Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

Diritto e Nuove Tecnologie

Ciclo XXIX

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: Ius 20

Distributed Ledger Technologies e Sistemi di *Blockchain*: *Digital Currency*, *Smart Contract* e altre applicazioni

Presentata da: Maria Letizia Perugini

Coordinatore Dottorato	Relatore	Correlatore
Prof. Giovanni Sartor	Prof. Cesare Maioli	Prof. Raffaella Brighi

Esame finale anno 2017

Maria Letizia Perugini

Distributed Ledger Technologies e Sistemi di *Blockchain*: *Digital Currency*, *Smart Contract* e altre applicazioni

Parole chiave: ***Distributed Ledger Technologies (DLT), Blockchain, Bitcoin, Ripple , Name Coin, ColoredCoins, Ethereum, Standard ISO***

Sommario

a Marco

Economists commonly assume that what is traded on the market is a physical entity, an ounce of gold, a ton of coal. But, as lawyers know, what are traded on the market are bundles of rights, rights to perform certain actions.

Ronald Coase, *Blackmail,* 1988[*]

[*]in 74 Virginia Law Review 655(1988)@ 1988 by The University of Virginia http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1003&context=occasional_papers

Abstract

Questo studio si propone di analizzare il complesso delle novità introdotte al sistema dei pagamenti e al trasferimento di diritti da *Distributed Ledger* e *Blockchain*, in una prospettiva che tenga conto delle applicazioni di mercato di queste innovazioni tecnologiche e della tutela giuridica degli interessi economici e delle posizioni soggettive che ne derivano. In particolar modo, l'opera vuole stimolare la discussione volta alla definizione di un quadro normativo socialmente adeguato che sostenga l'efficienza di questi strumenti in un'ottica di scambio economico globalizzato.

This essay aims at analyzing the ensemble of innovation introduced by Distributed Ledger and Blockchain to the payment system and the transfer of rights, in a perspective considering the market applications of these new technologies and the legal protection of deriving economics interests and individual rights. Purposely, our dissertation aspires to encourage the discussion for the definition of a socially adequate legal framework sustaining the efficiency of these instruments in a global exchange perspective.

1. Piano dell'opera

Il capitolo introduttivo contiene la ricognizione dello stato dell'arte e la definizione della metodologia; seguono tre parti dedicate rispettivamente a strutture e sistemi, *digital currency* e implementazioni; infine le conclusioni prendono in considerazione i vantaggi applicativi di questi sistemi sia a livello istituzionale che per quanto riguarda l'espressione della libertà contrattuale suggerendo alcune prospettive di ricerca futura.

La prima parte è dedicata a *Distrubuted Ledgers* e *Blockchain* e ai meccanismi di formazione del consenso necessario a inserire nuove voci in queste strutture. Abbiamo in primo luogo esposto la metodologia: sul piano tecnico abbiamo optato per l'analisi sequenziale, mentre sul piano giuridico la nostra scelta è andata a favore del metodo di *Law and Economics*, che pone a fondamento della ricerca i valori morali e sociali che hanno condotto all'emanazione della normativa. Abbiamo quindi proceduto alla disamina dello sviluppo storico di questi modelli esaminando il lavoro degli autori di riferimento David Chaum, Tim May, Nick Szabo, Wei Day, Hal Finney, Adam Back e la loro influenza sullo sviluppo dei modelli attuali. Sul piano applicativo abbiamo proceduto all'esame dei sistemi attuano trasferimenti di stringhe matematiche *no asset baked*, ossia prive di beni di riferimento sottostanti, analizzando

Bitcoin, *Ripple* ed *Ethereum,* i sistemi maggiormente diffusi e dedicando un ulteriore capitolo all'esame dei protocolli offuscati.

La seconda parte è dedicata all'applicazione in funzione di *Digital Currency* del sistema *Bitcoin* con analisi dei profili giuridici ed economici e dei risvolti socio istituzionali che hanno fatto seguito alle vicende del 2013, nel cui ambito un forte ruolo è stato rivestito dai movimenti speculativi generati dalla crisi bancaria di Cipro. In questa sezione abbiamo analizzato la funzione economica della moneta e la qualificazione giuridica in termini di funzione di pagamento, fissazione dei prezzi al consumo e funzione di risparmio, tracciando la storia moderna dei sistemi valutari dagli accordi di Bretton Woods alle moderne emissioni digitali. Abbiamo quindi proceduto all'analisi dei provvedimenti emanati delle Autorità economiche Nazionali e sovranazionali, allarmate dal fatto che il movimento speculativo in corso non trovasse compensazione in adeguate forme di garanzia degli investitori. Infine abbiamo esaminato le reazioni istituzionali all'allarme sociale destato dai siti di *blackmarket online* come Silk Road e dal *default* della piattaforma di exchange *MtGox* che hanno portato a iniziative di diverso rilievo e di discorde efficacia nella regolamentazione delle monete digitali.

La terza parte dello studio è dedicata all'esame delle implementazioni, a partire dai sistemi destinati a fini specifici fino agli *smart contract* e alle piattaforme di contrattazione, il cuore pulsante della materia. In questa sezione abbiamo delineato i confini della ricerca stabilendo di occuparci solo degli accordi degni di tutela secondo i precetti dell'ordinamento giuridico, tracciando una netta distinzione fra contratti, coperti da ogni più ampia tutela giudiziale, e accordi nulli, come quelli a commettere un reato in cambio di un corrispettivo economico, che non sono in alcun modo azionabili in via esecutiva; abbiamo quindi proposto un quadro introduttivo alle clausole *self executing,* individuando i tratti fondamentali del modello *smart.* In

seguito, abbiamo proceduto all'analisi delle maggiori piattaforme di contrattazione e di alcune interessanti applicazioni presenti sul mercato allo scopo di individuare i modelli efficienti di contrattazione e di scambio.

Abbiamo infine formulato le conclusioni dello studio seguendo la ripartizione dell'indice e rivolgendo la nostra attenzione rispettivamente alle *digital currency*, alle forme di espressione della libertà contrattuale, alla funzione di certificazione nel cui ambito abbiamo identificato i vantaggi istituzionali dei nuovi sistemi. Ad esito della ricognizione, abbiamo preso in considerazione la rilevanza sociale e le implicazioni di mercato di questi strumenti formulando considerazioni circa i possibili sviluppi normativi e la direzione auspicabile della ricerca futura in una prospettiva di efficienza basata sui valori morali e sociali che hanno portato all'implementazione delle *Distrubuted Ledger Technologies* e dei sistemi di *Blockchain.*

2. Metodologia

Sul piano metodologico, troviamo appropriata al nostro tema l'analisi sequenziale propria delle scienze statistiche, nel cui ambito si procede formando un campione rappresentativo senza determinarne a priori l'ampiezza o la numerosità. La definizione di questi fattori dipenderà dai risultati ottenuti col progredire dell'osservazione o dell'esperimento ovvero, nel nostro caso, dalle applicazioni pratiche e dalle implementazioni del modello iniziale.

La nostra scelta è intrinsecamente dipendente dalla natura stessa del tema esaminato: si tratta di una materia nuova, in continua metamorfosi degli effetti, al punto da rendere particolarmente difficoltosa la determinazione teorica del campione di studio.

Restringere l'analisi a un ambito predeterminato sarebbe addirittura controproducente, poiché una definizione troppo stringente della fattispecie porterebbe all'esclusione di alcuni sviluppi importanti.

De Jure condendo, la natura del tema suggerisce di costruire il modello normativo secondo il criterio economico. Le alternative possibili sono date dal metodo di Analisi Economica del Diritto, che considera la normativa come oggetto di studio dell'economia, e dal sistema di *Law and Economics* che ambisce alla determinazione di regole efficienti sulla base dei principi morali e sociali che costituiscono il fondamento del diritto[1].

Considerata l'importanza fondamentale che il concetto di reputazione riveste nell'ambiente *Internet*, riteniamo che la prospettiva di *Law and Economics* si riveli maggiormente opportuna per la regolamentazione dei sistemi basati su *blockchain*. L'analisi in questi termini consentirà di individuare incentivi, disincentivi e punti di equilibrio del sistema, delineando un quadro di riferimento normativo in cui regole socialmente orientate potranno contemperare le ragioni istituzionali con i principi etici e morali su cui si basano le istanze della società globalizzata.

Il risultato della nostra analisi è influenzato dall'ambiente in cui si è svolta la ricerca che ha consentito un dialogo accademico continuo con matematici, fisici, sociologi, filosofi e giuristi portando la discussione a un livello di approfondimento che non sarebbe stato possibile in un contesto tradizionale.

[1] *Vide*: Guido Calabresi, Of Tastes and Values, 2014, Yale Law & Economics Research Paper No. 500, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483947.
Il contenuto del paper è parte del libro *The Future of Law and Economics, http://yalebooks.com/yupbooks/book.asp?isbn=9780300195897*.

3. Tavoli di discussione

Nel luglio 2016 siamo stati invitati a partecipare al *Blockchain and Smart Contracts Discussion Group*[2] organizzato da *The Kantara Initiative*[3], un consorzio *no profit* nato nel 2009 per la gestione dell'identità digitale[4] con l'obiettivo di favorire l'adozione di principi quadro e di *best practice* a tutela della *privacy* e dell'accesso sicuro a *trusted service on line*[5].

Gli interlocutori di *Kantara* sono le Università e gli enti come *International Organization for Standardization* (ISO)[6],*Organization for the Advancement of Structured Information Standards* (OASIS)[7], *Internet Engineering Task Force* (IETF)[8], *Identity Ecosystem Steering Group* (IDESG)[9] e *ITU Telecommunication Standardization Sector* (ITU-T)[10].

Il gruppo di discussione riserva un'attenzione particolare alle implicazioni etiche delle nuove tecnologie, offrendo un impulso alla ricerca attento alla tutela degli individui. La prima fase è stata rivolta alla definizione della fattispecie: anche in questo la scelta metodologica è andata a favore dell' analisi sequenziale perché, l'applicazione di *blockchain* e *DLT* è in continua evoluzione e la predeterminazione del

[2] https://kantarainitiative.org/groups/blockchain-and-smart-contracts-discussion-group/
[3] https://kantarainitiative.org/confluence/display/BSC/Home
[4] L'Identity and Access Management (IAM) è la disciplina che gestisce la sicurezza degli accessi alle risorse controllando l'identità del soggetto, la validità temporale della richiesta, il permesso di attingere a risorse specifiche e abilitando ad azioni diverse a seconda delle credenziali personali.
[5] https://kantarainitiative.org/about/principles/
[6] http://www.iso.org/iso/home.html Nel 2016 l'International Standard Organization ha istituito la Commissione Tecnica 307 per la standardizzazione di blockchain e distributed ledger technologies e la promozione dell'interoperabilità e dello scambio di dati fra utilizzatori, applicazioni e sistemi. L'iniziativa ha preso avvio dalla proposta di *Standards Autralia* che guida il gruppo di lavoro; il nostro Paese partecipa al tavolo di discussione tramite l'Ente di Normazione Italiano (UNI) www.uni.com/
[7] https://www.oasis-open.org/
[8] https://www.ietf.org/
[9] https://www.idesg.org/
[10] http://www.itu.int/en/ITU-T/Pages/default.aspx

campione di studio potrebbe tradursi in un limite all'area di ricerca. Il dibattito ha coinvolto ricercatori in ambito tecnico o giuridico, selezionati fra accademici e professionisti[11]; le riunioni sono state tenute in *call conference* a cadenza bisettimanale, fino a maggio 2017.

Ad esito di questo periodo di studio abbiamo prodotto un documento di analisi e raccomandazione per la ricerca futura che, al momento, è ancora in fase di revisione; la seconda fase del progetto, che prenderà avvio a breve, prevede la creazione di due tavoli specifici, rispettivamente a contenuto tecnico e giuridico, e di un tavolo generale di confronto, confermando la precedente cadenza di due incontri alla settimana nel cui ambito il dibattito sarà ripartito secondo i criteri appena esposti.

Alla fine di agosto 2016 siamo stati invitati a partecipare al gruppo di lavoro su *Blockchain* e *Distributed Ledgers*[12] organizzato da *Cloud Security Alliance*[13] (*CSA*) organizzazione *no profit* che promuove l'adozione di *best practices* nel *Cloud Computing.* Anche in questo ambito abbiamo analizzato le tecnologie di registro distribuito applicando il metodo di analisi sequenziale in modo da consentire la dimensione più ampia del campione di ricerca.

Questo gruppo di lavoro accoglie principalmente ricercatori del settore tecnico e il profilo giuridico è stato inserito allo scopo di esaminare i confini applicativi della materia. Le riunioni si tengono in *call conference* a cadenza quindicinale e vertono principalmente sull'ambito della sicurezza. Ad esito della prima fase di analisi, ancora in corso, si prevede di attivare un gruppo di discussione europeo per la definizione delle linee guida in ambito UE.

---

[11] http://kantarainitiative.org/confluence/display/BSC/Participant+Roster, voting members list: Matisse Perugini e Marco Carlo Spada

[12] https://cloudsecurityalliance.org/group/*blockchain*/

[13] https://cloudsecurityalliance.org/

Parte I: Strutture dati e Sistemi

4. Sviluppo storico

4.1. Contesto sociale

La storia dei sistemi di pagamento digitale risale indietro nel tempo, precisamente al 1982 anno ricco di innovazioni che avrebbero trasformato la vita di tutti i giorni. In quell'anno la Commodore Business Machines Inc immetteva sul mercato il mitico home computer Commodore 64 sui cui orde di ragazzini appassionati avrebbero trascorso ore e ore a inserire programmi di videogioco. A distanza di pochi mesi, la Philips metteva in vendita il primo CD musicale, dando il varo all'operazione con la Sinfonia delle Alpi di Strauss eseguita dai Berliner Filarmoniker diretti da Herbert Von Karajan. A questa iniziativa, rivolta più ai genitori che ai figli, avrebbe fatto rapido seguito l'offerta degli album The Visitors degli Abba (il primo stampato su CD), 52nd Street di Billy Joel (il primo ad essere commercializzato su CD) e Love Over Gold dei Dire Straits (nativo digitale, fra i primi a sfruttare la capacità dinamica dei CD).

4.2. David Chaum

È nel contesto storico descritto in premessa che David Chaum, PhD alla Berkley University in C*omputer Science and Business*

Administration, esponeva nel paper *Blind signatures for untraceable payments*[14] il suo progetto di un sistema di pagamento a firma digitale cieca da applicare alle emissioni valutarie elettroniche e a nuove forme monetarie, prospettando l'alba di una nuova era. La ricerca sviluppava alcuni dei concetti introdotti nel precedente paper *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*[15], un testo di grande interesse nella ricerca sulle comunicazioni anonime.

Le idee di Chaum sono considerate uno dei fondamenti della corrente *cypherpunk,* un movimento di pensiero che incoraggia l'uso della crittografia come strumento di difesa della *privacy* dall'abuso del diritto di informazione tipico delle società globalizzate. Alcuni dettagli dello schema sarebbero poi stati definiti da Chaum nel successivo *paper Online Cash Checks*[16], pubblicato nel 1989.

4.3. Tim May

Nel 1988 Tim May, ingegnere elettronico dell'Intel e fondatore del movimento Cypherpunk[17], scriveva il Manifesto Crypto Anarchico[18] un

[14] in Advances in Cryptology Proceedings of Crypto82 (3): 199–203
[15] David Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, 1981 in* http://scholar.google.it/scholar_url?url=https://www.cs.umd.edu/class/spring2015/cmsc414/papers/chaum-mix.pdf&hl=it&sa=X&scisig=AAGBfm1iBavZ0gXhXjbLGZ-CLYH9FuNeyw&nossl=1&oi=scholarr&ved=0ahUKEwj61szm1b7PAhUJJx4KHabkDv0QgAMIJCgAMAA
[16]David Chaum, *Online Cash Cecks*, 1989 https://w2.eff.org/Privacy/Digital_money/?f=online_cash_chaum.paper.txt
[17] Corrente di pensiero libertaria che incoraggia l'uso massivo della crittografia come strumento anti-establishment per la promozione della libertà individuale
[18]Timothy C. May, The Crypto Anarchist Manifesto, 1988: "*A specter is haunting the modern world, the specter of crypto anarchy.*
Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings

documento breve che descrive con un anticipo di circa trent'anni l'evoluzione della società odierna. I concetti espressi nel Manifesto sarebbero poi stati sviluppati da May nel successivo *Cyphernomicon*[19], datato 1994, una pubblicazione in stile FAQ che suggerisce l'uso della crittografia come risposta lecita alle ingerenze dell'Autorità, da utilizzare come materia prima nella costruzione del *Cyberspace*.

---

than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.
The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.
The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.
Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.
Arise, you have nothing to lose but your barbed wire fences!
" http://www.activism.net/cypherpunk/crypto-anarchy.html

[19] Timothy C. May The Cyphernomicon, 1994.
16.3.2. "Do the views here express the views of the Cypherpunks as a whole?"
Several Cypherpunks who've thought about the issues of crypto anarchy have been disturbed by the conclusions that seem inevitable (markets for corporate information, assassianation made more liquid, data havens, espionage made much easier, and other such implications to be explored later in this section). So, take this section with these caveats.
https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html

Nel tempo, la ricerca sulla *blockchain* è stata portata avanti da scienziati indipendenti che hanno trovato un terreno comune negli studi di David Chaum, pietre miliari del settore, e nelle teorie di Tim May.

4.4. Adam Back

Nel 1997 veniva teorizzato uno dei punti cardine della futura architettura *Bitcoin:* la *hashcash proof of work,* implementata dal crittografo inglese Adam Back che aveva sviluppato questo strumento come misura *antispam*.

In *Bitcoin* l'uso di *hash* con caratteristiche numeriche specifiche determina un grado di difficoltà di calcolo proporzionale alla potenza computazionale impegnata (misurata in *hashrate/s*). Il risultato, che può essere verificato immediatamente, è ottenuto stabilendo il numero desiderato di *bit* in collisione, influenzando sensibilmente il costo dell'operazione e scoraggiando così i tentativi di *free riding*. Back, che non ha mai partecipato direttamente alla scrittura di *Bitcoin*, avrebbe offerto un ulteriore contributo fondamentale al sistema nel 2014, quando con un gruppo di esperti sviluppatori ha proposto l'adozione delle *sidechain*[20], un sistema collaterale agganciato a parità fissa con *Bitcoin* che permette di effettuare operazioni senza appesantire la *blockchain* di riferimento, sul cui funzionamento torneremo dettagliatamente in seguito.

[20] Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuill, Enabling Blockchain Innovations with Pegged Sidechains, 2014, https://blockstream.com/sidechains.pdf

4.5. Nick Szabo e Wei Dai

Seguendo la linea di ricerca tracciata da Chaum nel 1998 Nick Szabo[21], autore di riferimento nel panorama *data encryption*, pubblicava il *paper Contracts with Bearers*[22] in cui proponeva di estendere il sistema di *blind signature* al trasferimento di diritti diversi da quelli di credito[23]. Nello stesso anno veniva pubblicato il *paper B-money*[24] in cui Wei Dai, una figura emblematica dell'area cypherpunk[25], suggeriva due possibili schemi attuativi del contesto descritto da Tim May nel *Manifesto Cripto Anarchico* del 1988[26]. La prima soluzione, in particolare, consisteva nell'adozione di un sistema di moneta virtuale per gli scambi su *network* associato a un sistema di *enforcement* delle transazioni. Lo schema, pur considerato impraticabile dallo stesso autore[27], conteneva in sé le basi

[21]http://szabo.best.vwh.net/

[22]*Nick Szabo, Contracts with Bearers, 1998, http://szabo.best.vwh.net/bearer_contracts.html: "Chaumian bearer certificates implement standardized rights transferable regardless of the identity of the holder. Each kind of contract (for example, each denomination of "coin" in digital cash) corresponds to a digital signature, just as each issue of Federal Reserve Notes or stock certificates corresponds to a particular plate."*

[23] Ibidem: "*Bearer certificate protocols can be used to transfer references to a particular instance or set of instances of an object, just as they can be used to transfer other kinds of standardized rights*."

[24]http://www.weidai.com/bmoney.txt

[25]http://www.weidai.com/
I cypherpunk incoraggiano un uso massivo della crittografia come strumento anti-establishment per la promozione della libertà individuale.

[26]Timothy C. May, The Crypto Anarchist Manifesto, 1988
http://www.activism.net/cypherpunk/crypto-anarchy.html
Wei Dai, B-Money, 1998, http://www.weidai.com/bmoney.txt: " *I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.*
Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities."

[27]Wei Dai, B-Money, 1998, http://www.weidai.com/bmoney.txt : "*I will actually describe two protocols. The first one is impractical, because it makes heavy use of a*

dei modelli di *blockchain* a venire[28]. La seconda soluzione introduceva alcuni concetti altrettanto interessanti, tracciando la strada del futuro sistema di verifica BItcoin[29]

4.6. Hal Finney

Infine, un contributo fondamentale allo sviluppo dei sistemi di *blockchain* si deve al compianto Hal Finney (1956-2014), esperto crittografo, programmatore PGP, ed esponente della corrente *Cypherpunk.* Nel 2004 Finney aveva elaborato il concetto di *Reusable Proof of Work[30],* un prototipo[31] mai applicato ma che aveva guadagnato

---

synchronous and unjammable anonymous broadcast channel. However it will motivate the second, more practical protocol. In both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver."

[28] Ibidem: "*In the first protocol, every participant maintains a (seperate) database of how much money belongs to each pseudonym. These accounts collectively define the ownership of money, and how these accounts are updated is the subject of this protocol. 1. The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities."*

[29] Wei Dai, B-Money, 1998, http://www.weidai.com/bmoney.txt :"*In the second protocol, the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone. These servers are linked by a Usenet-style broadcast channel. The format of transaction messages broadcasted on this channel remain the same as in the first protocol, but the affected participants of each transaction should verify that the message has been received and successfully processed by a randomly selected subset of the servers".*

[30]https://cryptome.org/rpow.htm
To: cypherpunks@al-qaeda.net
Subject: RPOW - Reusable Proofs of Work
Date: Sun, 15 Aug 2004 10:43:09 -0700 (PDT)
From: hal at finney dot org ("Hal Finney")
I'd like to invite members of this list to try out my new hashcash-based server, rpow.net.This system receives hashcash as a Proof of Work (POW) token, and in exchange creates RSA-signed tokens which I call Reusable Proof of Work (RPOW) tokens. RPOWs can then be transferred from person to person and exchanged for new RPOWs at each step. Each RPOW or POW token can only be used once but since it gives birth to a new one, it is as though the same token can be handed from person to

il rispetto di tutta la comunità dei ricercatori. Anche per questo motivo sarà proprio Hal Finney la persona a cui Satoshi Nakamoto affiderà la revisione dell'intero sistema *Bitcoin*[32], come già aveva fatto nei primi anni '90 Phil Zimmerman con *Pretty Good Privacy*.

4.7. Patriot Act

Nonostante lo sviluppo di basi teoriche solide, per una decina di anni ancora, i sistemi di moneta virtuale avrebbero rivestito unicamente valore di nicchia, ricevendo scarsa attenzione da parte del pubblico: la possibilità di trasferire denaro contante senza doversi necessariamente autenticare, consentiva al tempo di risolvere le istanze di *privacy* registrandosi ai servizi di *money transfer* con nomi di fantasia.

Lo scenario giuridico è cambiato radicalmente nel 2001 quando, a seguito dell'attacco alle Torri Gemelle, lo *USA Patriot Act* ha introdotto l'obbligo di identificazione dei clienti dei servizi di money transfer (*Know*

person. Because RPOWs are only created from equal-value POWs or RPOWs, they are as rare and "valuable" as the hashcash that was used to create them. But they are reusable, unlike hashcash. The new concept in the server is the security model. The RPOW server is running on a high-security processor card, the IBM 4758 Secure Cryptographic Coprocessor, validated to FIPS-140 level 4. This card has the capability to deliver a signed attestation of the software configuration on the board, which any (sufficiently otivated) user can verify against the published source code of the system. This lets everyone see that the system has no back doors and will only create RPOW tokens when supplied with POW/RPOW tokens of equal value. This is what creates trust in RPOWs as actually embodying their claimed values, the knowledge that they were in fact created based on an equal value POW (hashcash) token. I have a lot more information about the system at rpow.net, along with downloadable source code. There is also a crude web interface which lets you exchange POWs for RPOWs without downloading the client. This system is in early beta right now so I'd appreciate any feedback if anyone has a chance to try it out. Please keep in mind that if there are problems I may need to reload the server code, which will invalidate any RPOW tokens which people have previously created. So don't go too crazy hoarding up RPOWs quite yet.
Thanks very much - Hal Finney

[31] https://web.archive.org/web/20071222072154/http://rpow.net/
[32] Hal Finney Bitcoin and me (Hal Finney) , 2013, https://bitcointalk.org/index.php?topic=155054.0

Your Customer Rule). Nel 2007 la *KYCR* è stata estesa al trasferimento di ogni genere di valore e dal 2012 è applicabile anche alle aziende straniere che consentono ai cittadini USA di aprire un account.

