IL PROTOCOLLO BITCOIN: ANALISI STORICA TRASVERSALE

a cura di

Lorenzo Ciccone

Tesi di laurea in

Economia e Management

Luiss Guido Carli

2015

Approvata da Chiar. Mo Prof. Stefano ZA

Relatore

Programma autorizzato
di laurea _____

Data _____

SOMMARIO

INDICE DELLE FIGURE

Numero *Pagina*

David: "Is this the game or is it real?"
Joshua: "What's the difference?"

(Wargames – 1983)

Capitolo 1

1.1. La nascita della moneta, del baratto e del concetto di debito

La storia della moneta, secondo la tradizione, ebbe inizio in Lidia, nel VII secolo a.C., quando il re Creso coniò l'Elettro, una moneta in lega di oro e argento, rivoluzionando così il sistema di scambi commerciali per tutti i secoli a venire. Dall'Asia Minore l'uso della moneta si diffuse in tutto il mondo greco mediterraneo: Roma ne ereditò l'uso e la introdusse nei paesi confinanti del Nord Italia e del Nord Europa.

In realtà è possibile ravvisare l'idea (e dunque il tentativo) di istituire un protocollo di scambio più complesso del semplice baratto già nel 5000 a.C., in Mesopotamia. I sumeri, infatti, possedevano già la conoscenza della scrittura ed i loro sacerdoti designarono il metallo (in particolare i metalli preziosi) come la merce più adatta per gli scambi, avendo oro e argento il pregio di mantenere costante il loro peso nel tempo. Si cominciarono a barattare così i prodotti con oggetti informi (pezzi di metallo a foggia di anelli, rozzi pani di bronzo, bastoni a punta) chiamati dagli studiosi "Premonete".

È interessante osservare, a livello antropologico, la tesi di David Graeber (2012): "Non abbiamo cominciato col baratto, per poi scoprire la moneta e alla fine sviluppare un sistema di credito. È successo proprio l'opposto. Non è il baratto la categoria fondante delle economie e delle società umane, bensì il debito[1]".

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

Non per caso, infatti, le prime forme di scrittura ritrovate in Mesopotamia, datate oltre 5.000 anni fa, furono tavolette d'argilla su cui i sacerdoti dei templi registravano i debiti dei contadini. L'ammontare del debito era commisurato a quantità di grano o di argento che fungevano da "moneta virtuale".

Il problema dello scambio differito nel tempo nasce ancor prima della necessità della "doppia coincidenza di bisogni", caratteristica del baratto. Il debito si basa sulla fiducia e sulle relazioni sociali; il baratto è, per gli studiosi di antropologia, un fenomeno marginale che per lo più si attua con gli stranieri. Passando dalla storia all'etnografia, ritroviamo molte società in cui, tuttora, una parte importante dell'economia si basa sul dono e sul debito reciproco. Il classico sistema proposto da Adam Smith viene così rovesciato: il debito e i sistemi creditizi sono all'inizio della storia, ancor prima del baratto.

1.2. Le funzioni della moneta, la fiducia come fondamento del valore di essa

Tre sono le funzioni della moneta:

1) Unità di conto: è l'unità di misura del valore dei beni da scambiare; in questo modo tutti i beni in oggetto vengono misurati con lo stesso metro;

2) Mezzo di scambio: funzione tramite la quale è possibile scambiare beni e servizi in qualsiasi quantità e tempo: ogni bene viene misurato e riceve un prezzo in base alle unità di moneta necessarie per acquistarlo;

3) Riserva di valore: la moneta può essere conservata e utilizzata nel futuro senza che si deteriori in senso fisico o nel suo potere d'acquisto.

Normalmente gli strumenti impiegati come moneta non sono beni di consumo per chi li riceve. Questo vale per la carta-moneta, ma anche per l'oro, il cui impiego come bene intermedio o di consumo è assai limitato.

La ragione per la quale queste monete vengono accettate in pagamento risiede nella fiducia di chi le riceve che altri faranno altrettanto, accettando in pagamento monete, banconote, depositi bancari o titoli di stato.

Senza tale fiducia difficilmente una moneta sarebbe accettata in pagamento e neppure il corso legale di una moneta, ovvero l'obbligo di accettarla in pagamento, potrebbe molto contro il rischio di trovarsi in mano carta straccia o un deposito bancario inutilizzabile.

1.3. Le monete alternative: alcuni cenni

La moneta come conosciamo oggi è detta moneta fiat, o moneta a corso legale, intendendo uno strumento di pagamento non coperto da riserve di altri materiali (ad esempio riserve auree), e quindi privo di valore intrinseco (anche indiretto). Questa possiede un valore grazie al fatto che esiste un'autorità statale che agisce come se avesse questo valore. Se un'organizzazione abbastanza grande emette, usa e accetta qualcosa come pagamento, automaticamente quel qualcosa acquisisce valore, dato che è riconosciuto come mezzo di scambio.

La moneta legale, totalmente svincolata dalla quantità di metalli preziosi, ha dunque valore in quanto mezzo di pagamento stabile riconosciuto nell'economia di un certo paese: la sua stabilità è garantita dal controllo sull'emissione da parte delle banche centrali, in modo da controllare gli effetti inflattivi dell'emissione di moneta in relazione alla crescita del paese. Il suo riconoscimento come mezzo di pagamento è inoltre garantito dalla legge.

Tuttavia, fin dal medioevo, nei momenti di crisi, o in periodi di intensa e rapida evoluzione dell'economia, è sorta la necessità di utilizzare monete diverse da quelle a corso legale per far fronte a molteplici problematiche quali iperinflazione, cattiva gestione da parte della banca centrale, carenza di liquidità, perdita del potere d'acquisto, guerre e molto altro. Talvolta questa iniziativa è presa da gruppi di persone con interessi comuni od organizzazioni, altre volte anche dalle istituzioni. La moneta a corso legale viene così sostituita, in tutto od in parte, da altre forme di valuta che vengono riconosciute, accettate ed utilizzate all'interno del gruppo. Affinchè un sistema monetario o di credito e scambio alternativo si possa sviluppare si rende necessaria perciò l'esistenza di alti livelli di solidarietà e di stima reciproca tra coloro che la usano, dato che tale moneta non ha corso legale ed è accettata solo su base volontaria[2] (Margrit Kennedy, 1995). Il carattere volontario della accettazione delle monete alternative si fonda in genere anche su principi e valori condivisi di salvaguardia del valore delle persone e dei patrimoni ambientali, naturali e culturali di una comunità, in quanto si intenda radicata in un proprio territorio.

Oggi nel mondo esistono più di cinquemila valute complementari ed alternative, ma la complementarietà non è una pratica di recente invenzione. Verranno qui esposti alcuni casi (storici e non) a titolo esemplificativo.

Tra il XII e il XVIII sec. in Francia vi erano i Méreaux, degli oggetti monetiformi realizzati con materiali poveri, emessi da soggetti o comunità senza diritto di battere moneta e validi in determinati acquisti o territori. Persino i gettoni di frequenza distribuiti nelle chiese potevano essere sfruttati per acquistare abiti, cibo o servizi. Nello stesso periodo il Doge di Venezia creò il Ducato immaginario per sopperire alla carenza di oro, dando vita ad una "banca di trasferimenti" che registrava le transazioni locali. Essa contribuì a generare

[2] M. Kennedy. (1995), "*Il denaro libero da interessi ed inflazione"*, Arianna Editrice, Trieste.

la ricchezza rinascimentale e forse sarebbe attiva tuttora. Purtroppo le armate svizzere bruciarono gli archivi dopo 500 anni di attività.

Passando a tempi più recenti, lo Wir è un sistema indipendente di valuta alternativa, creato in Svizzera per aiutare le piccole e medie imprese durante la crisi del 1929, e che ora copre un sesto delle transazioni svizzere: 1,1 miliardi di euro nel 2013.

Il Toreke è la moneta istituita e finanziata dalla città belga di Gand. Il progetto del Toreke è volto al conseguimento di opere sociali e ambientali, tramite la riqualificazione degli spazi urbani e la creazione di un grande giardino comunitario. L'affitto annuale di un appezzamento pubblico è di 150 Torekes (15euro) che possono essere guadagnati attraverso varie iniziative, come la attività socialmente utili o le giornate di lavoro collettivo, per poi essere spesi nel giardino comune, per i trasporti pubblici, o nei negozi partner.

In tutta Italia è oggi in rapida diffusione l'Arcipelago Scec che, proprio come il Toreke e l'Epi, non punta solo a contribuire all'economia locale, ma a responsabilizzare l'individuo e rafforzare il senso di comunità. La cooperazione e l'indipendenza dal potere d'acquisto ripartito in euro, lo rendono accessibile alle fasce più svantaggiate della popolazione, contribuendo alla riduzione della povertà e dell'emarginazione sociale.

A Milano le istituzioni stesse promuovono il Lombard, in Sicilia il Turi, a Napoli il Napo. A Brescia dal 2001 è invece attivo il BexB, un progetto che oggi accomuna 2.700 imprese italiane su 160 diversi settori. Uno strumento che consente di acquistare beni e servizi pagandoli con il proprio prodotto o servizio, senza utilizzare denaro. Sullo stesso principio, in Sardegna, il Sardex vanta una rete di 1500 imprese e 15 milioni di euro di scambi nel 2013.

1.4. Le criptovalute digitali: una moneta alternativa?

Le "alternative currencies" sono nate a centinaia negli ultimi decenni, queste sono in genere legate a forme di attivismo politico e a dichiarate finalità sociali, come istituire circuiti locali di scambio, creare comunità, porre rimedio alla mancanza di liquidità e alla scarsità del credito, a volte anche accelerare la circolazione attraverso meccanismi che disincentivano la tesaurizzazione.

Nello stesso periodo in cui le monete alternative (ma reali) hanno avuto una diffusione sempre maggiore, cioè dopo lo scoppio della crisi economica del 2007, un altro mezzo di pagamento alternativo assimilabile ad una moneta ha visto la luce, crescendo con rapidità e diffondendosi a livello mondiale: il protocollo Bitcoin[3].

Le monete virtuali, e il Bitcoin in particolare, hanno una natura del tutto differente, e per certi versi opposta rispetto alle monete alternative. Se queste ultime mirano a "rilocalizzare" l'economia, il Bitcoin si propone come uno strumento per "globalizzare la moneta", abolendo la problematica dicotomia tra un sistema di scambi globalizzato e il carattere ancora nazionale dei mezzi di pagamento.

Tuttavia, nonostante la direzione che le monete virtuali hanno preso, la diffusione del Bitcoin sembra poggiare, almeno in parte, su circuiti e principi di attivismo politico non troppo lontani da quelli che hanno promosso altre forme di moneta alternativa.

Una recente ricerca di J. Bohr e M. Bashir (2014)[4] ha messo in evidenza quanto la motivazione politica contribuisca all'adozione del Bitcoin. Una metà circa

[3] È doveroso specificare che un primo concetto di criptomoneta digitale era già stato teorizzato da David Chaum nel 1983 (D. Chaum, *Blind signatures for untraceable payments)* e messo in pratica dallo stesso nel 1989, con il progetto *"Digicash",* a cui parteciparono anche Credit Suisse, Deutsche Bank, Bank Austria, la svedese Posten AB e la St. George Bank in Autstralia. Il progetto è fallito nel 1998.

[4] J. Bohr e M. Bashir, 2014. *Who Uses Bitcoin? An exploration of the Bitcoin community*.

degli intervistati (47%), che si definisce "libertarian", vedendo nel Bitcoin uno strumento di liberazione dal potere pubblico, che permette di aggirare regolamentazioni e divieti, in un orizzonte che può arrivare a comprendere la "dissoluzione dello Stato" e l'instaurazione del "primo vero libero mercato della storia".

Ciò che però può sorprendere è che una parte minoritaria, ma non irrilevante, degli utilizzatori della criptovaluta si definisca socialista (9%), ecologista (7%), genericamente progressista (17%), o anche anarchica (7%). A prevalere, in questo caso, sono gli effetti di disintermediazione del Bitcoin, visti come limite al potere delle banche, identificate come responsabili della crisi e delle devastazioni sociali che ne derivano.

Le analogie con le valute alternative si esauriscono nella diffusione ancor limitata del mezzo, e della matrice ideologica che, almeno alla base, ha generato i due fenomeni. Come sarà spiegato a breve, le finalità e la portata del fenomeno che l'istituzione del protocollo Bitcoin porta con sé, va ben oltre questi orizzonti.

Capitolo 2

2.1. Il protocollo Bitcoin: un'analisi storica trasversale

Come sarà possibile osservare, il protocollo Bitcoin non è solo un sistema di pagamento, ma molto di più: è un'idea rivoluzionaria di potenza dirompente, uno strumento utile ed applicabile in tantissimi ambiti, una potenziale (ma brillante) soluzione a numerosi problemi del mondo attuale.

Ciò che questo scritto si propone di fare è una analisi storica di tipo trasversale, partendo dall'ideazione del protocollo, nel 2008, fino ad arrivare al presente. Saranno trattati nella maniera più ampia ed approfondita possibile tutti gli aspetti economici, monetari, sociali, tecnologici che hanno favorito la diffusione di questo sistema, come anche tutti i cambiamenti che questo ha generato all'interno dei suddetti ambiti.

2.2. La nascita di Bitcoin[5]: Satoshi Nakamoto

Il 18 agosto 2008 viene registrato il nome di dominio bitcoin.org su anonymousspeech.com. Il 31 ottobre dello stesso anno viene pubblicato il documento in cui viene presentata ufficialmente al pubblico la nuova criptovaluta. Il titolo del documento è "Bitcoin P2P e-cash paper" e viene pubblicato su "The Cryptography Mailing List" del sito metzdowd.com. Il 9

[5] È necessario precisare che, convenzionalmente, il termine Bitcoin maiuscolo si riferisce alla tecnologia ed alla rete mentre il minuscolo bitcoin si riferisce alla valuta in sé.

novembre il progetto Bitcoin viene registrato sulla risorsa SourceForge.net. L'autore del documento si firmò con lo pseudonimo di Satoshi Nakamoto[6].

Ad oggi non è stato possibile verificare se dietro a questo nome si nasconda una persona[7] o un gruppo di persone (spesso definito "collettivo"). Nakamoto ha continuato a collaborare con altri sviluppatori del software Bitcoin fino a metà del 2010. Dopo questa data, ha consegnato il controllo del codice sorgente a Gavin Andresen, il suo collaboratore più stretto fino a quel momento, e ha trasferito diversi domini di sua proprietà a vari membri prominenti della comunità Bitcoin interrompendo, di fatto, il suo coinvolgimento nel progetto. Le registrazioni delle transazioni Bitcoin mostrano che i portafogli di Nakamoto contengono circa 1 milione di Bitcoin.

