti numeri di account, oppure “pseudonimi digitali” differenti per ogni singola transazione. Gli utenti creeranno gli pseudonimi utilizzando un sistema elettronico”. In questo modo gli utenti, sia singoli individui che organizzazioni, possono contare sul fatto di non poter essere rintracciabili, e di poter cambiare ogni volta pseudonimi. Sebbene i nuovi indirizzi rimangano rintracciabili dall’utente stesso e quindi permettano di bloccare usi impropri.

La teoria di Chaum sembrò allora utopica ed irrealizzabile. Abbiamo dovuto attendere circa trent’anni per avere una condizione sia sociale sia tecnologia che consentisse di attuarla. La tecnologia Blockchain, e la natura decentralizzata del sistema di pagamento Bitcoin, rappresentano al meglio il pensiero di Chaum.

³³ Tapscott D., Tapscott A., *The Bitcoin Revolution*, Portfolio Penguin, 2016.

³⁴ L’attività di double-spending consiste nell’intento di un utente di voler agire in modo fraudolento, cercando di eseguire due pagamenti contemporaneamente, il sistema serve a convalidarne solo uno.

³⁵ David Lee Chaum: nato nel 1955, è un ingegnere informatico e crittografo. Divenuto noto per aver sviluppato l’e-cash, un tipo di moneta digitale in grado di mantenere l’anonimità degli utenti.

³⁶ Cypherpunk: è un movimento di attivisti, che sostengono fortemente l’utilizzo della crittografia informatica, in modo da attuare un cambiamento sociale e politico.

³⁷ D. Chaum: *Blind signatures, for untraceable payments*, department of Computer Science, University of California, 1983.

Entrando ora più nello specifico di cosa sia la tecnologia Blockchain, mi sembra giusto introdurla con la definizione di Vitalik Buterin³⁸: “è un magico computer in cui ognuno può caricare programmi e lasciare che questi programmi si eseguano automaticamente, dove tutti gli attuali e tutti i precedenti stati del programma possono essere visualizzati da tutti, e che garantisce una continua e solida sicurezza che i programmi continueranno ad essere eseguiti proprio come il protocollo della tecnologia stabilisce”³⁹.

La struttura Blockchain è applicabile a qualsiasi transazione digitale online. Il commercio su internet è pieno di autorità terze e istituzioni finanziarie che processano e mediano ogni singola transazione, non essendoci fino ad ora in vigore un sistema che provveda a garantire transazioni al 100% sicure. Il ruolo delle terze parti sta nel validare e salvaguardare le transazioni, a causa di un’importante percentuale di transazioni fraudolente. La mediazione di terze parti rende però le transazioni piuttosto onerose.

La cripto-valuta Bitcoin utilizza il sistema Blockchain per poter validare le transazioni senza l’utilizzo di intermediari. Il funzionamento è piuttosto semplice: ogni transazione è protetta da una firma digitale che è spedita alla chiave pubblica del ricevente, che è segnata digitalmente con una chiave privata dal mittente. Per poter spendere i propri Bitcoin, il detentore di moneta virtuale dovrà provare la sua effettiva proprietà.

Per quanto riguarda invece la trascrizione delle transazioni all’interno di questo registro pubblico, chiamato Blockchain, il processo è un po’ più complesso. Ogni transazione compone un nodo, una volta riempito viene inserito nel registro pubblico della Blockchain, dopo le dovute verifiche. Ogni transazione deve essere verificata prima che questa possa essere trascritta nell’archivio digitale. La verifica del nodo necessita di due fattori per essere validato: 1) L’acquirente possieda effettivamente cripto-valute. 2) L’acquirente possieda effettivamente la quantità di cripto-valuta che intende spendere. Ad ogni modo le transazioni non vengono inserite nell’ordine in cui vengono generate, infatti nella tecnologia Blockchain non esisteva un criterio affermato per decidere l’ordine; la soluzione è stata fornita dagli ideatori del Bitcoin, il sistema della cripto-valuta inserisce all’interno dello stesso blocco, tutte le transazioni che si presume siano avvenute nell’arco di 10 minuti, conclusosi questo lasso di tempo, il blocco viene chiuso ed inserito all’interno della blockchain, ed ordinati cronologicamente. Rimane comunque la criticità che alcuni blocchi potrebbero essere completati nello stesso arco di tempo, quindi il sistema dovrebbe trovare un modo per ovviare a questa ipotesi. Il quesito è stato risolto, introducendo un puzzle matematico. Ogni nodo viene accettato

³⁸ Vitalik Buterin: 1994, è uno sviluppatore russo, fondatore della piattaforma web Ethereum.

³⁹ Buterin, V., *Visions, Part 1: The Value of Blockchain Technology*. Ethereum Blog, <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>, 2015.

solamente dopo aver risolto il puzzle, questo processo è conosciuto come “proof of work”, cioè nel concreto ogni nodo deve saper dimostrare di aver impiegato abbastanza potenza di calcolo nell’aver risolto il puzzle. Questo non è affatto banale e la sua difficoltà può essere aggiustata, quindi nell’arco di dieci minuti è altamente improbabile che più di un nodo riesca a rispondere al quesito. Il primo nodo che risolve il puzzle, trascrive il blocco nella struttura Blockchain. I nodi che donano la propria potenza di calcolo per generare i blocchi sono chiamati “nodi da miner” e sono finanziariamente retribuiti con dei bitcoin. Ci sono due modi per remunerare i miner:

1. concede al miner una determinata quantità di bitcoin generati (inizialmente venivano remunerati con 25 Bitcoin per ogni blocco generato, ora con 12,5);
2. la tassa di transazione pagata in quel blocco viene remunerata al miner. La tassa di transazione viene calcolata da un computer in base a valore e quantità delle transazioni eseguite.

Il sistema accetterà solamente la catena di nodi più lunga e la più completa. E’ praticamente impossibile per un hacker inserire nella catena transazioni fraudolente, dal momento che non è l’unico che genererà un blocco e concederà la propria potenza di calcolo, inoltre, si troverà anche a competere matematicamente con dei nodi valevoli. Aggiungiamo il fatto che il tutto è reso ancora più difficile dal fatto che i blocchi sono crittati digitalmente.

Uno degli aspetti che rende però così sicuro questo genere di processo è il fatto che queste firme, o indirizzi, siano crittati dal sistema, e per poter essere utilizzate dal ricevente, quest’ultimo deve essere in grado di decrittare correttamente l’indirizzo inviato dal mittente. In realtà, come è facile intuire, la scienza della crittografia possiede radici molto antiche, ha, infatti, trovato sempre ampie applicazioni, soprattutto nel mondo contemporaneo, durante i conflitti mondiali. E’ uno strumento così usato perché si presta perfettamente alla protezione dei dati sensibili, sia nei registri che nelle comunicazioni. Inizialmente fu progettata per i sistemi di sicurezza informatici (Saper, 2013, p. 673).

L’opinione di molti esperti è quella di ritenere che la tecnologia Blockchain abbia la capacità di fermare molte aziende in giro per il globo, in un modo molto simile a come internet cambiò radicalmente le nostre vite qualche decade fa. Stiamo assistendo, infatti, al fatto che sempre più società nel mondo stanno iniziando ad adottare la Blockchain nel proprio flusso di lavoro e come nuovi registri digitalizzati. Questa tecnologia impatta, infatti, su ogni settore, dalla catena di produzione ai servizi finanziari, fino alle telecomunicazioni e alla sanità. Le istituzioni stanno provando sempre di più di capire come poter implementare e inserire questa tecnologia nei loro sistemi in futuro.

Secondo Nakamoto il commercio elettronico basa tutta la propria funzionalità sul fatto che esistano degli enti terzi che regolarizzano il tutto. Transazioni completamente irrevocabili non possono essere

eseguite, e le transazioni molto onerose costringono il mercato a non poter accettare importi molto piccoli, che caratterizzano, i solito, gli acquisti quotidiani. In più a causa delle molte frodi che avvengono nei commerci digitali la sfiducia nei confronti dei commercianti rende il tutto molto macchinoso. Si necessita quindi di un sistema di pagamento elettronico che non si fondi sulla fiducia ma su un protocollo imm modificabile, in modo tale da rendere molto difficoltosa la possibilità di truffa via internet. Quindi transazioni molto esose da annullare renderebbero molto più protetti i commercianti, mentre meccanismi automatici di deposito di garanzia renderebbero i compratori più sicuri.

La struttura Blockchain è evidentemente una tecnologia molto promettente, come vedremo nei prossimi paragrafi, vi è un ampio range di campi applicativi, o problemi che sarà in grado di risolvere, partendo dalle applicazioni finanziarie e quelle non finanziarie. Molte di queste applicazioni sono radicali innovazioni. Ma come ogni radicale innovazione può comportare dei rischi. Elenco alcuni dei più diffusi.

- *Cambio di comportamento*

“Il cambiamento è costante, ma c’è una resistenza a cambiare”⁴⁰. Nel momento in cui il Bitcoin ha promesso che tutte le transazioni dei propri utenti sarebbero state sicure, i suoi utenti devono abituarsi all’idea che le loro transazioni elettroniche siano sicure, il che implica del tempo ed un cambio di abitudini. In un’ottica futura, non solo gli utenti dovranno accogliere il cambiamento, ma anche intermediari come Visa o Mastercard dovranno sapersi adattare e dovranno pensare di sviluppare i propri sistemi sulla tecnologia Blockchain se intendono rimanere competitivi.

- *Ridimensionamento*

Adattarsi al sistema Blockchain attualmente rappresenta un grosso impegno. Infatti prima di poter effettuare le transazioni l’utente dovrà scaricarsi l’intera catena Blockchain, convalidarla e solo allora potrà eseguire la sua prima transazione. Tutto ciò potrebbe impiegare delle ore, considerando anche il fatto che il numero di blocchi aumenta esponenzialmente. In più si deve necessitare di strumenti informatici con una certa potenza computazionale.

- *Bootstrap*

L’idea di passare ad una tecnologia Blockchain, significa per le aziende trasferire e digitalizzare numerosissimi volumi di registri e documenti. Il che potrebbe significare un elevato volume di lavoro

⁴⁰ Crosby M., Nachiappan, Pattanayak P., Verma S., Kalyanaraman V., *BlockChain Technology: Beyond Bitcoin*, Applied Innovation Review, Issue No. 2 June 2016.

per questa migrazione da parte delle aziende, che a sua volta potrebbe trasformarsi in un grosso rallentamento.