Fra le conseguenze della nuova regola, che hanno costretto alla chiusura tutti gli operatori che non procedessero alla corretta identificazione dei clienti, vi è stato anche un risvolto inatteso, con un incentivo alla ricerca di sistemi di trasferimento in grado mantenere un legittimo anonimato che ha portato alla riscoperta dei sistemi di moneta digitale e alla loro implementazione *no asset backed*.

4.8. Satoshi Nakamoto

Alla fine del 2008 un articolo a firma dello pseudonimo Satoshi Nakamoto ha presentato alla rete i *Bitcoin*[33], un sistema di pagamento distribuito fra i nodi di una rete peer-to-peer che offre una garanzia di spendita unitaria indipendente dall'intervento di un garante esterno, inserendo i dati di ogni transazione in un registro pubblico e distribuito.

Il progetto Bitcoin rappresenta lo schema di riferimento per la maggior parte delle monete virtuali: alcuni dei quali sono stati riprogettati *Bitcoin-style,* come *Ripple*[34] mentre altri consistono in un'implementazione di alcuni elementi del sistema originale, come *Litecoin*[35]. Vi sono poi monete che consistono semplicemente in una duplicazione, tramite *fork* di sistema, del modello *Bitcoin* di cui replicano esattamente il funzionamento e rispetto al quale possono differire essendo dedicate a scopi particolari, come *Namecoin* la prima *fork* di sistema risalente al 2011[36], dedicata alla gestione di *domain naming,* o le implementazioni *Colored Coins* lanciate con *chainfork* del

[33] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008, http://*bitcoin*.org/*bitcoin*.pdf
[34] https://ripple.com/
[35] https://litecoin.org/
[36] https://namecoin.info/

2012[37] , dedicate alla gestione e al trasferimento di diritti di proprietà digitale. Un altro caso interessante è quello dei sistemi c.d. offuscati che utilizzano *ring signature* e *zero-knowledge proof* per rendere più complicato rintracciare le transazioni; la possibilità scelta è ampia e spazia fra oltre 800 differenti strumenti con capitalizzazione di mercato[38], cui si affiancano numerosi sistemi privati dedicati a pagamenti e trasferimenti interni, certificazioni e messaggistica.

[37] http://coloredcoins.org/
[38] http://coinmarketcap.com/all/views/all/

5. Strutture dati

5.1. Distributed Ledger e Database Centralizzati

I *Distributed Ledger* sono database decentralizzati e condivisi che possono essere distribuiti o replicati esattamente sui nodi di una rete *peer-to-peer:* le voci del registro vengono inserite nella struttura dati in maniera continua e sono collegate le une alle altre secondo criteri di consenso che variano in dipendenza del sistema utilizzato. L'aggiunta di voci al registro è protetta da meccanismi *anti-floding* come *proof of work* o *proof of stake* e ogni sistema dispone regole interne per la formazione del consenso sulle transazioni, ovvero sui trasferimenti, le attività e i fatti attestati nel registro che possono avere natura di accordo, dichiarazione o impegno fornendo al contempo la prova che quelle eventualità hanno avuto corso. La partecipazione al *network* può essere libera o richiedere agli utenti una qualche forma di autorizzazione; nel primo caso, per evitare attacchi interni, i criteri di validazione dell'attività sono predeterminati e non possono essere modificati senza il consenso dell'intera comunità. Le transazioni avvengono scambiando un *token*, detto moneta, che può presentare caratteri di piena autonomia o fare riferimento a un'altra divisa digitale; il rapporto di

cambio con le altre monete digitali può essere libero o fisso a seconda delle scelte economiche degli amministratori di sistema.

Nei sistemi che adottano *database* centralizzati, gli utenti accedono a un'architettura *client-server* accettando le regole determinate dall'amministratore di sistema che gestisce ogni istanza autorizzando le attività richieste e risolvendo eventuali problemi con potere proprio. L'organizzazione del *network* spetta al gestore che affronterà in piena autonomia ogni scelta strutturale e operativa offrendo all'utente un servizio predeterminato; eventuali modifiche potranno essere apportate nella misura in cui il gestore sarà incline ad assecondare le esigenze del cliente il quale, a propria volta, potrà valutare l'opportunità di acquistare pacchetti di servizio più o meno completi.

In termini di efficienza, sia i data base centralizzati che quelli distribuiti presentano dei pregi che sono fruibili in determinate situazioni e che si trasformano in pastoie e colli di bottiglia in altre, rimanendo la scelta operativa strettamente legata alle necessità del caso specifico[39].

In primo luogo viene in considerazione il rapporto di fiducia: in ogni sistema le parti hanno necessità di un meccanismo di verifica e garanzia delle transazioni. Nei sistemi centralizzati la figura dell'amministratore funge da punto cardine e intermediario di ogni istanza degli utenti, è responsabile per la conservazione e la gestione dei dati e ha poteri di direzione delle attività. Al contrario, nei *database* distribuiti i nodi della rete, organizzati in architettura paritaria, eseguono ogni prestazione processando le attività in maniera congiunta, seguendo regole predeterminate; mancando la fiducia nei confronti di un gestore terzo, ogni nodo è depositario di una copia del registro, integrale o parziale a seconda della sua natura *full* o *light,* che viene normalmente protetta con crittografia. Nei sistemi centralizzati, la

[39] Gideon Greenspan Blockchains vs centralized databases, 2016, http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

conservazione è effettuata a livello unico, con il conseguente rischio di un'eventuale perdita dei dati; peraltro, le *good practice* prevedono che il sistema sia ridondato, con conservazione simultanea dei dati in più archivi fisici, rendendo il due modelli analoghi sotto questo profilo.

L'elemento che segna una differenza fra le due strutture è la resistenza alle manipolazioni esterne, sicuramente maggiore nei *database* distribuiti che vedono ogni modifica soggetta all'approvazione dell'intera comunità dei nodi. Per questa ragione i sistemi distribuiti sono più lenti di quelli centralizzati: il meccanismo del consenso prevede tempi, più o meno lunghi, che si calcolano a partire dall'inserimento delle transazioni nel registro. Questo evento nei *database* centralizzati segue normalmente regole neutrali basate sul momento dell'invio al sistema, eventualmente dividendo gli utenti in categorie a priorità differente; nei *database* distribuiti, dove gli utenti sono uguali tra loro, la priorità di inserimento è invece spesso collegata alle commissioni che gli utenti sono disposti a pagare per la verifica della transazione, mentre la *seniority* assume un ruolo secondario utile solo a prevenire un rallentamento eccessivo dell'operazione.

Un ulteriore elemento da prendere in considerazione per la scelta del sistema di conservazione è dato dalla possibilità di *fork* tipica dei sistemi distribuiti: in caso di aggiornamento del programma (come è già accaduto in *Bitcoin* e in *Ethereum*) o di annullamento di una transazione inserita in *blockchain* con ricalcolo delle successive (come capitato nel *DAO* di *Ethereum*), il database può procedere in biforcazione da quel punto in avanti, creando rallentamenti e rischio di duplicazione delle transazioni.

Un ultimo punto da prendere in considerazione è quello della riservatezza: i dati conservati in un *database* distribuito sono visibili a ogni nodo che ne fa parte, al contrario di quelli custoditi nei *database* centralizzati che sono accessibili solo a livello di amministratori di

sistema. Alcuni sistemi distribuiti cercano di ovviare all'inconveniente implementando tecniche di offuscamento come le *ring confidential transaction*[40], che collegano le transazioni a firme facenti parte di un gruppo in modo da rendere noto che ha firmato un appartenente al gruppo senza specificare quale, o le *zero-knowlegde proof* che validano la transazione senza conoscerne origine, destinazione e ammontare, eseguendo la verifica a conoscenza zero[41] che le monete appartengano a una lista pubblica di monete valide e spendibili[42]. L'applicazione di queste tecniche rallenta però ulteriormente l'attività nei sistemi distribuiti che si rivelano particolarmente utili nei contesti in cui manchi la fiducia tra le parti o si punti sulla robustezza del sistema, rimanendo invece le istanze di riservatezza e celerità meglio servite dai sistemi centralizzati.

5.2. *Blockchain*

La *blockchain* è una struttura dati a lista concatenata, in cui i nodi della rete registrano blocchi di informazioni secondo le regole proprie del sistema di attuazione. Allo stato dell'arte, quando si parla di *blockchain,* si fa riferimento alla *blockchain* del sistema *Bitcoin,* il modello

[40] Cryptonote Technology, Ring signatures: Untraceable payments, https://cryptonote.org/inside; Greg Maxwell, Confidential Transactions, 2013, https://www.weusecoins.com/confidential-transactions/; Shen Noether, Adam Mackenzie and Monero Core Team, Ring Confidential Transactions, 2016, https://www.ledgerjournal.org/ojs/index.php/ledger/article/download/34/61

[41] In una dimostrazione a conoscenza zero una delle parti dimostra all'altra di possedere una determinata informazione senza svelarla ma ripetendo più volte un comportamento basato proprio sul possesso di quell'informazione, adottando un comportamento analogo a quello che nel mondo reale potrebbe essere aprire ripetutamente una porta, senza mostrare la chiave utilizzata. *Vide:* Jean-Jacques Quisquater, Louis Guillou, Marie Annick, Tom Berson: *How to explain zero-knowledge protocols to your children*, 1989, CRYPTO '89, Proceedings on Advances in Cryptology, pag 628-631.

[42] Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), Eli Ben-Sasson, Alessandro Chiesay Christina Garmanz Matthew Greenz, Ian Miersz Eran Tromerx Madars Virzay, 2014, http://zerocash-project.org/paper

applicativo per antonomasia, che è anche un database distribuito: le considerazioni che svolgeremo in seguito seguiranno il medesimo schema di ragionamento, prendendo in considerazione le regole matematiche generali nella loro applicazione al caso specifico.

Si tratta di una catena logica: ogni blocco che viene aggiunto alla lista comprende un riferimento univoco al blocco che lo precede: la relazione fra blocchi consente così di percorrere l'intero database con la possibilità di risalire da ogni blocco fino al primo inserito. Per convenzione il c.d. *Genesis Block* presenta il valore "*Null*", rappresentato con 256 *bit* consecutivi con valore 0, nella posizione riservata al riferimento al blocco precedente; in tutti i blocchi successivi questo valore è ottenuto calcolando due volte *l'hash* di una piccola porzione del blocco precedente, denominata intestazione, applicando l'algoritmo *SHA256*. *L'hash* calcolato in questo modo è ancora una stringa di 256 *bit*, o 32 *byte*, che viene registrata nell'intestazione e pertanto diviene parte integrante dei dati che serviranno a produrre *l'hash* identificativo del blocco stesso che verrà inserito nel blocco successivo; di conseguenza questa struttura oltre a determinare la concatenazione dei blocchi ne fissa con certezza i contenuti.

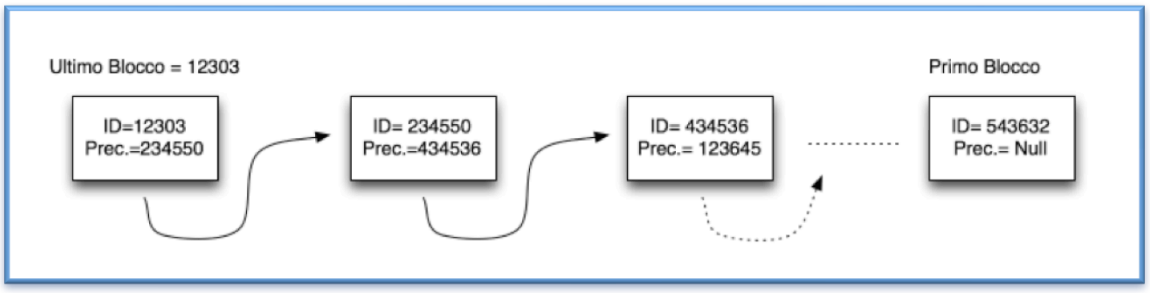


Figura 1: Struttura della *blockchain*

Modificando i dati registrati in un blocco il suo *hash* risulterebbe, infatti, completamente differente: dovendo riportare questo nuovo valore

nel blocco successivo, per mantenere la concatenazione si renderebbe necessario anche il ricalcolo di questo ulteriore *hash* poiché anche questo risulterebbe modificato: il ricalcolo degli *hash* necessario a preservare il collegamento matematico si propagherebbe così a tutti i blocchi successivi fino al raggiungimento dell'ultimo blocco della catena, rendendo l'operazione eccessivamente dispendiosa in termini di potenza di calcolo e di energia.

Il riferimento crittografico contenuto nei *blockheader* -basato su contenuto del blocco, marca temporale e *blockheader* precedente- viene considerato il modello di un nuovo tipo di firma di gruppo, la *dynamic-membership multiparty signature (DMMS)* [43]. Infatti, il sistema non pone limiti di ingresso alla competizione per il *mining,* impedendo di determinare *a priori* quali nodi parteciperanno*;* poiché i blocchi sono concatenati, la firma *DMMS* diviene cumulativa e la sua forza è direttamente proporzionale alla potenza computazionale globalmente impegnata.

Le dimensioni dei blocchi vengono liberamente determinate dal programma: ognuno di essi contiene un'intestazione che è formata da un numero fisso di dati e da un numero variabile, ma limitato, di transazioni e per aggiungere nuove operazioni al registro è necessario produrre nuovi blocchi da aggiungere alla struttura logica; le dimensioni della *blockchain,* invece, aumentano necessariamente nel tempo poiché la lista delle transazioni può solo essere integrata, senza possibilità di rimuovere alcuna voce. Nel sistema *Bitcoin* il programma limita attualmente il peso complessivo del blocco a 1 Megabyte[44]: la comunità *Bitcoin* sta valutando da tempo la possibilità di aumentare le dimensioni dei blocchi fino a un massimo di 16 *Megabyte*,

[43] Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuill, Enabling Blockchain Innovations with Pegged Sidechains, 2014, https://blockstream.com/sidechains.pdf

[44] Ogni blocco si compone di un prefisso che indica le dimensioni del blocco, un campo di 4 byte -che fissa per il blocco una dimensione massima di 2^{32} byte- un'intestazione di 80 byte e un numero variabile di transazioni.

un'eventualità che non è ancora stata realizzata per il timore delle conseguenze negative di una *fork* che potrebbe generare problemi in termini di certezza delle transazioni e di *double spending* come già è accaduto nel caso della *fork* di *Ethereum* che analizzeremo in seguito[45].

Poiché l'algoritmo che regola la difficoltà di calcolo diventa più complicato man mano che si aggiungono *miner* alla competizione, i nodi hanno un incentivo, in termini di risparmio energetico e impiego efficiente della potenza computazionale, a unirsi in *mining pool*. Ad esempio, la *blockchain Bitcoin* conta al momento 6875 nodi[46] concentrati in misura superiore all'80% in quattro *mining pool* cinesi[47]: questa scelta operativa introduce un problema ulteriore legato a eventuali attacchi all'*Internet Provider*[48]. Secondo un recente studio svolto in collaborazione fra i ricercatori dell'*ETH* di Zurigo e dell'Università Ebraica di Gerusalemme[49], sarebbe sufficiente prendere il controllo di meno di 100 prefissi *BGP*[50] per isolare fino al 47% della potenza computazionale, anche nel caso in cui la *mining pool* sia ridondata. Un attacco di questo genere riuscirebbe ad alterare il corso della *blockchain,* isolando i nodi di cui il *Provider* controlla la connettività e rallentando lo scambio di informazioni del protocollo, con tutte le conseguenze in tema di spreco di energia e *double spending*.

Alcuni dei rimedi suggeriti sul piano tecnico sono quelli di incrementare la ridondanza dei nodi, anche tramite *VPN* criptata;

---

[45] Vide ultra sub *Ethereum DAO*
[46] Global Bitcoin Nodes Distribution https://bitnodes.21.co/
[47] Naveen Joshi, 3 things to know about Bitcoin Blockchain, 2017, https://www.linkedin.com/pulse/3-things-know-bitcoin-blockchain-naveen-joshi?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BSOk75Q3zYBSq8FXP8dtdSg%3D%3D
[48]Richard Chirgwin Evil ISPs could disrupt Bitcoin's blockchain, 2017, https://www.theregister.co.uk/2017/04/11/evil_isps_could_disrupt_bitcoins_blockchain/
[49] Maria Apostolaki, Aviv Zohar, Laurent Vanbever , Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, 2016, https://arxiv.org/abs/1605.07524v2
[50] *Border Gateway Protocol*, il protocollo standard di comunicazione fra *router* disegnato per la comunicazione e lo scambio di informazioni sugli indirizzi di rete fra *Internet Provider*.

controllare che le connessioni fra nodi, generate in maniera casuale dal sistema, non dipendano tutte dal medesimo *Provider*, eventualmente aumentandone il numero*;* tenere monitorati i tempi di latenza, quelli di connessione, la distribuzione dei nodi e le disconnessioni simultanee; accettare le connessioni *random* proposte dal *network*, scelta che però appare poco probabile, dato il conflitto con eventuali regole di *firewall* e *NAT*[51] configurate nel nodo.

5.3. *Chameleon hash*

Una recente innovazione in materia di *blockchain* è rappresentata dal c.d. *chameleon hash* proposto da *Accenture*[52] per la gestione di *editable private blockchain*[53]; prima di procedere all'esame della proposta è opportuno segnalare che si tratta di un progetto in antitesi col principio fondamentale di immodificabilità della *blockchain* che ha suscitato più di una perplessità fra gli addetti ai lavori[54]. In questo modello il collegamento fra blocchi viene sostituito da un *hash* emendabile che consente all'amministratore di sistema di intervenire sulla catena modificando, sostituendo o rimuovendo singoli blocchi senza soluzione di continuità.

Il sistema è stato pensato per le *blockchain* private[55] gestite dalle banche[56]: ogni intervento di gestione, debitamente autorizzato e messo

[51] *Network Address Translation,* tecnica di traduzione degli indirizzi di rete privati in indirizzi pubblici. Si usa nella maggioranza delle reti private interne.
[52]Accenture Newsroom, Prototype of editable blockchain, 2017, https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm
[53] Accenture, Top 10 challenges for investments banks 2017, Blockchain moves to early adoption https://www.accenture.com/us-en/insight-investment-bank-challenge-10-distributed-ledgers
[54] Jeff John Roberts Why Accenture's Plan to 'Edit' the Blockchain Is a Big Deal, 2016, http://fortune.com/2016/09/20/accenture-blockchain/
[55] *Vide infra sub* 4.3

in sicurezza tramite l'uso di chiavi crittografiche tripartite, lascia comunque un'impronta permanente sul blocco a segnalare l'avvenuta modifica.

Mentre le funzioni di *hash tradizionali* sono funzioni calcolate su di un valore di ingresso singolo, detto testo, per cui:

$h(m) = y$;

nei *chameleon hash*[57] la funzione viene calcolata su due variabili di ingresso, delle quali una è il testo e l'altra è una chiave pubblica, per cui:

$h(m,r) = y$.

L'hash viene pertanto calcolato in riferimento a una chiave pubblica r assegnata; qualora sia necessario modificare il testo *m* in *m'*, il detentore della chiave privata associata ad *r* può trovare una nuova chiave pubblica *r'* tale che, la funzione ricalcolata su *m'* utilizzando la nuova chiave *r'*, provochi una collisione ottenendo così il *digest* originario; in formula:

$h(m',r') = y$.

Il calcolo può essere ripetuto in maniera ricorsiva, senza limite al numero di collisioni. La funzione *chameleon hash*, ovviamente, deve essere prevista dall'applicazione e può essere usata solo in *blockchain* private, essendoci la necessità di uno o più amministratori che detengano la chiave privata da usare in caso di correzione dei blocchi.

---

[56] Richard Kastelein Accenture Releases Patented Blockchain Editing Tool for Banks, 2016, http://www.the-blockchain.com/2016/09/20/accenture-releases-patented-blockchain-editing-tool-banks/

[57] Payman Mohassel, One-Time Signatures and Chameleon Hash Functions, 2010, https://www.researchgate.net/publication/221274662_One-Time_Signatures_and_Chameleon_Hash_Functions

Utilizzando i *chameleon hash,* la *blockchain* in figura 1 si modifica in questo modo:

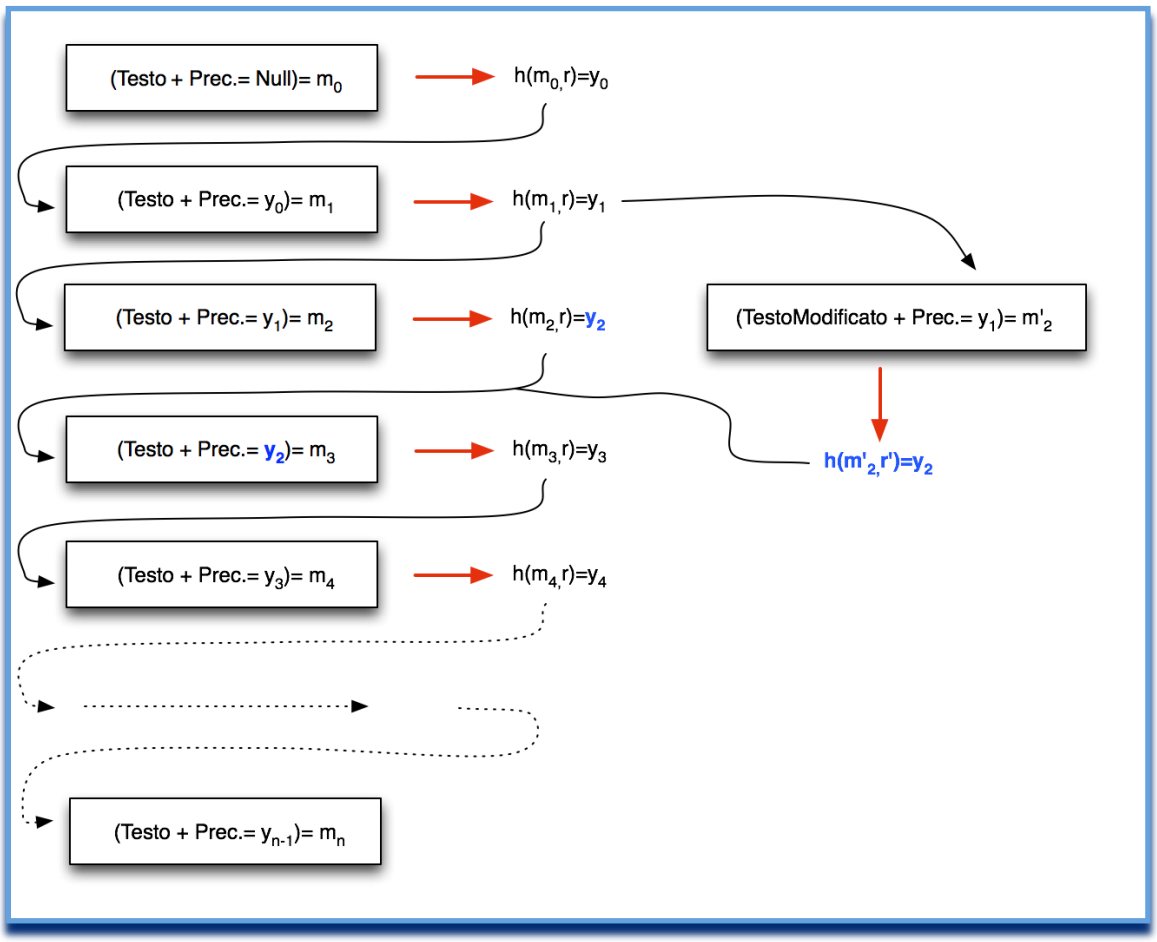


Figura 2: *Chameleon blockchain*

Un problema relativo all'uso di questa tecnica è la c.d. *Key Exposure,* una vulnerabilità di cui soffrono alcuni degli algoritmi *chameleon hash* sviluppati. In questi casi è possibile risalire alla chiave privata collegata con un'analisi crittografica che utilizzi il messaggio originale, quello modificato e le due chiavi pubbliche utilizzate per generare la collisione. È pertanto fondamentale che le applicazioni di *blockchain* che fanno uso del *chameleon hash* si basino su implementazioni robuste di questa funzione.