2.2.1. Il protocollo Bitcoin

Il 3 gennaio 2009 vede la luce il primo blocco Bitcoin (il cosiddetto "genesis block"). Vengono generati 50 BTC. Si rende necessario spiegare dettagliatamente come avviene la produzione dei bitcoin e come il sistema ideato da Nakamoto sia un gioiello sia per la genialità[8] del meccanismo che soggiace al suo funzionamento, sia per la sua semplicità disarmante che tuttavia non trascura in alcun modo la sicurezza.

Per comprendere il funzionamento di Bitcoin, è necessario innanzitutto conoscere quali sono le regole entro le quali il protocollo opera. L'idea sulla

---

[6] Idee simili (ma senza implementazioni P2P erano già state presentate da Wei Dai e Nick Szabo poco tempo prima (cfr. http://unenumerated.blogspot.it/2005/12/bit-gold.html). È possibile che dietro lo pseudonimo di Nakamoto vi sia almeno uno dei due ricercatori.

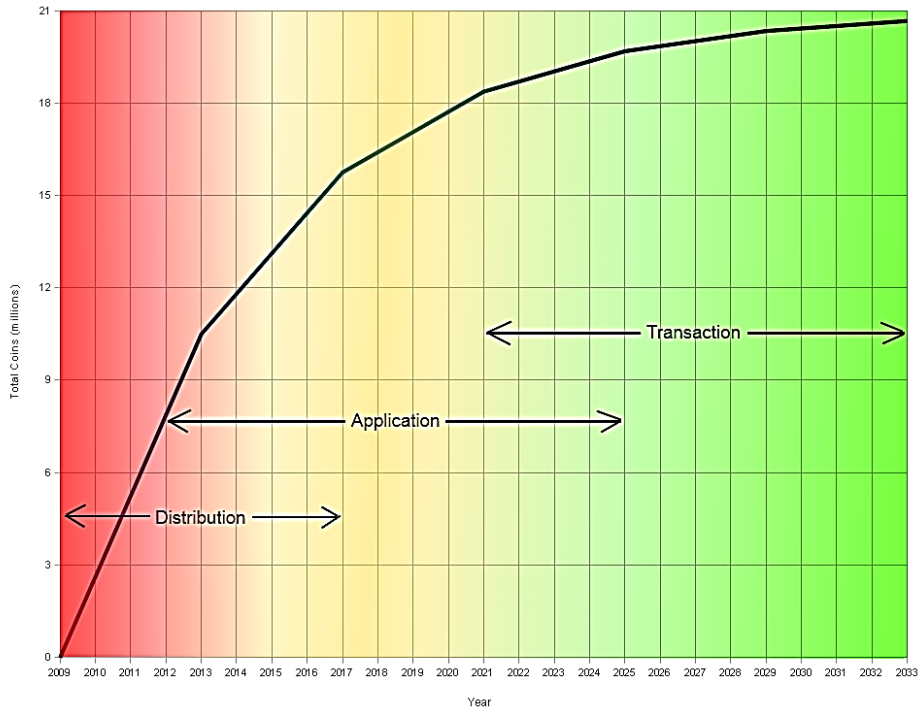
[7] Le teorie sulla vera identità di Satoshi Nakamoto sono numerose. In giapponese "Satoshi" significa "un pensiero chiaro, veloce e saggio". "Naka" può significare "medium, dentro o relazione". "Moto" può significare "origine" o "fondamento". Ma non è certo se questi significati siano utili da ricondurre alla persona o al gruppo di persone che ha inventato il sistema Bitcoin

[8] "*A stroke of genius*" come definito da D. Andolfatto, vice presidente FED della sede di St. Louis (31/04/2014)

quale Bitcoin è basato è che il sistema debba essere governato dalla scarsità, insieme al fatto che l'offerta di moneta sia fissa e dichiarata anticipatamente. Infatti, l'andamento della produzione di bitcoin è stabilito da un algoritmo con un andamento a rendimenti marginali decrescenti nel tempo.

La sua rappresentazione è esemplificata dal grafico[9] sottostante, che rappresenta su un asse gli anni di produzione dei bitcoin (2009-2033) e sull'altro i bitcoin che vengono assegnati (e prodotti) per il completamento di un singolo blocco.

Grafico 1: Le tre fasi della produzione dei bitcoin



Il numero totale di bitcoin tende asintoticamente al limite di 21 milioni. La disponibilità di nuove monete cresce come una serie geometrica ogni 4 anni; nel 2013 è stata generata metà delle possibili monete e per il 2017 saranno i tre quarti. All'avvicinarsi di quella data ed ipotizzando che la richiesta di bitcoin crescerà più che proporzionalmente rispetto alla disponibilità degli stessi, i

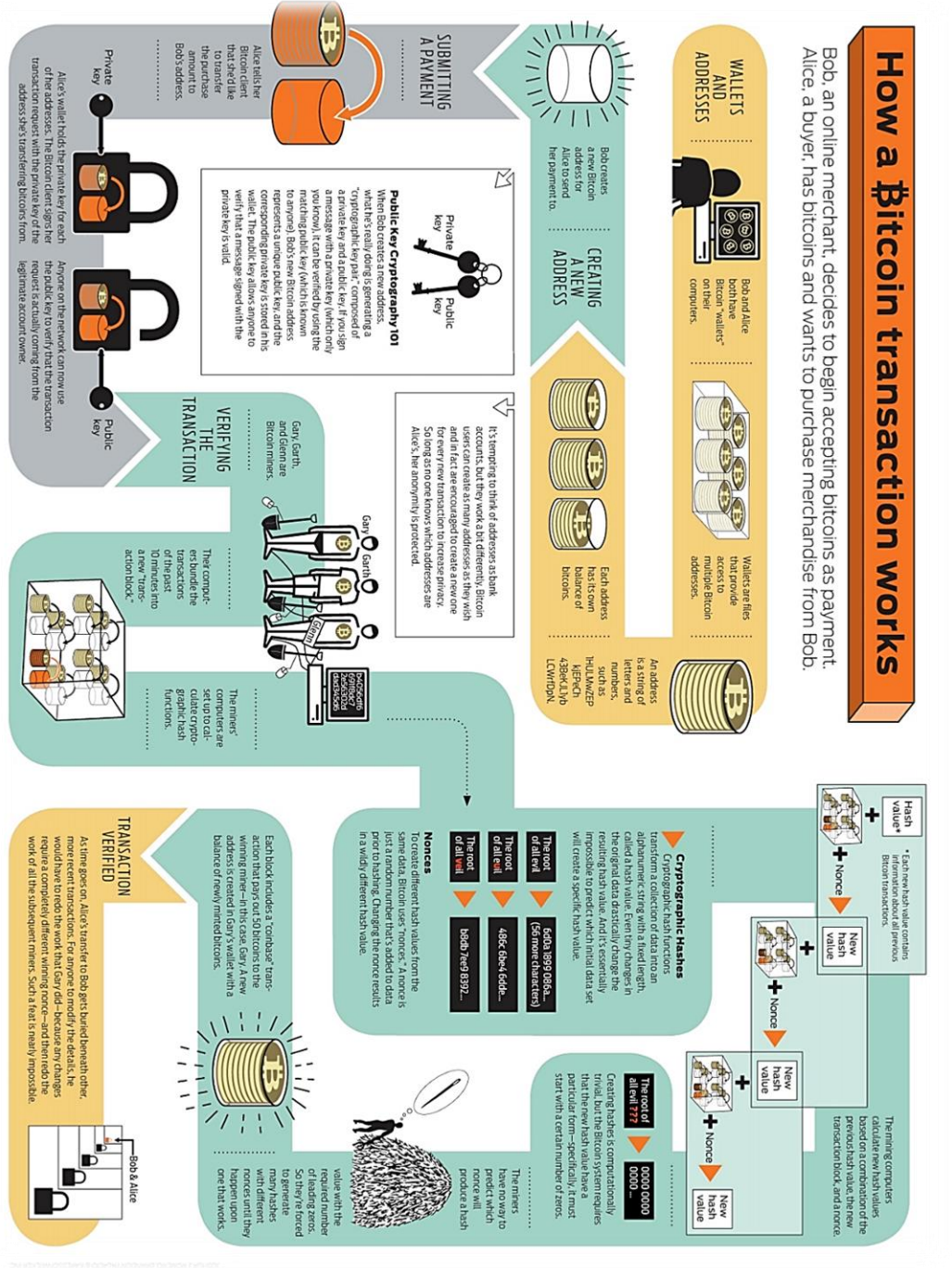
[9] Fonte: http://www.thebitcointrader.com/2011/10/three-stages-of-bitcoin.html

bitcoin probabilmente subiranno una deflazione nel valore (cioè un aumento del valore reale) dovuta alla scarsità di nuova moneta. Il grafico rappresenta inoltre, sommariamente, i tre livelli di adozione che la moneta presumibilmente avrà nel tempo.

Le transazioni tramite il protocollo Bitcoin avvengono attraverso un trasferimento da un "portafoglio[10]" ad un altro. Ogni volta che si effettua una transazione, il computer trasmette ai peer (i nodi più vicini) notizia della suddetta. Alla ricezione della transazione, ogni peer eseguirà una serie di circa 20 controlli per assicurarsi che la transazione è valida quindi inoltrarla a sua volta agli altri utenti. Attraverso questo processo la transazione verrà propagata in tutta la rete. Un "minatore" o "miner" è un peer nella rete che raccoglie le transazioni e opera per organizzarle in blocchi. Nei primi giorni di Bitcoin ogni utente è stato un minatore. Oggi, tuttavia, il mining è diventato redditizio solo per chi è disposto ad investire in una piattaforma hardware e software specializzata. Dopo che un minatore riceve e verifica una transazione, la aggiunge a un pool di memoria insieme a tutte le altre transazioni non confermate e comincia ad assemblarle in un blocco. Un tipico blocco conterrà circa due-trecento operazioni. Una volta che un minatore crea un blocco valido, egli lo trasmette alla rete. Ogni utente verificherà la sua validità aggiungendolo poi alla sua copia locale della Blockchain, il registro pubblico delle transazioni in bitcoin, che riporta in ogni momento tutti i movimenti tra portafogli fin dalla nascita di Bitcoin. La Blockchain è un registro unico e condiviso fra tutti gli utenti, riveste un ruolo centrale nel garantire la trasparenza, la sicurezza e la non falsificabilità dei pagamenti in bitcoin. Nella pagina successiva un diagramma illustrerà con migliore chiarezza quanto esposto.

[10] Il portafoglio è un indirizzo attraverso il quale si possono inviare e ricevere bitcoin. È composto da una stringa di 27-34 caratteri alfanumerici (es: 31uEbMgunupShBVTewXjtqbBv5MndwfXhb) e dalla chiave privata dell'utente necessaria per utilizzarlo. Gli utenti possono avere un numero arbitrario di indirizzi Bitcoin, infatti è possibile generarne a piacimento senza nessun limite in quanto la loro creazione costa poco tempo di calcolo (equivalente alla generazione di una coppia di chiavi pubblica/privata) e non richiede nessun contatto con altri nodi della rete. È stato calcolato che è possibile creare 10^{48} possibili chiavi diverse, e addirittura 10^{77} chiavi private.

Diagramma[11] – Come funziona una transazione in bitcoin?



[11] Il diagramma è stato elaborato da Joshua J. Romero, Brandon Palacio & Karlssonwilker Inc.

2.3. La Blockchain: un'analogia esplicativa

Il Bitcoin può essere accostato alle monete di pietra dell'isola di Yap[12], gli enormi dischi di pietra perforati (Rai) che gli abitanti dell'isola del Pacifico usavano come mezzo di pagamento in alcune importanti transazioni, come matrimoni, eredità, affari politici, alleanze, riscatto dei morti in battaglia o solo per uno scambio di cibo. Le pietre sono dischi circolari scavati nel calcare con un grande buco al centro. La dimensione delle pietre è molto variabile, le più grandi hanno un diametro di 3 metri, sono spesse 0,5 metri e pesano 4 tonnellate.

Figura 1 – I Rai, ancora esposti sull'isola di Yap

Il valore estrinseco (percepito) di una specifica pietra si basa non solo sulla sua dimensione e sulle modalità di produzione, ma anche sulla sua storia. Se molte persone - o nessuna - sono morte quando la pietra è stata trasportata, o se l'ha portata un noto marinaio, il valore della pietra Rai aumenta. A motivare questo singolare accostamento vi è la particolare modalità di trasferimento della

[12] Lo spunto è tratto da "Hidden Flipside", su "The Economist" del 15 marzo 2014.

proprietà delle pietre, che – essendo quasi inamovibili – cambiavano proprietario senza essere trasferite fisicamente, attraverso il riconoscimento pubblico della transazione incorporato in una storia orale, che tutti conoscono ma nessuno controlla. La principale fonte storica di notizie etnografiche è il libro di William Furness "The Island of Stone Money", pubblicato nel 1910. Ad attirare l'attenzione degli economisti sul Rai fu però John Maynard Keynes, che nel "Treatise on Money[13]"citò il trasferimento della sua proprietà come «il più antico esempio di "earmarking[14]"», mettendone in evidenza l'analogia con quanto accadeva per l'oro nei forzieri delle banche centrali. Keynes si soffermava anche sull'aneddoto secondo il quale una di queste pietre, pur sepolta in fondo al mare in seguito a un naufragio, continuava "in queste isole civilizzate" a essere annoverata nello stock di moneta.

Allo stesso modo, la Blockchain incorpora l'intero archivio storico di tutte le transazioni in Bitcoin, associando le transazioni ai rispettivi utenti che le hanno eseguite. Come sarà illustrato, questo sistema garantisce scambi eccezionalmente sicuri, trasparenti ed efficienti.