- *Regolamentazioni governative*

Nella nuova ottica delle transazioni digitali basate su BlockChain le agenzie governative potrebbero rallentare l'adozione introducendo nuove leggi per monitorare e regolamentare il settore per la conformità. Nelle economie più controllate come la Cina, l'adozione potrebbe trovarsi ad affrontare notevoli ostacoli.

- *Attività fraudolente*

Data la possibilità di adottare pseudonimi nelle transazioni, e facilitare lo spostamento di oggetti di valore, agenti appartenenti alla malavita potrebbero, con facilità, abusare della tecnologia per attività fraudolente come il traffico di denaro. Detto questo, con un numero sufficiente di regolamenti e supporto tecnologico, le istituzioni saranno in grado di monitorare e perseguire questi individui.

- *Quantum Computing*

La tecnologia BlockChain si basa sul fatto che è quasi impossibile per un singolo individuo poter mettere in crisi il sistema o riuscire a superare il fattore crittografico, a causa della mancanza della potenza di calcolo necessaria. Ma con l'avvento futuro dei computer quantistici, le chiavi crittografiche potrebbero essere abbastanza facili da decifrare in un tempo ragionevole. Ciò porterebbe l'intero sistema al crollo. La soluzione che si prefigura è che le chiavi diventino ancora più complesse, così da mettere il sistema in sicurezza da qualsiasi attacco.

In conclusione la Blockchain ha alto potenziale e altrettanti rischi. Un esempio del potenziale immediato viene dimostrato dall'accordo che la Maersk e IBM hanno stipulato per testare un sistema Blockchain sul traffico di container nel traffico intermodale. La partita è grossa, dato che se la newco riuscisse a conseguire l'obiettivo che si è posta di azzerare o minimizzare i costi amministrativi, cambierebbe i parametri di competitività del trasporto merci marittimo.

I rischi però sono altrettanto elevati, sia in termini di ulteriore finanziarizzazione dell'economia, sia in termini di sorveglianza generale del sistema. Il trend evolutivo della tecnologia è un percorso che non si inverte e i cui benefici vanno colti, ma non si può sottovalutare il rischio di ulteriore crescita del "digital divide", che già connota e classifica paesi e società, e persino singole industrie in base alla loro localizzazione. Il differenziale di accesso potrebbe ulteriormente acuirsi con l'adozione di tecniche che richiedono potenza di computazione, oltre che dominio delle tecniche. E purtroppo chi possederà questi strumenti avrà maggior controllo, inficiando in parte il punto di partenza degli

ideatori di questa cripto-economia: liberare da intermediari e da controlli, siano essi di grandi organizzazioni, di governi o di individui.

2.2 Le applicazioni legate alle cripto-valute

La tecnologia Blockchain sta riscontrando un fortissimo successo e sta trovando moltissime applicazioni, sia in campo finanziario sia altre aree non finanziarie. Tutte aree che, in passato, sono state presiedute da enti terzi che salvaguardavano la correttezza delle transazioni e degli asset digitali. Con l'avvento e l'implementazione di questa tecnologia, sempre più istituzioni stanno diventando obsolete ed inefficienti.

A testimonianza di questo riporterò ora alcuni dei più importanti esempi di applicazioni della tecnologia Blockchain e del Bitcoin.

- *Sidechain Technology*

La tecnologia Sidechain è un registro gestito manualmente, con il proprio codice di software. Questo software risulta “ancorato” alla catena principale e permette di trasferire le informazioni chiave da una catena all'altra. La Sidechain è un'idea che va di pari passo con l'idea di Smart contract (Maxwell, 2015), di cui parlerò in seguito. Questa tecnologia aiuta ad usare differenti valute, senza la necessità di dover creare per forza nuove cripto-valute, cosa che indebolirebbe l'effetto del sistema.

- *Ethereum*

Ethereum è un'innovativa macchina virtuale⁴¹, basata sulla tecnologia Blockchain, e sulla piattaforma Cloud 2.0⁴². Gli sviluppatori stanno lavorando su un sistema che faciliti lo scambio e la compilazione di contratti molto complessi. Con una maggiore interazione tra gli utenti sarà possibile una conclusione di contratti digitali sempre più complessi. Ethereum conta di poter sviluppare un'estensione della cripto-economia, andando oltre il semplice scambio di cripto-valute, arrivando a stabilire una vasta gamma di contratti digitali da coprire ogni area della quotidianità, con una solida base tecnologica e legale.

- *Gridcoin*

è una cripto-valuta peer-to-peer che fornisce benefici reali, differenziandosi dalle altre cripto-valute in quanto si definisce eco-sostenibile. Gridcoin permette scambi di valuta per tutto il mondo con costi di transazione irrisori. Al contrario del Bitcoin, questa cripto-valuta per rendere sicuro il proprio

⁴¹ Macchina virtuale: software informatico che agisce virtualmente come agirebbe una macchina fisica.

⁴² Cloud: piattaforma di archivio online.

sistema utilizza il sistema *proof-of-stake*⁴³ e ricompensa i miner che abbiano fornito potenza computazionale di ricerca per il BOINC⁴⁴. In questo modo i miner portano vantaggi alla medicina, biologia, meteorologia ecc, reindirizzando la loro potenza computazionale in ricerche. Infatti la classica applicazione della tecnologia Bitcoin produce un grande e non necessario spreco di energia e calore per risolvere i complicati algoritmi imposti dal sistema. Halford⁴⁵ nel suo paper, afferma: “Gridcoin è la prima cripto-moneta che riesce a convertire il grande spreco di energie in utili ricerche scientifiche, operando come un sistema decentralizzato peer-to-peer, fornendo una grande efficienza per gli utenti”.

- Ripple Labs

con la propria tecnologia Ripple, è diventata dal 2012 uno dei più grandi *player* dei pagamenti rivoluzionari: “con l’ambizione di costruire un protocollo globale”.

Cawrey, nel suo scritto⁴⁶ afferma: “stupisce abbastanza, che in un mondo guidato dalla globalizzazione tecnologia, sia ancora così complesso spostare denaro per il globo”. Ripple, sviluppando un struttura peer-to-peer permette un movimento facilitato del denaro attraverso le istituzioni finanziarie. Questo permette alle istituzioni finanziarie di fare pagamenti direttamente tra le agenzie, senza ricorrere all’utilizzo di intermediari. Il protocollo Ripple di transazione (RTXP), assicura pagamenti istantanei e quasi totalmente gratuiti, inoltre offre anche scambio di valute, senza differenza per il volume di scambio. Ripple consente inoltre la possibilità di trasferire token, valute fiat, cripto-valuta, commodity o qualsiasi altra unità di valore.

Ripple è considerata “una miscela intelligente di architettura autorizzata e priva di permesso” (Kelleher, 2015). L’algoritmo di Ripple crea un mercato decentralizzato all’interno del suo protocollo; “in un certo senso, è più vicino ad una *ledger chain* che a una *Blockchain*” (ibid.).

- *L’identità digitale basata sulla struttura Blockchain*

La questione dell’identità digitale online apre una discussione molto accesa su due punti fondamentali: il controllo degli accessi e le informazioni di identificazione personale (Daily Fintech, 2015). L’inclusione delle informazioni relative all’identità digitale all’interno di una catena Blockchain è di massima rilevanza politica, legale, sociale. Un pioniere del settore è il governo dell’India, come afferma la testata giornalistica The Times of India: “(l’India) attualmente gestisce il

⁴³ Proof-of-stake: tipo di algoritmo informatico che prova l’effettivo lavoro da parte dei nodi dei sistemi delle cripto-valute.

⁴⁴ BOINC: Berkeley Open Infrastructure for Network Computing.

⁴⁵ Rob Halford: pseudonimo del creatore del Gridcoin.

⁴⁶ Cawrey, D., Ripple Labs' Grand Plan to Build a Global Payment Protocol. CoinDesk, <http://www.coindesk.com/ripple-labs-grand-plan-build-global-payment-protocol/>, 2014.

più grande sistema nazionale di identità digitale del mondo, l'Unique Identification Authority of India (UIDAI), assegnando a ciascun residente un numero unico di 12 cifre chiamato Aadhaar⁴⁷.

La tecnologia Blockchain attribuisce, quindi, all'identità digitale un carattere di decentralizzazione innovativo e potenzialmente rivoluzionario nell'era digitale.

- *Sistema di voto basato sulla struttura Blockchain*

Nel 2015, la Bitcoin Foundation ha presentato un nuovo progetto, proponendo un sistema di voto basato sul sistema Blockchain, che "offre una trasparenza ancora maggiore nel processo di votazione, con ogni voto registrato sulla blockchain". Basandosi sull'immutabilità, la trasparenza e il consenso inerenti alla tecnologia blockchain, ogni voto viene registrato sotto un hash sicuro e crittografico. Questo tipo di sistema di voto è stato inizialmente implementato da un partito politico danese per scopi di elezioni interne (Millet, 2014).

- *Il sistema Blockchain per il sistema finanziario e bancario*

Esistono importanti applicazioni anche nel settore bancario e finanziario. Sebbene gli scandali che hanno caratterizzato il mondo Bitcoin inizialmente, mi riferisco al furto subito da Mt Gox nel 2014, la tendenza è quella di accettare completamente la tecnologia blockchain come principale driver dei servizi finanziari nel ventunesimo secolo (Shubber, 2015). Le banche rischiano di essere rimodellate, in seguito a un periodo di turbolenza, per rispondere meglio ai bisogni delle persone e delle istituzioni, fornendo loro servizi migliori. Il 24 marzo 2015, Nasdaq, il principale fornitore di servizi di trading, scambio e quotazione ha firmato un accordo con la startup new yorkese Noble Markets. Quest'ultima fornirà al Nasdaq una tecnologia di trading per costruire un nuovo mercato per le criptovalute (Casey, 2015). L'11 maggio 2015, Nasdaq ha annunciato i suoi piani per sfruttare la tecnologia Blockchain. Nasdaq applicherà la tecnologia blockchain, al fine di espandere le capacità di gestione azionaria. Implementando la sua piattaforma per il mercato privato, con una conseguente maggior integrità, capacità di audit, governance e di trasferimento delle capacità di proprietà (Nasdaq.com, 2015). Per Bob Greifeld, il CEO di Nasdaq (ibid.), La tecnologia blockchain non è rilevante solo per la gestione dei titoli fisici, ma sempre più per i beni immateriali, e dovrebbe ampiamente beneficiare i mercati dei capitali globali.