L'intervento dell'amministratore di sistema resta visibile perché l'*hash* del blocco modificato dovrà sempre essere verificato utilizzando la (nuova) chiave pubblica generata per la collisione *(r')* in luogo della precedente *(r)*.

5.4. *Merkle Tree*

Nel sistema *Bitcoin* la struttura *blockchain* è tale per cui le transazioni possono essere registrate in numero variabile nei diversi blocchi; inoltre, poiché ogni transazione porta con sé le informazioni relative ai propri vincoli di eseguibilità, le singole transazioni differiscono anche in dimensione. Allo scopo di agevolare il calcolo dell'*hash*, il sistema include nell'intestazione un campo unico che contiene un singolo *hash* ottenuto dai dati di tutte le transazioni incluse in quel blocco. Questo *hash* è ottenuto dagli *hash* calcolati su ogni singola transazione e riorganizzati in una struttura dati ad albero detta *Merkle Tree,* di cui rappresenta la radice.

La struttura così determinata consente di ottimizzare i tempi di calcolo e il trasferimenti dati fra i nodi quando si rende necessario verificare l'appartenenza di una specifica transazione, identificata dal proprio *hash*, a un certo blocco che conterrà *l'hash* della radice nel relativo *Merkle Tree*. Anche in questo caso ogni modifica dei dati relativi a una determinata transazione provocherebbe la modifica di tutti gli *hash* che formano i livelli superiori del *Merkle Tree*; modifica che si propagherebbe fino *all'hash* della radice che, essendo riportato nell'intestazione del blocco, provocherebbe la modifica *dell'hash* del blocco stesso. In questo modo la struttura dati garantisce l'inalterabilità del blocco anche a fronte di interventi sulla sua componente variabile che contiene il dettaglio delle transazioni.

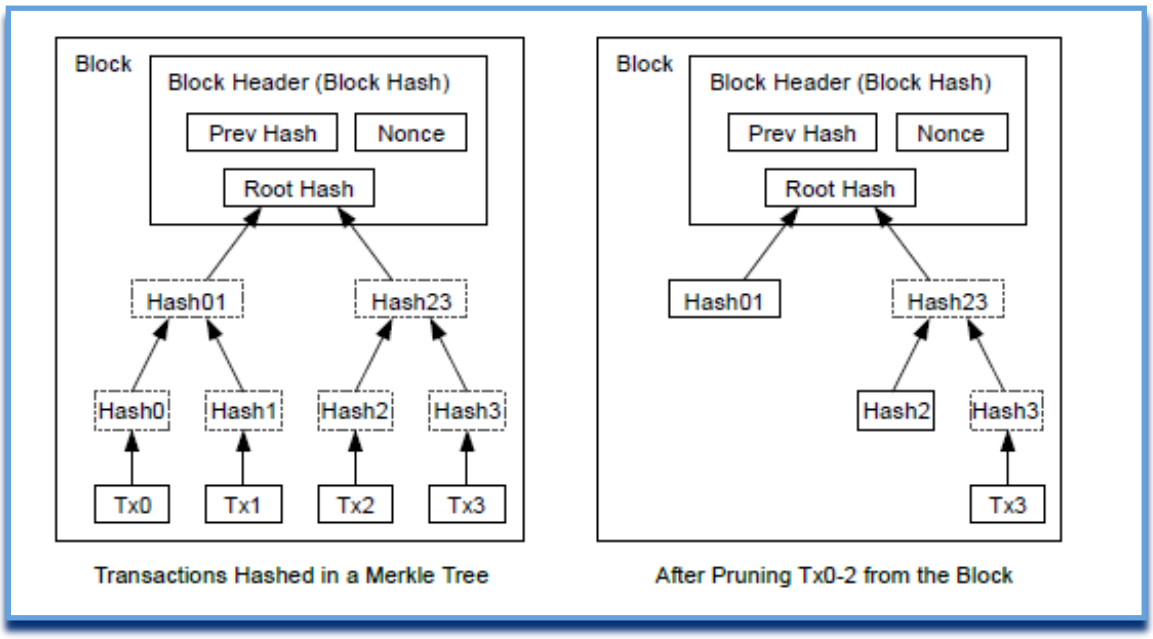


Figura 3: *Reclaming Disk Space - Bitcoin: A Peer-to-Peer Electronic Cash System* [58]

Come abbiamo accennato nel paragrafo precedente, la dimensione del registro è soggetta a un incremento costante, creando qualche problema di gestione a livello dei nodi: ad oggi per scaricare l'intera *blockchain Bitcoin* e diventare operativi come *full node* si possono impiegare anche tre settimane di tempo[59]. Nel *whitepaper Bitcoin*

[58] Satoshi Nakamoto, *Bitcoin*: A *Peer*-to-*Peer* Electronic Cash System, 2008, ,pag. 4 "*Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.*" https://*bitcoin*.org/*bitcoin*.pdf

[59] Alcuni programmi di gestione semplificata scaricano perciò solo i dati necessari alla gestione del portafoglio personale, identificabili con gli *hash* delle transazioni a cui il portafoglio fa riferimento. Questi dati, come indicato, sono poi verificabili tramite il valore radice del *Merkle Tree* contenuto nel blocco che deve coincidere con il valore ricavabile dalla radice tramite *hash chain,* una struttura dati ridotta costruita

Satoshi Nakamoto affronta il problema delle dimensioni della *blockchain* suggerendo di ridurre i blocchi da gestire usando la struttura *MerkleTree* per scartare tutte le transazioni spese che risultino antecedenti a un momento assegnato.

5.5. Side chain

Per non appesantire eccessivamente la *blockchain,* nel 2014 un gruppo di ricercatori capitanato da Adam Back[60] ha proposto di utilizzare le *side chain*, *soft fork* del sistema *Bitcoin;* il modello, descritto nel *paper Enabling Blockchain Innovations with Pegged Sidechains*[61] è dotato di *token* autonomo che viene scambiato a parità fissa con la moneta di un diverso sistema di riferimento. Ogni *blockchain* è, infatti, legata strettamente alla propria divisa e non è possibile disaccoppiarle: utilizzando una *sidechain* si possono però effettuare scambi con le monete di un sistema parallelo nel quale le transazioni verranno gestite *a latere* del sistema originario. I *token,* congelati sul sistema originario, saranno attivati su quello di destinazione in misura di uguale valore, con il vantaggio di poter implementare regole che non sono previste dalla *blockchain* originaria. La *sidechain* è, inoltre, completamente isolata dalla catena principale, ragion per cui gli eventuali problemi di gestione resteranno confinati al suo interno.

La necessità di lavorare su una catena logica *a latere* nasce dal bilanciamento di costi e benefici generati dalle rigide impostazioni di *Bitcoin*: si discute da tempo di aumentare le dimensioni delle

---

appositamente con i soli *hash* delle transazioni necessarie a ottenere ricorsivamente *l'hash* radice partendo dall*'hash* della transazione sottoposta a verifica.

[60] http://www.cypherspace.org/adam/

[61] Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuill, Enabling Blockchain Innovations with Pegged Sidechains, 2014, https://blockstream.com/sidechains.pdf

transazioni, di definirne di nuove di altra natura e varietà, ma gli sviluppatori concordano che, in considerazione dei problemi di *fork* e *double spending* che spesso si accompagnano agli aggiornamenti di questi sistemi, ogni innovazione debba essere apportata con la massima cautela. Si tratta di una necessità analoga a quella che ha portato alla creazione dei sistemi di moneta alternativi (*altchain*). Peraltro, la strada della creazione di nuove infrastrutture volta a superare tali limitazioni, spesso si rivela una soluzione poco efficiente considerando che in tal caso si dovrebbe far fronte a inevitabili sprechi di tempo e di energie, alla duplicazione di tutti i problemi di sicurezza del sistema originario e al diverso valore sul mercato che le monete dei nuovi sistemi inevitabilmente assumerebbero.

La tecnologia *sidechain* nasce allo scopo di consentire il movimento di risorse fra *blockchain* diverse consentendo agli utenti di continuare a utilizzare l'unità di moneta già in loro possesso; l'idea è attuata mettendo in parità fissa monete di sistemi diversi *(pegged sidechain),* soluzione che azzera il rischio di cambio nei movimenti di compravendita. Una volta spostate sulla *sidechain* le monete possono essere liberamente trasferite al suo interno, mentre il movimento all'esterno avviene necessariamente in direzione del sistema originario.

Nella *sidechain* possono essere implementate nuove regole, con apertura alla sperimentazione di eventuali modifiche da inserite nella *blockchain* principale: una specie di *sandbox* che consente di testare la bontà e l'efficienza di queste soluzioni di cui il sistema principale potrà fruire in un secondo momento, se e in quanto i *peer* concordino sulla loro adozione.

Allo stato dell'arte, *sidechain* basate su *BItcoin* vengono adottate da *Rootstock*[62]*,* una piattaforma dedicata all'implementazione di *smart*

[62] http://www.rsk.co/

contract; *MimbleWimble*[63], la maledizione lega-lingua di *Harry Potter*[64], un progetto che cerca di rafforzare la privacy degli utenti legando fra loro transazioni appartenenti a blocchi diversi; e *Bitcoin Hivemind*[65] dedicato alla raccolta di informazioni per i *prediction market,* mercati speculativi in cui i profitti derivano dai pronostici sui risultati di determinati eventi[66].

5.6. Amministrazione del sistema

Nei sistemi di *ledger* la tenuta del registro può essere pubblica, affidata cioè a tutti i nodi del *network*; distribuita all'interno di un gruppo selezionato che viene identificato con regole predeterminate; o addirittura privata, con presenza di un gestore unico, sia esso pubblico o privato: onde evitare equivoci è importante chiarire che gestione privata significa potere autonomo di un singolo, non amministrazione affidata a un privato.

Molto dipende anche da come vengono regolati i rapporti di forza fra i partecipanti: si può dare rilievo al numero dei nodi, alla percentuale di *token* in loro possesso o alla potenza computazionale impegnata.

I sistemi che adottano la prima regola vanno soggetti ai c.d. *sybil attack* (o attacchi a personalità multipla) in cui un nodo può tentare di

[63]MimbleWimble
https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt
[64] J.K Rowling, Harry Potter e la camera dei segreti, 1999, Adriano Salani Editore
[65] Bitcoin Hivemind http://bitcoinhivemind.com/
[66]Kyle Torpey, 5 Ways Bitcoins Could Be Transferred to a Sidechain, 2017, https://news.bitcoin.com/5-ways-bitcoins-transferred-sidechain/

moltiplicare fittiziamente la propria presenza sul *network* per esercitare più volte il diritto di voto.

Nel caso in cui venga adottata la regola della percentuale di possesso, è evidente che la predominanza di alcuni soggetti produrrebbe il rischio di una perdita di incentivo alla partecipazione al *network* dei nodi minoritari; sul lungo periodo, questa è la regola più disincentivante e quella che più contrasta con gli ideali alla base del modello.

La soluzione che fa riferimento alla potenza computazionale consente un bilanciamento delle esigenze, consentendo ai sistemi che la adottano di mantenere un peso paritario dei nodi ed eliminando in radice i problemi legati al *sybil attack:* anche se un nodo tentasse di mostrare un maggior numero di connessioni entrando più volte in rete con la stessa macchina sotto identità diverse, la potenza computazionale, misurata in *hashrate/s,* rimarrebbe inalterata impedendo all'eventuale *attacker* di moltiplicare fittiziamente la propria attività.

Quando il sistema distribuito è pubblico non sussistono regole per l'ingresso dei *miners* e chiunque può unirsi al *network*: per questa ragione i nodi non hanno alcun potere discrezionale sulle regole di validità delle transazioni, che sono predeterminate. Ogni modifica dovrà essere implementata ed eseguita in maniera uniforme dall'intera comunità: il modello che abbiamo appena descritto è adottato da *Bitcoin* e dai sistemi basati su di esso.

Altri sistemi, come *Ripple*, mettono un limite all'ingresso di partecipanti al sistema, demandando la gestione delle modifiche al consenso di un gruppo di *trusted validators*[67]. Si tratta di un meccanismo ampiamente rodato nei sistemi *open source,* come Linux che lascia alla comunità in generale la facoltà di proporre modifiche al

[67] Tiana Laurence, Blockchain for dummies, Wiley ed. , 2017: *Ripple* ha cessato di offrire servizi sul portale consumer, ma dà supporto agli sviluppatori che intendano implementare software basato sul loro *framework*.

sistema ma demanda la decisione su quelle implementazioni a un numero selezionato di sviluppatori.

Ogni sistema di *ledger* implementa regole proprie che vengono scritte in conformità con gli obiettivi perseguiti: la gestione privata, ad esempio, appare maggiormente efficiente nei sistemi in cui il *ledger* è utilizzato per finalità di conservazione documentale, come ne caso degli archivi dematerializzati, o di sperimentazione, come in alcune *sidechain.* In questo caso la *blockchain* viene implementata con regole autonome, senza ricorrere alla *proof of work* e mantenendo inalterati i requisiti di protezione crittografica e marcatura temporale per la sicurezza delle operazioni e la loro riferibilità a una data certa.

Dalla scelta del tipo di *blockchain* dipende la risposta del mercato in termini di affidamento sulla solidità del gestore e di fiducia nello strumento offerto. I diversi tipi di amministrazione si attagliano correttamente alle diverse funzioni che la *blockchain* può svolgere: come accennato, la certificazione può funzionare correttamente con affidamento a un gestore unico: si pensi a caso dei documenti sanitari che lo Stato Estone conserva concatenandoli in un'apposita *blockchain*[68], pianificando a breve l'estensione di questo metodo al settore dei documenti di identità[69]. Nel caso dei sistemi di pagamento, invece, il trasferimento di diritti vede nella partecipazione alla gestione dell'intero *network* un elemento di garanzia per la certezza dei trasferimenti e il contrasto a eventuali tentativi di *double spending*. La gestione consortile può infine offrire i vantaggi del contemperamento di esigenze opposte nel caso di quei progetti, come Ripple[70] o Corda[71], che

[68] E-health – Estonian Digital Solutions for Europe https://e-estonia.com/e-health-estonian-digital-solutions-for-europe/
[69] Mark Stone, The Tiny European Country That Became A Global Leader In Digital Government, 2016, https://www.forbes.com/sites/delltechnologies/2016/06/14/the-tiny-european-country-that-became-a-global-leader-in-digital-government/#6e2ef90ae13a
[70] https://ripple.com/

propongono l'offerta al pubblico di servizi bancari e finanziari, mettendo a disposizione degli utenti informazioni certe e trasparenti senza inficiare le istanze di amministrazione autonoma del gruppo di azione.

La scelta di una *blockchain* ad amministrazione privata o consortile consente di limitare i permessi di lettura: infatti, se la *blockchain* ad amministrazione pubblica deve essere visibile a tutti i nodi per potere essere eseguita, negli altri due tipi di gestione si possono assecondare specifiche istanze di riservatezza autorizzando all'accesso un numero determinato di soggetti. È il caso, ad esempio, della conservazione documentale dematerializzata cui si stanno recentemente orientando i professionisti appartenenti agli Ordini Notarili: l'inserimento in una *blockchain* ad accesso ristretto degli *hash* identificativi dei documenti dematerializzati consente una conservazione di tipo robusto introducendo un'ulteriore tutela delle istanze di *privacy* collegate a questa delicata attività.

[71] Richard Gendal Brown, Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, 2016, http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

6. Sistemi

Premessa

Parliamo di sistemi per indicare strutture complesse composte da programmi, protocolli di comunicazione e tutto quanto di infrastrutturale occorre al funzionamento: sistemi operativi, hardware, infrastruttura di rete per la comunicazione. I programmi, che a propria volta consistono della somma di strutture dati e algoritmi, girano sia su lato *client,* originando e validando le transazioni, che su lato *server,* validando i blocchi o i *ledger* e inserendoli nel registro logico con applicazione di una marca temporale. Di seguito ci occuperemo dei tre i principali sistemi in uso: Bitcoin, basato su *blockchain*, *Ethereum*, che implementa il sistema *Bitcoin* tramite il protocollo *Ghost*[72] e *Ripple*, basato su un meccanismo di consenso ad approvazione progressiva con registro distribuito (*distributed ledger)*, dedicando una quarta sezione ai sistemi che utilizzano metodi di offuscamento della *blockchain*.

[72] Ghost, Ethereum Glossary, 2016, https://github.com/ethereum/wiki/wiki/Glossary;
Ethereum, Design Rationale, 2016, https://github.com/ethereum/wiki/wiki/Design-Rationale#uncle-incentivization

6.1. *Bitcoin*

Le moderne tecnologie rendono sempre più auspicabile per il singolo di poter svolgere i propri acquisti in maniera riservata, evitando le procedure di raccolta di dati a fini commerciali normalmente poste in essere dagli intermediari di moneta elettronica. L'invio di una qualunque informazione via *internet,* come può essere un *file* di testo o un *MP3,* prevede che una copia dell'informazione venga trattenuta sul *computer* che procede all'invio. La stessa cosa accade per l'invio di moneta in forma elettronica e, in questo caso, diviene fondamentale l'intervento di un terzo garante per assicurare che l'ammontare di denaro a disposizione dell'acquirente abbia subito una variazione negativa pari a quanto speso ed evitare che possano essere attuate forme di doppia spendita della valuta.

Alla fine del 2008 un articolo a firma dello pseudonimo Satoshi Nakamoto[73] ha presentato alla rete *Bitcoin,* un sistema distribuito fra i nodi di una rete *peer-to-peer*[74], progettato allo scopo di mettere in sicurezza i pagamenti elettronici a prescindere dall'intervento di un garante esterno. L'*utility* procede al trasferimento elettronico sulla base di un sistema gestito dai *peer* della rete che provvedono alla verifica e convalida delle transazioni, offrendo garanzia di spendita unitaria, e mettendo in sicurezza il trasferimento tramite l'applicazione della funzione crittografica di *hash*[75] e della firma elettronica.

[73]Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008, http://*bitcoin*.org/*bitcoin*.pdf

[74]Una rete *peer-to-peer* è organizzata secondo un'architettura paritaria: i nodi differiscono tra loro solo per le capacità della macchina impiegata e l'ampiezza di banda di connessione di cui dispongono mentre le capacità di gestione sono del tutto analoghe e ognuno di essi è in condizione di portare a termine le medesime operazioni.

[75] Si tratta di una funzione crittografica non reversibile utilizzata per l'identificazione di un *file*. Applicando l'*hash* a un file si genera un numero, normalmente rapprsentato con una stringa esadecimale detta *digest,* che varia sensibilmente al variare anche di uno solo degli elementi del *file* esaminato: dal confronto dei *digest* si può agevolmente

6.1.1. *Mining*

Bitcoin è un'applicazione basata su *blockchain,* gestita da un *network peer to peer* che implementa un protocollo di gestione distribuito. Nella produzione dei *bitcoin,* detta *mining,* i nodi della rete utilizzano la propria potenza di calcolo per comporre e verificare i blocchi che registrano le nuove transazioni da aggiungere alla catena logica (cd *blockchain*). Questi complessi calcoli matematici devono essere convalidati da una *proof of work,* un dato particolarmente difficile da ottenere[76]: l'operazione genera in *output* un blocco di *bitcoin*[77] che viene attribuito al primo *computer* che ha risolto il problema e viene aggiunto alla catena logica insieme a tutte le transazioni associate.

Il sistema è progettato per mantenere costante la velocità di produzione dei blocchi al tasso di un blocco ogni 10 minuti circa: l'effetto è dovuto all'aumento della difficoltà richiesta per la produzione della *proof of work* che cresce in maniera proporzionale alla potenza computazionale impegnata. La ricompensa per la produzione è invece soggetta a un decremento del 50% ogni 210.000 blocchi (corrispondenti a circa 4 anni di tempo) in maniera che, col passare del tempo, la produzione di *bitcoin* tende asintoticamente a zero[78]: il sistema di Nakamoto stabilisce infatti un numero massimo di bitcoin da produrre

---

capire se due *file* sono identici o se siano intervenute modifiche, manipolazioni o corruzioni nel passaggio fra l'originale e la (presunta) copia.

[76] *Vide https://fr.bitcoin.it/wiki/Preuve_de_travail: " La version la plus commune est basée sur celle imaginée par David Chaum, utilisant une fonction de hashage. L'épreuve consiste donc, pour une chaîne alphanumérique donnée, à y concaténer une chaîne alphanumérique aléatoire jusqu'à ce que le hash de l'ensemble soit inférieur à un seuil donné."*

[77] Stringhe alfanumeriche idonee al trasferimento in applicazione del protocollo.

[78] Originariamente ogni blocco consisteva di 50 *bitcoin:* la consistenza si è ridotta a 25 a far data dal 28/11/2012, mentre dal 9 luglio 2016 vengono prodotti dei blocchi da 12,5 *bitcoin*: https://*blockchain*.info/block-index/322335/000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e

entro l'anno 2140 di cui, ad oggi, sono stati prodotte oltre 16.400.000 unità; il limite è dato dall'applicazione dell'algoritmo di dimezzamento del premio che consente la produzione di 20.999.999,9769 *bitcoin*[79]. Col progredire delle operazioni, il *mining* richiede sempre maggior capacità di calcolo ed energia: occorrono macchine dedicate[80] le cui spese di acquisto si sommano ai costi di produzione, calcolati in elettricità e potenza di calcolo impiegate[81], fissando così un *floor* al valore di cambio dei *bitcoin* in moneta corrente.

Nel *mining* i nodi per competono tra loro per agganciare nuovi blocchi alla catena logica: ognuno di essi forma un blocco candidato che contiene le transazioni con le commissioni maggiori e quelle che il sistema impone di processare in forza della loro *seniority*; *l'hash* identificativo di ogni nuovo blocco candidato deve rispettare un formato particolare, che comincia con un numero determinato di bit a zero: per ottenere questo valore, i nodi includono nell'intestazione del blocco un valore detto *nonce,* acronimo di *number used once,* che serve a far coincidere *l'hash* con la soglia stabilita dal sistema. La corretta individuazione del *nonce* determina la *proof of work:* rendere l'*hash* del blocco conforme al formato richiesto richiede uno sforzo computazionale direttamente proporzionale alla potenza impiegata dal *network*, richiedendo uno sforzo eccessivo per un eventuale *attacker*. Il *nonce* è un numero di 32 *bit* la cui individuazione, allo stato dell'arte, richiede l'esame di un numero di poco inferiore alla soglia di 4 miliardi e 300 milioni di combinazioni; il numero iniziale di *bit* a zero viene stabilito dal sistema in maniera proporzionale alla potenza computazionale

[79]https://www.reddit.com/r/Bitcoin/comments/20etko/why_21_million/
Nell'agosto 2010 Il software di produzione ha dovuto essere riscritto a causa di un *bug* che aveva causato un errore detto *integer overflow,* a causa del quale il blocco 74638 conteneva due transazioni la cui somma era superore a 184 miliardi di *bitcoin,* una quantità evidentemente incompatibile con il numero di soluzioni finite dell'algoritmo. *Vide* http://*bitcoin*magazine.com/3668/*bitcoin*-network-shaken-by-*blockchain*-fork/
[80]*https://en.bitcoin.it/wiki/Mining_hardware_comparison*
[81]http://www.rischiocalcolato.it/2014/01/*bitcoin*-costi-del-mining.html

impiegata dai nodi, misurata in *hashrate/s* cioè dal numero di *hash* che i nodi della rete riescono a calcolare in un secondo.

Il merito del lavoro svolto viene ricompensato attribuendo al nodo vincitore le *fees* collegate alle transazioni inserite nel blocco e un numero di nuovi *bitcoin* che varia nel tempo secondo le modalità previste dall'algoritmo di dimezzamento. Una volta agganciato il blocco candidato alla catena logica, i nodi riprenderanno l'attività computazionale formando nuovi blocchi candidati: le transazioni contenute nei vecchi blocchi candidati non ancora validate verranno inserite in altri nuovi e ricomincerà il calcolo della *proof of work*.

Ciascuna transazione viene confermata dalla generazione di 6 ulteriori blocchi il cui *hash* è sottoposto a verifica dai *peer* della rete man mano che eseguono i calcoli per la validazione dei blocchi successivi: l'operazione può richiedere fino a un massimo di 50 minuti di tempo dal momento in cui viene agganciato alla catena logica il blocco che contiene la transazione. In questo modo i nodi della rete procedono alla verifica e alla convalida dei pagamenti eseguiti, garantendo l'effettività delle transazioni: la continua esecuzione di calcoli matematici da parte dei *miner* evidenzia che il valore posto a base del *bitcoin* consiste non tanto in un bene, quanto nel servizio offerto.