2.4. Il mining

I client che prendono parte alla rete in modo attivo, ovvero che contribuiscono tramite la propria potenza di calcolo alla gestione e alla sicurezza della rete stessa, ricevono in maniera completamente casuale un certo ammontare di monete all'incirca sei volte l'ora, distribuiti e creati dalla rete Bitcoin. L'attività di generazione di bitcoin viene spesso definita in maniera figurata come "mining", un termine analogo al "gold mining" (estrazione di oro). La

[13] J.M. Keynes *Treatise On Money* (1930), Vol. II, p. 292

[14] Il termine significa "attribuzione di una risorsa economica". L'analogia con l'"earmarking" dell'oro è ripresa, tra gli altri, da James Tobin per la voce Money del *"New Palgrave Dictionary of Money and Finance"* (1992) e da Milton Friedman in *"Money Mischief"* (1992); quest'ultimo utilizza anche l'esempio del Rai per confutare la «fallacia metallista», la credenza cioè che ogni moneta debba consistere in (o rappresentare) una merce dotata di valore intrinseco.

probabilità che un certo utente riceva la ricompensa in monete dipende dalla potenza computazionale che aggiunge alla rete relativamente al potere computazionale totale della rete. Le modalità attraverso le quali un utente partecipa al mining sono diverse, e sono mutate nel tempo.

Qualsiasi minatore che crea un blocco valido viene premiato per il suo sforzo con i bitcoin appena creati. Il protocollo regola la velocità con cui si creano i Bitcoin. Attualmente, la ricompensa è fissata a 25 Bitcoin per blocco e viene pianificata per essere dimezzata ogni quattro anni, fino a quando il numero totale di bitcoin creato raggiungerà 21 milioni. Con la progressiva riduzione della ricompensa di generazione nel tempo, la fonte del guadagno per i minatori passerà dalla generazione della moneta alle commissioni di transazione incluse nei blocchi, fino al giorno in cui la ricompensa cesserà di essere elargita: da allora l'elaborazione delle transazioni verrà ricompensata unicamente dalle commissioni sulle transazioni stesse.

Tutti i nodi della rete competono per essere i primi a trovare una soluzione ad un problema crittografico che riguarda il blocco candidato, un problema che non può essere risolto in altri modi che tramite bruteforce[15] e che quindi richiede sostanzialmente un enorme numero di tentativi. Quando un nodo trova una soluzione valida l'annuncia al resto della rete attribuendosi contemporaneamente i bitcoin in premio previsti dal protocollo, i nodi che ricevono il nuovo blocco lo verificano e lo aggiungono alla loro catena, ricominciando il lavoro di mining al di sopra del blocco appena ricevuto.

Dal punto di vista tecnico il processo di mining non è altro che un'operazione di hashing[16] inverso: determinare un numero (nonce) tale per cui l'hash SHA-

[15] Il metodo bruteforce è un algoritmo di risoluzione di un problema dato che consiste nel verificare tutte le soluzioni teoricamente possibili fino a quando si trova quella effettivamente corretta. Il suo principale fattore positivo è che consente teoricamente sempre di trovare la soluzione corretta, ma per contro è sempre la soluzione più lenta o dispendiosa.

[16] L'hash è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

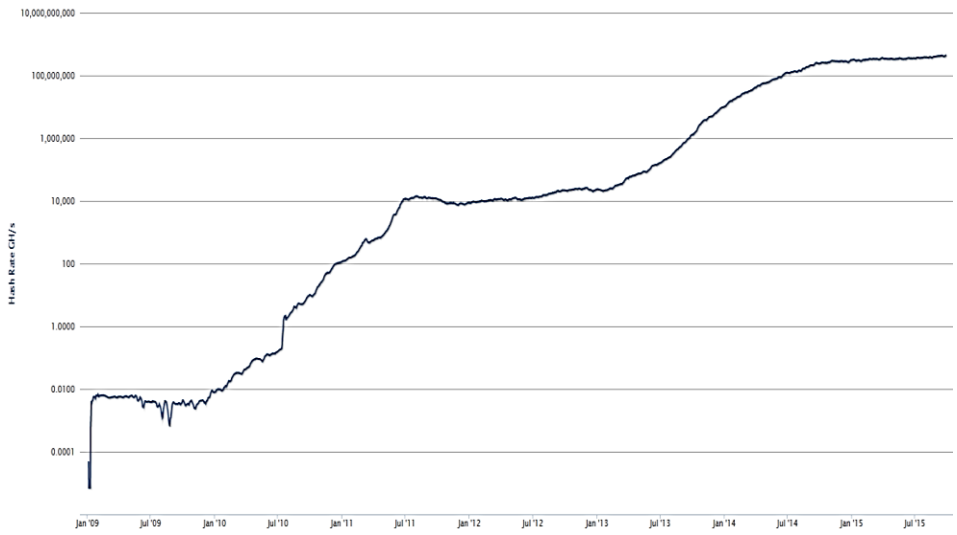
256[17] di un insieme di dati rappresentante il blocco sia inferiore ad una soglia data. Questa soglia, chiamata per l'appunto difficoltà, è ciò che determina la natura concorrenziale del mining di bitcoin: più potenza di calcolo viene aggiunta alla rete bitcoin e più questo parametro aumenta, aumentando di conseguenza il numero di calcoli mediamente necessari a creare un nuovo blocco e aumentando quindi il costo di creazione dello stesso, spingendo così i nodi a migliorare l'efficienza dei loro sistemi di mining per mantenere un bilancio economico positivo. L'aggiornamento di questo parametro avviene ogni 14 giorni circa, dimensionandosi in modo che un nuovo blocco venga generato in media ogni 10 minuti.

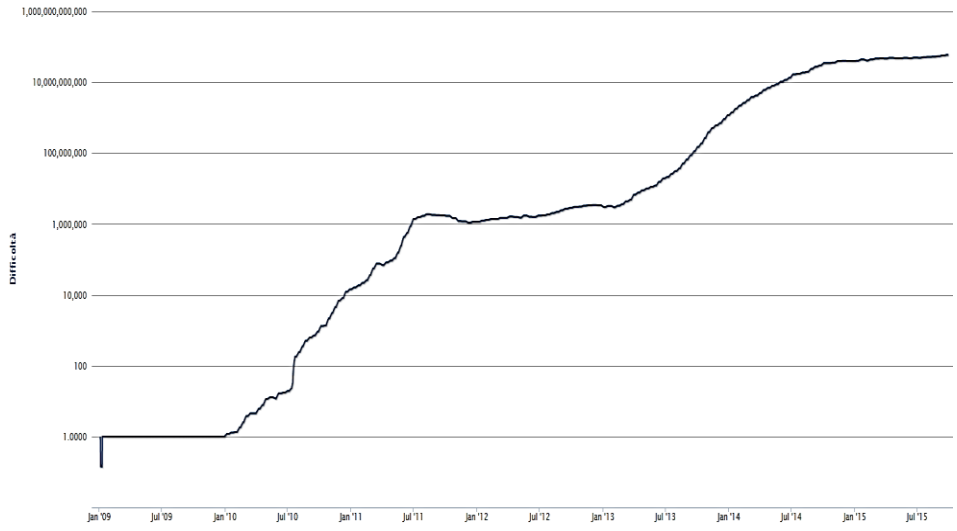
Il grafico sottostante mostra l'andamento della curva di difficoltà dalla nascita del Bitcoin ad oggi (2015). È possibile notare l'andamento costante (e di bassa difficoltà, proporzionale alla potenza computazionale dell'epoca) nel primo anno di adozione, la consistente crescita fino alla metà del 2011, una nuova stasi fino alla metà del 2013 e nuovamente una crescita da quel momento in poi. Confrontando i Grafici[18] è evidente il fatto che, al crescere della difficolta del mining imposta dal sistema, gli utenti si siano immediatamente adeguati, aumentando di numero o aggiungendo proporzionale potenza di calcolo. Infatti i due grafici hanno sostanzialmente il medesimo andamento, sintomo del rapporto costante fra le due variabili e della partecipazione attiva degli utenti al sistema.

[17] La sigla SHA sta per Secure Hash Algorithm, che in questo caso produce una stringa di 256 bit.

[18]In alto l'hash rate ed in basso la difficoltà. Fonte: https://blockchain.info/it/charts

Grafici 2 e 3 - Confronto dell'andamento di hashing rate e difficoltà nella blockchain





2.5. Le tappe iniziali dell'implementazione del protocollo Bitcoin

Il 9 gennaio 2009 è la data del rilascio della prima versione, Bitcoin 0.1. Le versioni dalla 0.1.0 fino alla 0.1.5 sono supportate solo da Windows 2000, Windows NT e Windows XP. Subito dopo il primo rilascio, Nakamoto perfeziona il client, corregge alcuni errori di comunicazione con i nodi e con alcuni collaboratori lavora per migliorare l'usabilità del client. Il 12 gennaio viene eseguita la prima transazione Bitcoin (blocco 170 della Blockchain). Il mittente è Satoshi Nakamoto, il destinatario Hal Finney[19]. Il 5 ottobre viene pubblicato il tasso di cambio del Bitcoin rispetto al dollaro sul mercato: $1 = 1,309.03 BTC. Vengono avviate le negoziazioni sul mercato New Liberty Standard.

Quasi un anno dopo, nel dicembre 2009 appare Bitcoin 0.2.0. Supporta Linux e la community inizia a partecipare attivamente allo sviluppo. Inoltre, questa nuova versione ha reso possibile l'utilizzo di più processori per la generazione dei blocchi. Fino a quel momento si poteva creare solo un processo se si utilizzava un processore multi-core come Core Duo o Quad, la nuova release permetteva invece di raddoppiare o quadruplicare la produzione.

In questo periodo, Bitcoin è conosciuto da un gruppo molto ristretto di early adopters. Il 22 maggio viene effettuato il primo acquisto online tramite bitcoin. Un utente chiamato "laszlo" offre 10.000 BTC (in quel momento pari a 50 dollari) a chiunque gli avesse comprato due pizze[20]. Nell'estate del 2010, venne rilasciato Bitcoin 0.3. Dal giorno successivo al rilascio, il 12 luglio, in cinque giorni il tasso di cambio della criptovaluta cresce di 10 volte: da 0.008 $/BTC a 0.08 $/BTC. Il numero di utenti inizia a crescere così come la difficoltà del

[19] Sviluppatore di videogiochi e crittografista, recentemente scomparso (2014).

[20] Data la sconvolgente crescita di valore che i bitcoin ebbero dopo breve tempo, la comunità si è interessata con spirito umoristico alla vicenda: esiste infatti il "Pizza "Index", che esprime il valore odierno dei bitcoin spesi per l'acquisto nel caso in cui fossero stati venduti piuttosto che spesi per le pizze. L'indice ha toccato 12,4 milioni di Dollari a novembre 2013.

mining. Con l'aumentare della potenza di calcolo totale della rete e a seguito della natura competitiva della generazione di bitcoin, il solo uso della CPU è diventato antieconomico ed è stato eliminato. Ad oggi esistono programmi specializzati che inizialmente sfruttano la potenza delle GPU[21] e delle FPGA[22], od utilizzano hardware dedicato basato su processori ASIC progettati appositamente per questo utilizzo. Dal momento che la quantità di operazioni mediamente necessarie a chiudere con successo un singolo blocco è diventata talmente elevata da richiedere grandi quantità di risorse in termini di energia elettrica e potenza computazionale, i miner hanno iniziato ad organizzarsi in gruppi o "pool" in modo da poter condividere le ricompense in modo più uniforme. Il 27 novembre del 2010 fa la sua comparsa Bitcoin Pooled Mining (BPM), meglio conosciuta come Slush's Pool, operante con una strategia di condivisione dei profitti che utilizzava una difficoltà ridotta artificialmente.

Il 17 luglio, intanto, viene creato un altro mercato, Mt.Gox[23]. Il 6 novembre la capitalizzazione del bitcoin ammonta a 1 milione di dollari USA. Il tasso di cambio della criptovaluta sul mercato Mt.Gox raggiunge la quotazione di $0.50/BTC. Il 9 febbraio 2011, il valore del bitcoin è pari a quello del dollaro. Il grande salto, a questo punto, è compiuto. Bitcoin si fa conoscere fra una vasta platea di piccoli investitori, banche, testate giornalistiche e appassionati, crescendo in valore di circa un ordine di grandezza ogni anno.

Nelle pagine seguenti saranno analizzati nel dettaglio gli sviluppi più recenti e, ambito per ambito, sarà possibile osservare come Bitcoin abbia influenzato (o perlomeno messo in discussione) il modo di concepire il denaro e tutte le attività legate ad esso.

---

[21] Graphic Processing Unit, anche detta scheda grafica.

[22] Acronimo per Field Programmable Gate Array, un circuito integrato le cui funzionalità sono programmabili via software. Tali dispositivi consentono l'implementazione di funzioni logiche anche molto complesse, e sono caratterizzati da un'elevata scalabilità.

[23] Questo sarà affrontato approfonditamente più avanti nella trattazione, in quanto MtGox è stata protagonista, nel 2013, di un grosso crack che ha portato alla bancarotta la società e alla dissoluzione di centinaia di migliaia di bitcoin.

Capitolo 3

3.1. Bitcoin e i Mercati

Come è stato già illustrato, Bitcoin ha iniziato a quotarsi su New Liberty Standards nel 2009, al tasso di cambio[24] con il dollaro USA di 1,309.03 bitcoin per dollaro. La prima grande piazza per lo scambio di bitcoin, Mt.Gox, viene fondata il 17 luglio 2010 da Jed McCaleb[25]. Il cambio in quella data era 0,08 $ per bitcoin.

Il 27 marzo 2011 viene lanciata una piazza di cambio tra bitcoin e sterlina britannica. Pochi giorni dopo, il 31 marzo, Bitcoin Brazil apre un servizio per lo scambio in Reais Brasiliano e in dollari USA. Il 5 aprile, BitMarket.eu viene inaugurato per supportare operazioni in euro ed altre valute. Insieme, essi hanno favorito il possesso e lo scambio di bitcoin e hanno dato la possibilità di fare trading a centinaia di milioni di nuovi utenti, espandendo enormemente il mercato.

Un giorno importante per la comunità è stato il 28 novembre 2012, anche detto "Halving Day" o "Giorno del Dimezzamento". In linea con l'algoritmo che governa la produzione dei Bitcoin, il numero di monete che i minatori ricevono come ricompensa subisce la prima riduzione (da 50 a 25), cominciando il lungo e graduale processo di diminuzione della quantità di nuova moneta che viene immessa nell'economia. Il dimezzamento è pianificato per avvenire ogni

[24] Essendo una comunità ristretta e senza molti punti di riferimento per l'epoca, nel corso del 2009 il tasso di cambio è stato calcolato dal sito come segue: si è diviso un dollaro per la quantità media di energia elettrica necessaria per mantenere operativa ad un alto livello di carico di lavoro una CPU per un anno, (1331.5 kWh), moltiplicato per il costo medio dell'energia elettrica residenziale negli Stati Uniti per l'anno precedente (0,1136 $) diviso per 12 mesi, diviso per il numero di Bitcoin generati dal computer negli ultimi 30 giorni.