- *Inclusione sociale nel mondo in via di sviluppo*

Una delle applicazioni maggiormente stimolanti riguarda l'inclusione sociale nel mondo in via di sviluppo. "Dal 2011 al 2014, 700 milioni di persone sono diventate titolari di conti presso banche, o

⁴⁷ The Times of India, Aadhaar world's largest biometric ID system, <http://timesofindia.indiatimes.com/india/Aadhaar-worlds-largest-biometric-ID-system/articleshow/47063516.cms>, 2015.

altre istituzioni finanziarie e fornitori di servizi monetari mobili. Il numero di individui che non posseggono un conto, invece, è diminuito del 20%" (World Bank, 2015). Pertanto, la Banca Mondiale ha fissato un obiettivo ambizioso: l'accesso finanziario universale entro il 2020 (Banca Mondiale, 2015).

Il più grande potenziale del progresso sociale nei paesi in via di sviluppo è l'inclusione, attraverso dispositivi mobili, che consentirà a milioni di persone svantaggiate di effettuare e ricevere micropagamenti. Per il CIO della Commonwealth Bank of Australia, "in questa economia e attraverso l'Africa, con una popolazione di circa 1,2 miliardi nel continente, l'inclusione mobile è superiore al 100%. Ci sono più dispositivi mobili che persone nella popolazione "(Wheteing citato in Ngo, 2015).

IHB, (I Have Bitcoins) è una società privata di servizi di media e dati, che fa affidamento sulla tecnologia Blockchain, considerata da loro una forza dirompente. IHB aiuta gli artigiani nelle zone rurali dell'India a beneficiare del potenziale di potere d'acquisto nel mondo sviluppato, vendendo i loro dipinti sulla loro piattaforma, senza commissioni. L'industria artigianale indiana è per lo più decentralizzata e diffusa in tutto il paese, principalmente nelle aree rurali e urbane. Impiegando un numero piuttosto rilevante di artigiani, tra cui un gran numero di donne e coloro che appartengono alla parte più povera della società, l'industria dell'artigianato potrebbe beneficiare enormemente del Bitcoin (Nirgunarthy, 2015).

Inoltre considerando anche il caso di altri paesi, come la Moldavia, in cui almeno un componente della famiglia emigra per cercare condizioni lavorative più vantaggiose, utilizza società come Western Union per inviare denaro a casa. I dati della Banca Mondiale hanno mostrato che nel 2013 oltre 700.000 moldavi lavoravano all'estero in modo permanente o temporaneo. Circa l'89% delle rimesse è stato effettuato tramite i sistemi di trasferimento internazionali e l'11% tramite bonifico bancario. Con costanti rimesse elevate, si prevede che emergano nuove modalità di trasferimento dai costi economicamente convenienti: "uno su sette manda soldi a casa [nella CEE] utilizzando i telefoni cellulari "(ibid.).

2.3 Anonimato, Smart Contract e Digital Wallet

Sin dall'inizio di questo lavoro abbiamo parlato delle caratteristiche che maggiormente distinguono questa innovazione, rispetto ai sistemi finanziari e monetari attuali. Le due caratteristiche maggiormente innovative sono state: decentralizzazione e anonimato. Mi sembra quindi giusto ora analizzare il fattore dell'anonimato, approfondendo subito dopo altri due fattori piuttosto determinanti: gli *smart contract* e il *digital wallet*.

- *Anonimato*

Usare la parola anonimato è tecnicamente errato, poiché gli utenti del sistema Bitcoin semplicemente non utilizzano i propri nomi, ma per ogni singola transazione utilizzano degli pseudonimi in modo tale da non poter essere ricondotti alle proprie identità. Trattandosi, la Blockchain, di un registro pubblico, e consultabile da tutti facilmente, utilizzare i propri nomi potrebbe risultare violata la privacy di molti utenti. Ogni utente del sistema è, quindi, identificato da una chiave pubblica e da una privata. Per utilizzare una metafora nel mondo reale “la chiave pubblica rappresenterebbe l’indirizzo di casa, mentre la chiave privata la combinazione per aprire la porta” (M. Amato, L. Fantacci, 2016).

La chiave pubblica sarà a conoscenza degli altri utenti, mentre la chiave privata verrà fornita solo nel momento in cui si inviino Bitcoin ad un altro soggetto, in modo tale che questo possa decriptare correttamente il file. Il sistema comunque per aumentare la sicurezza dei propri utenti, permette di generare una quantità molto elevata di copie di chiavi, sia pubbliche che private, e dà loro la possibilità di creare ogni volta associazioni di chiavi sempre diverse.

Vi è comunque un caso in cui l’anonimato garantito dal sistema Bitcoin possa essere interrotto, infatti nel momento in cui si utilizzino piattaforme di tipo Exchange, o comunque soggette a normative “ a seguito della quarta Direttiva dell’UE (n.2015/849) in tema AML, infatti, chi fornisce il servizio di compravendita di criptovalute deve richiedere ai clienti dei documenti identificativi.”⁴⁸ .

Esiste tuttavia una via alternativa per cercare di mascherare maggiormente la propria identità, esistono infatti siti e piattaforme, chiamati Mixer, che tentano di rendere ancora più difficoltoso risalire all’identità. Queste piattaforme raggruppano quante più transazioni possibili in un unico blocco, mescolando i dati che riportano gli indirizzi degli utenti Bitcoin.

Ad ogni modo con il diffondersi dell’uso di questa tecnologia, anche i metodi per risalire agli artefici crescono. E’ infatti grazie a questi metodi che è stato possibile rintracciare alcuni degli hacker che colpirono la nota piattaforma Mt Gox, responsabili di aver rubato notevoli volumi di Bitcoin.

- *Smart contract*

Gli smart contract sono contratti digitalizzati, risiedenti all’interno della catena Blockchain, che si eseguono autonomamente, non richiedono dunque alcun intervento umano e “fanno leva sul carattere irreversibile e incorruttibile delle scritture sulla Blockchain” (M. Amato, L. Fantacci, 2016). Furono teorizzati per la prima volta da Nick Zsabo⁴⁹ nel 1994. Egli li definiva come: “un protocollo di

⁴⁸ Visita: <https://www.webnews.it/2018/01/17/bitcoin-anonimato/>

⁴⁹ Nick Zsabo: è un ingegnere informatico e crittografo digitale, nel 1998 creò i Bit gold, considerati i precursori dei Bitcoin.

transazioni computerizzate che eseguono i termini di un contratto”⁵⁰. Zsabo codificò le classiche clausole di un contratto (proprietà, trasferimenti ecc). Il risultato doveva essere la realizzazione di contratti in grado di operare in modo autonomo, liberando gli utenti dal dover ricorrere a terze parti per evitare situazioni dannose o illegali. Con l’avvento della struttura Blockchain, gli smart contract sono risultati essere inseribili come script all’interno della catena.

La funzione degli smart contract comunque non si limita al solo uso commerciale, gli esperti ipotizzano innovative applicazioni anche in campo finanziario. Infatti ipotizzando una situazione in cui un utente abbia richiesto l’acquisto di un bene, usufruendo di un credito, nel contratto potrebbe essere inserita la clausola che in caso di mancato adempimento delle rate l’acquirente avrebbe perso la proprietà del bene. Nel caso si verificasse questa ipotesi, il sistema Blockchain, invece di ricorrere ad un tribunale ed ad un lungo iter burocratico, potrebbe negare l’utilizzo, cambiando la chiave d’accesso, del bene da parte dell’utente inadempiente.

Uno smart contract è di tipo deterministico; cioè lo stesso input produrrà sempre lo stesso output. Ed in una struttura Blockchain sviluppata secondo precise caratteristiche non può sussistere uno smart contract non deterministico, poiché il sistema non sarebbe in grado di compiere correttamente i processi di attivazione e completamento e conseguentemente li rigetterebbe.

Poiché tutte le interazioni di uno smart contract avvengono tramite messaggi firmati sulla Blockchain, tutti gli utenti della rete ottengono una traccia crittograficamente verificabile delle operazioni del contratto. Questa nuova generazione di contratti operano come dei veri e propri attori autonomi, attuando un comportamento completamente prevedibile. Come tali sono degni di fiducia, dato che rispettano perfettamente le regole imposte dalla Blockchain.

Una blockchain che supporta transazioni in stile Bitcoin consente trasferimenti di risorse tra controparti senza che queste si debbano conoscere e quindi fidarsi dell'uno o dell'altro. Una Blockchain che supporta gli smart contract tuttavia, consente processi multi-step (o più in generale: interazioni) tra controparti reciprocamente diffidenti. Gli utenti che effettuano transazioni attraversano vari step decisionali:

- a) Prima di decidere se impegnarsi in un contratto, verificano che gli indirizzi degli utenti e le chiavi fornite siano corretti e veritieri.
- b) Posseggono una maggiore fiducia nel sistema, essendo questo al di fuori del pieno controllo e/o manipolazione degli utenti.

⁵⁰ N. Szabo, Smart Contracts. [Online] <http://szabo.best.vwh.net/smart.contracts.html>, 2014.

- c) Gli utenti hanno varie prove durante il processo di completamento poiché tutte le interazioni sono firmate digitalmente. La possibilità di una controversia è eliminata.

Digital Wallet

- Un digital wallet, o un portafoglio digitale, è un software dove sono contenuti i Bitcoin.

Questi ultimi, per l'esattezza, non possono essere mantenuti ovunque; questi posseggono una chiave privata, per ogni Bitcoin che è salvato nel portafoglio digitale. I digital wallet rendono il meccanismo dell'inviare e il ricevere Bitcoin più facilmente. Parlando di portafoglio Bitcoin, ci si riferisce inoltre ai digital wallet. Possedere un portafoglio digitale è condizione necessaria affinché si possano possedere dei Bitcoin. Poiché come si identifica il Bitcoin come moneta digitale, il digital wallet si identifica esattamente al portafoglio fisico. Ad ogni modo, il portafoglio non registra il codice dei singoli Bitcoin, ma registra gli indirizzi associati a questi, può inoltre registrare chiavi private e pubbliche. Esistono in varie modalità:

Desktop

- I portafogli installati in modalità desktop si trovano sul desktop del proprio pc, e permettono all'utente di accedere a tutte le opzioni a sua disposizione per gestire correttamente il proprio wallet. Inoltre questa modalità permette all'utente di creare un indirizzo Bitcoin dove poter mandare o ricevere Bitcoin e di salvare chiavi private.