6.1.2. Sicurezza del sistema

Una volta applicato l'algoritmo di *hash* si può verificare in ogni momento che non siano state effettuate modifiche successive alla conclusione della transazione: eventuali alterazioni o manomissioni del *file* produrrebbero infatti un *digest* differente. Ogni operazione sui *bitcoin* viene completata dall'applicazione di una marca temporale, una procedura informatica che consente di associare data e ora al *file,* al

fine di verificare che le attività si siano svolte secondo l'ordine temporale dichiarato, evitando che il cedente possa procedere a una nuova transazione con unità che ha già trasferito in precedenza.

La sicurezza del sistema si basa sulla *proof of work,* un valore che, da un lato impedisce ai *miner* di produrre *bitcoin* indiscriminatamente consentendo loro di ottenerli solo come premio della loro attività efficace, dall'altro rende praticamente impossibile l'annullamento delle transazioni eseguite sui *bitcoin:* ogni blocco contiene infatti un *hash* che dipende dalla *proof of work* di tutti i blocchi precedenti, pertanto ogni modifica apportata su di esso si rifletterebbe su tutti quelli successivi[82] implicandone il ricalcolo. La *proof of work* contribuisce così in modo significativo al consolidamento del registro informatico: volendo modificare i dati di un blocco, si renderebbe necessario non solo il ricalcolo di tutti gli *hash* ma anche il ricalcolo di tutte le *proof of work;* questo attributo rende il sistema matematicamente resistente a ogni attacco che non possa disporre di almeno il 51% della potenza computazionale dell'intero *network*.

In questo senso il *whitepaper* di Nakamoto sottolinea che il trasferimento dei *bitcoin* si svolge in sicurezza se la maggioranza delle *CPU* nella rete *peer-to-peer* è controllata da nodi onesti[83]; il sistema è,

---

[82]L'11 marzo 2013, a causa di un aggiornamento del *software* di *mining* che era stato installato solo da una parte della comunità, si è verificato un problema denominato *blockchain fork* per cui si è avuta una biforcazione della catena dei blocchi durata circa 6 ore; durante questo tempo, parte dei *miner* hanno aggiunto i blocchi estratti con la versione 0.8 del programma a una derivazione autonoma della *blockchain* mentre il resto di loro proseguiva la catena orignaria utilizzando la versione 0.7, senza riconoscere i nuovi blocchi: il problema è stato risolto con il *downgrade* generale del *software* alla versione 0.7. Nelle sei ore in cui è stata operativa, la *blockchain fork* ha causato un crollo del 24% del valore di cambio contro il dollaro, la perdita di 24 blocchi da 25 *bitcoin* minati con la versione 0.8 per il controvalore di $ 26.000 e il *double spending* di $ 10.000 sul sito *okpay*.com. Anche nel caso del *bug* del 2010 l'applicazione della nuova versione del *software* aveva prodotto una biforcazione della *blockchain,* rientrata in corso unitario con uno scarto di 53 blocchi da 50 unità ma a quel tempo il valore e la diffusione dei *bitcoin* erano di portata talmente ridotta da consentire una gestione agevole delle conseguenze.
Vide http://*bitcoin*magazine.com/3668/*bitcoin*-network-shaken-by-*blockchain*-fork/

[83]"*By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the*

infatti, immune dagli attacchi con tecniche di forza bruta in cui si provano in sequenza tutti i codici possibili poiché il calcolo della *proof of work* è di per sé un procedimento a forza bruta e l'eventuale tentativo di inversione dell'algoritmo *SHA265* –unica alternativa all'attacco a forza bruta- richiederebbe secoli di lavoro anche al più potente dei *supercomputer* oggi esistenti. La reversibilità delle transazioni in *bitcoin* può essere efficientemente portata a termine solo dall'interno: un eventuale *51% attack* consentirebbe a un gruppo di nodi collusi di prendere il sopravvento sul sistema compromettendone definitivamente la stabilità[84]; ad oggi non vi è notizia di attacchi di questo genere e, nonostante l'aumento di valore dei *bitcoin* possa rappresentare un incentivo al comportamento disonesto, l'attuale concentrazione dell'80% dei nodi in quattro mining pool[85] costituisce una spinta più che efficiente al mantenimento della stabilità economica dello strumento. Infatti questi soggetti traggono il loro guadagno dalla stabilità del mercato e non hanno alcun incentivo a sovvertire la *blockchain* distruggendo la fiducia degli utenti e provocando un crollo delle quotazioni.

---

network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. […]The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth". Satoshi Nakamoto: Bitcoin A Peer-to-Peer Electronic Cash System, p. 4 http://*bitcoin*.org/*bitcoin*.pdf 2008.

[84]Satoshi Nakamoto, *Bitcoin*: A *Peer*-to-*Peer* Electronic Cash System, https://*bitcoin*.org/*bitcoin*.pdf ,pag. 3 " *If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes."*

[85] Naveen Joshi, 3 things to know about Bitcoin Blockchain, 2017, https://www.linkedin.com/pulse/3-things-know-bitcoin-blockchain-naveen-joshi?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BSOk75Q3zYBSq8FXP8dtdSg%3D%3D

6.1.3. Conservazione e trasferimento

La conservazione dei *bitcoin* può essere fatta sia in portafogli *on line*, c.d. *hot storage*, che su supporti esterni scollegati dalla rete, c.d. *cold storage,* normalmente protetti con crittografia. I primi offrono praticità d'uso ma espongono maggiormente il proprietario a eventuali attacchi degli *hacker*; i secondi richiedono una procedura più lunga per l'uso ma soffrono in misura ridotta dei problemi indicati: per sottrarli occorre infatti impossessarsi del supporto che materialmente li contiene e delle chiavi crittografiche installate. L'esperto informatico Hal Finney, destinatario della prima transazione in *bitcoin*, revisore del *software* e protagonista della prima ora del sistema, decise di trasferire i bitcoin che possedeva in un *cold wallet* quando il loro valore in moneta reale divenne significativo[86].

Il trasferimento dei *bitcoin* si basa su un sistema crittografico a chiavi asimmetriche[87] che garantisce l'anonimato dei contraenti: si utilizza cioè un sistema di comunicazione sicura che prevede un'alterazione dei messaggi inviati secondo uno schema predefinito sufficientemente complicato da evitare la decrittazione da parte di terzi non autorizzati. Il sistema utilizza due chiavi, una pubblica e distribuita e l'altra privata e strettamente personale, per ognuno dei soggetti coinvolti nella trasmissione. Il mittente utilizza la chiave pubblica del destinatario come se fosse un lucchetto aperto che chiude sul messaggio da inviare, criptandolo; il destinatario compie l'operazione inversa, utilizzando la propria chiave privata per riaprire il lucchetto e

[86] Hal Finney Bitcoin and me (Hal Finney) , 2013, https://bitcointalk.org/index.php?topic=155054.0

[87] Per maggiori informazioni *vide* Stalling W., Crittografia e sicurezza delle reti,2/ed Apogeo 2007 e Trappe W., Washington L.C. Crittografia con elementi di teoria dei codici, Pearson Ed. Italia 2009.

decrittare il messaggio[88]. Le parti vengono identificate tramite l'indirizzo *IP,* l'etichetta numerica che individua in maniera univoca un dispositivo connesso a una rete che usa il sistema internet, e un nome a loro scelta che coincide con un indirizzo *bitcoin* e che può essere diverso per ogni transazione eseguita[89]; nei casi in cui intervengano più parti alla transazione o ci sia necessità di verificare l'esecuzione della prestazione prima del pagamento, si possono utilizzare degli indirizzi, detti *multi-signature* (*multisig*), che fanno capo a un gruppo di tre firme richiedendo l'inserimento di più chiavi per l'autorizzazione del trasferimento e accentuano le caratteristiche *anti-tampering* del sistema.

Il denaro ricevuto in una transazione deve essere speso in maniera unitaria, così ricevendo su un determinato indirizzo l'importo di 0.10 *bitcoin* si dovrà movimentare l'intero importo nella transazione successiva; il mittente deve altresì specificare su quale indirizzo preferisce ricevere l'eventuale resto, ferma restando la capacità di un indirizzo di ricevere più transazioni indipendenti fra di loro. Ogni transazione può combinare importi diversi ricevuti in varie transazioni: continuando nell'esempio precedente l'importo di 0.10 potrebbe essere sommato con gli importi di 0.20 e 0.30 ricevuti in due distinte transazioni precedenti dando luogo a un pagamento unitario di 0.60. Fermi restando i limiti della normativa antiriciclaggio, un pagamento unico può essere frazionato in operazioni distinte: invertendo le operazioni del nostro esempio si potrebbe così disporre un pagamento complessivo di 0.60 in tre *tranche* da 0.10, 0.20 e 0.30.

---

[88]Si ritiene che la prima transazione effettuata in *bitcoin* sia stata quella con cui il 21 maggio del 2010 Laszlo Hanyecz, uno dei primi sviluppatori del progetto *bitcoin*, acquistò due pizze da asporto alla pizzeria Papa John's di Jacksonville (FL) per 10.000 *bitcoin*. In realtà Hanyecz aveva venduto i *bitcoin* a un acquirente inglese il quale aveva, a propria volta, inviato alla pizzeria il controvalore concordato di $25 con un trasferimento internazionale su carta di credito; al valore di cambio raggiunto nel giugno 2017 l'equivalente del prezzo in *bitcoin* delle due pizze sarebbe stato nell'ordine di $ 30.000.000.

[89] quest'ultima caratteristica introduce la questione della pseudo - anonimia, caratteristica permeante dei *bitcoin*: è l'utente che, impostando i parametri identificativi e variandoli a propria insindacabile scelta, sceglie il grado di riservatezza di cui desidera fruire.

La catena delle transazioni è pubblica e ininterrotta e consente di tracciare la storia dei blocchi di *bitcoin* e delle transazioni loro associate in tutti i passaggi che la compongono[90]: ogni *bitcoin* è composto da 100.000.000 *satoshi* e può avere origine dal *mining* di un blocco, essere ricevuto in pagamento o essere acquistato sul mercato secondario dove tutte le unità e le loro frazioni possono essere spese.

Ad oggi, esistono diverse centinaia di strumenti analoghi ai *bitcoin*[91]: uno dei loro usi principali è quello relativo alla c.d. Tecnofinanza o *Fintech*[92] e, oltre il sistema dei pagamenti, esiste tutta una serie di applicazioni che possono trarre giovamento dalla struttura dati della *blockchain Bitcoin*. Fra queste possiamo annoverare le operazioni di esercizio e verifica del voto, la tracciabilità della filiera di provenienza, la certificazione e la conservazione documentale; l'area che a nostro parere appare più innovativa è quella della contrattazione *smart*, in cui la tecnologia consente di eseguire alcune clausole in maniera automatica al ricorrere di determinate condizioni, come esamineremo dettagliatamente in prosieguo.

Come detto, molte di queste applicazioni girano su *blockchain bitcoin* rendendo sempre più attuale il problema delle dimensioni della struttura, già affrontato nel *Bitcoin Whitepaper.* Diventa così auspicabile l'uso di monete alternative (*altchain*), che registrino le proprie attività su infrastrutture indipendenti da *Bitcoin*, o di *sidechain* che, tramite il sistema di parità fissa illustrato nel capitolo precedente, consentano di gestire le attività in via parallela conservando sulla *blockchain Bitcoin* solo le operazioni in ingresso e in uscita.

---

[90] *Vide* http://*blockchain*.info/

[91] *Vide http://coinmarketcap.com/*

[92] The Economist, The fintech revolution, 2015: "*From payments to wealth management, from peer-to-peer lending to crowdfunding, a new generation of startups is taking aim at the heart of the industry—and a pot of revenues that Goldman Sachs estimates is worth $4.7 trillion."* http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution

6.2. *Ripple*

6.2.1. Formazione del consenso

Ripple è una piattaforma di trasferimento che utilizza un *database* distribuito in cui il registro delle operazioni di ogni *account* è conservato in *ledger* legati tra loro in una *hashchain*: il registro contiene tutte le informazioni di sistema, con particolare riguardo ai depositi, alle transazioni effettuate, alle offerte di acquisto e vendita di monete digitali e valute tradizionali, alle commissioni offerte e all'ammontare delle riserve di ogni account; le operazioni vengono riscontrate con *time stamping,* associando ora e data certa a ogni attività.

I nodi del *network* si dividono in *monitoring* (o *tracking*) e *validating*: i primi ricevono le transazioni dalle applicazioni *client* del sistema, come *web wallet*, società bancarie e finanziarie, piattaforme di *trading*, e le aggregano in proposte che inviano ai secondi per la convalida. I *validator* ricevono le transazioni candidate dai nodi presenti in una lista di riferimento (*Unique Node List*)[93]: il termine *Unique* fa riferimento al requisito formale per cui ogni nodo deve essere gestito da un soggetto

[93] *Unique Node List* https://wiki.ripple.com/Unique_Node_List

diverso, mentre la composizione della lista è libera e viene gestita in maniera autonoma da ogni nodo; la scelta effettuata determinerà le capacità di interazione del *validator* col sistema, infatti le proposte che provengono da soggetti estranei alla *UNL* vengono scartate *a priori*. Gli amministratori di sistema suggeriscono di comporre la lista facendo riferimento a un numero di *tracking node* superiore a 100; infatti, anche nell'ipotesi di un *sybil attack,* in cui un attacker gestisce più nodi, vi è una scarsa probabilità statistica che i nodi della *UNL* siano controllati dalla medesima fonte in misura superiore 50% dei partecipanti; ad ogni modo, poiché è importante tenere presente che una collusione superiore al 20% potrebbe comunque provocare seri rallentamenti al *network*, sarebbe opportuno che l'elezione dei partecipanti alla *UNL* tenga in conto criteri di differenziazione geo-politica, commerciale, legislativa e giurisdizionale portando all'inclusione di soggetti portatori di interessi molto diversi tra loro che avrebbero scarso incentivo a colludere proprio in considerazione del rapporto costi-benefici che questa strategia implica.

I *tracking node* possono essere *full* o *light* a seconda del fatto che conservino l'intera cronologia delle transazioni o solo parte di essa, analogamente a quanto accade nel sistema *Bitcoin*; poiché i *validator* ignorano le transazioni accettate dai nodi estranei alla *UNL*, il sistema è necessariamente distribuito.

L'inserimento di nuovi dati nel registro si basa sul consenso ad approvazione progressiva[94] dei *validator*[95]: non essendo prevista la partecipazione pubblica, non è richiesto il calcolo della *proof of work,* accelerando sensibilmente l'esecuzione delle transazioni. Il sistema crea nuovi *ledger* a intervalli temporali che variano fra i 10 e i 30 secondi,

[94] https://ripple.com/files/ripple_consensus_whitepaper.pdf
https://ripple.com/build/ripple-ledger-consensus-process/
[95]https://charts.ripple.com/#/validators Allo stato dell'arte, il gruppo è composto di 32 elementi, di cui 5 gestiti direttamente da *Ripple e* consigliati ufficialmente https://wiki.ripple.com/Consensus_Process); altri importanti v*alidator* sono gli *MIT Media Lab*, il *data center @Tokio,* il *gateway XAGATE* e il *trader Gatehub.*

attestandosi su tempi molto più brevi dei 10 minuti richiesti dalla produzione dei blocchi di *Bitcoin*.

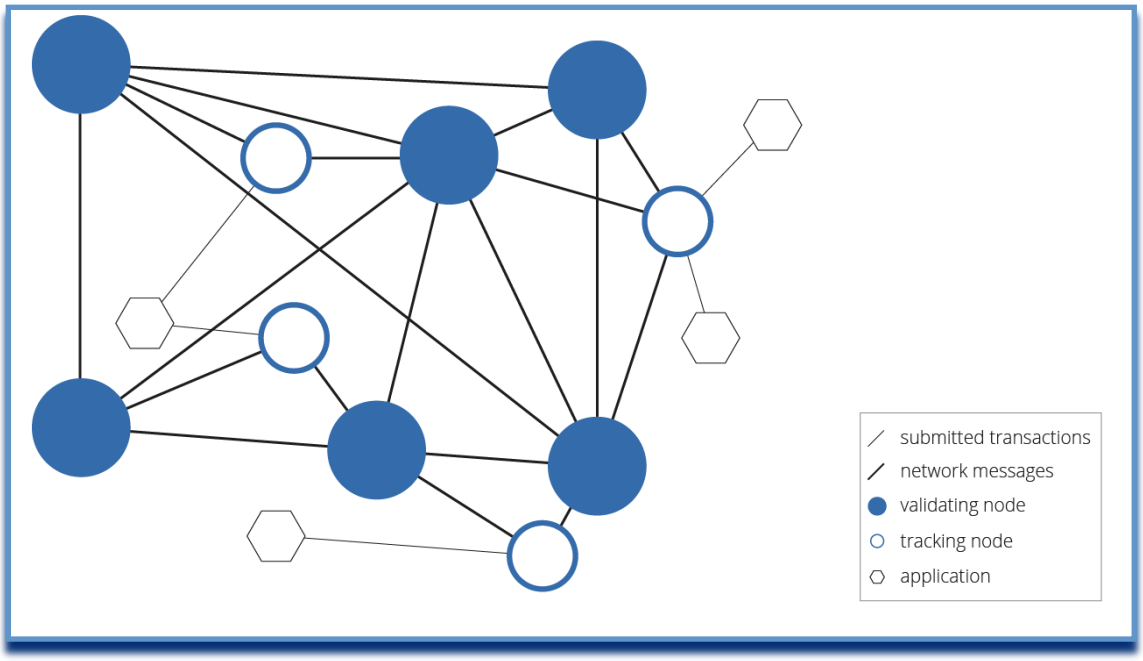


Figura 4*: Participants in the Ripple Protocol - The Ripple Ledger Consensus Process*[96]

I nodi, identificati tramite la loro chiave pubblica, validano le transazioni firmandole con la chiave privata; i *validator* applicano un ulteriore strumento di controllo espellendo dalla UNL quei nodi che sistematicamente approvino transazioni errate. I *tracking node* aggregano le transazioni in proposte e le inviano *validator* che, dopo averle approvate, le inseriscono in un *set* candidato all'inserimento nel registro logico; le transazioni contenute in ogni proposta successiva ricevuta dal *validator* verranno confrontate con quelle del *set* candidato, ricevendo voto positivo qualora coincidano con quelle già convalidate da quel nodo.

[96] Dave Cohen, David Schwartz and Arthur Britto, The Ripple Ledger Consensus Process, 2014, https://ripple.com/build/ripple-ledger-consensus-process/

Il processo di approvazione si svolge in quattro fasi successive, regolate da un *timer* che calcola un tempo di dieci secondi: ad esito della prima validazione, le proposte che abbiano ricevuto almeno il 50% dei voti dei *validator* vengono raggruppate in una nuova proposta che viene inviata agli altri *server* del *network* per una seconda approvazione in cui la percentuale di consenso necessario vene innalzata al 60%. Il procedimento si ripete in maniera analoga a quella appena descritta e allo scadere del *timer* le transazioni approvate vengono aggregate in una ulteriore proposta la cui convalida richiederà il 70% dei consensi. L'ultima fase prevede che la convalida avvenga al raggiungimento dell'80% dei consensi; questa soglia consente di chiudere il *ledger*, che verrà ora in considerazione come *Last Closed Ledger (LCL)*, con aggregazione al *network* di tutte le transazioni in esso contenute. Le altre transazioni ricevute nel procedimento che non siano state scartate per invalidità vengono inserite in un nuovo *candidate set* che il sistema processa in un nuovo *ledger*.

6.2.2. Origini della piattaforma

Il sistema originario di Ripple[97] è nato nel 2005 da un'idea di Ryan Fugger, un programmatore di Vancouver (CA) che ha sviluppato le teorie di Michael Linton sui *LETS, local exchange trading system*[98]: l'idea era quella di risolvere il problema del *free riding* che affliggeva quel progetto, mettendo in contatto tra loro gli utenti della *community* in modo da individuare degli intermediari che entrambe le parti dello

[97]https://ripple.com/
[98]http://www.themoneyfix.org/interviewee/michael-linton

scambio ritengano affidabili, sviluppando un sistema economicamente efficiente[99].

Il meccanismo originale ruotava attorno a una serie di affidamenti e promesse di pagamento: ogni utente dichiarava il limite del credito che era disposto a concedere a determinati altri utenti; il sistema, registrate le dichiarazioni, metteva in contatto i collegamenti di grado superiore al primo generando un traffico economico basato su una catena di riconoscimenti di debito (*IoU, I owe You*).

Ad esempio, nel caso di caso di Alice, disposta a concedere a Bob un credito di $ 10, Bob poteva, a propria volta, essere disposto a concedere a Charlie un credito di $ 100: il ruolo originario del sistema consisteva nel generare una serie di contatti registrati *intra-network.* Charlie poteva così utilizzare il credito concesso da Bob nei confronti di Alice rilasciando una promessa di pagamento a Bob che faceva lo stesso nei confronti di Alice; il sistema compensava le dichiarazioni *IoU,* incrociando quelle di segno opposto fra i medesimi soggetti e cancellandole dal registro.

In questo modo diventava possibile fare a meno del denaro contante: l'iniziativa aveva raccolto l'adesione di circa quattromila utenti e destato un certo interesse fra gli addetti ai lavori.

[99] In un'intervista del 2012 Ryan Fugger ha spiegato così l'idea alla base del suo sistema: *"All that you need is a routing system for finding intermediaries to connect payers with payees who don't trust them directly."* Reutzel, Bailey, "Disruptor Chris Larsen Returns with a Bitcoin-Like Payments System", 2012, https://www.americanbanker.com/news/disruptor-chris-larsen-returns-with-a-bitcoin-like-payment-system

6.2.3. Ristrutturazione *Bitcoin-style*

Nel 2011, Jed Mc Caleb, programmatore originario del *bitcoin exchange Mt.Gox*[100], Arthur Britto e David Schwartz hanno aderito al progetto di Fugger, ridisegnando l'intero impianto di progettazione: il modello di riferimento è quello di *Bitcoin* ma il meccanismo di approvazione è stato completamente rielaborato, con eliminazione della *proof of work,* in maniera da consentire un sensibile risparmio di energia e potenza computazionale, e introducendo l'irreversibilità delle transazioni per evitare la *transaction malleability*.

Le nuove monete sono state emesse in *pre-mining* nella misura di 100 miliardi di unità; ognuna di esse può essere divisa fino al sesto decimale: il sistema è perciò astrattamente in grado di processare 10^{17} transazioni contro i $21*10^{14}$ di *Bitcoin,* numero, quest'ultimo che sarà realizzato solo al termine dell'emissione nel 2140, ma che, stante il numero di *bitcoin* emessi, al momento attuale è approssimativamente $16,5*10^{14}$. In questa seconda fase, sono divenute predominanti le funzioni di pagamento e cambio moneta: gli XRP, *token no asset backed* della piattaforma hanno assunto funzione solutoria *user-to-user;* mentre il protocollo di sistema ha incrociato le richieste degli utenti per l'acquisto e la vendita di monete virtuali e valute correnti.

Dal 2012 Fugger si è ritirato dal progetto cedendo la gestione ai *Ripple Labs*[101], società di San Francisco (USA), fondata da Jed McCaleb

[100]Ceduto nel 2011 a Mark Karpelès.

[101] jimbobway *Is Ripple a Bitcoin Killer or Complementer? Founder of Mt Gox will launch Ripple*, 2012, *https://bitcointalk.org/index.php?topic=128413.0* "*I'm happy to announce that there is finally a team seriously building a distributed Ripple network at Ripple.com. The team is led by founder Jed McCaleb, who also founded the MtGox Bitcoin exchange and created eDonkey2000, and CEO Chris Larsen, founder of Prosper.com. I've been talking to Jed, Chris and other members of their team over the past few months, and*

e Chris Larsen con il nome originario di *OpenCoin*; anche Larsen era già attivo da tempo in questo settore con i progetti *E-Loan*, piattaforma dedicata ai mutui *on line* che risale addirittura al 1997, e *Prosper,* un sistema di prestito *peer to peer* creato nel 2005.

Le caratteristiche peculiari di *Ripple* rispetto al sistema *Bitcoin* consistono in

- *Premining* e distribuzione dei *token* di sistema*:* gli *XRP* sono già tutti in circolazione nel numero di 100 miliardi; di queste solo il 55% è stato messo in vendita al pubblico, mente la parte restante è divisa fra i creatori del progetto, cui è stato assegnato il 20%, e i *Ripple Labs* che detengono il rimanente 25%;

- verifica delle transazioni basata sul registro dei consensi, un sistema progressivo a percentuale di approvazione sempre maggiore da parte dei *server* del progetto che sostituisce le verifiche di *hash* del sistema *bitcoin.*

- approvazione pressoché immediata dei pagamenti;

- irreversibilità dei pagamenti, con soluzione del problema della c.d. *transaction malleability* che, in astratto, consente la doppia spendita della moneta nelle more fra l'approvazione di una transazione e il suo inserimento in un blocco convalidato.