[25] Jed McCaleb è un programmatore conosciuto soprattutto per la creazione della rete peer-to-peer eDonkey nel 2000. Mt.Gox è basato su un progetto precedente finalizzato a creare una piazza di scambio online per il gioco di carte "Magic: The Gathering", e successivamente convertito.

quattro anni circa, fino a quando la ricompensa avrà valore 0 (nel 2140) a fronte di un'offerta[26] fissa e definitiva di denaro corrispondente a 20,999,999.9769 BTC. Il tasso di cambio nell'Halving Day è 12,25 $ per bitcoin.

Pochi mesi dopo, la crisi cipriota[27] del marzo 2013 fa impennare il prezzo dei bitcoin, e la stampa internazionale nonché la Banca Centrale Europea si occupano per la prima volta delle criptovalute digitali con la dovuta importanza. Il presidente di Cipro, Nicos Anastasiades, l'Eurogruppo, la Commissione Europea, la BCE e il Fondo Monetario Internazionale organizzano un piano di salvataggio da 10 miliardi di Euro nella speranza di consolidare l'economia cipriota, ormai sul lastrico. Tra le condizioni imposte, tuttavia, una considerevole parte del denaro raccolto sarebbe dovuta provenire dai conti bancari con pacchetti azionari oltre i €100.000. Ciò costituì una seria preoccupazione non solo per ricchi ciprioti, ma anche per molti stranieri, in particolare russi, che avevano approfittato delle politiche favorevoli di Cipro (configurandolo, di fatto, alla stregua di un paradiso fiscale).

Alla ricerca di soluzioni per conservare i loro averi prima che il prelievo forzoso avvenisse, i correntisti iniziano ad acquistare bitcoin in massa, facendo impennare i tassi di cambio per tutto il mese successivo, da un valore di circa 80 $ a oltre 260 $.

Nel novembre 2013, nel giro di meno di una settimana il prezzo di bitcoin (salito nel frattempo oltre i 600 $) compie un incredibile balzo, raddoppiando nuovamente il suo valore, arrivando, il 30 del mese, a 1075 $. Le principali motivazioni di questa impennata nel valore non sono da ricercarsi nei mercati, né in iniziative private, bensì nelle dichiarazioni governative di USA e Cina di quei giorni.

[26] Questo processo di inflazione prestabilita è delle principali cause di controversie sul Bitcoin, riguardo al suo apprezzamento in valore ed ai comportamenti speculativi che può generare.

[27] Fonte: http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/.

Nell'udienza[28] dal titolo "*Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*", tenutasi il 18 novembre, il Governo Usa cerca di aprire un dibattito con la comunità bitcoin. Fin dall'inizio del procedimento, tuttavia, molti dei relatori e senatori[29] riconoscono le potenzialità di Bitcoin. Il 20 novembre, intervenendo ad un forum economico, Yi Gang (Vice Governatore della Banca Popolare Cinese e Direttore dell'Ufficio Statale dei Cambi) dichiara che "la gente è libera di partecipare al mercato Bitcoin", e che avrebbe "personalmente messo a punto un piano a lungo termine sulla valuta." La notizia[30] delle sue affermazioni fa entusiasmare il già molto attivo mercato bitcoin cinese, con la piazza più grande, BTC Cina, che inizia a registrare volumi commerciali più che doppi rispetto al secondo mercato più grande del mondo, il già citato Mt.Gox in Giappone.

La crescita rapida e costante degli investimenti in Bitcoin dalla Cina porta a prezzi sempre più elevati, raggiungendo il picco[31] di 1132.26 $ il 29 novembre. Sottoposti a severi controlli per quanto riguarda il movimento di denaro oltre i confini del paese e cercando un'alternativa per l'ormai troppo inflazionata moneta ufficiale, il Renminbi, i cittadini cinesi accolgono a braccia aperte la libertà offerta da Bitcoin. L'origine dell'interesse delle masse per Bitcoin in gran parte è dovuto alla One Foundation di Jet Li, che pubblicò il suo indirizzo Bitcoin per permettere di compiere donazioni a favore delle vittime del terremoto verificatosi 20 aprile 2013 nel distretto di Lushan, ricevendo oltre

---

[28] Tutti gli interventi sono disponibili a: http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

[29] Il consenso è espresso in particolare da Jennifer Shasky Calvery, direttore del Financial Crimes Enforcement Network del governo americano (FinCEN), che dichiarò "Vogliamo operare in maniera tale da non ostacolare l'innovazione." Le conclusioni del dibattito sono disponibili all'indirizzo: http://onbitcoin.com/2013/11/18/senate-committee-listens-bitcoin-experts-expresses-open-mindedness/.

[30] Fonte: http://sinosphere.blogs.nytimes.com/2013/11/22/bitcoin-gets-a-cautious-nod-from-chinas-central-bank/?_php=true&_type=blogs&_r=3.

[31] Per esplicitare in termini reali la crescita del valore di Bitcoin, si richiama il "Pizza Index" esposto nel capitolo precedente. Il 29 novembre, le due pizze pagate da laszlo avrebbero avuto un valore di più di 6 milioni di dollari ciascuna.

230 bitcoin (più di 250.000 $) in soli due giorni, insieme ad una copertura mediatica senza precedenti.

Pochi giorni dopo, la Banca di Cina inizia a imporre le prime restrizioni in risposta alla popolarità crescente di Bitcoin, dichiarando che il bitcoin non deve essere considerato una valuta[32]. Il cambiamento di politica vieta a qualsiasi istituto finanziario di commerciare, assicurare o offrire servizi comunque legati a Bitcoin. Nel corso delle settimane seguenti, ulteriori restrizioni lentamente strangolano i mercati cinesi delle criptovalute, mentre i gli operatori cercano affannosamente nuovi, fantasiosi modi per compiere scambi nel tentativo di rimanere operativi. I prezzi, a livello mondiale, picchiano pericolosamente. Poco tempo dopo, Mt. Gox, Bitstamp e BTC-e[33] vedono crollare la loro operatività a causa di massicci attacchi DDoS[34], apparentemente finalizzati a sfruttare alcune falle nel software che gestisce le transazioni. Mt.Gox, già da tempo in piena espansione, è costretto a sospendere l'operatività il 6 febbraio, negando di fatto la possibilità agli utenti di accedere alla piattaforma per prelevare il proprio denaro e contribuendo in maniera consistente ad un'ulteriore ribasso del prezzo dei bitcoin (717 $); l'attacco DDoS è stato rilevato solo il 11 febbraio 2014. Dopo l'attacco, ormai in ginocchio, Mt.Gox è costretta ad oscurare il sito senza una dichiarazione ufficiale. Gli altri siti che si occupano di trading di Bitcoin stilano una dichiarazione congiunta[35] che condanna la cattiva gestione di Mt.Gox, gridando all'inganno ed ipotizzando la corruzione dei vertici della società, accusandoli di averla portata al collasso, dopo che un documento interno ha lasciato trapelare che all'interno della

[32] Il New York Times diede ampia risonanza alla notizia: http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html.

In seguito il dibattito sulla vera natura di Bitcoin (asset o valuta) sarà approfondito maggiormente.

[33] Due famose piazze di scambio nell'Europa dell'est.

[34] Un attacco Distributed Denial of Service (DDoS) è il tentativo di rendere non disponibile un servizio online tentando di saturarne il traffico con una enorme quantità di richieste di connessione, provenienti da molteplici sorgenti.

[35] Disponibile al sito: https://blog.coinbase.com/2014/02/25/joint-statement-regarding-mtgox/

società erano spariti, e dunque persi per sempre, 744.000 bitcoin. Il tasso di cambio per quel giorno (il 24 febbraio 2014) è 547.09 $. Un ulteriore colpo è assestato dalle banche cinesi il 10 aprile. In aggiunta alle già citate restrizioni la Banca di Cina ordina che venga interrotto lo scambio di bitcoin, imponendo ai vari mercati operanti in Cina di chiudere i loro conti entro il 15 aprile. Anche se alcuni hanno seguito le direttive, il contesto normativo incerto consente di procedere attraverso metodi alternativi che praticamente tutti gli scambi cinesi hanno adottato rapidamente. Le piattaforme di trading cinesi continuano a funzionare, ma a volumi notevolmente ridotti dal loro periodo di massimo splendore. Il valore di bitcoin a metà del 2014 è intorno ai 400 $. Toccando i 610 $ il 17 luglio, si assiste all'ultimo balzo di prezzo, che si è stabilizzato, da quel momento in poi, tra i 250 e i 300 $ senza subire variazioni consistenti. Un periodo così lungo di relativa stabilità dei prezzi non era osservabile dal semestre maggio-novembre 2013. Probabilmente l'entusiasmo si è ridotto, la bolla speculativa è scoppiata, la corsa all'investimento e all'adozione è rallentata. Si è passati in un certo senso, forse ad un periodo più "maturo". Ora sarebbe opportuno cercare di consolidare la fiducia in bitcoin, mantenendo il più possibile stabile il suo prezzo favorendo così il suo avviarsi verso l'essere una riserva di valore più affidabile. Verranno inseriti alcuni grafici esplicativi dell'evoluzione del valore di cambio di Bitcoin, del tasso di crescita della Blockchain e della difficoltà crescente del mining. È abbastanza facile identificare la maggior parte degli eventi precedentemente esposti con le "creste" e le "conche" che l'indice compie nel tempo (Grafico 4[36]). Altrettanto intuitiva è la tendenza della Blockchain a crescere di dimensioni ad un tasso quasi esponenziale nel tempo (Grafico 5[37]).

[36] Immagine tratta da http://www.zerohedge.com/news/2014-03-12/complete-annotated-price-history- bitcoin

[37] Fonte: https://blockchain.info/it/charts

Grafico 4 – Valore storico del Bitcoin in Dollari 2010-2014 (fino al crollo di Mt.Gox)

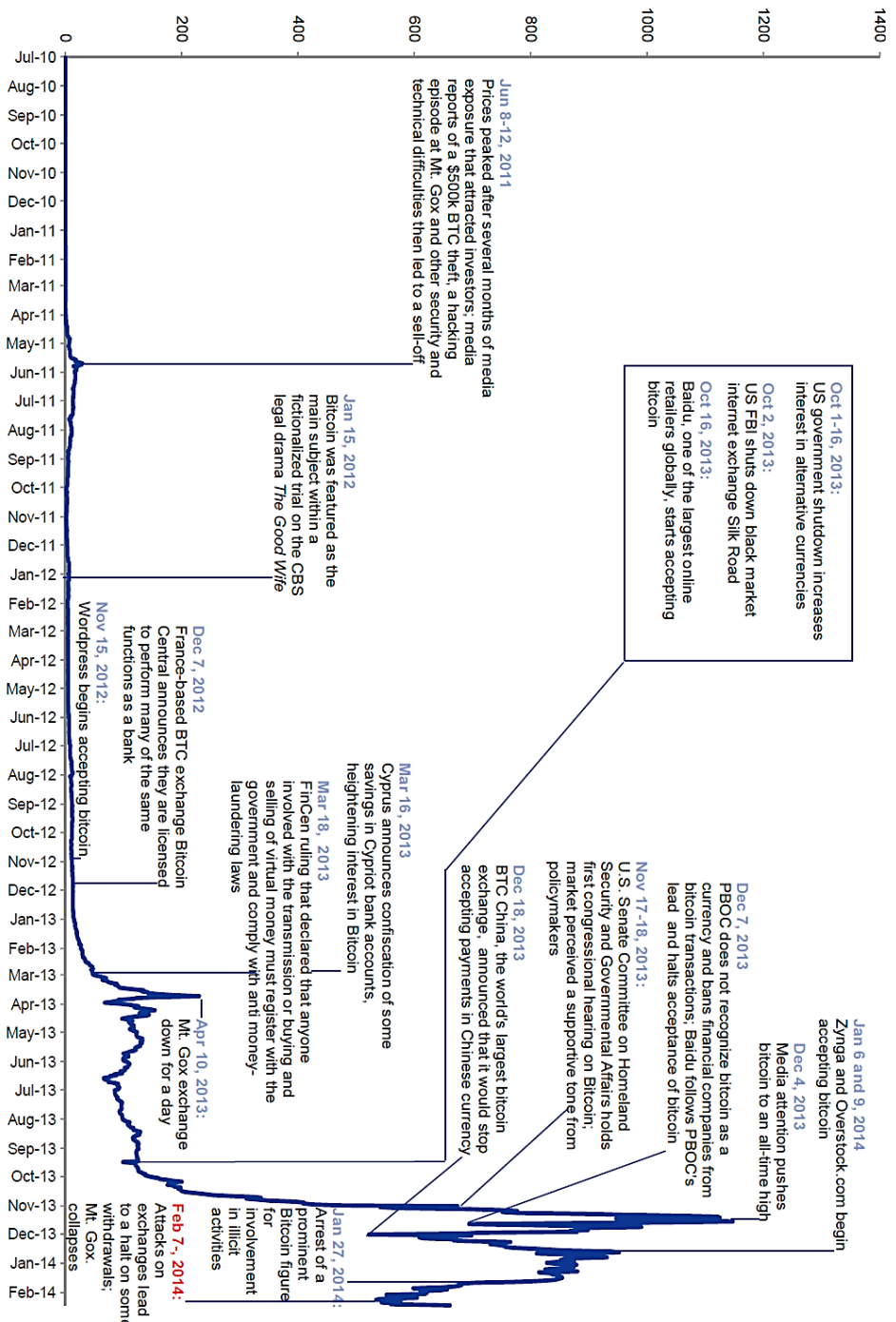
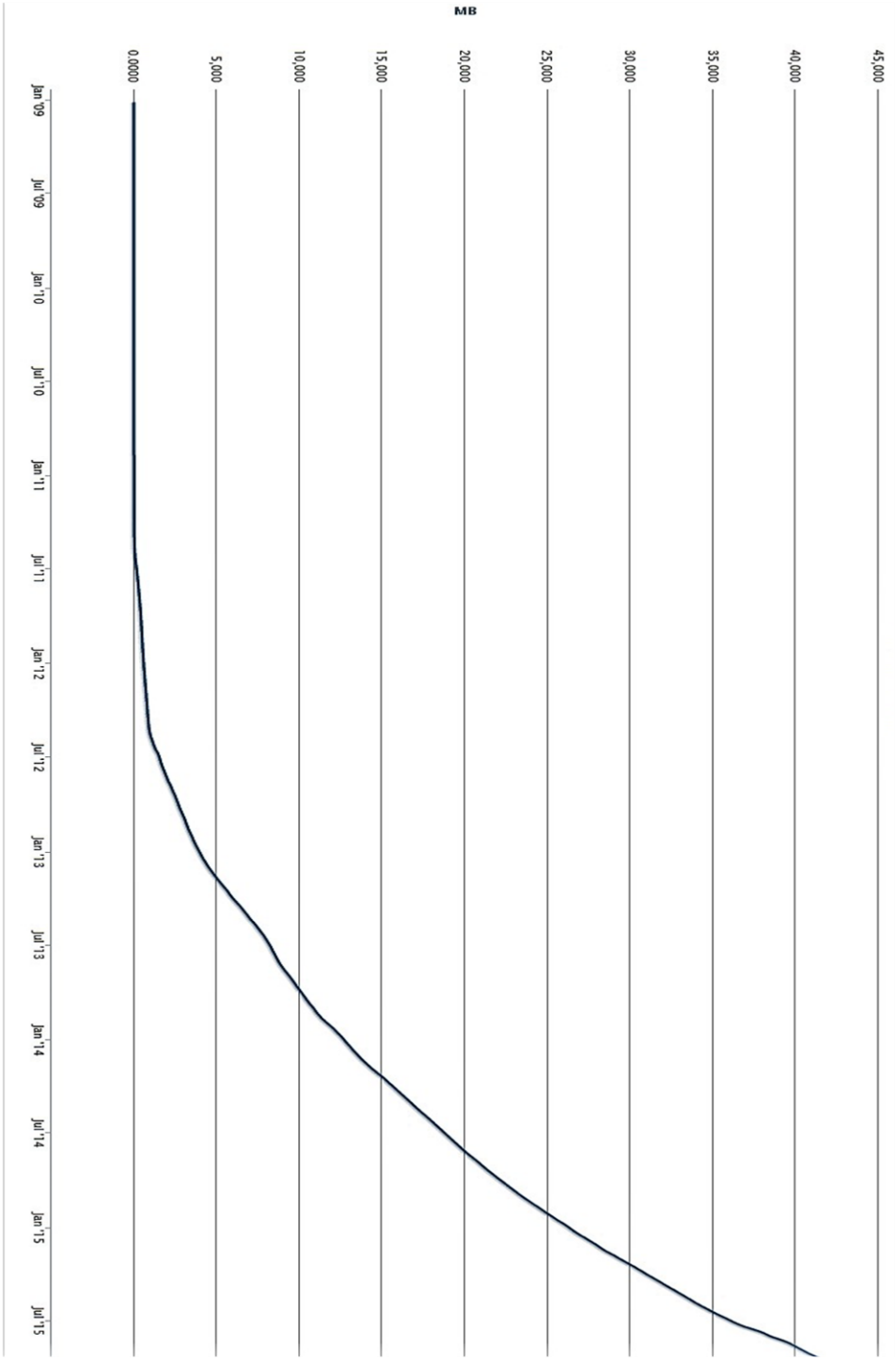