Mobile

- La versione per smartphone del digital wallet ha il grande vantaggio di essere sempre a portata di mano. Le applicazioni con cui si può gestire il proprio wallet sono moltissime e presentano le stesse funzionalità della versione per desktop. In più però la versione mobile permette di effettuare acquisti nei negozi fisici, utilizzando la tecnologia contactless o "touch-to-pay".

Web

- Come per i più classici wallet accessibili via web, anche quelli per bitcoin non si discostano dalle classiche caratteristiche che questi altri presentano. Sono accessibili da ogni browser, bisogna però prestare molta attenzione, perché si stanno inserendo le proprie chiavi private online, su browser che potrebbero non essere sicuri. Coinbase e Blockchain sono i maggiori fornitori di digital wallet.

Hardware

- Per quanto riguarda l'ultima versione in cui un utente può mantenere il proprio digital wallet, questi sono sicuramente i più sicuri, poiché i codici si trovano conservati all'interno di un

hardware fisico, come ad esempio una chiavetta usb. Il fattore positivo è che queste sono immuni da virus e pochissimi problemi sono stati riportati in passato. Il lato negativo è che questi hardware hanno un costo che può variare dai 100\$ ai 200\$⁵¹.

Infine vanno anche qui considerati rischi e potenzialità. Da una parte i digital wallet e le transazioni peer-to-peer potranno portare ad una grande esplosione della sharing economy (le cui transazioni sono oggi interamente sottoposte ad uno se non due passaggi di intermediazione, ad esempio gli affitti turistici di appartamenti o il car sharing).

Dall'altra sarà crescentemente difficile e costoso proteggere questa massa di transazioni da frodi, hackeraggi e interessi non leciti.

Infine le bolle speculative derivanti dalle transazioni su cripto-valute possono porre a rischio l'andamento di molti degli aspetti della nuova cripto-economia.

⁵¹ Fonte: <https://www.investopedia.com/terms/b/bitcoin-wallet.asp>

CAPITOLO III

3 Bitcoin: una nuova forma di speculazione o un'esigenza reale dell'economia?

3.1 Sviluppi futuri del Bitcoin

Il successo riscontrato dalla creazione lungimirante di Satoshi, non ha dato solamente luce ad un profondo cambiamento economico e giuridico, ma ha aperto la strada anche a tutti gli altri cripto-entusiasti che hanno visto la possibilità di poter realizzare un prodotto simile, o, secondo alcune opinioni, migliore.

Ideologie anarco-capitaliste⁵², idee creative, e prospettive di guadagno sono solo alcune delle motivazioni che Amato e Fantacci riscontrano come fattori che hanno mosso molte persone e sviluppatori nell'investire risorse ed energie in questo nuovo mercato digitalizzato.

Non è un caso, infatti, che il mondo digitale abbia vissuto, e stia vivendo tutt'ora, un momento di grande sviluppo tecnologico, coinvolgendo sempre più alti volumi di investimenti e di risorse umane che vi operano. A testimonianza di ciò, è possibile notare come nel 2014 le cripto-valute rilevate fossero circa 400⁵³, mentre in soli quattro anni si sia arrivati a contarne 1921⁵⁴.

In tutto ciò, purtroppo, bisogna notare come nonostante ognuna di queste valute digitali cerchi di differenziarsi dalla cripto-valuta più famosa, il Bitcoin, proponendo vantaggi e caratteristiche differenti, guardando più analiticamente, si nota come soffrano tutte dei medesimi deficit che accusa il Bitcoin. Nello specifico gli aspetti più criticati sono: un'emissione di moneta predeterminata ed una troppo frequente ed accentuata volatilità. Secondo molti esperti, tutte le caratteristiche che abbiamo appena elencato sono ravvisabili maggiormente in strumenti speculativi piuttosto che in uno strumento finanziario a tutti gli effetti.

L'opinione generale che portano avanti i sostenitori delle cripto-valute, è che l'esistenza di un ingente numero di valute digitali non implica un problema per il mercato, in quanto essi credono fortemente che sarà il mercato a far prevalere quelle più vevoli. Si accostano, infatti, al pensiero di Hayek secondo il quale l'equilibrio è raggiungibile attraverso la concorrenza monetaria.

⁵² M. Amato, L. Fantacci, Per un pugno di Bitcoin, università Bocconi, 2016.

⁵³ EBA, opinion on "virtual currencies", 2014, p. 10.

⁵⁴ Fonte: <https://coinmarketcap.com>

Tuttavia, Amato e Fantacci riscontrano due principali motivi secondo cui, nel contesto delle cripto-valute, non sarà mai raggiungibile un equilibrio attraverso la semplice concorrenza monetaria.

- 1) Prima di tutto il valore delle valute digitali, ed in particolare del Bitcoin, non dipende in realtà dal proprio utilizzo come mezzo di scambio, ma il suo prezzo è principalmente dipeso dalla domanda speculativa. Essendo questa a prevalere su tutto, la domanda degli utenti sarà tutta di tipo speculativo. Dovendo servire come strumento di speculazione, verranno prese di mira soprattutto le valute più scarse, poiché queste ultime avranno maggiori possibilità di apprezzarsi. In conclusione, si può affermare che le cripto-economia sarà tutt'altro che supportata da manovre stabilizzatrici, anzi sarà vittima di comportamenti speculativi.
- 2) Abbiamo già accennato al fatto che i sostenitori del Bitcoin condividano a pieno il pensiero di Von Hayek. Quello che però i suoi sostenitori non hanno compreso a pieno è che quando il premio Nobel parla di valute private aveva in mente un concetto ben diverso da quello che sono poi diventate le cripto-valute. La differenza risiede nel fatto che le prime, quelle teorizzate da Hayek, sono valute sì private, ma gestite comunque dai propri "ideatori", in modo da poter portare avanti quella ricerca di equilibrio e di stabilità economica tanto agognati, per riuscire in questo dovrebbero essere in grado di adattare, ad esempio, l'offerta di moneta. E', invece, ormai chiaro che le maggiori cripto-valute hanno delle quantità di moneta erogabile già decise antecedentemente.

Tuttavia, ci sono diversi esempi di come i creatori di cripto-valute abbiano cercato nel tempo di rispondere a queste criticità. Infatti, mentre Bitcoin, Ripple e Litecoin non concedono l'opportunità di operare sul lato dell'offerta, ci sono altre valute che lo fanno; è il caso di *Freicoïn*⁵⁵, che si ispira al concetto di Freigeld, elaborato da Silvio Gesell. L'idea di fondo è quella di stimolare la circolazione di moneta, introducendo una tassa sui depositi. Freicoïn ogni anno, utilizza la struttura Blockchain per prelevare dagli utenti il 5% del proprio totale di valuta in possesso nei portafogli, il valore recuperato viene poi diviso, un 20% del totale spetta ai miner, mentre il restante 80% viene reinvestito in un fondo per attività sociali e per continuare a sostenere lo sviluppo del protocollo. Un'altra valida soluzione viene fornita da due sistemi distinti, chiamati: *Coloredcoin* e *Mastercoin*. Questi due sistemi permettono ad ogni utente, appoggiandosi alla struttura Bitcoin di creare la propria valuta. La proposta di queste due piattaforme potrebbe definirsi la chiave di volta nella risoluzione di alcune delle criticità di cui sopra. Il motivo per cui questi due sistemi sembrano essere così promettenti è per il fatto che uno dei principali compiti della moneta è quello di fungere da mezzo di scambio. E' opinione di molti che creare un linguaggio crittato, di cui è fautore Bitcoin, che risulta da un lato

⁵⁵ M. Amato L. Fantacci, Per un pugno di Bitcoin, università Bocconi, 2016.

molto sicuro per gli utenti, ma dall'altro che in pochi siano in grado di comprendere, sia quasi più un esercizio di stile piuttosto che una necessità del mercato.

L'idea che Kelly, nel suo scritto, condivide è che debbano essere gli imprenditori a creare moneta. D'altro canto "il poeta fa la lingua, e la lingua fa la nazione"⁵⁶. Ed il poeta in questo caso si identifica con la figura dell'imprenditore. Una possibile soluzione a questo problema sembra poter risiedere in un nuovo ente, chiamato: DAO (*Decentralized Autonomous Organizations*).

Queste organizzazioni si autofinanziano emettendo cripto-valuta, che, però, presenta caratteristiche che si trovano a metà fra azione e moneta. Il processo secondo il quale queste organizzazioni funzionano è il seguente: i finanziatori concedono valute correnti alle DAO, che in cambio consegnano cripto-valuta. La cripto-valuta conferisce ai propri possessori vari diritti, ad esempio, da quota di partecipazione nel momento della ripartizione dei dividendi, oppure in un'altra ipotesi la cripto-valuta potrebbe fungere da moneta per comprare i beni prodotti dall'impresa.

Rimangono comunque delle criticità non trascurabili, anche se l'idea delle DAO rappresenta già dei passi avanti, infatti vista l'attuale struttura del sistema finanziario e bancario, le valute coniate dalle DAO non possiedono determinate caratteristiche che invece una valuta corrente possiede. Mi riferisco al fatto che una moneta corrente, coniata da una banca centrale, è sicuramente uniforme, identica e sensibile. Per fare un esempio pratico che chiarirà il perché si tratta di una criticità, immaginiamo di depositare un euro in una banca, se volessimo prelevare lo stesso importo da un'altra banca avremmo la sicurezza che il valore di quell'euro non sia variato, mentre le cripto-valute coniate dalle organizzazioni non sono né fungibili, né ancorate alla valuta corrente, conseguentemente soffriranno ancora di quella grande volatilità di cui abbiamo parlato più volte. Come più volte abbiamo notato in questo lavoro, le posizioni degli esperti spesso si dividono. Infatti, se da un lato c'è chi vede un fattore positivo nell'eliminazione della centralizzazione, dall'altro lato si può annoverare il fatto che con l'eliminazione della centralizzazione vi è una inevitabile perdita di mediazione, che lega, di solito, moneta e investimenti.