Le monete virtuali di *Ripple* valgono pochi centesimi di dollaro e possono essere scambiate nel sistema senza che vengano applicati costi

---

while their plan is very ambitious, I believe if anyone can develop the Ripple concept on a global scale, they can. Their system is based on a Bitcoin-style blockchain, much as we have discussed here over the last few years as an interesting possibility, but with a novel miner-less consensus mechanism that allows transactions to be confirmed nearly instantaneously. After discussions with Jed's team, and some long-standing members of the Ripple community, I've agreed that Jed's project should use the name Ripple and be considered our primary implementation. It was hard for me to let others step in to this role, but from the beginning I always intended for someone else to implement the concept, and I'm lucky to have finally found a group that is more than worthy of taking the project to the next level. Please check out http://ripple.com, sign up for the beta if you're interested, and watch for the launch coming soon... Ryan"

di transazione; le operazioni che coinvolgono valuta o monete virtuali diverse dagli *XRP* sono, invece, soggette all'applicazione di una piccola commissione: si tratta di una misura *antispam* volta a evitare che il sistema vada soggetto a quella specifica forma di attacco informatico conosciuta come *denial-of-service* o *network floading*[102].

6.2.4. Implementazione dei servizi finanziari

Nella terza fase di evoluzione, *Ripple* ha implementato servizi di intermediazione finanziaria: nel 2013 è stato introdotto il c.d. *bitcoin bridge* che consente agli utenti di effettuare pagamenti in *bitcoin* senza la necessità di acquistarli preventivamente; è il protocollo di sistema a mettere in contatto chi desidera vendere con chi desidera comprare, sulla falsa riga di quanto avvenuto nel primo pagamento in *bitcoin, quando Laszlo Hanyecz* vendette le monete virtuali a un acquirente inglese il quale, a propria volta, dispose il pagamento del controvalore in dollari a favore della pizzeria Papa John's di Jacksonville (USA)[103]. Questa caratteristica è stata poi estesa a tutte le monete gestite dal sistema[104]: si può così immettere una moneta nella piattaforma che, eseguite le dovute operazioni, provvederà al pagamento in una divisa differente (c.d.*rippling*).

[102]In questo tipo di attacco il server viene sommerso di richieste dall'esterno, fino ad impedirne il funzionamento.
[103] *Vide nota* 79
[104] *Ripple* considera monete e valute alla stregua di riconoscimenti di debito (*IOU*). Allo stato dell'arte, il sistema accetta le valute: Euro, Franco Svizzero, Sterlina Inglese, Corona Norvegese, Dollaro Statunitense, Dollaro Canadese, Peso Messicano, Dollaro Australiano, Dollaro Neozelandese, Yen Giapponese, Yuan Cinese; oltre agli XRP vengono scambiate anche le principali criptomonete come *bitcoin, litecoin, namecoin* e i metalli preziosi platino, oro, e argento.

Peraltro, l'attività di cambio ha attirato l'attenzione del *FinCEN*, il *Financial Crimes Enforcement Network* del Dipartimento del Tesoro *USA*, che proprio nel 2013 ha sanzionato *Ripple* per violazione degli obblighi di identificazione della clientela (*KYCR*)[105], comminando una sanzione di $ 700.000. L'Agenzia Governativa ha acconsentito a ridurre la pena pecuniaria a $ 450.000 in cambio dell'adeguamento del sistema alla normativa antiriciclaggio: dal 2014 l'accesso al *network* è perciò soggetto alla preventiva identificazione dei partecipanti.

Infine, *Ripple* ha specializzato sempre più i servizi offerti rivolgendosi alle istituzioni bancarie e finanziarie cui ha proposto una soluzione *DLT* per il sistema dei pagamenti interbancari: questa fase ha dato vita al consorzio R3 e alla Piattaforma Corda, che analizzeremo nella III parte, assistiti da una serie di implementazioni che rendono l'offerta di mercato comparabile con quella della piattaforma Visa. Entro la fine del 2017 verranno congelati in depositi di garanzia (*escrow*) 55 miliardi di *XRP*, divisi in 55 *tranche* che verranno immesse sul mercato a cadenza mensile; la parte invenduta di ogni quota sarà congelata in un nuovo *escrow* da liquidare in coda all'ultima tornata prevista (struttura di coda ad anello). Tramite l'implementazione *XRP Payment Channel,* la velocità del sistema verrà elevata a decine di migliaia di transazioni al secondo, portando le capacità di *Ripple* a livelli comparabili con Visa[106].

Il sistema assume così sempre più una funzione di registro specializzato sulla notazione di fatti come i pagamenti o lo scambio di valute e monete, in cui la vendita dei blocchi unitari mette in circolo gli spazi per le registrazioni: infatti se si trattasse di unità di per sé idonee al pagamento, facendo entrare ogni mese sul mercato l'1% della moneta il *network* sarebbe travolto dall'inflazione.

---

[105] *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger* https://www.fincen.gov/news_room/nr/pdf/20150505.pdf

[106] Miguel Vias, New Features Increase XRP Ledger Transaction Throughput to Same Level as Visa, 2017, https://ripple.com/insights/ripple-continues-to-bring-internet-of-value-to-life-new-features-increase-transaction-throughput-to-same-level-as-visa/

6.3. *Ethereum*

6.3.1. Struttura

Ethereum[107] è un sistema derivato da *Bitcoin*, progettato per la scrittura degli *smart contract* nel codice della moneta di riferimento, *l'ether;* lo strumento è divisibile in sottomultipli, in ragione delle migliaia di unità[108], rispettivamente identificati tramite i cognomi dei matematici, crittografi e informatici Hal Finney, Nick Szabo, Claude Shannon, Charles Babbage, Ada Lovelace, Wei Dai.

Così posto il valore unitario di 1 eth, abbiamo:

- 1 finney = $1/10^3$ *eth*
- 1 szabo = $1/10^6$ *eth*
- 1 shannon = $1/10^9$ *eth*
- 1 babbage = $1/10^{12}$ *eth*
- 1 lovelace = $1/10^{15}$ *eth*
- 1wei = $1/10^{18}$ *eth*

[107]www.etherum.com
[108] Introshine, Ether unit converter (wei, finney, szabo, btc) forum.ethereum.org, 2016, https://www.reddit.com/r/ethereum/comments/3g8grm/ether_unit_converter_wei_finney_szabo_btc/

Per evitare *free-riding* e altri tentativi di manipolazione, ogni attività di sistema richiede il pagamento di una commissione[109], detta *gas* che è espressa in *szabo*; i nodi sono liberi di modificare al rialzo o al ribasso le quote *gas* previste dal programma.

Lanciato con un *crowdfunding* nel 2014, *Ethereum* ha raccolto 31.591 *Bitcoin*, che in quel momento corrispondevano a circa $ 18.439.086 e a 60.102.216 ETH; il progetto ha riscosso un successo costante fra gli utenti della rete, tanto da avere attualmente raggiunto la seconda capitalizzazione di mercato, subito dopo *Bitcoin*[110]. Queste le sue fasi di evoluzione:

- *Prerelease Step 0: Olympic testnet - 2015*
- Release Step 1: *Frontier* – 2015 : versione base dedicata ai tecnici per fare *mining*, eseguire transazioni, far girare il sistema, sviluppare e testare applicazioni decentralizzate;
- Release Step 2: *Homestead* – 2016 avrebbe dovuto essere la versione finale del progetto ma lo sviluppo di *Frontier* l'ha trasformata in una *fix-release*;
- Release Step 3: *Metropolis* – *future release* dedicata agli utenti finali con interfacce testate e funzionanti (come, ad esempio, i *desktop wallet*);
- Release Step 4: *Serenity* – *future release* con prototipo disponibile su *Github* che ha lo scopo di cambiare il sistema di consenso da *Proof of Work* a *Proof of Stake*[111] con riduzione del consumo di

[109] Gavin Wood, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
EIP-150 REVISION (Yellow paper), Appendix G. Fee Schedule, 2013, http://gavwood.com/paper.pdf
[110]http://coinmarketcap.com/
[111] *Proof of Stake FAQ*, 2017, https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

energia della rete[112]. Quando verrà implementato l'algoritmo di consenso *Casper*, il sistema dividerà i nodi in *validating e tracking,* in maniera analoga a quanto accade in *Ripple*: per poter inserire i blocchi nel registro logico i nodi dovranno depositare in garanzia di una determinata somma in *ether* dando appunto prova della loro partecipazione all'interesse di gruppo.

La piattaforma *Ethereum* è dotata di una *blockchain* autonoma, grazie a cui può sviluppare alcune delle estensioni che la caratterizzano senza necessità di un sistema di supporto esterno. A far data dal giugno 2015 l'implementazione *Frontier* consente agli sviluppatori di costruire, testare, sviluppare e utilizzare sulla *blockchain Ethereum* delle applicazioni decentralizzate. Nel successivo mese di novembre, *Microsoft* e *ConsenSys[113],* una *blockchain software foundry* che sviluppa servizi e applicazioni basati su *Ethereum*, hanno siglato un accordo per creare una *Ethereum blockchain as a service (EBaaS)* su *Microsoft Azure*[114]: l'obiettivo del progetto è quello di creare un ecosistema *cloud* di sviluppo su *blockchain* dedicato alla sperimentazione tecnica e alle applicazioni commerciali.

L'attività principale di *Ethereum* consiste nell'implementazione degli *smart contract,* accordi commerciali caratterizzati dall'esecuzione digitale automatica di cui analizzeremo gli effetti giuridici nella sezione dedicata; il codice degli *smart contract* viene inserito nella *blockchain,* diventando così pubblico, ed è eseguito da tutti i nodi che fanno parte della rete nel momento in cui minano i blocchi da aggiungere alla catena. La moneta inserita in *blockchain* contiene, infatti, il codice sorgente (la traduzione in linguaggio di programmazione dell'attività richiesta) o un suo

[112]Vinay Gupta, The Ethereum Launch Process, 2015, https://blog.ethereum.org/2015/03/03/ethereum-launch-process/
[113] https://consensys.net/
[114] Sofia, 3 Companies Leading the Blockchain as a Service (BaaS) Revolution, 2015, https://letstalkpayments.com/3-companies-leading-the-blockchain-as-a-service-baas-

riferimento univoco, in maniera da rendere oggettivo e pubblicamente verificabile il contratto. Lo scambio del *token* di sistema costituisce il meccanismo propulsore dello *smart enforcement*: ogni scambio incrementa infatti la dimensione del registro logico al cui interno vengono memorizzate sia le transazioni che gli *smart contract.*

Il sistema è stato sviluppato da Vitalik Buterin[115], con il contributo in revisione di Gavin Wood[116]: l'intento specifico di questa operazione era quello di implementare *Bitcoin* sotto i profili:

- della *Turing completeness,* in modo da rendere praticamente possibile qualsiasi tipo di programmazione;
- dell'interattività fra *blockchain*, consentendo alla piattaforma di prendere in considerazione più monete digitali;
- degli stati alternativi delle transazioni, che oltre che spese o non spese, in questo sistema possono essere anche vincolate all'avveramento di una condizione o al decorso di un termine.

Al contempo è stata incrementata la velocità di *mining,* portando la produzione a un blocco ogni 12s circa[117], contro i dieci minuti di *Bitcoin*: questa scelta rende la velocità di produzione analoga a quella di propagazione, che corrisponde a circa 10 secondi per un blocco di 1 *MB*[118], facendo sì che i nodi abbiano immagini diverse del registro logico

---

[115]Vitalik Buterin, Ethereum, Ethereum A Next-Generation Smart Contract and Decentralized Application Platform (Whitepaper), Whitepaper, 20 13,https://github.com/ethereum/wiki/wiki/White-Paper

[116] Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger" EIP-150 Revision (Yellow paper), 2013, http://gavwood.com/paper.pdf

[117]Ethereum wiki, Mining, https://github.com/ethereum/wiki/wiki/Mining

[118] https://blog.ethereum.org/2016/10/31/uncle-rate-transaction-fee-analysis/ Vitalik Buterin, Uncle Rate and Transaction Fee Analysis, Ethereum Blog, 2016, "*One important fact is that the more transactions a block contains (or the more gas a block uses), the longer it will take to propagate through the network. In the Bitcoin network, one seminal study on this was Decker and Wattenhofer (2013), which found that the average propagation time of a block was about 2 seconds plus another 0.08 seconds per kilobyte in the block (ie. a 1 MB block would take ~82 seconds). A more recent Bitcoin Unlimited study [Peter R. Rizun, A Transaction Fee Market Exists Without a Block Size Limit, 2015] showed that this has since reduced to ~0.008 seconds per kilobyte due to transaction propagation technology improvements. We can also see that if a block takes longer to*

e che la *blockchain* vada di conseguenza soggetta a *fork*. Le conseguenti riorganizzazioni eliminano il ramo più corto, quello che esprime minore sforzo computazionale; i blocchi che ne facevano parte perdono validità e vengono detti orfani. L'implementazione di protocollo *Ghost*[119] include nel computo della catena più lunga anche questi blocchi, lasciandoli sopravvivere in *dead end* collaterali; data la nuova allocazione questi blocchi vengono denominati appunto zii e nipoti, e vengono calcolati fino al settimo grado di relazione.

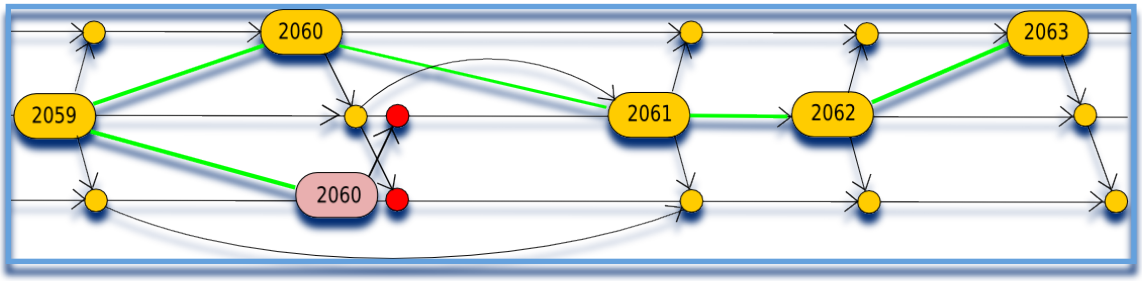


Figura 5*: Ethereum Blog - Uncle Rate and Transaction Fee Analysis*[120]

La ricompensa per il mining è di 5 ETH, che vengono attribuiti anche nel caso in cui il blocco perda di validità a seguito di una riorganizzazione; l'algoritmo crea un premio stabile nel tempo che non è destinato a subire dimezzamenti come nel sistema *Bitcoin*.

---

propagate, the chance that it will become a stale is higher; at a block time of 600 seconds, a propagation time increase of 1 second should correspond to an increased 1/600 chance of being left behind. In Ethereum, we can make a similar analysis, except that thanks to Ethereum's "uncle" mechanic we have very solid data to analyze from."

[119] What is the GHOST protocol for Ethereum?, 2017, https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/
https://github.com/ethereum/wiki/wiki/White-Paper#modified-ghost-implementation

[120] Vitalik Buterin, Uncle Rate and Transaction Fee Analysis, Ethereum Blog, 2016, https://blog.ethereum.org/2016/10/31/uncle-rate-transaction-fee-analysis/

6.3.2. The DAO

Nell'aprile 2016 i programmatori Christoph e Simon Jentzsch hanno lanciato un *crowdfunding* in *ether* per finanziare la creazione di *The DAO* (*Decentralized Autonomous Organization*); allo stato dell'arte, si tratta della raccolta fondi di maggior successo fra quelle effettuate: nel maggio 2016 avevano aderito al progetto oltre 11.000 investitori con uno stanziamento superiore al controvalore di $ 150.000.000 e nel fondo erano confluiti 11.500.000 *eth*, pari a circa il 14% del circolante.

Già alla fine del mese, un gruppo di ricercatori del consorzio *IC3* (*Initiative for Cryptocurrencies & Contracts*) della *Cornell University* aveva fatto presente in un *paper* lo scarso livello di progettazione del *DAO,* che rendeva possibile l'esecuzione di attacchi tesi al congelamento o alla sottrazione dei fondi, invitando i fratelli Jentzsch a una moratoria del lancio e all'esecuzione di un *fixing* idoneo[121]. Nel successivo mese di giugno si era prodotto un gran fermento attorno alla vulnerabilità di "*recursive call*" nell'operazione responsabile dell'invio degli *ether* che consentiva di ripetere l'esecuzione le transazioni in maniera illimitata. In una *mail* inviata a *Coindesk,* Peter Vessenes[122] aveva riconosciuto la vulnerabilità[123] e in un post pubblicato sul suo sito aveva suggerito due possibili soluzioni a quello che sembrava considerare solo un attacco teorico[124]. Taylor Gerring dell' *Ethereum Foundation* aveva confermato a

[121] Dino Mark, Vlad Zamfir, Emin Gün Sirer A Call for a Temporary Moratorium on The DAO, Hacking Distributed, 2016, http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/

[122] ex *CEO* di *Bitcoin Foundation* https://bitcoinfoundation.org/ e attuale *CEO* di *CoinLab* https://coinlab.com

[123] *"All public Solidity functions that send money or use "call" on another contract may be called recursively by an attacking recipient. This isn't how Bitcoin works, so it might be a surprise to inexperienced Ethereum developers. The practical implication is that each of your functions (and in fact your entire contract) should be 'reentrant', which is to say they should function the same if parts of it are re-called prior to completion."* Michael del Castillo Leaderless DAO Put to the Test Following Ethereum Vulnerability, 2016, http://www.coindesk.com/leaderless-dao-put-test-following-reported-ethereum-vulnerability/

[124] Peter Vessenes, More Ethereum Attacks: Race-To-Empty is the Real Deal, 2016, http://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/ :

Coindesk l'accuratezza della ricostruzione, affermando che il sistema non necessitava di una riscrittura ma solo di alcune correzioni a cui avrebbero provveduto i programmatori[125].

Il 16 giugno il monito sulla vulnerabilità veniva rilanciato da un secondo paper dei ricercatori del consorzio *IC3* che ribadivano il pericolo insito nella funzione ricorsiva[126]. Il giorno successivo i timori divenivano realtà quando un *attacker,* sfruttando proprio questo *bug,* riusciva a ritirare le somme investite nel *DAO* senza un limite di corrispondenza col proprio deposito; venivano così sottratti i due terzi degli *ether* depositati nel fondo: il controvalore in *USD* oscillava fra i 60.000.000 e i 40.000.000, tenendo conto del crollo di cambio provocato proprio da questa azione. L*'hacker* aveva quindi pubblicato una lettera aperta[127] in

---

"*In Brief: Your smart contract is probably vulnerable to being emptied if you keep track of any sort of user balances and were not very, very careful. As always, I'm available for smart contract review and audit, email me. You can read about other security considerations on my blog here [http://vessenes.com/tag/smart-contracts/]".*

[125] Michael del Castillo Leaderless DAO Put to the Test Following Ethereum Vulnerability, 2016, http://www.coindesk.com/leaderless-dao-put-test-following-reported-ethereum-vulnerability/

[126] Zikai Alex Wen, Andrew Miller, Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug, Hacking Distributed, 2016, http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/

[127] http://pastebin.com/CcGUBgDG

" ===== *BEGIN SIGNED MESSAGE* =====

To the DAO and the Ethereum community,

I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs".

I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO:

"The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation."

cui si firmava semplicemente *the attacker;* dopo aver formulato una serie di considerazioni riguardo l'opportunità economica per *Ethereum* di procedere a un'azione di contrasto, sosteneva comunque di avere operato secondo il proprio diritto, diffidando gli amministratori dal recupero delle somme sottratte e riservandosi di adire l'autorità giudiziaria (*sic!).* Dal punto di vista giuridico queste affermazioni sono destituite di fondamento: la pretesa secondo cui i numerosi milioni di dollari ritirati dal fondo di investimento costituirebbero un premio per la cessazione della partecipazione è contraria a buona fede e, nonostante l'*hacker* sostenesse di essere stato rassicurato della bontà di questa teoria da un legale, riteniamo che la sua posizione non avrebbe trovato tutela davanti a una Corte, anche se le giurie popolari spesso prendono decisioni imprevedibili dal punto di vista del diritto. Le considerazioni riguardo la tutela giudiziaria cedono però il passo alla natura tecnica dei beni sottratti: il problema consiste nel fatto che lo spossessamento aveva trasferito i codici di deposito degli *ether* nella disponibilità materiale dell'agente anonimo, che ne disponeva in via esclusiva, e non vi era modo di procedere al trasferimento contrario in via esecutiva. Un procedimento giudiziario in questo caso avrebbe ottenuto solo una pronuncia astratta, materialmente impossibile da realizzare, con spreco

---

A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.
I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the mail shortly.
I hope this event becomes an valuable learning experience for the Ethereum community and wish you all the best of luck.
Yours truly,
"The Attacker"
===== END SIGNED MESSAGE =====
Message Hash (Keccak):
0xaf9e302a664122389d17ee0fa4394d0c24c33236143c1f26faed97ebbd017d0e
Signature:
0x5f91152a2382b4acfdbfe8ad3c6c8cde45f73f6147d39b072c81637fe81006061603908f692dc15a1b6ead217785cf5e07fb496708d129645f3370a28922136a32"

del tempo e del denaro investiti nella presentazione del caso. Peraltro, l'impossibilità di recuperare gli *ether* sottratti non avrebbe pregiudicato eventuali richieste di risarcimento degli investitori per comportamento colposo della piattaforma, consistente nell'omesso controllo sul programma difettoso in maniera contraria alla diligenza specifica richiesta nella gestione di fondi altrui. Gli amministratori del *DAO* si sono quindi trovati davanti all'alternativa, fronteggiata da altri prima di loro[128], se subire le conseguenze dell'illecito o attivare una soluzione tecnica in grado di ridurre le perdite.

6.3.3. La Hard fork

La possibile soluzione è stata individuata in una *hard fork,* con ricalcolo della *blockchain* al blocco precedente l'attacco e perdita di validità dei blocchi che contenevano gli *ether* sottratti: a termini del contratto di sottoscrizione, il ritiro di fondi dal *DAO* era infatti soggetto a un periodo di latenza di 28 giorni e in questo periodo la *community* aveva lungamente discusso sul da farsi. Le osservazioni riguardo la fiducia di mercato e la stabilità del sistema contenute nella lettera dell'*attacker* erano sicuramente corrette, anche se da un punto di vista di tecnica dell'argomentazione provenivano, altrettanto sicuramente, dal pulpito sbagliato. Una parte dei *miner* riteneva che il consenso della maggioranza fosse elemento necessario e sufficiente per procedere alla riorganizzazione, in legittima difesa dei diritti di proprietà messi a repentaglio dall'attacco; mentre una corrente di pensiero opposta sottolineava che è proprio l'immutabilità della *blockchain* a generare la fiducia di mercato necessaria alla tenuta del progetto e al suo successo: la ricostruzione storica delle transazioni deve essere ineccepibile e il registro non deve subire censure o manipolazioni, neppure dall'interno.

[128] *Vide ultra sub MtGox*

Ad esito delle votazioni la community ha optato per l'esecuzione della *fork*, votata a maggioranza dell'89% dai nodi del sistema, ricalcolando la *blockchain* a partire dal blocco n 1.920.000 il 20 luglio 2016. Riteniamo opportuno spendere alcune parole sul metodo di calcolo che, in realtà, ha preso in considerazione il voto espresso dalla maggioranza interna alle *mining pool* estendendolo a tutti i partecipanti: il conflitto era stato pesante e, a volte, la maggioranza interna era stata raggiunta per pochi voti; un ricalcolo delle preferenze secondo quanto effettivamente dichiarato consente di comprendere i motivi alla base del successivo scisma del progetto. Infatti, una parte consistente della *community* ha ripudiato la *fork*, rimanendo legata alla *old chain* e continuando a implementarla; questa scelta ha portato alla divisione del sistema originario nei due rami attuali *Ethereum (ETH)*, il nuovo registro derivato dalla *fork*, ed *Ethereum Classic (ETC)*, il registro originario che è proseguito intatto.

L'operazione ha creato una serie di problemi aggiuntivi sotto il profilo del *double spending*: gli investitori del *DAO* sono stati rimborsati 100 a 1 sul nuovo registro *ETH* ma il registro classico *ETC* ha mantenuto fermi i loro possedimenti residui. Con la conseguenza che coloro che possedevano *ether* prima della *fork* si sono ritrovati ad essere titolari di somme duplicate: il blocco di origine è il medesimo ma i *token* hanno valore autonomo su ognuna delle catene logiche e possono essere spesi in via indipendente.