Grafico 1 – La dimensione della Blockchain nel tempo

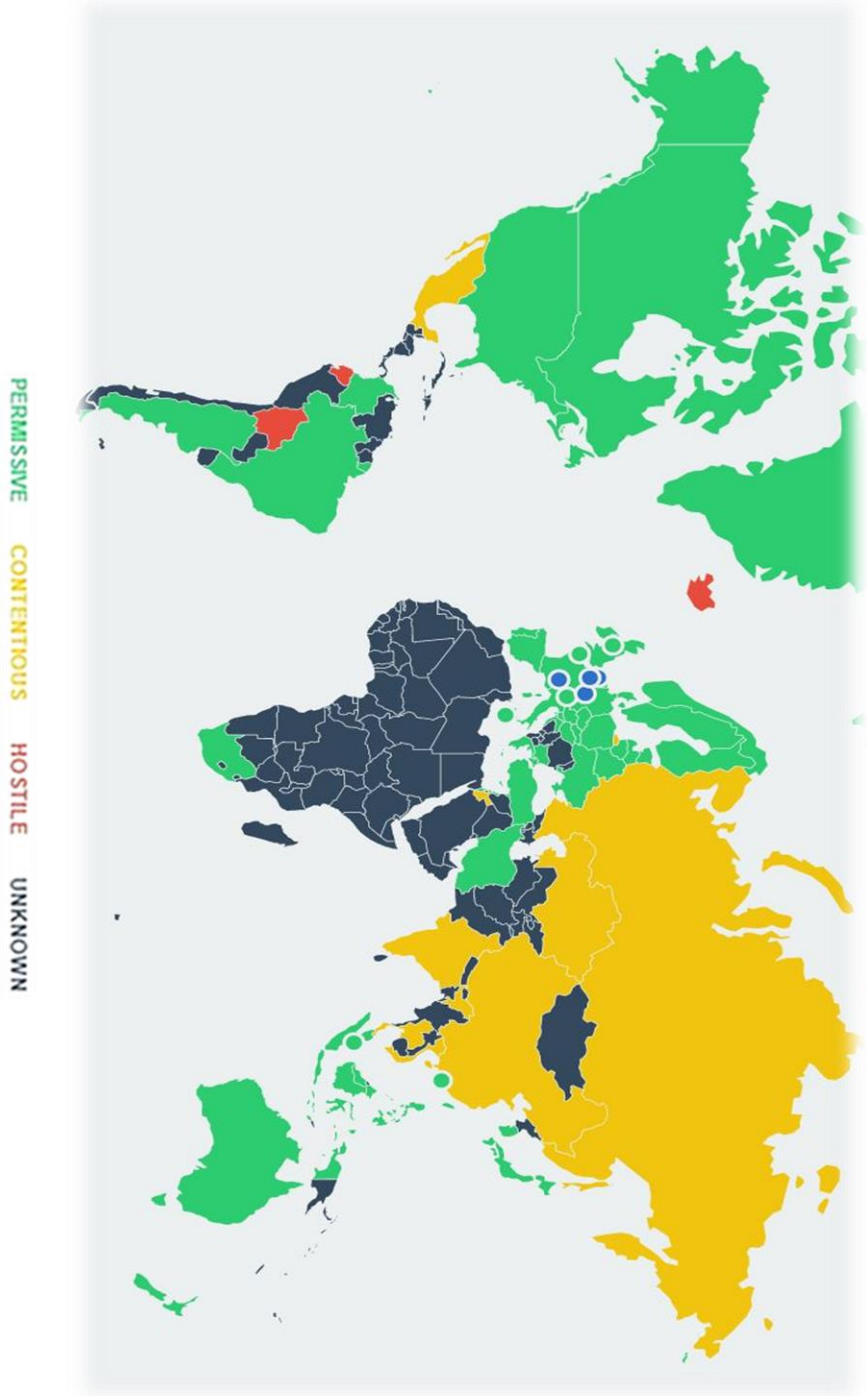


3.2. Bitcoin e le istituzioni: analisi storico-comparativa

Come è stato già accennato, Bitcoin è una moneta che non dipende per il suo valore o la sua validità da alcun ente emittente: è generata da un sistema, non da una Banca Centrale, non c'è alcun sottostante, nessuna garanzia di un ente certificatore. Ciò è completamente nelle mani di coloro che possiedono i bitcoin, oltre che nella fiducia che essi stessi mostrano nei confronti del sistema e degli altri utenti. Al sopraggiungere di una certa massa critica di utenti, e del fatto che i media hanno ad un certo punto puntato drammaticamente i riflettori sul Bitcoin, gli stati nazionali (almeno i più avanzati) sono stati costretti a fare dichiarazioni ed interventi al fine di tentare di controllare il fenomeno, cercando di comprenderlo e gestirlo. È quindi possibile confrontare quali paesi si siano mossi per prima in questo senso, ed è utile, inoltre, verificare e paragonare quali misure e quali posizioni siano state prese dai singoli stati in merito a Bitcoin. La carta tematica[38] nella pagina seguente mostra, a grandi linee, le posizioni assunte a livello mondiale riguardo alla detenzione e al commercio in bitcoin.

[38] Fonte: http://www.merkletree.io/

Figura 2 - Planisfero tematico: La posizione dei vari governi del mondo rispetto a Bitcoin



Come è possibile osservare, i paesi più aperti nei confronti di Bitcoin sono gli stati europei e delle due Americhe, seguiti da Australia, Indonesia e Giappone. Russia, Cina, India ed altri paesi asiatici consentono l'uso di Bitcoin solo sotto particolari restrizioni[39]. Pochi paesi si dichiarano apertamente contro le criptovalute. Nel continente africano[40], sebbene non vi siano dati disponibili, il bitcoin è diffusamente usato dalla popolazione, che usa il proprio portafoglio digitale alla stregua di un conto in banca (un vero conto in banca ha costi proibitivi per la maggior parte della popolazione).
Nel dettaglio, le questioni fondamentali su cui gli stati generalmente si sono espressi sono 4:

A. La legalità del possesso di bitcoin

B. La legalità dell'acquisto di bitcoin

C. La legalità delle transazioni in bitcoin

D. La legalità del mining

In linea puramente generica, tutti i paesi classificati come "permissivi" riconoscono la legalità di tutte e quattro le operazioni[41].

Tra i paesi che operano con restrizioni, la Cina[42] ha limitato il possesso dei bitcoin ai soli soggetti privati, specificando che è possibile possedere e utilizzare Bitcoin per operazioni commerciali "a proprio rischio". In Russia, il governo

---

[39] Come già detto, in Cina (dal 10 aprile 2014) gli intermediari finanziari non possono detenere o commerciare bitcoin.

[40] Ad esempio il Kenya ha recepito molto bene l'innovazione portata da Bitcoin, applicandola all'ingegnoso sistema di transazioni mobile mPesa, introdotto nel 2006, creando TagPesa e bitPesa, due criptovalute compatibili col sistema preesistente.

Fonte: http://cointelegraph.com/news/113639/kenya-adopts-bitcoin-with-bitpesa-tagpesa-and-m-pesa

[41] L'unica eccezione degna di nota è la Francia, che specifica che le compagnie di trading operanti in Francia devono operare solo previa autorizzazione dalla Banca centrale, oppure appoggiandosi ad una società per la gestione di fondi registrata. Cfr. ACPR (Banque De France) – 29 Janvier 2014

[42] PBOC (People's Bank of China) Bank Notice No. 239 [2013]

ha programmato di istituire entro la fine del 2015 multe per chi compie ciascuna delle 4 azioni sopra riportate ed ha oscurato i siti della maggior parte delle società di trading di bitcoin. Apparentemente, al momento, non è legale possedere bitcoin, non è sicuramente legale acquistarne o commerciarne, e probabilmente sarà reso sanzionabile anche il mining. Il governo, la Banca di Russia e il Ministero delle Finanze si sono unanimemente pronunciati contrari all'uso delle criptovalute, censurando ed ostacolando in ogni modo la loro diffusione[43]. L'India, d'altro canto, vanta un vuoto legislativo consistente in materia. L'unico documento prodotto dalla Reserve Bank of India è una nota di avvertimento, emanata a dicembre 2013. Nonostante la dichiarazione si pronuncia con parere negativo in merito alle azioni sopracitate, questa non ha avuto seguito, secondo la precisa intenzione di non regolamentare (per ora) il fenomeno. Bitcoin pertanto, non è illegale nel paese, e non vi sono particolari restrizioni all'acquisto salvo quelle che i commercianti si sono imposti autonomamente in via precauzionale, in merito alla quantità e al tipo di transazioni. In Messico, l'ultimo grande paese dove la situazione è ancora incerta, il vuoto legislativo è ancora più marcato. Nessun documento o comunicato è stato emanato dal Governo o dalla Banca Centrale, ad oggi. Tutte le operazioni sui bitcoin sono ufficiosamente consentite, pur svolgendosi senza controllo. L'iniziativa privata[44] ha già fatto diversi passi in avanti senza che lo stato sia intervenuto, considerando, tuttavia, che quando il Governo si pronuncerà in materia la sua posizione sarà verosimilmente di stampo permissivo.

Tra i paesi che si dichiarano "ostili" al bitcoin è possibile trovare l'Ecuador[45] e la Bolivia (il bitcoin è considerato illegale tout court da specifiche leggi) e

---

[43] Fonte: https://www.cryptocoinsnews.com/russia-blocked-several-bitcoin-sites-preperation-russian-bitcoin-ban/

[44] Bitso, una società che cambia bitcoin con i pesos messicani, ha messo a punto un sistema integrato di POS, servizi online e supporto per i piccoli commercianti. Può contare su un ampio bacino di utenza ed è in crescita costante.

Fonte: http://www.coindesk.com/bitso-mexico-merchants-bitcoin-ecommerce/

[45] Tuttavia, lo stato sudamericano ha in programma di creare una propria criptovaluta in futuro.

l'Islanda, la cui situazione è più particolare e meritevole di attenzione. È consentito infatti possedere bitcoin, ma è vietato scambiarli con la valuta nazionale. L'economia islandese si sta ancora riprendendo dal tracollo finanziario del 2008, quando i banchieri portarono la nazione, tradizionalmente benestante, sull'orlo della bancarotta. Per evitare di far perdere valore alla propria moneta, dunque, il Governo ha stabilito che è possibile vendere bitcoin in cambio di valuta nazionale (facendo dunque entrare capitale nel paese ed apprezzare la Corona islandese) ma non l'operazione inversa, cioè vendere la valuta nazionale in cambio di bitcoin, impedendo di fatto il prodursi dell'effetto contrario, cioè un'uscita di capitali. A questa politica "protezionista" gli islandesi hanno risposto con la propria criptovaluta nazionale, Auroracoin[46].

Per quanto riguarda la rapidità che gli stati hanno dimostrato nel prendere posizione su Bitcoin, è possibile affermare che prima del 2012 praticamente nessun paese ha sentito la necessità di esprimere la propria opinione in merito al fenomeno. I primi passi sono stati mossi dal Brasile e dagli Usa[47], che hanno tentato, com'è ovvio, di ricondurre Bitcoin ad una fattispecie che fosse compatibile con qualcosa di già regolamentato. Ogni stato, a seconda delle interpretazioni, considera i bitcoin come un asset, una valuta virtuale, oppure come un bene digitale.