E' interessante notare come si stia facendo strada tra gli esperti la possibilità che le banche centrali possano coniare cripto-valuta. La stessa EBA, nel proprio report, anche se accennando solamente a questa probabilità, ipotizza che teoricamente le banche centrali potrebbero emettere cripto-valuta. Per chiarezza dobbiamo ricordare che le valute digitali non sono associabili alle valute correnti, non avendo un cambio fisso e non essendo liberamente convertibili in altre valute.

⁵⁶ Vedi nota 52.

Staccandoci momentaneamente dallo scenario attuale ed immaginando che le banche possano emettere valute digitali, possiamo analizzare i risvolti positivi di questo scenario. In primis il fatto che, se le cripto valute venissero emesse dalle banche, le istituzioni potrebbero attuare politiche monetarie, superando la critica che le cripto-valute sfuggono a politiche monetarie. Non è un caso infatti che siano nati enti come Realcoin e Bitreserve che abbiano cercato di “ancorare le crito-valute alle valute correnti”. L’idea principale di queste imprese è quella di prendere tutti i vantaggi dei Bitcoin, come ad esempio l’anonimato e la sicurezza, e di compensare gli svantaggi inglobando i vantaggi delle valute correnti. Per essere più pragmatici, utilizzando la tecnologia Blockchain per trasferire valuta digitale velocemente e senza costi di transazione, ma al tempo stesso mantenendo la possibilità di convertire valuta digitale in valuta corrente a tassi fissi prestabiliti.

Nonostante questa soluzione si presenti come una via percorribile, i sostenitori più estremi del Bitcoin la ripudiano, poiché nel momento in cui si garantisca un tasso di cambio stabile, torni ad essere preponderante il tema della centralizzazione. Questa soluzione riporta alla luce comunque due ulteriori problematiche, che affliggono tutte le valute a corso legale: insolubilità e illiquidità. Per le valute a corso legale, potrebbe infatti verificarsi l’ipotesi che le quantità di valuta accantonate possano non essere sufficienti a garantire la conversione in valuta standard. (Vigna, Casey 2015, pp 242-243).

Tutti questi rischi sparirebbero se una banca centrale si adoperasse per emettere valuta digitale, potendone garantire la validità essendo un’autorità centrale e soprattutto potendo operare sulle quantità emesse si potrebbe agire sulle politiche monetarie.

In ogni caso questa cripto valuta sta dimostrando di essere ancora ai primi stadi evolutivi, fin troppo acerba per diventare una valuta a corso legale a tutti gli effetti. Discorso ben diverso si può fare per la Blockchain che invece sta rivelando le proprie potenzialità, non soltanto in campo finanziario.

Riprendiamo il caso del prestito ipotecario, in cui una volta registrato nel sistema Blockchain, esso si trasforma in uno smart contract a tutti gli effetti, perfettamente conservato all’interno della Blockchain, senza timore che qualcuno possa manometterlo o perderlo. Inoltre il contratto diventa operativo e vincolante, senza la necessità di autorità giuridiche o iter burocratici di sorta, in cui ogni inadempienza viene rapidamente risolta dal sistema. Come affermano Vigna e Casey, l’adozione di questo genere di innovazioni implicherebbe vantaggi non solo per i creditori, ma anche per i debitori. Non a caso il sistema Blockchain potrebbe essere impiegato anche nella valutazione del credito, mettendo a disposizione finanziamenti anche per gli utenti a cui, ad oggi, non verrebbero concessi. Gli autori di questa riflessione motivano il loro ottimismo, affermando che gli smart contract superano lo step di valutazione dell’affidabilità della controparte, poiché la garanzia di adempienza risiede nello stesso protocollo, che si assicura che tutte le clausole del contratto vengano rispettate. Quindi

non c'è la necessità da parte del creditore di istituire onerosi iter di accertamento nei confronti del debitore, o in caso di inadempienza, di ricorso a costosi istituti di recupero credito.

E' stata riscontrata un'ulteriore applicazione in campo finanziario, infatti sempre grazie agli smart contract è possibile gestire anche gli strumenti derivati. Esistono già molte piattaforme online come ad esempio Hedgy, che permette di negoziare titoli OTC inseriti in una catena Blockchain come smart contract, seguendo questo meccanismo alla scadenza del titolo, la differenza tra il prezzo contrattato e il prezzo corrente viene direttamente liquidata all'utente senza necessità di pagare onerosi costi di transazione.

In questo contesto di cambiamento oltre la tecnologia Blockchain, anche gli *smart contract* stanno partecipando attivamente a questa tendenza. Non a caso Amato e Fantacci affermano che l'utilizzo degli *smart contract* possa in futuro sempre più agevolare lo sviluppo della *sharing economy*⁵⁷. Infatti in un'economia caratterizzata da una sempre maggiore domanda da parte degli utenti di memoria *cloud*, in cui poter archiviare i propri dati, corre in soccorso una piattaforma chiamata *SafeMaid*, che consente agli utenti di mettere a disposizione la propria memoria inutilizzata, e ricevere un corrispettivo in denaro da parte di coloro che ne fanno uso. (Vigna, Casey 2015, pp 238-239).

Tuttavia, concordo con molti, nel non poter reputare queste innovazioni solo da un punto di vista ottimistico, poiché se da un lato abbiamo un'esecuzione molto più precisa e veloce di contratti, transazioni etc, dall'altro però ci si deve relazionare con il fatto che tutte le maggiori dinamiche della nostra società verranno controllate da computer e sistemi automatizzati. "Vengono a cadere tutte le cause di nullità e annullabilità che il sistema prevede e tutela per l'interesse delle parti"⁵⁸. Inoltre l'esecuzione automatica rende impossibile la rinegoziazione dei termini. Aggiungono Vigna e Casey che l'esecuzione automatica può inoltre avere un ulteriore risvolto negativo, immaginiamo di trovarci nel caso di un prestito tra due persone, il creditore nonostante non abbia ricevuto un pagamento potrebbe avere nel suo interesse il fatto di voler lasciare dell'ulteriore tempo al proprio debitore. La domanda che sorge spontanea è se un sistema informatico sia in grado di rendersi conto di certe circostanze e sappia adattarsi ad esse.

Spostandoci ora su altri esempi, è stato notato come la tecnologia alla base della cripto-valuta possa essere utilizzata anche per raccogliere capitale e per investimenti a lungo termine. Sotto un certo punto di vista la cripto-valuta può assomigliare ad una vera e propria azione. Ad esempio, è possibile programmare delle operazioni all'interno del protocollo che vengono, poi, eseguite automaticamente,

⁵⁷ *Sharing economy*: anche definite "economia collaborative", con questo termine si intendono un nuovo tipo di concezione economica, secondo la quale un bene viene messo a disposizione di più utenti, che pagano per usufruirne, senza entrarne strettamente in possesso.

⁵⁸ Vedi nota 52.

ad esempio si può programmare l'azione di fornire ad ogni azionista a fine esercizio la propria quota di dividendi, o ancora, il protocollo potrebbe agire autonomamente a conferire determinati tipi di diritti, come quello di voto agli azionisti, in base alla loro quota di partecipazione. Nonostante alcune somiglianze con una vera e propria azione, le differenze sono altrettanto rilevanti. A differenza di un'azione, una cripto-valuta non rientra nel passivo del bilancio di una società, non è una partecipazione al capitale sociale dell'impresa e non dà diritto al possessore di ottenere un rimborso in valuta corrente della propria quota. Allo stesso tempo però la cripto-valuta potrebbe essere usata dagli "azionisti" immediatamente come denaro contante per acquistare beni forniti dall'azienda. "Bitcoin stesso può essere visto come una società che offre servizi di pagamento il cui valore si riflette nella quotazione dei titoli, (i Bitcoin), che rappresentano quote di partecipazione alla società"⁵⁹.

Un grande vantaggio offerto dalla tecnologia Blockchain per le imprese, è la possibilità di raccogliere capitale senza la necessità di quotarsi in borsa. E' possibile infatti eseguire operazioni di *crowdfunding*, in cui il capitale raccolto viene direttamente concesso dagli investitori che acquistano cripto-valuta. Nel 2015 il CEO del sito overstock.com, ha fatto richiesta per poter emettere 500 milioni di dollari in azioni digitali. Ma al di là di questo episodio, bisogna ragionare sul fatto che un simile avvenimento potrebbe significare un accantonamento anche delle borse nel mondo, come quella di Wall Street. Si sostituirebbe alle classiche borse finanziarie un sistema telematico decentrato e soprattutto automatico.

Come afferma Kelly: "prima si realizzano i profitti e poi si decide cosa farne", è per questo che il finanziamento per via dei Bitcoin rappresenta un cambio strutturale importante. Anche se aggiunge sempre Kelly, "La *cryptonomics* non si fonda sulla massimizzazione del profitto, bensì sulla massimizzazione delle risorse".⁶⁰

Reputo giusto approfondire il concetto di DAO, che ripetiamo essere delle organizzazioni decentralizzate e digitali. Queste per funzionare in realtà non necessitano di persone. Ad informarsi e ad approfondire molto il fenomeno delle DAO, c'è sempre Kelly, che da un lato le definisce come: "un gruppo di persone accomunate da un'affinità di pensiero che si mettono assieme per svolgere un compito determinato". Fattore interessante è il fatto che le DAO, comunque, non sono create con il solo scopo di raggiungere obiettivi economici, ma anche sociali, scientifici o culturali.

Una DAO, certe volte anche ci si riferisce ad un'entità completamente automatizzata di business, in generale si tratta di un network decentralizzato, guidato da meccanismi informatici, che producono

⁵⁹ Larimer S., Bitcoins and the three laws of robotics, <https://letstalkbitcoin.com/bitcoin-and-the-three-laws-of-robotics>, 2013.