I grafici sottostanti mostrano l'andamento economico dei due rami del progetto:

Figura 6*: Ethereum (ETH) 1Y chart – coimarketcap.com*[129]

Figura 7*: Ethereum Classic (ETC) chart – coimarketcap.com*[130]

Il primo grafico mostra inoltre che il nuovo progetto *Ethereum* non ha riportato particolari variazioni nemmeno in occasione delle successive *fork* cui gli amministratori sono stati costretti per fare fronte

[129] https://coinmarketcap.com/currencies/ethereum/
[130] https://coinmarketcap.com/currencies/ethereum-classic/

a ulteriori attacchi al *network*. Nell'ottobre 2016 è stata effettuata una seconda *fork* all'altezza del blocco 2.457.000 con previsione di una terza nei giorni immediatamente successivi per far fronte a una situazione di ritardo nelle transazioni dovuta a una falsa attività del *network*. Sfruttando il prezzo ridotto delle commissioni in *gas* richieste per le attività, alcuni *attacker* avevano inondato il sistema di account vuoti, codici incompleti, bilanci, depositi e *nonce* uguali a zero: le due *fork* avevano rispettivamente l'obiettivo di alzare il prezzo del *gas* e di rimuovere i frammenti inerti; il grafico del periodo mostra un andamento laterale delle quotazioni, espressione di una sostanziale indifferenza del mercato alla ristrutturazione interna.

Il 22 novembre 2016 è stata attivata una quarta *fork* all'altezza del blocco 2.675.000, per far fronte a una serie di *DDoS* che avevano rallentato il *network* e mandato in *crash* alcuni nodi; il risultato di mercato è stato sostanzialmente neutro, in maniera analoga a quelli precedentemente descritti.

Le vicende dei sistemi di moneta virtuale sembrano contraddire l'impostazione classica per cui il capitale ha la memoria dell'elefante, le zampe della lepre e il cuore del coniglio: nonostante i problemi descritti la fiducia del mercato non sembra avere subito flessioni relative alle quattro *hard fork.* Per spiegare questa situazione potrebbe forse sovvenire la considerazione di *behavioral economics* per cui in materia di innovazione la visione soggettiva del futuro si sovrappone ai segnali della realtà circostante rendendo il comportamento degli esseri umani immune dall'apprendimento derivato dalla paura. Si porta normalmente l'esempio del *phising,* sottolineando che carpire via *web* la buona fede degli utenti richiede minori artifici rispetto a quelli applicati nella pesca tradizionale: infatti, dopo un po' di tempo che si pesca nel medesimo bacino con la stessa tecnica i pesci mostrano diffidenza, mettendo in atto una cautela che gli esseri umani sembrano ignorare. In maniera analoga, sembra che gli avvenimenti passati come la *Internet Bubble* o il

più recente *default* di *MtGox* non abbiano costituito segnali di pericolo idonei a prendere in considerazione un evenienza come quella che ha portato al disastro del *DAO*.

6.4. Sistemi offuscati

6.4.1. Blockchain analisys

L'efficienza di mercato dimostrata da *Bitcoin* ha dato luogo, come normalmente accade, a numerosi tentativi di *exploiting:* in tempi di *ransomware* appare normale la notizia della richiesta di riscatto in *bitcoin*. Il motivo è molto semplice, questi trasferimenti sono effettuati fra destinatari la cui identità è protetta con crittografia; quello di cui, però, a volte non si tiene conto è che le transazioni avvengono in chiaro e che la loro storia è pubblicamente disponibile[131]. La *blockchain* viene così analizzata dagli esperti informatici che applicano varie tecniche per seguire il movimento dei *bitcoin*[132].

Una prima tecnica consiste nell'esame diretto dei pagamenti[133]. Poiché il quantitativo di *bitcoin* ricevuti con una singola transazione di

[131] *Vide inter alia https://blockchain.info/it*
[132] Per un'analisi approfondita *vide* Paolo Dal Checco, *Bitcoin Forensics,* http://www.bitcoinforensics.it/
[133] Per un esempio pratico di *blockchain analysis vide: Bitcoinica Theft with unusual transaction to Theymos*, 2015, https://www.youtube.com/watch?v=LlJkec-CQRM. Eloquente il commento postato su *Reddit* dall'autore del video: "*I've demo'd Bitcoin for law enforcement. By the time the local cops figure these forensics out, the statute of limitations will have expired twice"*
https://www.reddit.com/r/Bitcoin/comments/3k5zen/looks_like_the_stolen_bitcoinica_funds_returned/

input non può essere speso parzialmente, ma deve essere o interamente ceduto a un destinatario o suddiviso fra più beneficiari con più transazioni contemporanee di *output*, si può provare a seguire il flusso dei pagamenti sui cui viene diviso il valore della transazione di *input*. Si avranno così movimenti ad anello (A paga una quota a B e dispone il resto a favore sé stesso), movimenti a *fork* (A cede una parte della transazione di *input* a B e un'altra parte a C), movimenti a rimbalzo (A paga una quota a B e una quota a C che, a propria volta, gira l'intera somma ricevuta a D). Nelle transazioni ad anello è più facile seguire il movimento dei valori; mentre negli altri due schemi descritti il pagamento è indistinguibile dal resto. La facilità di creazione di nuovi indirizzi consente di utilizzare queste tecniche liberamente, senza preoccupazioni relative a tempi e a costi; poiché gli indirizzi sono pseudonimi, non è facile capire se indirizzi diversi facciano capo alla medesima persona: negli esempi precedenti ogni indirizzo B, C e D potrebbe fare capo ad A che, in questo caso, avrebbe prodotto unicamente dei movimenti fittizi.

Un interessante metodo di indagine è quello che esegue il raggruppamento in *cluster* di operazioni apparentemente autonome per collegarle a soggetti unici[134]. L'algoritmo di *clustering* raggrupperà gli elementi dell'analisi sulla base della loro attinenza a determinati parametri: verranno esaminate le loro caratteristiche specifiche e la relazione che presentano con il campione assegnato; uno degli elementi decisivi per il raggruppamento è la c.d. metrica ovvero la distanza che l'algoritmo deve prendere in considerazione rispetto ai criteri di *default*.

La tecnica inversa, detta *declustering*, viene utilizzata da tempo per proteggere la privacy *on line*: tramite un algoritmo di natura opposta a quello appena descritto, le informazioni che compongono gli elementi di

[134]Michele Spagnuolo, Federico Maggi, Stefano Zanero , *BitIodine: Extracting Intelligence from the Bitcoin Network* , 2014, fc14.ifca.ai/papers/fc14_submission_11.pdf

riconoscimento vengono sparpagliate in modo tale da richiedere un grado di difficoltà superiore a una soglia assegnata per la loro *reductio ad unum.* [135]

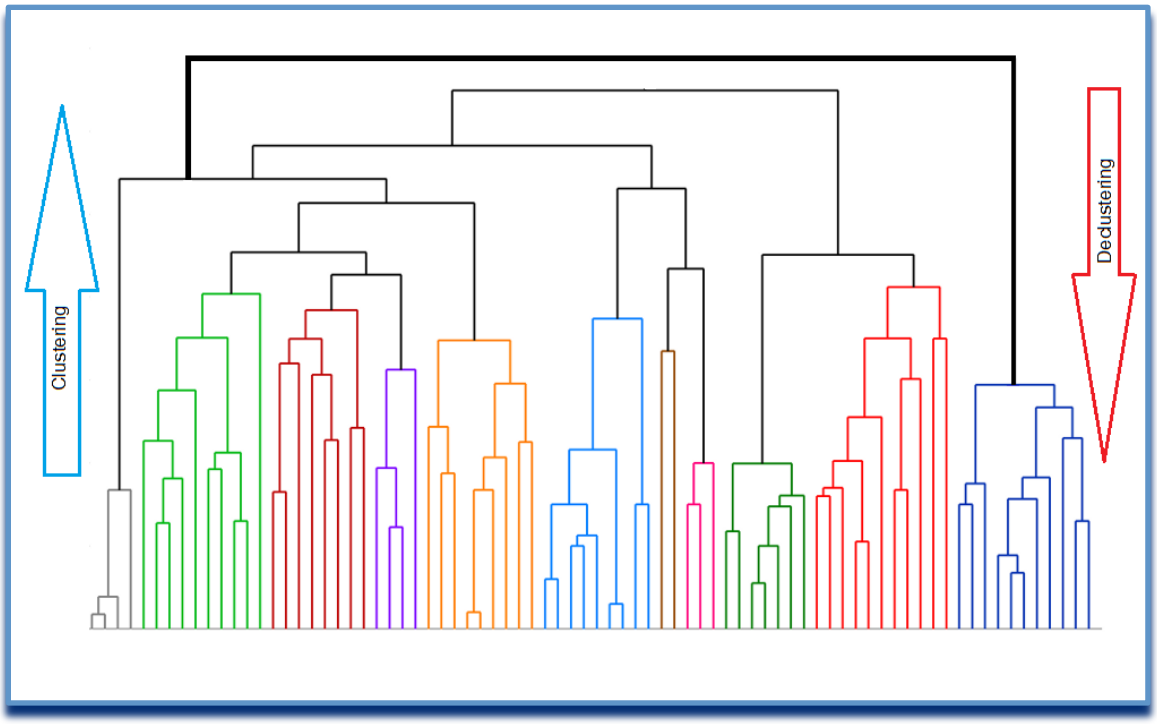


Figura 8: *Clustering* e *declustering*[136]

La ricerca parte dal concetto che i dati contenuti in un *database,* per quanto resi anonimi, possono ancora essere identificati tramite aggregazioni di elementi esterni; quello specifico database che è la *blockchain* non fa eccezione e i dati possono essere aggregati, ad esempio, raggruppando gli indirizzi a cui vengono effettuati i pagamenti. Una volta resi pubblici, gli indirizzi *Bitcoin* identificano in maniera univoca lo pseudonimo che li utilizza: l'obiettivo dell'indagine di *forensics* è quello di trovare un collegamento fra i trasferimenti registrati

[135] Qiong Wei, Yansheng Lu , Qiang Lou, Privacy-Preserving Data Publishing Based on De-clustering, 2008, http://ieeexplore.ieee.org/document/4529813/figures
[136] http://www.sthda.com/english/wiki/cluster-analysis-in-r-unsupervised-machine-learning

in *blockchain* e il mondo reale: una o più transazioni come l'acquisto di un bene registrato, che avrà perciò un intestatario, o di un bene materiale, che sarà da consegnare a un determinato indirizzo, potrebbero consentire di associare un nome reale allo pseudonimo digitale.

A volte il compito si rivela più facile del previsto, come nel caso delle indagini sul *black market Alphabay* dove le merci vengono scambiate per un controvalore in *bitcoin.* Uno dei venditori si era presentato con le due diverse identità AREA51 e DARKAPOLLO. Invece che tramite l'analisi di *blockchain,* gli investigatori lo hanno individuato tramite la chiave pubblica *PGP,* che include l'indirizzo *mail* fornito dall'utente: i due *nickname* facevano capo a un unico indirizzo che era stato attivato con dati anagrafici reali[137].

6.4.2. *Cryptonote*

Il protocollo *Crypto note*[138] offre una *blockchain* autonoma su cui implementa le due funzioni di *untraceability* e *unlinkability:* la prima è una caratteristica per cui le transazioni in entrata vedono il trasferimento come se provenisse da gruppi di nodi del sistema*;* la

[137] Paolo Dal Checco, Arresti nel dark web grazie (anche) alle chiavi PGP, 2016, http://www.bitcoinforensics.it/2016/08/arresti-dark-web-chiave-pgp/:
"*durante la generazione della chiave pubblica, per comodità dell'utilizzatore più che altro, viene richiesto l'indirizzo email al quale tale chiave sarà associata e* ***tale indirizzo email verrà inserito all'interno della chiave pubblica PGP****, quindi pubblicamente visibile da chiunque abbia la chiave. [...]La "leggerezza" dei due venditori di AlphaBay AREA51 e DARKAPOLLO è stata quella di inserire nella loro chiave pubblica l'indirizzo di posta elettronica, Adashc31@g___l.com, che ha permesso agli investigatori di risalire ai loro profili Facebook, Twitter ed Instagram anche tramite l'utilizzo del nick "Adashc31". Ci è voluto poco, quindi, a richiedere a Facebook i dati di registrazione e accesso al profilo e scoprire che i due venditori erano in realtà la stessa persona residente a Brooklyn, New York."*
[138] Nicolas van Saberhagen, CryptoNote v 2.0, 2013, https://cryptonote.org/whitepaper.pdf

seconda impedisce invece di collegare con certezza due diverse transazioni in uscita al medesimo nodo.

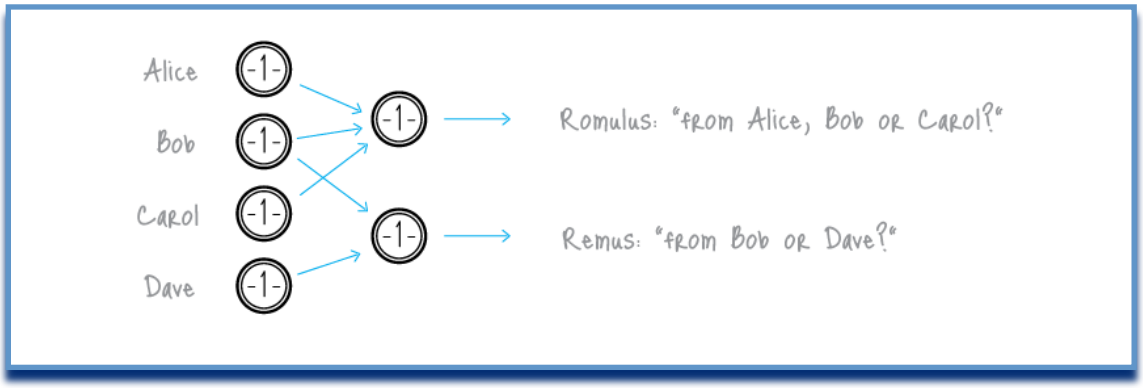


Figura 9: Transazioni Cryptonote[139]

Il whitepaper *Cryptonote* è stato presentato nel 2013 Nicolas van Saberhagen, uno pseudonimo che coerentemente con la soluzione di *ring signature* proposta fa capo a una o più persone non identificabili all'interno di un gruppo[140]. Il lavoro prende le mosse dal *paper* del 1991 *Group signatures a firma* di David Chaum ed Eugene van Heyst[141] che propone un sistema di firme crittografiche identificabili solo con riferimento ad un gruppo di appartenenza, rimettendo a un terzo garante, detto *Group Manager*, la possibilità di verificare quale delle chiavi private sia stata effettivamente impiegata. L'idea di Chaum e van Heist aveva riscosso parecchio successo nel mondo della crittografia ed era stata implementata in maniera da rimuovere la figura del *Group Manager*. Nel 2007 Eiichiro Fujisaki and Koutarou Suzuki della *Nippon Telegraph and Telephone Corporation* hanno proposto un'ulteriore implementazione, ritenendo che l'anonimato consentito dalle *ring*

[139] https://cryptonote.org/inside
[140] Monero Beta, What is known about Nicolas van Saberhagen https://monero.stackexchange.com/questions/162/what-is-known-about-nicolas-van-saberhagen
[141] David Chaum, Eugene van Heyst, *Group signatures*, *Advances in Cryptology EUROCRYPT 1991*, D.W. Davies (Ed.), Springer-Verlag, pp. 257-265

signature consentisse forme di azione fraudolenta. Nel paper del *Traceable ring signature*[142] i due autori hanno formalizzato un metodo da applicare ai sistemi di voto per cui il sistema identifica in maniera automatica chiunque tenti di esprimere più volte la preferenza. La soluzione *one-time ring signature* proposta in *Cryptonote* è stata dichiaratamente elaborata sulla base di quest'ultima ricerca. La destinazione di ogni trasferimento *Cryptonote* è unica per *default:* ogni utente pubblica un singolo indirizzo da cui il sistema ricava una serie di indirizzi derivati, composti dalla chiave pubblica di quello specifico utente e da alcuni dati inseriti nella transazione in maniera casuale dal mittente. Non vi è perciò alcun riutilizzo degli indirizzi a meno che, come sottolineato nel *whitepaper*, il mittente non utilizzi gli stessi dati *random* in più transazioni inviate al medesimo destinatario. L'analisi di *clustering* si scontra con l'impossibilità di raggruppare le transazioni, non essendo possibile stabilire se i trasferimenti siano avvenuti a favore di un indirizzo determinato o leghino insieme indirizzi diversi. La tecnica di offuscamento del protocollo risiede nella possibilità per ciascun utente di utilizzare firme verificabili tramite un gruppo di chiavi pubbliche, invece che tramite una sola come accade in *Bitcoin*: l'identità digitale di ogni utente diviene irrintracciabile proprio perché il sistema assegna a ciascun destinatario un *set* di chiavi pubbliche. L'indagine forense, in questo caso, sarà orientata alla ricerca di eventuali errori umani, specialmente da parte del mittente che per praticità potrebbe aver utilizzato gli stessi dati *random* in più di un'operazione a favore del medesimo destinatario. Il sistema utilizza l'algoritmo di consenso *CryptoNight* in cui i *miner* hanno diritto paritario di voto, che è dichiaratamente orientato a realizzare l'idea originaria di Satoshi Nakamoto *"one CPU one vote*". Fra le monete virtuali che utilizzano *Cryptonote*, alcune fra le più diffuse sono *Bytecoin*, che contiene informazioni aggiuntive come coordiante geografiche o citazioni di libri;

[142] Eiichiro Fujisaki e Koutarou Suzuki, Traceable ring signature, In Public Key Cryptography, 2007, https://eprint.iacr.org/2006/389.pdf

Monero[143] che è salito alla ribalta per l'uso nei *black market* del *dark web*; *DigitalNote* che può inserire nelle transazioni messaggi protetti da crittografia.

6.4.3. Altri applicativi

Molti sistemi di moneta virtuale hanno proposto un metodo per proteggere la *privacy* degli utenti. *Zerocoin*[144], ad esempio, consente di inviare moneta a una sorta di deposito collettivo, detto *blackbox:* al momento del pagamento il sistema farà un prelievo casuale dalla *blackbox,* ovviamente soggetto ai limiti del deposito effettuato; in questo modo le transazioni vengono sganciate dall'indirizzo di provenienza, lasciando però ancora visibili il loro ammontare e la loro destinazione.

Altri sistemi, come *Dash,* propongono servizi *tumbler*[145] *by default* che eseguono il *mix* delle transazioni di sistema rendendo impossibile rintracciarne provenienza, destinazione e consistenza. A differenza dei servizi di *tumbler* veri e propri, che richiedono l'invio delle monete a un terzo che le gestirà agendo da stanza di compensazione in cambio di una commissione percentuale, i sistemi nativi sono integrati e gratuiti; gli utenti potranno utilizzarli senza necessità di dare fiducia a soggetti estranei: i *Tumbler* potrebbero infatti trattenere il denaro ricevuto o tracciare i pagamenti effettuati per trarne profitto. Ora, è vero che un insegnamento economico di base ricorda che sul mercato è fondamentale la reputazione, per cui il *Tumbler* ha un incentivo economico a comportarsi onestamente altrimenti non avrà più clienti; è però altrettanto vero che il *Tumbler* potrebbe agire con una tecnica

[143] https://getmonero.org/
[144] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2011, zerocoin.org/media/pdf/ZerocoinOakland.pdf
[145] Il *tumbler* è il bicchiere da *cocktail* in cui si mescolano gli ingredienti

analoga a quello dello Schema di Ponzi bruciando la propria credibilità quando la posta in gioco sia sufficientemente alta.

I due metodi, applicativo esterno e sistema integrato, differiscono anche per il loro funzionamento: i *tumbler* intervengono nell'attività di singoli utenti mascherando i trasferimenti con la stanza di compensazione, in cui utilizzano i fondi di transazioni multiple in entrata per effettuare quelle in uscita con importi di provenienza *random*[146]; i sistemi nativi amalgamano, invece, i dati delle transazioni durante la loro esecuzione, creando i riferimenti di *blockchain* in questo modo.

Anche il *bitcoin client Darkwallet*[147] propone un metodo per rendere anonime le transazioni, offrendo addirittura istruzioni sull'uso della rete *TOR* e delle *VPN*; a riguardo è interessante notare come proprio gli utenti di *Monero*, la moneta che in questo momento sembra andare per la maggiore nel *Dark Web*, abbiano sottolineato i pericoli per la *privacy* legati a un uso *naive* della rete *TOR*. Un post pubblicato su *Reddit* nel 2016 con il titolo eloquente "*IMPORTANT WARNING to those who want to use Monero/ShapeShift and NOT end up in jail"* ha infatti evidenziato come i programmi che non sono stati scritti appositamente per *TOR*, possano lasciar trapelare i dati identificativi degli utenti[148], ad esempio facendo eseguire al sistema operativo le *query DNS* verso i server della rete pubblica *Internet* invece che verso quelli gestiti da TOR.

Un metodo ulteriore di protezione della *privacy* è quello adottato da *Zcash,* un sistema del 2014 che implementa *Zerocoin* consentendo di sganciare le transazioni non solo dal mittente ma anche dal destinatario e di offuscarne l'importo. Il risultato viene raggiunto caricando nella

[146] What is a Bitcoin Tumbler ? 2014
https://bitcoin.stackexchange.com/questions/17807/what-is-a-bitcoin-tumbler
[147] https://darkwallet.is/
[148] Sapiophile, IMPORTANT WARNING to those who want to use Monero/ShapeShift and NOT end up in jail, Reddit, 2014,
https://www.reddit.com/r/DarkNetMarkets/comments/4zf25q/important_warning_to_those_who_want_to_use/?compact=true

blockchain una versione crittografata della transazione che il sistema accetta sulla base di una *non-interactive zero-knowledge proof*[149], ovvero una prova a conoscenza zero priva di interazione fra chi fornisce la prova e chi la verifica[150]. In questo caso, i *miner* verificano le monete usate nelle transazioni sulla base di un seriale che prova l'appartenenza della moneta al sistema e il suo stato di *UTXO* (*unspent transaction output*) ma che non consente l'identificazione dello specifico *token* utilizzato.

Vi sono molti altri sistemi che implementano tecniche di protezione della riservatezza, e la maggior parte di essi risponde a un'esigenza lecita degli utenti: le transazioni inserite nella *blockchain bitcoin* sono pubbliche e questo comporta un'esposizione potenziale alle tecniche di profilazione: secondo un adagio in voga nella *tech community* i dati sono il nuovo petrolio e la protezione della *privacy* è la nuova legislazione ambientale. Considerato che nel caso dell'utente medio non vengono messi in atto particolari accorgimenti per rendere anonimi i movimenti, la tutela delle informazioni da parte del sistema potrebbe fare la differenza sul mercato, portando a scambi economici di maggiore efficienza. In questo senso riteniamo opportuno tracciare una distinzione fra i sistemi attuativi, quelli che agiscono direttamente su *bitcoin,* contribuendo ad aumentare le dimensioni della *blockchain*, e i modelli autonomi. Fra questi ultimi troviamo maggiormente adeguata allo spirito dell'iniziativa che stiamo studiando l'azione dei sistemi indipendenti che, come *Zcash*, innovano su una *blockchain* proprietaria; mentre le stanze di compensazione esterne, siano esse *Tumbler* commerciali o sistemi autonomi, assegnano un potere molto forte a chi le gestisce contraddicendo in termini il disegno iniziale di un sistema di

[149] What are zk-SNARKs? https://z.cash/technology/zksnarks.html
[150] Eli Ben-Sasson, Alessandro Chiesa, Christina Garmanz, Matthew Greenz, Ian Miersz, Eran Tromerx, Madars Virzay, Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), 2014, http://zerocash-project.org/paper

scambio decentralizzato, privo di autorità e controllori, che ha animato il progetto delle monete virtuali fino dall'inizio.

Parte II: Digital Currency

7. Monete digitali

7.1. Dagli accordi di *Bretton Woods* all'emissione digitale

Nei paesi di *Common Law*, il termine *digital currency* viene utilizzato per indicare la moneta espressa in codice binario 0-1: l'accezione del termine è ampia a sufficienza da ricomprendere sia le monete a corso legale, valute in senso proprio, sia le *utility* che si comportano come una moneta pur senza presentarne le proprietà, c.d. monete virtuali.