La Banca Centrale Europea classifica Bitcoin come una valuta virtuale decentralizzata e convertibile nell'ottobre 2012 pubblicando un case study dal

---

[46] Auroracoin nasce nel febbraio 2014, basandosi sul protocollo litecoin. Il suo inventore, anch'esso anonimo, ha deciso di pre-minare il 50% delle monete, per poi renderle disponibili equamente (ciascuno dei 330.000 abitanti ha potuto ricevere 31,8 auroracoin) a tutti i cittadini islandesi presenti all'anagrafe. Questo per facilitarne la diffusione anche tra le persone che non intenzionate a dedicarsi al mining. Quasi subito, Auroracoin è diventata la terza moneta alternativa per capitalizzazione di mercato con un valore di quasi 50 $. L'entusiasmo è presto scemato, con una picchiata fino al valore stabile di 0.02 $ in meno di due mesi dal suo lancio.

Fonte: http://coinmarketcap.com/currencies/auroracoin/#charts

[47] La CVM (Comissão de Valores Mobiliários), l'equivalente dell'italiana AGCM, si è pronunciata per prima sul tema, rispetto agli altri paesi, riconoscendo che Bitcoin funziona come una sorta di fondo di investimento o di titolo (2012). Gli USA considerano Bitcoin una moneta virtuale, secondo quanto stabilito dalla FinCEN Official Guidance, FIN-2013-G001 (18/03/2013).

titolo "Virtual Currency Schemes[48]",dove il Bitcoin è protagonista indiscusso, senza tuttavia emanare nessuna direttiva particolare. In Germania[49], un tribunale tedesco ha definito Bitcoin come un'unità di conto, tassato in modo diverso a seconda di chi lo usa e a che scopo. Il governo finlandese[50] ha stabilito che deve essere trattato alla stregua di una merce, dando tuttavia al Bitcoin un'esenzione fiscale sul valore aggiunto classificandolo come servizio finanziario. Il Servizio Pubblico Federale delle Finanze del Belgio ha stabilito che la criptovaluta è esente dall'imposta sul valore aggiunto. A Cipro, il Bitcoin non è controllato o regolato, ma non è illegale. Nel Regno Unito, il Financial Conduct Authority (FCA) ha espresso un parere molto positivo sull'argomento, auspicando che il contesto normativo sarà favorevole alla moneta digitale. L'Agenzia delle Entrate della Bulgaria ha recentemente implementato la criptovaluta con le leggi fiscali vigenti. A luglio 2014 la BCE sconsiglia (ma non vieta) alle banche europee di trattare in valute virtuali come bitcoin, fino a quando un regime normativo sarà posto in atto[51].

---

48 European Central Bank (October 2012). *Virtual Currency Schemes*. Frankfurt am Main: European Central Bank.

49 Fonte: http://www.cnbc.com/id/100971898

50 Kati Pohjanpalo (20 January 2014). "*Bitcoin Judged Commodity in Finland After Failing Money Test*". Bloomberg (New York)

51 "*EBA Opinion on virtual currencies*". European Banking Authority. 4 July 2014.

3.3. La vera natura di Bitcoin: spunti per la regolamentazione in Italia[52]

Si può dunque vedere che, negli altri paesi UE, in assenza di una guida centrale, i singoli paesi hanno sviluppato delle posizioni proprie sul Bitcoin. In Italia, si è iniziato a parlare di Bitcoin a livello mediatico durante la fase ascendente della bolla speculativa, sul finire del 2013. La Banca d'Italia si è pronunciata per tre volte del 2014 e nel 2015 divulgando avvisi ed avvertenze al fine di informare il pubblico sul rischio di riciclaggio, di volatilità e di sanzioni fiscali pur non vietando, nella sostanza, l'uso dei bitcoin. Non vi è un vero divieto neanche per gli intermediari finanziari, che possono operare con le criptovalute su richiesta del cliente, se opportunamente informato dei rischi. Bitcoin, dunque, in Italia è sostanzialmente consentito, anche se non è disponibile una definizione per inquadrarlo meglio.

Dal punto di vista della tassazione, è opportuno fare il punto su quale accezione di Bitcoin sarebbe meglio abbracciare, e quali effetti la scelta di ciascuna di queste accezioni comporterebbe, nonché quale livello di regolamentazione sarebbe più giusto adottare per non deprimere la circolazione delle monete nel paese, perdendo così un'importante occasione di crescita.

È necessario ricordare il fatto che Bitcoin nasce come forma di moneta sottratta al controllo (e alle possibilità di inflazione) da parte delle banche centrali, è una valuta nata dal mercato e decentralizzata che (almeno negli intendimenti dei fondatori) affonda le sue radici nella cultura anarchica della rete. Un tentativo o una proposta di regolamentazione andrebbe contro lo spirito stesso di Bitcoin, a priori. Tuttavia, dove lo Stato avverta che la moneta a corso forzoso si trovi in pericolo, ha solitamente la facoltà di intervenire per mettere in sicurezza la situazione. Fortunatamente, gran parte degli stati ha compreso le

[52] Per questo capitolo si è fatto ampiamente ricorso al paper di Paolo Luigi Burlone e Riccardo de Caria: "*Bitcoin e le altre criptomonete: Inquadramento giuridico e fiscale*", IBL Focus N. 234, (01/04/2014) disponibile a http://www.brunoleonimedia.it/public/Focus/IBL_Focus_234-De_Caria_Burlone.pdf

potenzialità di Bitcoin e sta operando in un regime di minima regolamentazione, cercando di favorirne la diffusione e attendendo di assistere a tutte le evoluzioni e gli usi che la società implementerà sul sistema Bitcoin e, soprattutto, sulla Blockchain. Paolo Luigi Burlone e Riccardo de Caria hanno cercato di "illuminare la strada" per una corretta interpretazione del fenomeno. Viene riportata, in forma ridotta, una sezione del loro paper[53] dedicata all'argomento.

[…] La prima accezione entro la quale viene naturale includere il Bitcoin è la categoria giuridica di denaro. Viene, infatti, impiegato tipicamente per soddisfare le quattro esigenze fondamentali che soddisfa il denaro, ovvero fungere da riserva di valore, mezzo di scambio, unità di conto e strumento per pagamenti futuri. In Italia come nel resto d'Europa e del mondo, non è di per sé vietato produrre e far circolare forme alternative di "denaro", ma i creditori possono legittimamente rifiutare tale denaro, ed esso non sarà di per sé valido per estinguere le obbligazioni tributarie. Dal punto di vista delle autorità statali è dunque impossibile che queste ultime lo considerino come denaro in senso tecnico. È facile, quindi, escludere questa prima possibile ricostruzione. […] La seconda ipotesi da considerare è la possibilità di ricondurre i Bitcoin alla categoria dei "prodotti finanziari": essi possono infatti essere estratti o acquistati anche con finalità di investimento dei propri risparmi, per guadagnare dall'atteso aumento di valore degli stessi. Ma anche i "prodotti finanziari" in senso tecnico sono soltanto quelli che ricadono in una definizione ufficiale, fornita in questo caso dal Testo Unico della Finanza, secondo il quale sono tali "gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria". Precisa inoltre il TUF: "i mezzi di pagamento non sono strumenti finanziari".

L'ultima via è quella che discende corretto inquadramento storico-giuridico del denaro tradizionale. Il denaro, come già detto, nasce come merce: una merce con delle caratteristiche particolari che lo rendono, per l'appunto, adatto ad essere impiegato per le quattro funzioni fondamentali sopra richiamate; ma pur sempre, originariamente, una merce. Bitcoin recupera in parte questa funzione originaria del denaro. Esso ha valore non perché il suo uso sia imposto

[53] Vedere nota precedente.

da una banca centrale, ma perché e solo fintantoché le persone e le aziende sul mercato decidono liberamente di attribuirgli valore. […] Pertanto, è possibile che l'inquadramento più corretto di Bitcoin sia anche il più semplice: esso è prima di tutto un bene, nel senso fatto proprio e definito dal codice civile: «sono beni le cose che possono fare oggetto di diritti» (art. 810 c.c.). Naturalmente si tratterà di un bene mobile, e soprattutto, per via della sua ricordata natura priva di qualunque supporto fisico, di un bene immateriale. […]

Per ora, per l'Italia, si possono solo fare ipotesi su come il fisco potrebbe trattare il Bitcoin. L' 11 giugno 2014 si è tenuta una interessante conferenza[54] a Montecitorio, per illustrare le caratteristiche delle criptovalute e, attraverso gli interventi di relatori dal campo dell'informatica, della macroeconomia e delle scienze delle finanze è stato possibile avanzare alcune di queste ipotesi. L'auspicio che ha permeato l'incontro è che l'eventuale l'intervento del Governo sia semplice e leggero, in maniera da non penalizzare i soggetti finali e gli utilizzatori che hanno iniziato, prima degli altri, a credere nel Bitcoin.

In particolare l'intervento[55] del Dott. R. Tudini[56], ha scandagliato ogni possibilità di tassazione (o non tassazione) dei bitcoin, offrendo un quadro (per quanto ipotetico) molto chiaro.

Cercando di qualificare il bitcoin dal punto di vista della moneta, la forma più simile alla valuta in oggetto, è la moneta elettronica[57]. Ma un vero e proprio emittente, così come è definito dalle direttive europee, non esiste. È il sistema ad emettere i bitcoin. Non esiste un credito verso un emittente, senza considerare inoltre che l'unità di conto dei due tipi di moneta è differente e la convertibilità dei bitcoin resta non regolata e non garantita. Partendo dalla

---

[54] 11 giugno 2014, Camera dei Deputati, Sala Aldo Moro: *"Bitcoin in Italia: quali opportunità per le "monete matematiche" nel nostro paese?"*

[55] Di cui le pagine seguenti sono una sintetica trascrizione

[56] Dottore commercialista presso lo studio "Tudini e Tudini Associazione Professionale" Via Quintiliano, 10 00136 Roma

[57] Intesa come il valore monetario memorizzato elettronicamente […] rappresentato da un credito nei confronti dell'emittente che sia emesso dietro il ricevimento di fondi.

definizione più semplice di moneta, è possibile intendere il bitcoin come mero mezzo di scambio, sebbene immateriale. È necessario distinguere due soggetti: "utente finale persona fisica" e "utente finale impresa[58]". Se l'impresa utilizza i bitcoin all'interno della propria attività, l'unica ragionevole possibilità è l'equipararli a delle valute estere e al trattamento fiscale loro riservato[59]. Il tutto a condizione, come da legge, che i bitcoin siano stati detenuti a fini speculativi[60] e per delle giacenze superiori ai "vecchi" 100 milioni di lire. Se invece non venissero qualificati come moneta estera, bensì come un titolo rappresentativo di merce vigerebbe lo stesso principio, ma la previsione relativa alla giacenza media delle valute estere non si applicherebbe in questo caso. In entrambi i casi i bitcoin sarebbero stati però assoggettati a imposta sostitutiva. Per l'IVA l'unico riferimento disponibile riguarda il governo svedese, che ha proposto un interpello (come già illustrato, assimilando il bitcoin a un servizio finanziario) per poter considerare i redditi in bitcoin esenti da IVA.
Il miner professionista è un altro soggetto che potrebbe creare un reddito di impresa. E dovrebbe essere (in via teorica) soggetto a tassazione, in quanto non produce bitcoin, ma li riceve in cambio di un servizio prestato. Il valore del bitcoin minati rappresenterebbe il corrispettivo del servizio prestato e concorrerebbe alla formazione del reddito d'impresa. Ai fini IVA, questo corrispettivo andrebbe assoggettato a normale imposizione.

Concludendo la sezione, e volendo parlare infine della reale esigenza di regolamentazione governativa di Bitcoin, saranno riportate tre esaustive citazioni di tre relatori che hanno preso parte alla conferenza, interpellati in merito a questa stessa questione.

---

[58] Intendendo l'impresa come l'utente finale che utilizza i bitcoin non come oggetto della propria impresa (altrimenti si parlerebbe di servizio di Exchange) ma come utilizzatore del servizio che riceve un pagamento a fronte della vendita di beni e servizi

[59] Secondo il quale i differenziali sui cambi concorrono alla formazione del reddito d'impresa. I bitcoin potrebbero essere assoggettati sotto voce "redditi diversi", che prevede la convenzionale tassazione delle plusvalenze e minusvalenze

[60] Intendendoli come bene immateriale detenuto senza intento speculativo non si potrebbe verificare la realizzazione di un reddito in capo al percettore e dunque non vi sarebbero riflessi fiscali.

Prof. Ferdinando Ametrano[61]

"*I rischi macroeconomici del bitcoin sono legati essenzialmente al rischio di svalutazione delle monete cosiddette tradizionali (Euro, Dollaro) che potrebbero portare a una crisi sistemica senza precedenti. I rischi di una crisi sistemica potrebbero essere evitati o perlomeno ridotti nel caso in cui i regolatori si dimostrassero non miopi, ma capaci di guidare la transizione."*

Prof. Franco Vatalaro[62]

"*Introducendo per la prima volta il concetto di concatenazione di dati non duplicabili, il protocollo Bitcoin rappresenta una fondamentale innovazione nella direzione di una "internet certificata" che travalica l'aspetto monetario oggi di moda: per non disincentivare questa tecnologia innovativa non è opportuno regolamentarla in una visione ristretta di tipo monetario.*"

Dr. Roberto Tudini[63]

"*L'utilizzo di bitcoin implica sicuramente dei riflessi fiscali importanti per tutti gli utilizzatori, le imprese utilizzano sempre di più bitcoin per pagamenti tramite internet, Bitcoin si scontra con una normativa che potrebbe già essere effettiva ma che nella pratica è molto complicata da applicare. Quindi auspichiamo un intervento normativo di semplice attuazione ed efficace controllo che possa risolvere questioni ancora aperte.*"

[61] Professore aggiunto all'università di Milano Bicocca e analista presso banca IMI.

[62] Docente presso l'Università di Roma Tor Vergata, dipartimento di ingegneria dell'impresa.