⁶⁰ Kelly B., The Bitcoin Big Bang. How Alternative Currencies Are About To Change The World, Wiley, 2015, p. 162

output massimizzando la funzione di produzione, Una società autonoma decentralizzata (a volte indicata come entità aziendale completamente automatizzata o una società autonoma distribuita, spesso abbreviata "FAB" o "DAC") è una rete decentralizzata (o distribuita) di agenti autonomi a intelligenza limitata che eseguono un massimale di output funzione di produzione e che divide il suo lavoro in compiti computazionalmente intrattabili (che incentiva gli esseri umani a fare) e compiti che svolge autonomamente. Può essere pensato come una società gestita senza alcun coinvolgimento umano sotto il controllo di un insieme incorruttibile di regole aziendali. Queste regole sono in genere implementate come software open source pubblicamente controllabile distribuito tra i computer delle parti interessate. Un umano diventa uno stakeholder acquistando azioni della società o pagate in quelle azioni per fornire servizi alla società. Questo titolo può conferire al suo proprietario una quota dei profitti del DAC, la partecipazione alla sua crescita e / o un'opinione sul modo in cui viene gestito. Le DAO principalmente assurgono all'uso di raccogliere capitale, di regolarlo, di definire le quantità di output, tutto ciò viene deciso da processi informatici, dove l'intervento umano trova relativa applicazione.

3.2 Mercati finanziari, innovazione e Bitcoin

Come Emmanuele Massagli, presidente di ADAPT, afferma: “La “tecnologia *blockchain*” è uno di quegli argomenti che possiede tutte le caratteristiche per il successo: il fascino misterioso dell'evoluzione informatica, crescenti orizzonti di utilizzo, clamore mediatico, il sapore della libertà fuori dalle regole tradizionali, il democraticismo delle soluzioni nate “dal basso”⁶¹.

Con una sempre maggiore diffusione di internet, con l'introduzione del concetto di “*iot*”, e la sempre maggiore digitalizzazione dell'economia, ogni settore del mercato sta trovando nuove applicazioni, ed in questo momento di cambiamento, anche il sistema bancario, strutturalmente una delle organizzazioni più conservatrici esistente in economia, sta ravvisando delle opportunità di cambiamento non indifferenti.

Con la digitalizzazione che sta investendo anche i canali bancari, per le banche è giunto il momento di valutare le proprie scelte di posizionamento. Come afferma Anna Omari nel proprio *paper*⁶²: “(è necessario) Adeguare la propria proposta al mercato impone l'analisi del potenziale di domanda e della percezione che esso ha nei confronti del nuovo canale e di una strategia distributiva multicanale. L'evoluzione dell'attività bancaria in Internet sta avvenendo con gradualità; il pericolo è che le

⁶¹ Fonte: <http://adapt.nova100.ilsole24ore.com/2018/09/10/blockchain-persona-e-mercato-del-lavoro/>

⁶² Omari A., Internet banking Dalla strategia multicanale alla ridefinizione della value proposition in banca, *Economia&Management* n° 1, 1999.

banche si adeguino all'evoluzione tecnologica e a quella dei consumi con ritardo rispetto a operatori non bancari, che già sono presenti.”

Secondo l'autrice, infatti, internet rappresenta per il sistema bancario un'importante mezzo di sviluppo strategico, in modo tale da rimodellare la propria value proposition, andando a costruire modelli di offerta che supportino quanti più possibili ambiti del mercato.

Con lo sviluppo di nuove tecnologie come l'*home banking* o con l'espansione dell'e-commerce, non stupisce che moltissime piattaforme stiano prendendo piede, con lo scopo di implementare questo genere di innovazioni, come ad esempio la tecnologia “*touch and pay*”, oppure che grandi istituzioni, come Goldman Sachs, inizino ad interessarsi alle cripto-valute.

A proposito di questo ultimo caso, stupisce venire a conoscenza che una delle più grandi istituzioni bancarie, come Goldman Sachs, abbia intenzione di iniziare ad accettare pagamenti in Bitcoin. E' possibile affermare con una certa sicurezza che si tratti di un evento più che rivoluzionario, poiché le grandi istituzioni finanziarie sin dalla comparsa delle valute digitali hanno cercato di porre un freno alle cripto-valute, per ovvie ragioni; ma fino ad ora erano stati tentativi vani, se non per qualche isolata eccezione.

E' chiaro che la volatilità nei prezzi delle cripto-valute, soprattutto del Bitcoin, sia una delle maggiori peculiarità che compongono la struttura di queste valute. Per questo continuano ad essere viste come un investimento troppo rischioso, incapace di assurgere ai ruoli principali della moneta, e che si continui a trattare di uno strumento speculativo, piuttosto che di uno strumento finanziario.

Proprio questa natura speculativa e l'andamento poco stabile hanno tenuto lontane le più grandi istituzioni bancarie dall'idea di poter intraprendere un cammino di implementazione con le valute a corso legale. I più grandi esperti, ed i più noti economisti hanno criticato le cripto-valute, definendole una moda, una mania del mercato. Bisogna, però, ricordare che nonostante queste opinioni decisamente avverse le valute digitali hanno saputo attirare, con le proprie prospettive di guadagno e la propria struttura innovativa, la grande attenzione del mercato. Il colosso finanziario americano Goldman Sachs, qualche mese fa, in seguito al rialzo registrato della cripto-valuta Bitcoin, dopo il primo grande crollo di dicembre 2017, ha deciso di iniziare ad accettare Bitcoin come metodo di pagamento. Si tratta di un primato che la banca possiede, non essendoci mai stato nessun altro che a Wall Street avesse annunciato una così radicale presa di posizione. La banca si sta infatti preparando ad ufficializzare la prima transazioni a base Bitcoin. “Lo scopo è usare la sua moneta negli scambi finanziari utilizzando contratti legati al prezzo di Bitcoin”⁶³. Rana Yared, a capo di questa operazione, ha affermato che secondo Goldman Sachs, in seguito ad analisi maggiormente approfondite, non si tratterebbe di un cattivo investimento su cui puntare, visto che la domanda di questo genere di valuta

⁶³ Vedi nota 52.

aumenta esponenzialmente di giorno in giorno. Rana Yared non ha nascosto la possibilità che la stessa Goldman Sachs crei una propria cripto-valuta.

Tuttavia, Goldman Sachs non è stata l'unica banca d'affari ad essere entrata in questo mercato digitale, anche la concorrente Morgan Stanley ha dichiarato che renderà disponibili canali per fare trading online nel mercato delle cripto-valute, più precisamente scambiando derivati. Patrizia Licata su Corcom.it⁶⁴ afferma: "Morgan Stanley è stata anche tra i primi e più entusiasti sostenitori dei future su bitcoin, che ha appoggiato subito dopo il debutto (dicembre 2017) sui mercati CME e CBOE.". Attualmente però gli scambi con valute digitali risultano ancora in fase di implementazione, per vari motivi, alcuni dei quali hanno come motivazione principale le forti fluttuazioni del Bitcoin ed il fatto che questo genere di trasformazioni prevede ingenti investimenti in infrastrutture tecnologiche.

Anche il colosso Citi Group ha intravisto dei possibili guadagni nel mondo delle cripto-valute. Anche se, quest'ultimo, avrebbe intenzione di creare e lanciare un nuovo tipo di prodotto finanziario con funzioni differenti; lo scopo principale dello strumento finanziario sarebbe di "consentire agli investitori istituzionali di accedere ai mercati delle cripto-valute senza entrare direttamente in possesso di asset cripto".⁶⁵ Anche se non c'è attualmente una qualche conferma ufficiale dal gruppo, sembrerebbe che questo nuovo prodotto possa chiamarsi *Digital Asset Receipt* (DAR), il che trova molte somiglianze con un altro prodotto esistente di nome ADR (*American Depositary Receipts*), cioè uno strumento finanziario che permette agli investitori di ottenere titoli stranieri che non potrebbero trovare, altrimenti, nelle proprie borse nazionali.

Tuttavia queste indiscrezioni vengono alla luce in un momento pessimo per i Bitcoin e le maggiori cripto-valute, come *Ethereum* o *Litecoin*, che da gennaio hanno perso circa 640 miliardi di dollari⁶⁶. Parlando inoltre di altre possibili applicazioni, ad inizio paragrafo abbiamo parlato di come il sistema "touch and pay" sia sempre di più al centro delle attenzioni. Cresce il numero di sviluppatori che, nel mondo delle valute digitali, sta cercando di sviluppare sempre di più tecnologie *contactless*, in modo tale da semplificare e velocizzare i pagamenti. Un certo numero di portafogli di cripto-valute sta fornendo le proprie tecnologie in modo tale da velocizzare lo sviluppo e la crescente adozione dei pagamenti di questo tipo, permettendo alle valute digitali di prendere parte al flusso di pagamenti via smartphone. Di seguito elencherò le maggiori piattaforme.

1. Airbitz:

Il portafoglio digitale Airbitz permette agli utenti di mandare Bitcoin con il bluetooth. Il vantaggio di usare questo sistema è certamente quello di semplificare, in modo significativo, il sistema di

⁶⁴ Vedi: <https://www.corrierecomunicazioni.it/finance/morgan-stanley-avanti-sul-trading-in-derivati-bitcoin/>

⁶⁵ Fonte: <http://www.wallstreetitalia.com/bitcoin-citi-snobba-vendite-e-prepara-lancio-di-un-nuovo-prodotto/>

⁶⁶ Fonte: <http://www.ilsole24ore.com/art/finanza-e-mercati/2018-09-10/criptovalute-bolla-si-sgonfia-da-gennaio-bruciati-640-miliardi-160041.shtml?uclid=AE4XY6pF>

trasferimento tra utenti, inoltre l'applicazione ha una funzione in cui mostra la posizione e la rispettiva distanza da tutte le attività che accettano Bitcoin.

2. Bitpay:

Il processore di pagamenti Bitcoin ha sviluppato lo scorso anno la propria app di Checkout, ed ha portato la tecnologia del “one tap” nelle cripto-valute. Questa app funziona con ogni singolo portafogli digitale su ogni dispositivo. Gli utenti possono scaricare il proprio codice QR ed effettuare pagamenti in pochissimi passaggi. Ad ogni modo questa app è disponibile ancora per i soli dispositivi che supportano il software Android, lasciando quindi ancora scoperta una grande porzione di mercato. Inoltre hanno integrato SumUp, un tecnologia di POS europea, e l'hanno modificata in modo tale da fargli accettare anche Bitcoin.