La caratteristica che distingue con maggiore definizione la valuta dalle monete virtuali consiste nella funzione di pagamento; ogni sistema legale contiene disposizioni che obbligano i consociati ad accettare i pagamenti in valuta: nell'ordinamento italiano questa previsione è contenuta nell'art. 1277 cc.[151].

La valuta viene emessa in rapporto matematico con la riserva aurea dello Stato: nella storia contemporanea, dal 1944 al 1971, le politiche monetarie dei 44 paesi impegnati nella guerra contro l'Asse furono regolati dagli accordi di *Bretton Woods;* il sistema, che ha dato luogo alla creazione del Fondo Monetario Internazionale e della Banca

[151]Art. 1277 c.c.: I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale . Se la somma dovuta era determinata in una moneta che non ha più corso legale al tempo del pagamento, questo deve farsi in moneta legale ragguagliata per valore alla prima.

Internazionale per la Ricostruzione e lo Sviluppo, aveva fissato la conversione aurea in $35 l'oncia e un rapporto di parità fissa con il dollaro per le valute delle altre Nazioni partecipanti all'accordo. Nel 1971 il Presidente Nixon annunciò la sospensione della conversione dollaro-oro; pochi mesi dopo, il Gruppo dei Dieci[152] sottoscrisse lo *Smithsonian Agreement* che poneva ufficialmente termine agli accordi di conversione, consentendo l'attuazione di una politica di inflazione del dollaro e introducendo la fluttuazione dei cambi. Il circolante poteva così venire accresciuto tramite la stampa di un numero di banconote superiore a quelle corrispondenti al rapporto unitario con la riserva aurea e il denaro prendeva un valore frazionale rispetto all'oro conservato nelle casse dello Stato; nel 1973 il *gold standard* venne definitivamente sostituito dal sistema dei cambi flessibili[153].

In quanto moneta a corso legale in un ordinamento, la valuta è sempre soggetta riserva di produzione a favore dello Stato e degli Enti da esso autorizzati; la riserva copre espressamente anche le emissioni in forma elettronica[154] che differiscono da quelle tradizionali per essere

---

[152] Il Gruppo dei Dieci (G10) è costituito da 11 paesi industrializzati (Belgio, Canada, Francia, Germania, Giappone, Italia, Paesi Bassi, Regno Unito, Stati Uniti, Svezia e Svizzera). I Ministri economici e finanziari e i Governatori delle banche centrali del G10 si riuniscono annualmente in occasione dell'assemblea annuale dell'FMI. I Governatori dei paesi del G10 si riuniscono regolarmente a Basilea (CH) presso la Banca dei Regolamenti Internazionali (*http://www.bis.org/)*
vide: http://www.bancaditalia.it/studiricerche/coop_intern/partecipa_org_int/G10ide

[153] *Vide* Benjamin Cohen, *Bretton woods Agreement, the Routledge Encyclopedia of International Political Economy*,
http://www.polsci.ucsb.edu/faculty/cohen/inpress/bretton.html

[154] Ad esempio nell'Unione Europea, la riserva di emissione è disposta dalla Direttiva 2009/101/CE, che nel TITOLO I, AMBITO DI APPLICAZIONE E DEFINIZIONI, recita espressamente: *Articolo 1,* Oggetto e ambito di applicazione. 1. La presente direttiva fissa le norme in materia di esercizio dell'attività di emissione di moneta elettronica ai cui fini gli Stati membri riconoscono le seguenti categorie di emittenti di moneta elettronica: a) enti creditizi, quali definiti all'articolo 4, punto 1), della direttiva 2006/48/CE, incluse, ai sensi del diritto nazionale, le loro succursali, secondo la definizione di cui all'articolo 4, punto 3), di tale direttiva, se esse hanno sede nella Comunità e la loro sede sociale si trova al di fuori della Comunità, conformemente all'articolo 38 di tale direttiva; b) istituti di moneta elettronica, quali definiti all'articolo 2, punto 1), della presente direttiva, incluse, conformemente all'articolo 8 della presente direttiva e al diritto nazionale, le loro succursali se esse hanno sede nella Comunità e la loro sede sociale si trova al di fuori della Comunità; c) uffici postali autorizzati a emettere moneta elettronica a norma del diritto nazionale; d) la Banca

la valuta espressa da un codice binario 0-1 invece che dalla stampa su carta o dal conio su metallo. Indipendentemente dalla forma in cui è stata emessa, alla valuta compete funzione di pagamento secondo il valore fissato dalle politiche della Banca Centrale di riferimento: si tratta di un valore stabilito dall'interno su cui gli utilizzatori non possono intervenire.

7.2. Ruolo della normativa antiriciclaggio

Allo scopo di contrastare le attività di riciclaggio, in molti Stati i servizi di trasferimento valuta devono essere autorizzati in via preventiva e la loro attività è soggetta a forme di vigilanza istituzionale volte ad assicurare l'adeguamento alle normative in vigore.

Nell'Unione Europea la normativa di riferimento è rappresentata dalle quattro direttive 1991/308/CEE, 2001/97/CE, 2005/60/CE, 2015/849/UE: fino dal 1991 la prima direttiva antiriciclaggio ha imposto a banche e intermediari finanziari gli obblighi di identificazione della clientela, di registrazione dei dati e delle operazioni sospette,

centrale europea e le banche centrali nazionali ove non agiscano in veste di autorità monetarie o altre autorità pubbliche; e) gli Stati membri o le rispettive autorità regionali e locali ove agiscano in veste di autorità pubbliche.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:it:PDF 2009.
In Italia a direttiva è stata attuata con d.lgs. n.45 del 16/04/2012 che all'art 1 n. 3) dispone: Il Titolo V-bis del decreto legislativo 1° settembre 1993, n. 385, È sostituito dal seguente:"Titolo V-BIS: MONETA ELETTRONICA E ISTITUTI DI MONETA ELETTRONICA. Art. 114-bis Emissione di moneta elettronica 1. L'emissione di moneta elettronica è riservata alle banche e agli istituti di moneta elettronica. 2. Possono emettere moneta elettronica, nel rispetto delle disposizioni ad essi applicabili, la Banca centrale europea, le banche centrali comunitarie, lo Stato italiano e gli altri Stati comunitari, le pubbliche amministrazioni statali, regionali e locali, nonché Poste Italiane. [omissis]
http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012;045

nonché di segnalazione alle autorità delle operazioni sospette di riciclaggio. Nel 2001 la seconda direttiva ha esteso l'ambito di applicazione della disciplina antiriciclaggio anche alle attività di case da gioco e case d'aste, alle attività di commercio di metalli e pietre preziose nonché ai liberi professionisti. Nel 2005 la terza direttiva ha introdotto un dovere di collaborazione attiva anche di assicurazioni e professionisti nella prevenzione del riciclaggio. La quarta direttiva, il cui decrto di attuazione è stato approvato dal Governo Italiano il 24 maggio 2017, ha ad oggetto la disciplina del sistema finanziario in termini di *risk assessment* e il coordinamento delle attività di prevenzione e vigilanza, con previsione di un sistema di controllo delle società di *money transfer* che sono considerate a rischio elevato di infiltrazione criminale[155]. Il documento è particolarmente interessante ai fini di questo studio poiché introduce il concetto di "*valuta virtuale*" quale "*rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*"[156].

Gli stati appartenenti allo spazio economico europeo, Islanda, Norvegia e Liechtenstein applicano normative analoghe a quelle dell'Unione Europea in forza dell'Accordo sottoscritto nel 1993[157]; di recente, il decreto MEF del 9 maggio 2016 ha aggiornato la *white list* dei Paesi che consentono un adeguato scambio di informazioni[158],

[155] http://www.governo.it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-31/7447

[156] Per le considerazioni sulla scelta del termine valuta, anziché moneta *vide ultra*.

[157]http://europa.eu/legislation_summaries/internal_market/living_and_working_in_the_internal_market/em0024_it.htm

[158]Il decreto esenta dall'applicazione dell'imposta sostitutiva sugli interessi, premi e altri frutti delle obbligazioni e titoli similari, pubblici e privati, i soggetti residenti in: Albania, Alderney, Algeria, Anguilla, Arabia Saudita, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bangladesh, Belgio, Belize, Bermuda, Bielorussia, Bosnia Erzegovina, Brasile, Bulgaria, Camerun, Canada, Cina, Cipro, Colombia, Congo (Repubblica del Congo), Corea del Sud, Costa d'Avorio, Costa Rica, Croazia, Curaçao, Danimarca, Ecuador, Egitto, Emirati Arabi Uniti, Estonia, Etiopia, Federazione Russa, Filippine, Finlandia, Francia, Georgia, Germania, Ghana, Giappone, Gibilterra, Giordania, Grecia, Groenlandia, Guernsey, Herm, Hong Kong,

includendo un numero di stati molto più elevato del precedente decreto del 2013[159].

Negli USA, i servizi di *money transfer* devono rispettare le previsioni antiriciclaggio contenute nel *Patriot Act*[160]: l'atto, emanato nel 2001, eleva a reato federale il trasferimento valori in difetto della licenza statale. Fino dalla sua emanazione si era cominciato a discutere sulla portata effettiva di questa previsione e nel 2002 lo Stato della California aveva rigettato alcune domande di licenza ricevute perché, a termini del *Transmission of Money Abroad Law* Act[161], in quello stato l'oro non era considerato una moneta[162]. Nel 2004 una società del settore aveva richiesto una pronuncia in merito del dipartimento del Tesoro a chiarimento dei dubbi incessanti. Conclusa l'istruttoria, nel 2006 il dipartimento del Tesoro aveva emesso un *report* ufficiale in cui si comunicava che, a termini dello *United States Code* e del *Code of Federal Regulations,* i sistemi di trasferimento basati su metalli preziosi non erano da considerare *money transfer*[163]. Tra il 2006 e il 2008 il

---

India, Indonesia, Irlanda, Islanda, Isola di Man, Isole Cayman, Isole Cook, Isole Faroe, Isole Turks e Caicos, Isole Vergini Britanniche, Israele, Jersey, Kazakistan, Kirghizistan, Kuwait, Lettonia, Libano, Liechtenstein, Lituania, Lussemburgo, Macedonia, Malaysia, Malta, Marocco, Mauritius, Messico, Moldova, Montenegro, Montserrat, Mozambico, Nigeria, Norvegia, Nuova Zelanda, Oman, Paesi Bassi, Pakistan, Polonia, Portogallo, Qatar, Regno Unito, Repubblica Ceca, Repubblica Slovacca, Romania, San Marino, Senegal, Serbia, Seychelles, Singapore, Sint Maarten, Siria, Slovenia, Spagna, Sri Lanka, Stati Uniti d'America, Sud Africa, Svezia, Svizzera, Tagikistan, Taiwan, Tanzania, Thailandia, Trinitad e Tobago, Tunisia, Turchia, Turkmenistan, Ucraina, Uganda, Ungheria, Uzbekistan, Venezuela, Vietnam, Zambia. La lista è soggetta a revisione periodica, in maniera conforme ai risultati della verifica sull'adeguatezza dello scambio di informazioni.
http://www.gazzettaufficiale.it/eli/id/2016/08/22/16A06123/sg

[159] Che all'art. 1 includeva: Australia, Brasile, Canada, Hong Kong, India, Giappone, Repubblica di Corea, Messico, Singapore, Repubblica del Sudafrica, Svizzera e Stati Uniti d'America; aggiungendo all'art. 2 Mayotte, Nuova Caledonia, Polinesia francese, Saint-Pierre e Miquelon, Wallis e Futuna, Aruba, Curaçao, Sint Maarten, Bonaire, Sint Eustatius e Saba http://www.airant.it/content/decreto-mef-paesi-white-list

[160] http://www.justice.gov/archive/ll/highlights.htm

[161] In vigore fino al 2010 http://www.venable.com/california-enacts-sweeping-new-law-targeting-money-transmitters-10-05-2010/

[162] http://www.dgcmagazine.com/the-e-gold-story/

[163] http://www.moneymakergroup.com/gold-Closed-Fbi-t106411.html&pid=2962379&mode=threaded e http://web.archive.org/web/20060322134922/https://www.e-gold.com/letter2.html

FinCen[164] e il Dipartimento di Giustizia hanno progressivamente allargato la nozione di denaro fino a ricomprendervi il trasferimento di ogni genere di valore fra soggetti diversi[165].

7.3. I servizi *value transfer*: il caso *E-Gold*

Una delle conseguenze più importanti dell'interpretazione estensiva del *Patriot Act* consiste nell'applicabilità delle previsioni che impongono di verificare l'identità dei clienti (*Know Your Customer rule*) anche ai servizi di *value transfer*: La nuova definizione delle regole ha condotto alla sospensione delle attività di *E-Gold*, la piattaforma di pagamento da molti considerata antesignana del sistema *Bitcoin*[166].

E-Gold era un sistema di trasferimento valori basato su un controvalore in lingotti d'oro depositati nei *caveau* di alcune banche; la società era stata fondata nel 1996 da Douglas Jackson e Barry Downey ed era incorporata a *S.Kitts and Nevis*, nell'arcipelago delle piccole Antille mentre le operazioni finanziarie venivano gestite dalla città di *Melbourne* in Florida (USA).

Nella fase iniziale dell'attività, l'oro depositato a riserva era sufficiente alla copertura dei movimenti di trasferimento, realizzando così un sistema di pagamento con funzioni di moneta aurea virtuale. Il servizio di trasferimento, particolarmente efficiente, aveva fatto sì che

164 Financial Crimes Enforcement Network
165 http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Cash-Intensive-Businesses-Audit-Techniques-Guide-Chapter-7
166 A partire dalla fine di marzo 2012, il nuovo regolamento *FinCen* ha esteso la normativa statunitense alle compagnie straniere che consentono ai cittadini americani di aprire un *account;* questa impostazione restrittiva ha costretto la piattaforma Goldmoney.*com* alla chiusura preventiva del sistema di pagamenti diretti fra utenti, già nel dicembre 2011. http://www.dgcmagazine.com/pdf/DGC-Dec11.pdf

nel corso del tempo *E-Gold* arrivasse a gestire transazioni per un controvalore di 20 miliardi di dollari l'anno; per quanto la riserva depositata fosse stata incrementata fino al peso di 3.8 tonnellate, pari a $85.000.000 del tempo, la media giornaliera di volumi di scambio era idonea a impegnarla da sola[167]. Le ragioni del successo di *E-Gold*, risiedevano, da un lato, nella sicurezza offerta dal *gold standard*, dall'altro, nell'immediatezza delle procedure di pagamento; peraltro, un ruolo fondamentale nella diffusione dello strumento fra il pubblico era svolto dalla possibilità di registrare gli *account* sotto un nome di fantasia, senza che vi fosse alcuna forma di controllo dei dati reali. Si realizzava così una forma di anonimità dei pagamenti che risultava essere particolarmente gradita ai clienti, purtroppo anche a quelli dediti ai traffici illeciti. Molte indagini finanziarie conducevano a *E-Gold* e l'*FBI* aveva aperto un fascicolo di indagine sulla società. Nel 2007, in conseguenza dell'interpretazione estensiva da parte del *FinCen* delle norme anti *money laundering* contenute nel *Patriot* Act, i gestori del sito vennero incriminati per aver contravvenuto alle disposizioni di identificazione dei clienti. L'anonimato che *E-Gold* offriva agli utenti era stato utilizzato per una serie di attività di *money laundering* che secondo l'accusa, erano da imputare in via concorsuale ai due gestori della piattaforma[168]. La vicenda giudiziaria che ne era conseguita ha portato, nel 2009, al congelamento delle attività del sito[169]; a nostro parere, si è trattato di una grave perdita per il mercato perché *E-Gold* era un mezzo di pagamento efficiente[170] la cui regolamentazione avrebbe portato maggiori vantaggi di quelli prodotti dalla sua estromissione dal sistema. Peraltro il mercato è un'entità viva e quando uno spazio economico efficiente viene lasciato libero in breve tempo si riempie con una

[167] *Vide* http://www.wired.com/2009/06/e-gold/all/
[168] *Vide* http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helping-cybercrooks?lite
[169] *Vide* http://www.dgcmagazine.com/the-e-gold-story/ et http://blog.stakeventures.com/articles/2008/07/22/the-man-finally-brought-e-gold-down
[170] In senso economico l'efficienza indica l'attitudine di uno strumento a servire uno scopo con un rapporto di costi -benefici ottimale.

soluzione alternativa: nella fetta di mercato lasciata libera da *E-Gold,* c'era lo spazio per mettere a dimora uno strumento che consentisse il trasferimento anonimo nel rispetto delle disposizioni del *Patriot Act.*

7.4. I sistemi di moneta virtuale

A partire dal 2009 sono stati immessi in rete una serie di sistemi di moneta virtuale: sempre più diffusi, negli ultimi anni questi strumenti sono divenuti di conoscenza comune grazie alla risonanza mediatica ottenuta dai *bitcoin* di Satoshi Nakamoto.

I sistemi analoghi a *Bitcoin* si basano sull'applicazione di un algoritmo di pagamento che prevede l'emissione di un numero determinato di monete: ogni progetto ne adotta uno specifico[171] e i *token* di sistema, non sono altro che le soluzioni di quell'algoritmo. La produzione di queste *utility,* detta *mining,* richiede complessi calcoli matematici gestiti da una rete di *computer* che procede anche alla verifica e alla convalida dei trasferimenti, garantendo la spendita unitaria della moneta. Il sistema è organizzato in maniera tale che ogni nodo della rete sia in grado di svolgere le medesime funzioni, differendo le macchine impiegate solo per la potenza di calcolo e l'ampiezza di banda di connessione.

Tecnicamente, le monete virtuali consistono in sequenze di bit (0-1) rappresentati con stringhe alfanumeriche esadecimali, composte cioè di sequenze di lettere che variano dalla A alla F e di numeri da 0 a 9; ognuna di queste stringhe è funzionale al trasferimento di algoritmi idonei alla descrizione della transazione con l'utilizzo di sistemi

[171] *Vide http://coinmarketcap.com/*

crittografici. Il trasferimento operato su questa base è verificato e messo in sicurezza: i nodi della rete convalidano la trasmissione evitando forme di doppia spendita del denaro mentre la procedura crittografica evita che soggetti terzi possano interporsi appropriandosi di quanto è stato trasferito.

Queste *utility* si comportano come monete pur non presentandone le caratteristiche funzionali: nei sistemi in esame la circolazione ha, infatti, base meramente volontaria. Pur in assenza dell'obbligo di accettarli in pagamento, i consociati hanno mostrato una notevole inclinazione verso questi nuovi strumenti e la loro diffusione ha portato all'emanazione della normativa di dettaglio che esamineremo nel prossimo capitolo.

8. Profili giuridici

8.1. Natura giuridica

Per comprendere la natura giuridica dei *bitcoin* occorre tenere conto della loro genesi, un procedimento che è estraneo al modo classico di concepire e creare la moneta: in questa nuova *utility* gli stessi calcoli matematici che generano le unità di scambio danno valore economico al servizio offerto, garantendo l'autenticità delle transazioni effettuate sulla rete e la riservatezza personale. Si tratta di uno schema innovativo: normalmente i servizi di pagamento e la loro messa in sicurezza consistono in un'attività dell'intermediario che viene compensata in valuta corrente; qui invece l'applicazione di alcuni algoritmi genera dei *token* utilizzabili come moneta che non hanno un valore sottostante tangibile. Il valore delle unità così create, probabilmente, consiste proprio nell'assicurare la riservatezza in quelle transazioni che non si desidera dichiarare: i casi sono vari e vanno dalla legittima tutela della *privacy* e dei dati sensibili, agli acquisti *borderline,* fino a quelli completamente illegali; in tutti questi casi è molto probabile che l'utente preferirà uno strumento di pagamento anonimo.

Fin dall'inizio della loro storia, i *bitcoin* si sono rivelati uno strumento adatto allo scopo indicato: di scarso valore e facilmente

scambiabili nella comunità della rete, si potevano accettare ed offrire in pagamento per somme modiche[172]; in quella fase apparivano destinati a un uso di nicchia e potevano essere ancora definiti come una moneta nel senso puramente economico del termine: rappresentavano cioè lo strumento di pagamento accettato da una comunità, piccola o grande che fosse, in un determinato momento storico[173]. La successiva evoluzione del valore di cambio[174] avrebbe posto l'accento sulla natura di *commodity*[175] dello strumento, aprendo l'orizzonte alla riflessione sulla speculazione finanziaria che ne caratterizza il commercio di cui ci

---

[172]In questo senso Satoshi Nakamoto aveva addirittura rivolto un appello agli sviluppatori del progetto Wikileaks affinché si astenessero dall'uso dei *bitcoin:* "*The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to Wikileaks not to try to use bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.*" *The Rise and Fall of Bitcoin* 2011 http://www.wired.com/magazine/2011/11/mf_*bitcoin*/

[173]Costituiscono un esempio di moneta locale i c.d. *linden dollar* che vengono utilizzati in *second life* www.secondlife.com

[174]Nei primi mesi del 2011 i *bitcoin,* ancora utilizzati in maniera pressoché esclusiva dagli appassionati di internet, registrarono un incremento di valore del 400%, raggiungendo la parità col dollaro all'inizio del febbraio 2011. Nell'aprile 2011 Satoshi Nakamoto si ritirò dal progetto *bitcoin,* semplicemente smettendo di rispondere alle *mail* dei propri collaboratori. Il ruolo di sviluppatore capo del progetto passò così a Gavin Anderson che in un intervista a Forbes dichiarò "*i bitcoin sono meglio dell'oro*" e che l'attrattiva che i *bitcoin* rappresentano per le attività criminali è pari a quella di qualsiasi altra forma di "*sistema analogo al contante*", *vide:*
http://www.forbes.com/forbes/2011/0509/technology-psilocybin-*bitcoin*s-gavin-andresen-crypto-currency.html.
A seguito di questa intervista, si verificò un forte rialzo nel valore dei *bitcoin*, che arrivò a toccare i $30 nel mese di giugno. Successivamente lo strumento entrò in una fase di calo costante che portò il valore a un minimo di $4 nel mese di novembre con un assestamento a $5 per la fine dell'anno. Il 15 gennaio 2012 la *CBS* offrì un'ulteriore spinta pubblicitaria al fenomeno mettendo in onda l'episodio 3.13 della serie televisiva *The Good Wife* intitolata *"Bitcoin for dummies".* La *réclame* riguardo l'esistenza e la natura dei *bitcoin* produsse un incremento nelle transazioni tale da far salire il valore di cambio a $14 nel dicembre del 2012.

[175] Per comprendere meglio l'argomento può essere utile leggere la definizione di *commodity* contenuta nel Morgan Stanley *commodity Book*: "*Tutti credono di sapere cos'è una commodity finché non provano a darne una definizione. Talvolta le commodity sono materie prime, ma più in generale si tratta di materiali destinati alla creazione di altri prodotti. Spesso le commodity sono dei beni fisici, ma non sempre è così: tra quelle meno tangibili si ricordano l'energia elettrica e le emissioni di carbonio. Le commodity negoziabili possono offrire agli investitori opportunità interessanti e diversificate [...] Investendo in prodotti strutturati come le note e i certificati, gli investitori possono beneficiare dei movimenti dei prezzi delle commodity senza bisogno di doverle possedere fisicamente*".
http://www.morganstanleyiq.it/pdf/downloads/82_commodity%20Book_Sett07.pdf 2007

occuperemo nel prossimo capitolo. Esistono, infatti, due distinte forme di impiego dei *bitcoin* che danno risalto, alternativamente, alla funzione di moneta virtuale o alla natura di *commodity* finanziaria: la rete utilizza questo strumento con prevalente funzione solutoria di natura convenzionale[176]; gli investitori, per contro, trattano i *bitcoin* alla stregua di una *commodity* finanziaria, investendo decisamente su di essi.

La definizione di moneta elettronica non ci sembra peraltro idonea a descrivere il fenomeno: per quanto *bitcoin* e *token* analoghi si comportino in determinati frangenti alla stregua di una moneta[177], non ne presentano le caratteristiche strutturali. Perché si possa parlare di moneta, lo strumento deve infatti assolvere alle tre funzioni fondamentali: di pagamento, di fissazione di un indice dei prezzi al consumo e di risparmio: la moneta in senso giuridico regola così lo scambio di beni e servizi, servendo al contempo da strumento di pagamento, unità di conto e riserva di valore[178].