[63] Vedere nota 50

3.4. Le potenzialità inespresse di Bitcoin: uno sguardo al futuro

Guardando come il protocollo Bitcoin e la Blockchain sono configurati, e la loro odierna rappresentazione, possiamo dire che costituiscono un sistema con le seguenti proprietà:

- Trasparente
- Unico
- Non falsificabile
- Sicuro
- Certificato (pur senza un ente certificatore)
- Potenzialmente eterno[64]
- Concatenato
- Segmentabile (pur mantenendo l'unicità informativa)
- Irreversibile
- Universale
- Pubblico
- Pseudonimo (facoltativamente)

È possibile che tutte queste caratteristiche, così preziosamente racchiuse in un unico protocollo, possano esaurirsi solo nell'applicazione monetaria di Bitcoin? Di questi undici punti, la moneta[65]ne rispetta al massimo quattro (unicità, irreversibilità, non falsificabilità e certificazione). Il sistema Bitcoin, invece, ha dimostrato tutta la sua solidità sotto questo aspetto, e non solo: in meno di sei anni il sistema -senza sponsorizzazioni di governi o istituzioni finanziarie- è stato in grado di generare valore per miliardi di dollari[66], di coinvolgere milioni di persone e di interessare i governi del mondo intero, costringendone la maggior parte a pronunciarsi in merito. Il protocollo ha ben sopportato sia il pesante ostracismo della Cina (dove all'epoca il 20% del valore delle transazioni

[64] Perché distribuito su tutti i nodi della rete, che molto poco probabilmente spariranno "in un sol colpo", come si suole dire.

[65] Intesa nel senso più stretto, escludendo dunque gli strumenti finanziari.

[66] Nel periodo di massima espansione, il market cap di Bitcoin è arrivato a raggiungere l'equivalente dell'1% della massa monetaria mondiale M1 espressa in dollari.

giornaliere totali avveniva tramite bitcoin, e da dove provenivano circa l'80% dei volumi totali di scambi nel sistema) sia il fallimento, con frode oltretutto, del suo primo mercato di riferimento (Mt.Gox), dimostrando una resilienza[67] senza precedenti.

Bitcoin permette di scavalcare, potenzialmente, qualsiasi istituzione od authority che abbia un ruolo di intermediazione, di certificazione o notariale, sostituendo l'autorità centrale con una versione peer to peer, in tempo reale e crittograficamente sicura della stessa. In un certo senso, il lato monetario è solo il primo "esperimento" su cui si è voluto testare il funzionamento del protocollo.

[67] Perdendo, in sostanza, "solo" meno del 50 % del suo valore di mercato.

Capitolo 4

4.1. Oltre la moneta: le potenzialità della Blockchain

Senza la funzione monetaria che attualmente prevale nel sistema bitcoin, non verrebbe comunque meno la capacità transazionale che il sistema garantisce; anzi, si possono immaginare (per un futuro sia vicino, sia lontano) diversissimi casi d'uso, che potrebbero potenzialmente rivoluzionare il nostro vivere quotidiano ed il modo di rapportarci con le istituzioni e le autorità centrali. La società di investimento privato Ledra Capital[68] ha lanciato, meno di un anno fa, una curiosa sfida agli utenti di Twitter: immaginare tutti i possibili scenari in cui la Blockchain potrebbe innovare sensibilmente il sistema di gestione vigente oggi, ed i risultati sono andati molto oltre le aspettative.

La tabella[69] nella pagina seguente riassume i risultati dell'indagine. Come è possibile vedere, le applicazioni della Blockchain sono molto numerose, e la lista è in continuo aggiornamento. Alcune proposte sono nella pratica più complicate da realizzare di altre, ma tutte potranno essere di aiuto per garantire maggiore sicurezza ed efficienza nelle operazioni quotidiane di ogni cittadino. Molte delle idee proposte si possono racchiudere sotto il concetto di "smart contracts[70]". Si tratta di protocolli informatici che facilitano, verificano o rinforzano la negoziazione o l'esecuzione di un contratto, o che ovviano alla necessità di una clausola contrattuale. In questo modo molti tipi di clausole di un contratto possono quindi essere rese parzialmente o completamente automatizzate, auto-ottemperanti, o entrambe le cose. La finalità per i contraenti è fornire una protezione superiore al diritto contrattuale tradizionale e ridurre gli altri costi di transazione associati.

---

[68] http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

[69] Elaborazione propria su dati di Ledracapital.

[70] Termine coniato nel 1994 da Nick Szabo.

Tabella – I potenziali campi di applicazione della Blockchain

Strumenti finanziari, atti e modelli	Atti Pubblici	Atti Privati	Altri atti semi-pubblici	Titoli di proprietà su beni tangibili	Titoli di proprietà su beni intangibili	Altro
Valuta	Catasto	Contratti	Lauree	Ciavi di casa	Buoni sconto	Dati meteo
Private Equities	Pubblico Registro Automobilistico	Testamenti	Certificazioni	Chiavi stanza di albergo	Prenotazioni	Schede SIM
Public Equities	Registro delle Imprese	Crediti	Votazioni	Chiavi auto	Biglietti	Codici di sblocco armi
Obbligazioni	Database	Depositi presso terzi	Dati HR (salari, performance, risultati)	Chiavi auto a noleggio	Brevetti	Identità su rete GPS
Derivati (futures, forwards, swaps..)	Passaporti		Registri sanitari	Chiavi cassetta di deposito	Diritti d'autore	
Diritti di Voto	Certificati di Nascita		Registri contabili	Consegna spedizione	Marchi	
Commodities	Tessere Elettorali		Dati genetici	Registro scommesse	Licenze Software	
Registri Spese	Registro ispezioni sanitarie		Documenti di spedizione		DRM (Musica, Film, Libri)	
Registri Commerciali	Permessi di costruzione		Arbitrati		Domini	
Registri di Prestiti e Ipoteche	Fedine Penali					
Registri di Revisione	Licenza di porto di arma					
Crowdfunding	Registro prove indagini magistratura					
Microfinanza	Registro sentenze civili e penali					
Microbeneficienza	Contabilità di enti no-profit					

4.1.2. Smart Contracts

Ci sono attualmente due importanti progetti open source che lavorano per promuovere gli smart contracts: Codius ed Ethereum. Codius è stato sviluppato da Ripple Labs, che ha anche creato la sua propria moneta digitale chiamata, appunto, Ripple. Codius punta sull'interoperabilità tra una varietà di valute.

Per spiegare nella pratica il funzionamento di uno smart contract, ipotizziamo lo scenario una scommessa sportiva. Si dichiara che si desidera scommettere 10 Euro o l'equivalente in bitcoin su un determinato risultato, ammettiamo una vittoria della squadra X mentre un altro scommettitore sta scommettendo la stessa quantità di denaro sul risultato opposto, la vittoria della squadra Y. L'unico passo da fare per entrambi è depositare la scommessa su un conto "neutro" controllato dallo smart contract. Una volta finita la partita, è il protocollo stesso in grado di verificare il risultato finale, e di distribuire le vincite (ovvero la somma delle due scommesse piazzate), inviando al portafoglio dello scommettitore vincente il denaro in maniera automatica[71] e con costi di transazione quasi nulli.

Lo stesso principio è applicabile ai mutui (molto spesso la banca cede il proprio credito ad un terzo, ma il debitore continua a pagare la banca, con conseguenze ricarico dei costi di intermediazione) alle ipoteche, ai testamenti e agli acquisti on line. Se le due parti si accordano sotto la tutela di uno smart contract, entrambe corrono un rischio minore, con una conseguente riduzione dei costi. Gli istituti finanziari dovrebbero essere più disposti a correre rischi su soggetti che altrimenti non potrebbero ottenere prestiti.

Oltre ad ampliare le opportunità di ottenere credito, i contratti intelligenti consentono di dare l'accesso ad un sistema legale di qualità a prezzi inferiori,

[71] Essendo inoltre gli smart contracts fondamentalmente dei programmi, sarebbe molto facile aggiungere elementi per partecipare a scommesse più complesse, come le quote e le differenze di punteggio.

per persone che non potrebbero altrimenti essere in grado di accedervi. Potrebbe nascere un florido mercato di scambio di modelli di smart contracts, dotati di una flessibilità interna modulabile secondo necessità dall'acquirente.

4.2. Un esempio di uso alternativo della Blockchain: Augur[72]

Augur è una piattaforma decentralizzata ed open source per mercati predittivi. Si tratta di un'estensione del protocollo Bitcoin che ne preserva il collaudato codice sorgente e tutti gli standard di sicurezza. Ogni caratteristica richiesta per un mercato predittivo è ricostruito con operazioni di input/output nello stile di Bitcoin.

Un mercato predittivo è un luogo dove è possibile scommettere sui risultati degli eventi futuri. L'utente che prevede correttamente il risultato riceve un premio in denaro. Gli utenti (solitamente) danno valore al denaro, e sono perciò incentivati a stimare una previsione con la massima certezza possibile. Così, il prezzo di un mercato di previsione su Augur può essere un eccellente indicatore della probabilità che un evento si verifichi.

Storicamente, le caratteristiche richieste per un mercato previsionale sono:

– essere in grado di accettare scommesse, decidere sull'esito di un evento, e

poi pagare le puntate in base ai risultati verificatisi,

– essere un sistema centralizzato.

L'approccio migliore per aggregare le scommesse è di avere uno strumento affidabile e stabile nel tempo per registrarle: una Blockchain. In questo modo Augur elimina il rischio di controparte. Tutti i fondi, infatti, vengono gestiti sotto degli smart contracts, senza possibilità che una scommessa piazzata

[72] Tra le 25 startup più finanziate al mondo, con 4 milioni di fondi stanziati. In alpha fino al 25/15/2015. Tutti i dati e gli schemi per questa sezione sono stati ricavati da http://www.augur.net/ e dal loro whitepaper

correttamente non venga pagata. Augur supporta bitcoin, ethereum ed altre tra le criptovalute più diffuse.

4.2.1. Strategia e funzionamento

Sulla piattaforma, qualunque utente ha il potere di creare un mercato predittivo su qualsiasi evento futuro di suo interesse. Esso riceverà la metà delle commissioni di negoziazione delle scommesse relative all'evento da lui creato. Dopo il verificarsi dell'evento, il risultato corretto (ciò che è realmente accaduto) deve essere confermato per pagare le puntate agli scommettitori nel mercato. Invece di affidarsi a terzi[73], Augur invita i suoi utenti a riferire sul risultato, creando così un sistema di "consenso decentrato" Gli utenti che riportano il risultato dell'evento, ottengono anch'essi metà delle commissioni di negoziazione (sulla base del loro livello di "reputazione[74]"). Il sistema di reporting di Augur si basa sul concetto di "Punto di Schelling[75]". Essenzialmente, la serie di risultati forniti dagli utenti tenderà ad essere

[73] Da intendersi come qualsiasi sito di notizie o agenzia o fonte privilegiata.

[74] Su Augur vengono negoziate soprattutto tre tipi di currency: il bitcoin, ethereum e il REP, ovvero la reputazione di un utente sulla piattaforma: questa è in quantità fissa, determinata al lancio della piattaforma. Detenere REP consente all'utente riportare il risultato su un evento, dopo che questo si è verificato. È per molti aspetti simile ai bitcoin: divisibile fino ad otto cifre decimali, accumulabile e scambiabile tra gli utenti. Ma non è da intendere come una riserva stabile di valore. I REP si perdono e si guadagnano a seconda di quanto i voti dell'utente sono coerenti con la maggioranza. I detentori di REP sono tenuti a riportare degli eventi ogni 8 settimane. I REP inoltre, non sono "minati", ma assegnati tramite asta.

[75] Nella teoria dei giochi un punto di Schelling (chiamato anche punto focale) è una soluzione che i giocatori tendono ad adottare in assenza di comunicazione, poiché esso appare naturale, speciale o rilevante per loro. Facendo esempio: a due persone, che non possono comunicare tra loro, è mostrato un pannello con quattro quadrati e gli viene chiesto di selezionarne uno; se e solo se entrambi selezionano lo stesso ricevono un premio. Tre quadrati sono blu e uno è rosso. Assumiamo quindi che non conoscano nulla sull'altro giocatore, ma che entrambi vogliano vincere il premio, ragionevolmente sceglieranno entrambi il quadrato rosso. Di certo, il quadrato rosso non è un quadrato migliore degli altri; i giocatori possono vincere scegliendo entrambi un qualsiasi quadrato. È il quadrato giusto da scegliere solo se possiamo essere sicuri che l'altro giocatore ha scelto quello; ma per le ipotesi del gioco nessun quadrato è certamente quello giusto. È il quadrato che si nota maggiormente e i giocatori sceglieranno quello con frequenza maggiore di tutti gli altri. Questo fatto viene verificato grazie a prove empiriche.

concorde, senza che vi sia collusione, sul risultato più ovvio, o in questo caso, la verità.

Agli utenti viene data la possibilità di vendere e comprare quote delle scommesse degli altri utenti su un determinato evento, come in un mercato azionario. Il prezzo della quota è, ovviamente, la stima della probabilità con cui l'evento in oggetto si verificherà. Il concetto base su cui il meccanismo genera profitto è la cosiddetta "saggezza della folla[76]", ovvero l'assunto secondo il quale la previsione su un determinato evento formulata da un gruppo sufficientemente ampio di persone, sarà sempre più accurata dell'opinione di un singolo esperto sulla stessa questione, per quanto informato egli sia. Questo fa di Augur anche uno dei più accurati strumenti di previsione mai creati: in un sistema centralizzato i report vengono redatti solo dopo che la situazione si è ormai configurata, e molto spesso da una singola persona. Questo rende i mercati previsionali centralizzati potenzialmente inaccurati, rischiosi ed esposti ad errori, false notizie, manipolazioni e corruzione. Un sistema decentralizzato, basato sulla Blockchain, è immune da questo tipo di rischi. Ogni singolo utente consegna la sua personale intuizione al sistema, insieme alla sua quota di scommessa, dando un contributo unico e sempre tracciabile alle statistiche previsionali di un evento.