3. Coinbase:

Il famoso portafoglio digitale permette di trasferire Bitcoin per email, codice QR, e tecnologia NFC. Coinbase raccoglie tutti i digital wallet, il che significa che gli utenti possono accedere ai portafogli sia tramite web, sia tramite smartphone, e gli aggiornamenti tra le due piattaforme sono istantanei. I soldi degli utenti sono mantenuti al sicuro nel cloud (con un 90% di immagazzinaggio offline), quindi anche se l'utente perdesse il proprio telefono, i suoi soldi sarebbero comunque al sicuro. Nel caso di furto, gli utenti comunque possono disabilitare l'accesso dal proprio telefono.

Mi sembra giusto anche notare come dal punto di vista finanziario, i Bitcoin possano rappresentare una via percorribile. Ne è un esempio il Venezuela, che a causa di una crescita dell'inflazione e del costo della vita divenuto insostenibile, si sta rivolgendo sempre di più alla domanda di cripto-valute. Il Venezuela, non a caso, può vantare anche il primato di aver coniato la prima cripto-valuta governativa, di nome Petro, considerata in grado di risolvere i problemi inflattivi del paese, ma come afferma Pierangelo Soldavini si tratterebbe semplicemente di una valuta ideata “per aggirare l'embargo economico del petrolio”⁶⁷. Tuttavia, i venezuelani hanno riscontrato nelle cripto-valute la possibilità di comprare beni e scambiare denaro senza la necessità di passare per la moneta nazionale. Tra la vasta gamma di cripto-valute che circolano per il web, quella maggiormente in uso in Sud America è chiamata “Dash”. Si tratta di una valuta digitale creata nell'interesse delle comunità locali. La società che gestisce il Dash afferma che il Venezuela sia diventato il loro secondo mercato più grande, sempre più persone, infatti, lo utilizzano per commerciare e comprare beni. Il motivo di questo grande successo risiede nel fatto che gli abitanti del Venezuela necessitassero di uno strumento con cui difendersi dall'inflazione, che colpisce il paese da diverso tempo ormai, ed il Dash rappresenta una possibile soluzione al problema. Non a caso, risulta significativo il fatto che si stia riscontrando

⁶⁷ Fonte: <http://www.ilsole24ore.com/art/mondo/2018-08-24/venezuela-crisi-boom-criptovalute-difendersi-dall-iperinflazione--175659.shtml?uuiid=AEJMk3eF>

un'ingente crescita di attività commerciali che accettino il Dash come metodo di pagamento “(già) a inizio luglio erano 400, quasi tutti nella prima parte dell'anno, poi in soli due mesi sono raddoppiati a 800, un centinaio solo nell'ultima settimana, dopo l'annuncio della svalutazione del bolivar”⁶⁸

E' interessante notare come il Dash si discosti, come caratteristiche, dal Bitcoin. Questa cripto-valuta risulta piuttosto giovane, se comparata alle altre più diffuse, nasce infatti solo nel 2014, e come il Bitcoin su base open-source. Il Dash presenta costi di intermediazione ancora più ridotti, ma significativi sono soprattutto i tempi veramente irrisori che il Dash impiega per completare le operazioni, al contrario delle ore che il sistema Bitcoin impiega. Proprio a questo proposito, il fattore velocità ha sicuramente influito molto nell'affermazione di questa cripto-valuta in paesi, come il Venezuela, in cui l'aumento dei prezzi è all'ordine del giorno. Altro fattore peculiare che contraddistingue il Dash, è il fatto che l'organizzazione sia composta da stakeholder che organizzano al meglio i fondi provenienti dall'attività di *mining*.

Per riassumere quanto detto fino ad ora, possiamo affermare che con la Quarta rivoluzione industriale e con tutte le implicazioni che questa porta, stiamo assistendo ad una rivoluzione di moltissimi aspetti dei mercati e dell'economia. Si sono trovati davanti alla necessità di cambiare anche enti che hanno ricoperto lo stesso ruolo per secoli e sempre con le stesse modalità, come l'appena citato sistema bancario. Ancora una volta però si nota come le cripto-valute siano un'idea implementabile nella realtà e non solo sui libri o su qualche sito internet. Ma ancora si necessita di tempo e di qualche modifica delle fondamenta di queste, per essere attuabili a tutti gli effetti. Considero importante che organizzazioni come Morgan Stanley o Citi Group abbiano preso atto dell'importanza di queste entità e stiano cercando di trovare una via che permetta di utilizzarle, non dimenticando, però, il fatto che si tratta ancora di un concept che necessita dei dovuti aggiornamenti strutturali e giuridici.

3.3 Applicazioni non monetarie del protocollo

Come abbiamo avuto modo già di accennare nei paragrafi precedenti le applicazioni della catena Blockchain non si limitano soltanto all'ambito economico e monetario. E' ormai chiaro che il punto focale di questa tecnologia sia il fatto che possa rendere sicure le registrazioni nel proprio database iniziate attraverso altra tecnologia, quale internet, che è di base poco sicura. Fino ad ora abbiamo parlato solamente di iscrizione di transazioni monetarie, ma non sono le uniche operazioni inscrivibili nel database, si possono includere in questo gruppo anche contratti, diritti di proprietà, comunicazioni e scambi commerciali. Oltre ad essere un sistema sicuro, la Blockchain, rende superflui gli interventi

⁶⁸ Vedi nota 67.

degli intermediari. Come affermano Wright e De Filippi⁶⁹ la Blockchain rappresenta a pieno il desiderio dei sostenitori delle cripto-valute, in quanto, essa rappresenta l'affermazione di un nuovo modo di rivedere la *governance* politica ed economica, ma soprattutto segna il tramonto delle entità gerarchiche e centralizzate.

Cercherò in questo paragrafo di introdurre le maggiori applicazioni di questa tecnologia, partendo dal concetto di *smart property*, che nel concreto si tratta di un'effettiva proprietà, di un bene fisico o non, gestita attraverso la catena Blockchain, il tutto reso funzionante dall'ausilio degli *smart contract*. L'idea che si fonda su questa funzionalità è che rendendo la proprietà "*smart*" è possibile trasferirla senza la necessità di passare per enti terzi, venendo meno l'accertamento della "fiducia", come principio determinante di uno scambio. Questo processo permette di ridurre le frodi, ma soprattutto i costi di commissione. Amato e Fantacci aggiungono: "tecnicamente la Blockchain può essere usata come una sorta di catasto digitale diffuso, per la registrazione di qualunque genere di proprietà, mobiliare ed immobiliare.". Ad ogni modo, questa funzionalità non è ancora del tutto applicabile. Prendendo ad esempio l'ordinamento italiano, la proprietà privata è limitata dal legislatore per non rischiare che venga meno la funzione sociale ed il fatto che la proprietà privata possa essere accessibile a tutti, contemplando in alcuni casi, per il raggiungimento dell'interesse collettivo, anche l'esproprio. Ciò implica che non basti il solo volere degli utenti per far valere contrattualmente il trasferimento, vi è bisogno anche di essere affiancato da un ordinamento giuridico aggiornato. La premessa appena fatta vale nell'ottica in cui al contrario, nel caso delle smart property, il proprietario dei diritti ha un controllo assoluto, indiscusso ed illimitato, il che potrebbe portare a comportamenti irresponsabili ed illeciti. Keynes, già, nel suo scritto: *la riforma monetaria*, affermava l'importanza di ricercare elementi di moderazione in tutti i campi della società civile, identificando come i peggiori nemici della società coloro che difendevano l'inviolabilità dei contratti a tutti i costi.

Vi sono comunque altri campi del mondo digitale in cui la Blockchain rappresenta uno strumento molto promettente. Mi riferisco all'ambito del *file sharing* e nello sviluppo di sistemi di comunicazione, come sistemi di voto e gestione dei domini internet. "Inoltre la Blockchain costituisce potenzialmente un'infrastruttura informatica sicura per quella che viene chiamata "internet delle cose" offrendo un mezzo di comunicazione macchina-macchina per la gestione sicura di dispositivi collegati in rete"⁷⁰ .

Parlando invece di un fattore che molti trascurano, penso sia importante ragionare sul fatto che internet, per come lo conosciamo noi oggi, abbia eliminato la proprietà privata in rete, basti pensare al fatto che file multimediali, come musica o film, possono essere facilmente riprodotti gratuitamente,

⁶⁹ Wright A., De Filippi P., Decentralized blockchain technology and the rise of lex cryptographia, <https://ssrn.com/abstract=2580664>, 2015.

⁷⁰ Vedi nota 52.

oltrepassando ogni tipo di diritto d'autore e simili concetti. Nel nostro internet attuale, si è completamente perso il senso di “scarsità”, tutto è riproducibile e duplicabile all'infinito.

La Blockchain “reintroduce la proprietà privata nel mondo dei beni digitali, sinora ritenuti indefinitamente replicabili e trasmissibili”⁷¹.

Poco fa abbiamo accennato ad una necessità intrinseca che il web necessiterebbe nel riportare nella propria dimensione il concetto di scarsità. Se da una parte la Blockchain può assurgere a ciò, e rappresentare per alcuni un punto focale su cui puntare, c'è chi, dall'altra parte, ha il timore che questo fattore possa rivelarsi dannoso per gli utenti e per l'intero web, andandosi a creare quello che Doria chiama “mercificazione generalizzata”. Nel concreto si andrebbe a monetizzare ogni singolo contenuto visualizzabile dagli utenti, con il rischio che diventi un'attività esosa in tutti i sensi, facendo conseguentemente perdere interesse nei propri utenti. Aranguena, nel proprio scritto⁷², prendendo spunto da Vigna e Casey teorizza l'idea di un “mercato della reputazione”; si tratterebbe di un sistema di pagamenti in cripto-valuta, per l'esattezza di un “sistema di rating basato su un indice di gradimento registrato sulla Blockchain”⁷³, monetizzando, ad esempio, i “mi piace” di Facebook o le recensioni di Tripadvisor.

Nel secondo capitolo, avevo già accennato al fatto che si intravedono possibili applicazioni nell'utilizzo della catena nell'ambito politico delle votazioni. Oltre ad essere ravvisabili le implicazioni positive come una maggiore sicurezza e la quasi impossibilità di manomissione, ma vi sono altre implicazioni di cui penso sia importante parlare.

Questo sistema, infatti, potrebbe di gran lunga aiutare l'affluenza alle urne, essendo uno strumento digitale ed il nostro mondo è sempre più connesso, risulterebbe più facile per le persone, anche sparse per il mondo partecipare a delle elezioni, per esempio. Seguendo questo progetto la Blockchain potrebbe essere la soluzione per una maggiore partecipazione alla vita politica dei cittadini, si potrebbe addirittura arrivare a poter includere i cittadini nelle decisioni governative. Tutto ciò, secondo gli esperti, potrebbe trovare supporto da imprese e dagli stessi governi.

Inoltre con il progredire di sistemi sofisticati ed elaborati, attraverso la raccolta dei Big Data, si potrebbe andare a creare quello che si definisce “algorithmic governance”. Si tratta di un nuovo sistema capace di regolamentare la società in modo più semplice e meno costoso (riducendo infatti i costi delle forze dell'ordine) e permettendo di creare regole personalizzate sui cittadini.

Ovviamente non mancano le critiche a questo genere di sviluppo, Amato e Fantacci lo criticano aspramente, definendolo: “Il Truman Show sembrerebbe al confronto un'utopia libertaria”. Di questa

⁷¹ Vedi nota 52.

⁷² Aranguena G. et al, Bitcoin l'altra faccia della moneta, goWare, 2014.

⁷³ Vedi nota 72.

idea si critica fortemente il fatto che le persone sarebbero sempre “schedate” da un sistema e monitorate, e le scelte ottimali che ricadrebbero su di essi sarebbero processate da un computer.

Alcuni definiscono questo genere di proposta addirittura totalitaria, decisioni, regole, una società sostanzialmente governata da contratti digitali eseguiti automaticamente.

Per riassumere si è notato come la catena Blockchain non abbia un solo ambito di esecuzione, ma anzi svariati, considerando anche il fatto che visti gli sviluppi che sta avendo il mercato e le sue tendenze, si possano trovare vari ambiti di applicazione al di fuori di quello economico. E' chiaro però che questo genere di prodotto è in realtà ancora molto acerbo, ed ora come ora non risulterebbe un investimento totalmente riuscito.

Ha dalla sua moltissimi vantaggi, e soprattutto sembra rispondere, almeno in parte, alle esigenze che il mercato cerca in questo specifico momento ma soprattutto negli anni a venire. La mia personale opinione è che servano tuttavia delle modifiche, provenienti sia dal mondo Bitcoin, quindi i suoi sostenitori dovrebbero abbandonare la completa avversione verso le istituzioni ma piuttosto collaborarvi, e sia dalla controparte, cioè gli enti, di riporre l'avversione e la paura al cambiamento.

Conclusioni

Bitcoin e cripto-valute nascono come idea tecnologicamente avanzata, sganciata da intermediari onerosi e macchinosi, rispondendo, quindi, ad esigenze di un'economia digitale e veloce che caratterizza il tempo della Quarta rivoluzione e caratterizzerà il futuro delle transazioni globali.

Al momento, però, essendo le cripto-valute, ed in particolare il Bitcoin, oggetto di interesse speculativo, questo connotato sta prevaricando il vero scopo per cui queste sono nate, inibendo il loro potenziale.

In ogni caso, per rispondere al quesito posto fin dall'inizio di questo lavoro, le cripto-valute sembrerebbero non essere ancora un'esigenza reale dell'economia. Non disponendo, al momento attuale, di infrastrutture sufficienti per il proprio funzionamento.

Le cripto valute potrebbero rappresentare uno strumento del futuro, di cui oggi si sta facendo una iniziale esperienza, che presentano molti vantaggi, ma anche, altrettanti svantaggi.

Per quanto riguarda i vantaggi:

- Le valute digitali non richiedono la presenza fisica delle controparti, aggiungendo il fatto che usando il sistema Bitcoin il processo di trasferimento è molto più veloce, sicuro ed economico.
- Le transazioni possono avvenire in qualsiasi luogo ed in qualsiasi momento, aumentando la flessibilità dei business.
- Il Bitcoin presenta le stesse caratteristiche dell'oro, come ad esempio la rarità.
- Il Bitcoin, e le cripto-valute in generale, non sono soggette ad inflazione.

Gli svantaggi invece:

- Le cripto-valute, come ripetuto più volte, presentano una troppo accentuata e frequente volatilità.
- I registri delle transazioni sono pubblici, questo significa che ognuno può essere al corrente dei volumi commerciati.
- Le transazioni di Bitcoin, sono potenzialmente incontrollabili, essendo gli utenti anonimi.
- L'utilizzo di questa tecnologia implica investimenti esosi di avviamento ed un utilizzo di elettricità spropositato.

In molti hanno ipotizzato la possibilità che il bitcoin possa di fatto essere accantonato o superato, o persino distrutto dagli intenti speculativi che si sono addensati con il passare del tempo. Ma abbiamo altresì visto come la tecnologia su cui si basa, la Blockchain, abbia un altissimo potenziale, sia per traslarsi a transazioni digitali sicure peer.to-peer, sia per numerosi ambiti di interesse per la società digitale: sistemi di voto, accatastamento e mantenimento di documenti, riscossione delle tasse e molto altro.

Concludendo, il Bitcoin nasce come un interessantissimo esperimento, capace di catturare una grande attenzione, purtroppo trascinato (a cura di alcuni difetti) in una bolla speculativa che fa dubitare della sua utilità e delle sue valenze. Forse l'economia non ha bisogno del Bitcoin al momento attuale o nel prossimo futuro, ma segna una linea di tendenza da non sottovalutare sia per il mondo finanziario sia per le imprese, nell'uso di tecnologie quali la blockchain. Il bitcoin potrebbe sparire ma su questa linea potrebbero sorgere cripto-valute più "solide" e strutturate, che abbiano aspetti di "salvaguardia" del valore più idonei, capaci di assicurare una diffusione e un utilizzo sia da parte del mondo finanziario che dei privati.

Bibliografia

Amato M., Fantacci L., Per un pugno di Bitcoin, università Bocconi editore, Milano, 2016.

Ateniese G., Magri B., Venturi D., Andrade E., Redactable Blockchain or Rewriting History in Bitcoin and Friends, 2nd IEEE European Symposium on Security and Privacy|EuroS&P, 2017.

Bohr J., Bashir M., Who Uses Bitcoin? An exploration of the Bitcoin community, Twelfth Annual Conference on Privacy, Security and Trust (PST), 2014.

Burlone P. L., de Caria R., Bitcoin e le altre criptomonete Inquadramento giuridico e fiscale, IBL Focus, n 234, 2014.

Casey, M., Nasdaq to Provide Trading Technology for Bitcoin Market place. The Wall Street Journal, <http://www.wsj.com/articles/nasdaq-to-provide-trading-technology-for-bitcoin-marketplace-1427140006>, 2015.

Chohan U. W., A History of Bitcoin, University of New South Wales, Canberra, 2017.

Crosby M., Nachiappan, Pattanayak P., Verma S., Kalyanaraman V., BlockChain Technology: Beyond Bitcoin, Applied Innovation Review, Issue No. 2 June 2016.

Folkinshteyn D., Lennon M., Reilly T.; A tale of twin tech: bitcoin and the www. Journal of Strategic and International Studies, 2015.

Gandal N., Halaburda H., Competition in the cryptocurrency market, Bank of Canada Working Paper, No. 2014-33, Bank of Canada, Ottawa, 2014.

Hanley B. P., The False Premises and Promises of Bitcoin, 2013.

Hughes E., A Cypherpunk's Manifesto, 1993.

Joancomart J. H., Research and Challenges on Bitcoin Anonymity, 9th International Workshop on Data Privacy Management. Springer. LNCS 8872, 2014, pp. 1-14.

Kelleher, T.S., Ripple's Overlooked Path to Decentralization. American Banker, <http://www.americanbanker.com/bankthink/ripples-overlooked-path-to-decentralization-1075603-1.html?pg=2>, 2015.

King S., Primecoin: Cryptocurrency with Prime Number Proof-of-Work, Mathematics of Computation Volume 37 Number 156, 2013.

Lemme G., Peluso S., Criptomoneta e distacco dalla moneta legale: il caso bitcoin, rivista dottrina e giurisprudenza commentata, Estratto dal n. 11, 2016.

Luther W. J., White L. H., Can Bitcoin Become a Major Currency?, George Mason University Department of Economics Working Paper No. 14-17, 2014.

Nakamoto S., Bitcoin A Peer-to-Peer Electronic Cash System, 2008.

Nirgunarthy, A., Bitcoin art from India. IHB, <https://ihb.io/2015-01-06/news/bitcoin-art-india-help-artisans-go-global-14956>, 2015.

Ngo. D., Commonwealth Bank of Australia to Integrate Ripple for Instant Settlements. Cointelegraph, <http://cointelegraph.com/news/114419/commonwealth-bank-of-australia-to-integrate-ripple-for-instant-settlements>, 2015.

Omarini A., Internet banking Dalla strategia multicanale alla ridefinizione della value proposition in banca, Economia&Management n° 1, 1999.

Pilkington M., Blockchain Technology: Principles and Applications, University of Burgundy, France, 2016.

Plassaras N. A., Regulating Digital Currencies: Bringing Bitcoin *within the Reach of the IMF*, Chicago Journal of International Law, Volume 14, Number 1 Article, 2013.

Prathyusha T., Kavya M., Sree P., Akshita L., Block Chain Technology, International Journal of Computer & Mathematical Sciences IJCMSISSN 2347 – 8527Volume 7, Issue 3, 2018.

Reid F., Harrigan M., An Analysis of Anonymity in the Bitcoin System, IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, 2011.

Rogojanu A., Badea L., *The issue of competing currencies. Case study – Bitcoin*, Theoretical and Applied Economics Volume XXI, No. 1(590), 2014, pp. 103-114.

Rothbard M., *A Genuine Gold Dollar vs Th Federal Reserve*, Ludwig von Mises Institute, 2016.

Rothbard M., *Man Economy and State with Power and Market*, Ludwig von Mises Institute, 2009.

Saper, N., International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*, 2013, pp. 673-88.

Salleo C., *Bitcoin: profili economici*, BCE, 2015.

Sinha A., *Bitcoins: a super bubble ready to burst*, FIIB business review, Issue 3, 2014.

Yermack D., *is bitcoin a real currency?*, nuber working paper no. 19747, 2013.

Vigna P., Casey M., *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*, Picador, 2015, pp. 242-243.

World Bank, *Achieving Universal Financial Access by 2020* (Overview),

<http://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020.print>, 2015.