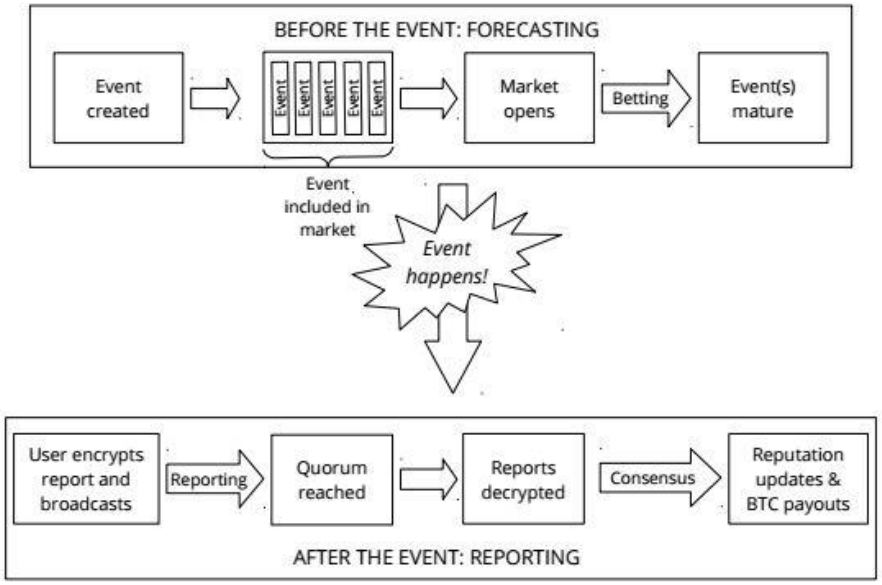
[76] La teoria è controversa, ma è stata largamente applicata con successo sia da imprese private che da enti governativi per stimare probabilità di eventi con discreta precisione. Esempi famosi sono l'Hollywood Stock Exchange, che stima gli accoppiamenti più probabili per gli Oscar (meglio di 4 critici cinematografici su 5 nel 2000); la Hewlett-Packard che nel 1998 fece stimare l'andamento delle vendite dei propri prodotti a 12 dipendenti (con 1 $ di ricompensa nel caso la previsione si fosse rivelata giusta) ottenendo risultati più realistici rispetto alle previsioni dei propri esperti; ed ovviamente le elezioni presidenziali americane, con il 74% in più di accuratezza rispetto alle previsioni ufficiali.

4.2.2. Esempio di una scommessa

Si vuole ora illustrare l'ipotesi di aprire una scommessa relativa ad un evento su Augur, per poi inserirla in un mercato, passare la fase di negoziazione ed arrivare al report finale e alla distribuzione delle vincite.

Lo schema che riassume il funzionamento concettuale di Augur è il seguente:

Diagramma del funzionamento di Augur



Fase 1: Prima dell'evento – Previsione

Si crea un assunto ipotetico per un avvenimento futuro, con un risultato di tipo binario[77] (o scalare) fra cui gli scommettitori potranno scegliere (o indicare un valore numerico). L'evento viene incluso nel mercato dopo la sua apertura e "negoziato" fino ad una data stabilita, in cui si è abbastanza prossimi al risultato e dunque la negoziazione viene interrotta.

Fase 2: Dopo L'evento – Reporting

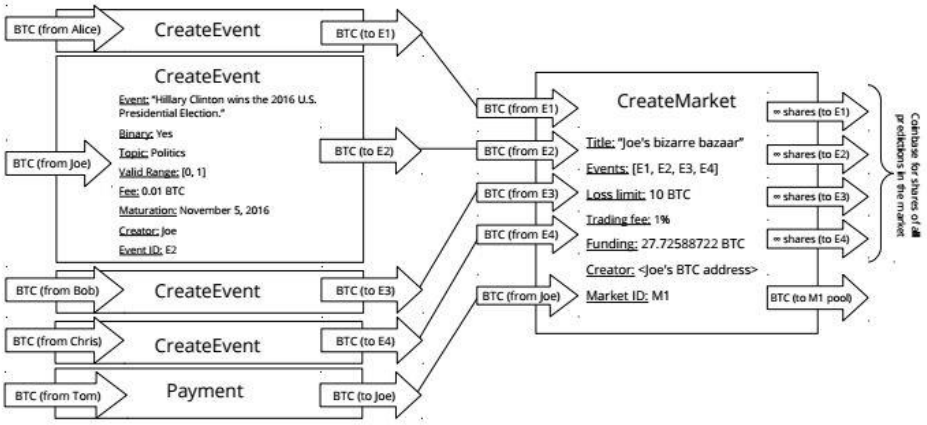
Gli utenti iniziano a verificare il risultato della scommessa e la riportano criptata alla piattaforma, la quale raccoglie le informazioni e una volta

[77] Dunque che può avere come unici risultati "l'evento si verifica" o "l'evento non si verifica".

raggiunto un quorum prestabilito, decripta i risultati aggregati e aggiorna la reputazione degli utenti, contestualmente alla ripartizione delle quote ai vincitori.

Più nello specifico, e guardando le azioni di più utenti insieme, accade questo:

Diagramma: creazione di un evento e di un mercato



I bitcoin fluiscono attraverso la piattaforma dalla creazione dell'evento verso il mercato, arrivando sia dalla creazione di eventi (che devono essere finanziati da un capitale minimo conferito dal loro ideatore) sia dagli scommettitori. Nella Blockchain vengono immagazzinate le informazioni riguardanti la scommessa ed il mercato in cui viene negoziata. In particolare:

- Descrizione dell'evento
- Binario/Non binario
- Argomento
- Sezione
- Il range di valori ammessi dalle scommesse (in caso di scommessa binaria, 0 oppure 1)

- La commissione per il creatore dell'evento
- La durata del periodo di negoziazione (segnando un blocco "target" oppure, più intuitivamente, una data)
- Il creatore dell'evento
- L'ID dell'evento

Nel mercato vengono registrati invece:

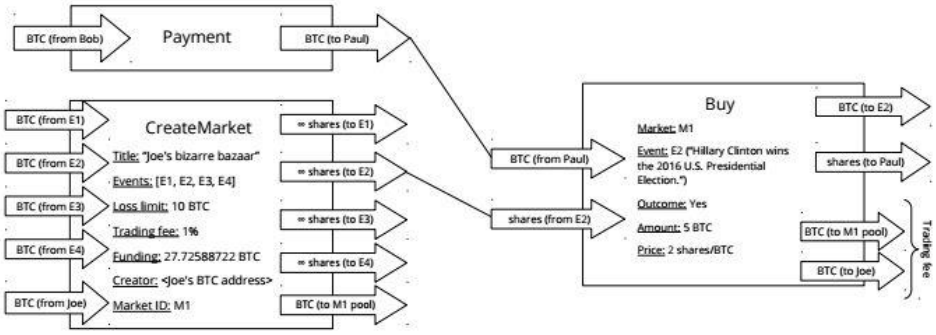
- Il nome del mercato
- Gli ID degli eventi che racchiude
- La massima perdita consentita al creatore del mercato se il numero di quote va a 0
- Il valore dei fondi conferiti dal creatore del mercato, almeno pari alla massima perdita consentita
- Il creatore del mercato (o meglio, il suo portafoglio bitcoin)
- L' ID del mercato

Il comando "CreateEvent" ha un singolo output[78], che contiene i dati dell'evento, in nessun modo duplicabili da un utente che volesse creare un evento con le stesse informazioni. Un utente che crea più uno o più eventi può organizzarli in un mercato col comando "CreateMarket", con le stesse caratteristiche.

[78] In hash-160, con un ID univoco

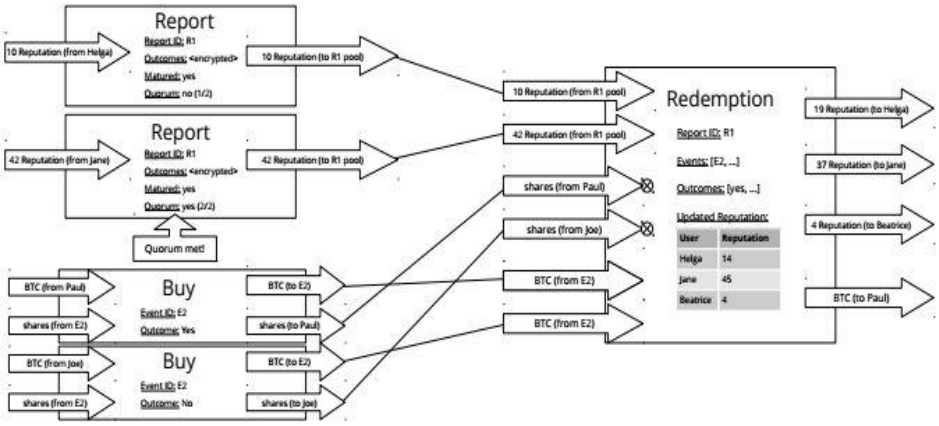
Una volta completate tutte le operazioni preliminari, l'utente trasmette la transazione alla rete Augur. I minatori la possono dunque prendere in consegna e includere la sua transazione in un blocco. Una volta eseguita questa operazione, il mercato diventa visibile agli altri utenti e si apre la fase di negoziazione.

Diagramma: acquisto di una quota



Nell'immagine soprastante è simulato un acquisto di quota. Paul, pagando le commissioni, spende 5 BTC per acquistare le quote per il "sì" all'evento proposto. Dato il prezzo di 2 quote/bitcoin, egli entra in possesso di 10 quote.

Diagramma: report, distribuzione vincite e reputazione



Una volta arrivati alla scadenza della fase di negoziazione, si raccolgono i report e si procede alla distribuzione delle quote vincenti.

Ogni utente invia i propri report criptati, fino al raggiungimento del quorum che valida la scommessa e svela i risultati finali. Ogni report vale un'unita al fine del quorum, ma i REP degli utenti fanno la differenza in ragione del peso che conferiscono al dato da loro riportato come esito finale dell'evento, rispetto al totale. Nell'esempio, Jane ha 42 REP, e il suo peso avvalora l'esito finale 4,2 volte di più rispetto al report di Helga, che possiede 10 REP. Sia gli utenti che hanno partecipato attivamente consegnando il report, sia quelli che non hanno comunicato l'esito dell'evento, aggiungono al proprio portafoglio altri REP, seppur in misura diversa. Una volta conclusa la procedura, i pagamenti vengono instradati dal mercato verso la Blockchain e trasferiti ai portafogli degli utenti vincitori non appena vengono incorporati in un blocco.

4.3. Conclusioni

Sono state mostrate diverse possibili applicazioni del protocollo Bitcoin e della Blockchain che vanno ben oltre l'uso monetario sul quale il sistema attualmente si attesta. È stata mostrata la sua validità, la sua estrema sicurezza, la velocità e la geniale semplicità che sottostà al suo funzionamento. Il futuro di questa criptovaluta è ancora incerto, ma molte società e molte istituzioni hanno avuto la saggezza e la lungimiranza necessaria per intuire che dietro alla cupidigia che può spingere l'uomo a speculare, il grande dono che attribuiamo ad uno sconosciuto, quasi anonimo benefattore, sta lentamente venendo alla luce. Ed egli forse non ha semplicemente voluto donare al mondo un protocollo per innovare il nostro sistema economico, benché di certo sia più sicuro ed intelligente di ciò che abbiamo ora. Ha voluto donarci un'idea. L'uso che sceglieremo di farne, sta a noi. Il mondo intero, almeno sotto questo punto di vista, è sulla buona strada e procede veloce verso innovazioni geniali che segneranno una svolta fondamentale nella storia dell'umanità, guidato auspicabilmente da menti brillanti e votate al Bene ed al Progresso. Tanto grande è la portata della rivoluzione della Blockchain.

BIBLIOGRAFIA

D. Graeber (2012), "*Il Debito"*, Il Saggiatore.

M. Kennedy, (1995), "*Il denaro libero da interessi ed inflazione"*, Arianna Editrice

D. Chaum, (1983), *"Blind signatures for untraceable payments",* pp. 199–203.

J. Bohr, M. Bashir, (2014), *"Who Uses Bitcoin? An exploration of the Bitcoin community".*

The Economist, (15/03/2014), *"Hidden Flipside".*

J.M. Keynes (1930), *"Treatise On Money"*, Vol. II, p. 292.

J. Tobin. *"New Palgrave Dictionary of Money and Finance"* per la voce Money.

M. Friedman, (1992), *"Money Mischief".*

Kati Pohjanpalo (20/01/2014), "*Bitcoin Judged Commodity in Finland After Failing Money Test*", Bloomberg (New York).

Banca Centrale Europea, (10/2012), "*Virtual Currency Schemes*".

Autorità Bancaria Europea, (04/07/2014), "*EBA Opinion on virtual currencies*".

P. L. Burlone, R. de Caria, (01/04/2014) "*Bitcoin e le altre criptomonete: Inquadramento giuridico e fiscale*", IBL Focus N. 234.

F. Ametrano, F. Vatalaro, R. Tudini, (11/06/2014), *"Bitcoin in Italia: quali opportunità per le "monete matematiche" nel nostro paese?",* presso Camera dei Deputati, Sala Aldo Moro.

Thomas Schelling, (1960) *"La strategia del conflitto"*, p. 57

Dr. Jack Peterson & Joseph Krug (17/11/2014) *"Augur: a Decentralized, Open-Source Platform for Prediction Markets"*

SITOGRAFIA

Per il Capitolo 1:

https://antropologiaesviluppo.wordpress.com/2015/02/16/in-principio-non-fu-il-baratto-ma-il-credito/

http://www.monetacomplementare.org/1/storia_della_moneta_156368.html

http://www.ilfattoquotidiano.it/2014/04/07/crisi-economica-le-monete-complementari-che-sfidano-lausterita/942155/

https://letstalkbitcoin.com/the-island-of-stone-bitcoins/

http://www.eticaeconomia.it/bitcoin-paleomonete-alternative-currencies/

http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

Per il Capitolo 2:

https://bitcoin.org/bitcoin.pdf

https://bitcoinhelp.net/know/more/price-chart-history

http://cointelegraph.it/news/113952/storia-della-criptovaluta-parte-1-dalla-creazione-di-bitcoin-al-cripto-boom

https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/

http://www.oecd.org/futures/35391062.pdf

http://it.bitcoinwiki.org/Storia_di_Bitcoin

http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/

Per il Capitolo 3:

https://www.cryptocoinsnews.com/banks-choose-block-chain-can-save-20-billion-per-year/

http://sinosphere.blogs.nytimes.com/2013/11/22/bitcoin-gets-a-cautious-nod-from-chinas-central-bank/?_php=true&_type=blogs&_r=3.
http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html

http://cointelegraph.com/news/113639/kenya-adopts-bitcoin-with-bitpesa-tagpesa-and-m-pesa

http://onbitcoin.com/2013/11/18/senate-committee-listens-bitcoin-experts-expresses-open-mindedness/

http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies

Per il Capitolo 4:

http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

http://www.tasse-fisco.com/varietassefisco/bitcoin-valore-prezzo-cosa-e-come-funziona/15916/

http://www.augur.net/

http://docs.augur.net/

http://augur.link/augur.pd