La funzione di pagamento consiste in un dovere generale di accettare in pagamento la moneta avente corso legale nello Stato secondo il suo valore nominale: nell'ordinamento italiano tale previsione

---

176 Esistono addirittura sportelli ATM che erogano valuta corrente cambiandola dai depositi in rete Il primo sportello di questo genere è stato installato in Canada, a Vancouver e consente il prelievo di contante nel rispetto delle leggi antiriciclaggio, individuando il richiedente tramite impronta del palmo della mano; ciononostante, il governo locale ha tenuto a precisare che i *bitcoin* non costituiscono una valuta a corso legale nel paese. Attualmente, esistono circa 200 sportelli ATM dedicati ai *bitcoin:* il primo in Europa è stato quello della stazione centrale di Helsinki, in Finlandia ma non mancano gli sportelli italiani che si trovano nelle città di Roma, Pisa, Reggio Emilia, Udine e Milano.
http://www.ilsole24ore.com/art/notizie/2013-12-17/il-primo-bancomat-*bitcoin*-un-negozio-dischi-helsinki-122300.shtml?uuid=ABDHdak
http://business.time.com/2013/10/30/worlds-first-bitcoin-atm-launched-in-canada/
http://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-*bitcoin*-isnt-legal-tender/
http://www.repubblica.it/tecnologia/2014/10/20/news/*bitcoin*_italia-98573671/
http://coinatmradar.com/country/105/*bitcoin*-atm-italy/
http://www.webnews.it/2015/02/05/bitcoin-bancomat-milano/

177Ad esempio, sui siti di *blackmarket* il pagamento in forma crittografica é obbligatorio ai fini dell'anonimato.

178Eugenio Ruggiero, Moneta, Cambio, Valuta in Novissimo Digesto, Utet Torino 1995, vol X, pagg. 5 ss.

è contenuta nell'art. 1277 cc.; nel caso dei *bitcoin,* invece, la base delle transazioni è volontaria e non sussiste alcun dovere giuridico di accettarli in pagamento. La funzione di unità di conto, che consiste in una chiara definizione dei valori di scambio, viene invece ostacolata dalla forte volatilità dei *bitcoin* che rende difficile utilizzarli per la creazione di un indice di prezzi al consumo. Esprimendo in *bitcoin* un indice come il *Big Mac*, che prende in considerazione il prezzo del famoso panino per stabilire il potere di acquisto della moneta locale, si otterrebbero valori da ricalcolare in base all'alta volatilità di questo strumento che porta a fluttuazione rilevanti, soprattutto nei periodi di alta speculazione. Se si considera che ogni soggetto in fila in un *fast-food* ha la legittima aspettativa di pagare il panino acquistato la stessa cifra pagata dal soggetto in fila davanti a lui e che la volatilità dei *bitcoin* è talmente forte da aver registrato delle variazioni *intraday* del 200%, diventa fondamentale stabilire chi tra l'alienante e l'acquirente dovrà farsi carico della variazione[179]. Analoghe considerazioni valgono, infine, con riguardo alla funzione di risparmio: la volatilità di questo strumento è talmente alta da integrare una forma speculativa; in questo senso, l'intermediazione in un investimento in *bitcoin* imporrebbe di definire la classificazione MIFID dell'eventuale acquirente al livello di massima esperienza[180].

8.2. Direttiva 2009/101/CE

[179] Sulla *intraday* volatility *vide 'Bank of America Merrill Lynch: Bitcoin a first assessment' 2013* in https://ciphrex.com/archive/bofa-*bitcoin*.pdf

[180] In base alla direttiva 2004/39/CE del 21 aprile 2004, *Markets in Financial Instruments Directive*, normalmente indicata con l'acronimo *MIFID*, gli istituti di credito devono attribuire agli investitori la qualifica di cliente al dettaglio, cliente professionale o controparte qualificata e regolare di conseguenza le informazioni fornite e gli investimenti effettuati per loro conto.
Vide http://ec.europa.eu/internal_market/securities/isd/mifid/index_en.htm

Le considerazioni svolte rendono giuridicamente impropria la descrizione dei *bitcoin* in termini di moneta elettronica: l'espressione viene utilizzata nella lingua parlata come termine generico di riferimento ma non identifica le caratteristiche legali dello strumento, anzi, per definizione, i *bitcoin* si pongono al di fuori dell'ambito applicativo della direttiva 2009/101/CE[181]. L'atto fissa le norme in materia di esercizio dell'attività di emissione di moneta elettronica nell'Unione Europea, istituendo un monopolio a favore delle Banche Centrali e degli istituti autorizzati[182]. A propria volta, il d.lgs. 45/2012 che attua la direttiva nell'ordinamento italiano individua i confini della materia all' art 1 n. 3) che recita testualmente: "*Il Titolo V-bis del decreto legislativo 1° settembre 1993, n. 385, È sostituito dal seguente:*

Titolo V-BIS: MONETA ELETTRONICA E ISTITUTI DI MONETA ELETTRONICA.

Art. 114-bis - Emissione di moneta elettronica 1. L'emissione di moneta elettronica è riservata alle banche e agli istituti di moneta elettronica. 2. Possono emettere moneta elettronica, nel rispetto delle disposizioni ad essi applicabili, la Banca centrale europea, le banche centrali comunitarie, lo

[181]Attuata nello Stato italiano con decreto legislativo n. 45 del 16/04/2012.
[182]Direttiva 2009/101/CE, TITOLO I, AMBITO DI APPLICAZIONE E DEFINIZIONI, *Articolo 1,* Oggetto e ambito di applicazione. 1. La presente direttiva fissa le norme in materia di esercizio dell'attività di emissione di moneta elettronica ai cui fini gli Stati membri riconoscono le seguenti categorie di emittenti di moneta elettronica: a) enti creditizi, quali definiti all'articolo 4, punto 1), della direttiva 2006/48/CE, incluse, ai sensi del diritto nazionale, le loro succursali, secondo la definizione di cui all'articolo 4, punto 3), di tale direttiva, se esse hanno sede nella Comunità e la loro sede sociale si trova al di fuori della Comunità, conformemente all'articolo 38 di tale direttiva; b) istituti di moneta elettronica, quali definiti all'articolo 2, punto 1), della presente direttiva, incluse, conformemente all'articolo 8 della presente direttiva e al diritto nazionale, le loro succursali se esse hanno sede nella Comunità e la loro sede sociale si trova al di fuori della Comunità; c) uffici postali autorizzati a emettere moneta elettronica a norma del diritto nazionale; d) la Banca centrale europea e le banche centrali nazionali ove non agiscano in veste di autorità monetarie o altre autorità pubbliche; e) gli Stati membri o le rispettive autorità regionali e locali ove agiscano in veste di autorità pubbliche.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:it:PDF
http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2012;045

Stato italiano e gli altri Stati comunitari, le pubbliche amministrazioni statali, regionali e locali, nonché Poste Italiane".

È evidente che la struttura decentralizzata dei *bitcoin,* che consente a ogni nodo della rete di partecipare al *mining* è incompatibile con la riserva a favore di Banche ed Enti stabilita dalle disposizioni in esame; per poter ragionare in senso contrario, considerando le monete virtuali come moneta elettronica, occorrerebbe un'esplicita previsione normativa ma, in questo caso, la riserva di emissione farebbe venir meno la decentralizzazione caratteristica di queste monete che passerebbero nella disponibilità esclusiva delle istituzioni.

8.3. *Bitcoin report* del Congresso *USA*

Nell'analisi della normativa italiana riguardo i *bitcoin,* il report del Congresso USA *Regulation of Bitcoin in Selected Jurisdictions* del gennaio 2014[183] giunge peraltro a conclusioni opposte a quelle appena esposte, considerando i *bitcoin* quale oggetto diretto della direttiva 2009/101/CE e del d. lgs. 45/2012. Ci sembra, tuttavia, che nel *report* vengano a sovrapporsi i concetti di emissione dei *bitcoin*, attività di *mining* che non conosce vincoli in rete, con l'intermediazione professionale nei pagamenti in moneta elettronica, attività istituzionale consentita solo ai servizi autorizzati[184]. In questo senso appare opportuno ricordare che

[183]http://www.loc.gov/law/help/*bitcoin*-survey/2014-010233%20Compiled%20Report_.pdf 2014, pag 13.

[184]*Ibidem* " Italy implemented this Directive through Legislative Decree No. 45 of April 16, 2012,77 which defines the concept of electronic currency, including the cases in which it is issued electronically in exchange for funds to be used as a means of payment, and identifies the persons authorized to issue electronic money. *The Decree allows the use of electronic currencies in accordance with the EU Directive at the level of the European Central Bank, and by the central banks of European Members, the Italian*

nella spendita della moneta elettronica, l'utente non può prescindere dai servizi del terzo garante e che nell'Unione Europea questo servizio deve essere autorizzato a norma della direttiva 2007/64/CE[185]; viceversa, nel caso dei *bitcoin* esistono piattaforme di cambio autorizzate ma gli utenti sono liberi di procedere al pagamento in maniera autonoma, trattandosi di un sistema decentralizzato basato sull'applicazione di marche temporali e sulla verifica tramite algoritmo di *hash* in cui l'approvazione della transazione da parte di almeno sei nodi della rete sostituisce l'intervento del terzo garante. Appare esplicativo, in tal senso, il provvedimento dell'Autorità Federale Tedesca di Supervisione Finanziaria, che ha stabilito che ciò che deve essere autorizzato non è il procedimento di creazione dei *bitcoin* o il loro uso in funzione di strumento di pagamento, fatti che ricadono al di fuori dalle responsabilità istituzionali, ma il loro commercio autonomo che li trasforma in strumenti finanziari[186].

8.4. Corte di Giustizia UE

Con la sentenza 22 ottobre 2015, resa nella causa C-264/14[187], la Quinta Sezione della Corte di Giustizia dell'unione Europea ha stabilito

public administration at the regional and local government levels, and the Italian postal system. However, the use of electronic currency is restricted to banks and electronic money institutions—that is, private legal entities duly authorized and registered by the Central Bank of Italy."

[185]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:it:PDF

[186]http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Jahresbericht/2013/jb_2013_II_9_2_trading_in_*bitcoin*s.html *'The creation of Bitcoins and their use as a means of payment does not require authorisation within the scope of BaFin's responsibilities. However, if the Bitcoins themselves are traded, contrary to their actual function, they are deemed to be financial instruments requiring authorisation in accordance with section 1 (1a) sentence 2 nos. 1 to 4 of the KWG'.*

[187] Il testo integrale della sentenza è disponibile in http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=IT

che ai sensi dell'articolo 267 TFUE le operazioni di cambio tra bitcoin e valute tradizionali sono esenti da IVA.[188]

La domanda alla Corte nasceva da una controversia che vedeva opposti l'amministrazione finanziaria svedese, Skatteverket, e il cittadino sig. Hedqvist con riguardo al parere preliminare di assoggettabilità all'imposta sul valore aggiunto di alcune operazioni di cambio *bitcoin*/valuta che intendeva effettuare tramite una sua società. La commissione tributaria svedese, Skatterättsnämnden, aveva emesso il parere del 14 ottobre 2013 aveva dato parere favorevole all'esenzione IVA del servizio di cambio a titolo oneroso che il sig Hedqvist intendeva esercitare, ritenendo che i *bitcoin* svolgessero una funzione analoga a quella dei mezzi legali di pagamento.

L'amministrazione finanziaria svedese aveva proposto ricorso contro la decisione della commissione tributaria dinanzi allo Högsta förvaltningsdomstolen (Corte suprema amministrativa), facendo valere che il servizio di cui alla domanda del sig. Hedqvist non ricade nell'esenzione prevista dal capo 3, articolo 9, della legge sull'IVA e il caso era giunto infine alla Corte di Giustizia dell'Unione Europea che aveva pronunciato sentenza di esenzione, addirittura su parere favorevole dell'Avvocato Generale[189].

La motivazione riportata nel punto 17 della sentenza è di difficile comprensione nella versione italiana che soffre di alcune imprecisioni giuridiche nella traduzione: i *bitcoin* vengono così indicati come "valuta virtuale" e il loro uso come "corrispondente" a quello dei mezzi legali di pagamento; inoltre si specifica che sono fuori campo IVA le operazioni in banconote e "monete" ma non quelle in "valuta". In realtà, la sentenza descrive i *bitcoin* come strumenti di pagamento utilizzati in

[188] La versione consolidata del Trattato è disponibile in http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12012E%2FTXT

[189] CGUE, Causa C‑264/14, Parere dell'Avvocato Generale http://curia.europa.eu/juris/document/document.jsf?text=&docid=165919&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=691150#Footnote3

maniera analoga (*similar way*) agli strumenti di pagamento a corso legale, definendoli come *virtual currency*. Il termine *currency* indica qui la moneta in senso economico e non la valuta, che è la moneta avente corso legale in uno Stato, e riguardo a cui sarebbe quantomeno singolare ipotizzare un obbligo di accettazione virtuale: come tracciare, infatti, i confini giuridici di questa imposizione? Anche con riguardo alla determinazione del campo IVA, i termini *coin* e *currency,* tradotti rispettivamente in monete e valuta, indicano invece con tutta evidenza le monete metalliche (*coin*) e la moneta in senso economico, quale strumento di pagamento (*currency*). Ragionando altrimenti, sorgerebbe spontaneo il quesito: se la valuta è soggetta ad applicazione IVA, da chi sono emesse le banconote e le monete esenti?[190] Un'interpretazione volta a conciliare i termini della traduzione con il senso giuridico appropriato, potrebbe vedere l'uso del termine *currency* in quest'ultima frase come riferito ai giorni valuta, forma di interesse non soggetto a IVA, distinguendo così il montante in capitale, composto da banconote e monete, e interessi, indicati appunto con il temine valuta: resta comunque il fatto che il termine adoperato crea confusione sotto il profilo legale.

---

[190] Per rendere agevole la lettura riportiamo di seguito il testo del paragrafo 17 anche in lingua inglese.

17 *" Secondo la commissione tributaria, la valuta virtuale «bitcoin» è un mezzo di pagamento utilizzato in maniera corrispondente a mezzi legali di pagamento. Peraltro, l'espressione mezzi di pagamento con «valore liberatorio» di cui all'articolo 135, paragrafo 1, lettera e), della direttiva IVA sarebbe utilizzata per circoscrivere l'ambito dell'esenzione relativa alle banconote e alle monete. Ne deriverebbe che la disposizione dovrebbe essere letta nel senso che è riferita solo alle banconote e alle monete, ma non alla valuta. Tale interpretazione sarebbe altresì coerente con lo scopo dell'esenzione di cui all'articolo 135, paragrafo 1, lettere da b) a g), della direttiva IVA, vale a dire quello di evitare le difficoltà che deriverebbero dall'assoggettamento dei servizi finanziari all'IVA.*

17 According to the Revenue Law Commission, the 'bitcoin' virtual currency is a means of payment used in a similar way to legal means of payment. Furthermore, the term 'legal tender' referred to in Article 135(1)(e) of the VAT Directive is used in order to restrict the scope of the exemption as regards bank notes and coins. It follows, according to the Revenue Law Commission, that that term must be taken to mean that it relates only to bank notes and coins and not to currencies. That interpretation is also consistent with the objective of the exemptions laid down in Article 135(1)(b) to (g) of the VAT Directive, namely to avoid the difficulties involved in making financial services subject to VAT".

http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=IT

L'Agenzia delle Entrate Italiana ha reso la propria azione uniforme al disposto della sentenza della Corte di Giustizia dell'Unione Europea, specificando nella Risoluzione 02/09/2016 n° 72[191] che le operazioni di cambio valuta/*bitcoin* non sono soggette a IVA mentre ricavi e costi di esercizio dell'attività di intermediazione contribuiscono alla formazione dell'imponibile soggetto a tassazione ordinaria.

8.5. BitLicense

Nell'agosto 2015 lo Stato di New York ha introdotto *BitLicense*, una licenza obbligatoria per chi intenda commerciare professionalmente in monete virtuali. Il regolamento prevede un'ampia zona di esenzione per l'uso privato e per il pagamento di beni o servizi, consentendo anche l'attività di sviluppo e ricerca senza necessità di autorizzazione[192]. La

[191] www.agenziaentrate.gov.it/

[192] *NY Department of Financial Services, "Regulations of the Superintendent of Financial Services, part 200: virtual currencies", 2017,*
http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf
Section 200.2 - Definitions
[...](q) Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident: (1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency; (2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others; (3) buying and selling Virtual Currency as a customer business; (4) performing Exchange Services as a customer business; or (5) controlling, administering, or issuing a Virtual Currency. The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity. [...]
Section 200.3 - License
(a) License required. No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity. Licensees are not authorized to exercise fiduciary powers, as defined under Section 100 of the Banking Law.
(b) Unlicensed agents prohibited. Each Licensee is prohibited from conducting any Virtual Currency Business Activity through an agent or agency arrangement when the agent is not a Licensee.
(c) Exemption from licensing requirements. The following Persons are exempt from the licensing requirements otherwise applicable under this Part:
(1) Persons that are chartered under the New York Banking Law and are approved by the superintendent to engage in Virtual Currency Business Activity; and

licenza è obbligatoria per tutti i soggetti professionali che intendano svolgere la loro attività nello Stato di New York, o con riguardo a persone che risiedono, si trovano, hanno uffici o gestiscono attività commerciali a *New York*. L'atto aveva anche assegnato un periodo di 45 giorni per mettersi in regola con la nuova normativa alle società che già svolgevano questa attività prima dell'emanazione del regolamento. Questa disposizione, aveva però provocato un risultato inverso a quello sperato, inducendo dieci delle maggiori società di intermediazione in monete virtuali a lasciare la piazza di New York, in quello che i giornali avevano indicato come *the great bitcoin exodus*[193]. La scelta è stata determinata dai costi eccessivi della burocrazia da sbrigare: gli imprenditori hanno infatti lamentato che per ottenere la licenza occorre farsi carico di una spesa nell'ordine $ 50.000, composta di $ 5.000 da versare per la tassa locale e $ 45.000 per i professionisti incaricati delle verifiche e degli adempimenti previsti dalla nuova normativa. Nonostante il *NY Department of Financial Services* si offra di venire incontro alle esigenze delle *start up* offrendo due anni di licenza condizionata alle piccole società che ancora non presentino tutti i requisiti richiesti, è un dato di fatto che molte delle domande presentate sono state scartate e in tre anni di vigore del provvedimento le licenze concesse sono state pochissime: ne hanno ottenuta una *Circle*, *Ripple* e *CoinBase*, tre giganti del settore. A nostro parere, l'autorizzazione alla gestione di fondi altrui richiede sicuramente che le istituzioni valutino ogni richiesta con un'attenzione particolare; inoltre le previsioni di *BitLicense* hanno preso avvio nel 2014 in occasione del gravissimo fallimento dell*'ecxchange MtGox,* che analizzeremo nel dettaglio in un paragrafo dedicato. Peraltro, lo scarso numero delle licenze concesse dallo Stato di *New York* potrebbe fare riflettere sulle conseguenze di

(2) merchants and consumers that utilize Virtual Currency solely for the purchase or sale of goods or services or for investment purposes.

[193] Michael del Castillo, *The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem,* 2015, http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html

un'eccessiva rigidità nel giudizio che sembra aver portato a uno stallo del mercato privato, considerato che gli enti già registrati a termini della *New York Banking Law* sono esenti dalla procedura di registrazione.

Per le società che ottengono la *BitLicense,* il forte investimento in *compliance* viene ripagato da un'ampia credibilità di mercato: in seguito all'autorizzazione nello Stato di *New York*, *Circle* ha infatti ottenuto una licenza analoga nel Regno Unito in base alla quale ha allargato il proprio commercio ai trasferimenti monetari intercontinentali; *Ripple* è divenuta il centro di imputazione della fervente attività del Consorzio R3, dedicato anch'esso allo studio e all'implementazione di soluzioni per i trasferimenti interpiattaforma; *Coinbase*, che già si occupava del *trading* professionale di *digital asset*, ha ampliato la propria offerta con degli *wallet* per *bitcoin* ed *ether* in offerta sull'Apple Store[194].

8.6. Definizioni giuridiche e definizioni semantiche

L'analisi dei testi normativi che precedono suggerisce di formulare alcune riflessioni sulla traduzione dei termini in uso in questo settore: le monete virtuali nascono negli Stati Uniti e la lingua inglese ha una struttura diversa da quella della lingua italiana, per cui il medesimo termine può indicare situazioni ben diverse tra loro. Si pensi al vocabolo *sound* che oltre che in 'suono', può essere tradotto in vero, integro, genuino, completo, saldo, resistente, forte, legittimo, legalmente valido, che sembra, che segnala, che appare... In alcuni casi la traduzione è più semplice, come per l'espressione inglese *safe and sound* che si traduce

[194] https://itunes.apple.com/us/app/coinbase-bitcoin-ethereum-wallet/id886427730?mt=8

con l'italiano 'sano e salvo', dato che 'salvo e suono' non avrebbe alcun senso. Altre espressioni, come *sound forensics,* creano invece maggiori difficoltà: l'autore intendeva riferirsi alla *forensics* del suono, a un'attività di indagine rigorosa o addirittura ad accertamenti legalmente vincolanti? In casi come questo diviene fondamentale l'analisi del contesto e la traduzione deve essere sostenuta, oltre che da un livello adeguato di conoscenza della lingua straniera, anche da una competenza appropriata nella materia di cui si discute.

Dal punto di vista giuridico, le definizioni adottate possono portare a una grande differenza di trattamento e diviene fondamentale l'uso di termini pertinenti. La traduzione di documenti con valore legale richiede spesso la collaborazione di giuristi, appartenenti ai due diversi ordinamenti, che abbiano competenze linguistiche idonee. Questo perché a volte istituti con il medesimo nome possono regolare fattispecie differenti, come nel caso del termine generale 'contratto' che per i giuristi anglosassoni indica unicamente un contratto a prestazioni corrispettive, con esclusione ad esempio del comodato; viceversa, le medesime situazioni possono essere disciplinate da istituti con nomi diversi: la fattispecie del contratto di comodato di cui ci siamo appena occupati, in *Common Law* viene prevista con il nome di *bailment.*

Occorre dunque individuare la regolamentazione effettiva del caso concreto, con pari attenzione alla traduzione linguistica e al significato giuridico dei termini adottati. Nel settore di cui ci stiamo occupando, il termine *digital currency* viene tradotto con diverse espressioni, molte delle quali non sono idonee a identificare correttamente il fenomeno sul piano del diritto.

Una delle prime definizioni utilizzate è stata quella di moneta elettronica che, a nostro parere, non è idonea a descrivere correttamente il fenomeno *bitcoin*: essa indica semplicemente che la moneta, invece di essere rappresentata da una banconota o da un conio

metallico, è espressa da un codice binario, senza che ricorra una differenza di funzione. La direttiva 2009/101/CE ha, inoltre, introdotto la riserva di questa emissione a favore di banche ed enti istituzionali, avviando un regime normativo del tutto incompatibile con la struttura degli strumenti di cui ci stiamo occupando.

Per quanto riguarda, invece, il temine criptovaluta, ci sono da svolgere due distinti ordini di considerazioni. Il primo è relativo al valore semantico attribuito al prefisso cripto, la cui etimologia rimanda al tardo latino *cryptĭ*cu(m), a propria volta derivato dal greco *kryptikós*, originato da *krýptein* 'nascondere'[195]. In questa accezione il termine criptovaluta rappresenta un ossimoro in cui il prefisso di segretezza viene ad elidere il significato stesso di valuta che, in quanto moneta avente corso legale in un ordinamento, ben difficilmente potrà avere natura segreta. L'altra accezione del prefisso cripto indica che nel caso concreto è stato fatto uso della crittografia. È importante ricordare che il sistema *Bitcoin* è basato sul trasferimento in chiaro di dati fra utenti le cui identità sono protette con crittografia, a differenza dei sistemi tradizionali di pagamento elettronico che operano trasferimenti criptati fra utenti in chiaro. Il secondo ordine di considerazioni riguarda invece l'uso del temine valuta come traduzione di *currency,* lemma utilizzato nei paesi di *Common Law* per indicare sia le monete a corso legale, valute in senso proprio, che tutte le *utility* monetarie in senso lato; in questo senso, *cryptocurrency* indica una moneta in senso economico protetta con impiego della crittografia.

Anche con riguardo la definizione 'valuta virtuale', adottata dal legislatore italiano nel decreto legislativo di attuazione della IV direttiva antiriciclaggio 2015/846/UE, formuliamo considerazioni analoghe a quelle espresse in prima battuta per l'uso della definizione 'criptovaluta': giuridicamente il termine valuta indica la moneta a corso legale in un determinato ordinamento. Purtroppo o per fortuna, le

[195] http://www.garzantilinguistica.it/ricerca/?q=criptico

monete virtuali sono ben lungi dal ricoprire un ruolo analogo a quello della valuta tradizionale sebbene in assenza dei requisiti di legge, come accadde in Italia per i vecchi gettoni telefonici che venivano accettati comunemente come strumento di pagamento cumulativo alle Lire e che vedevano addirittura un adeguamento immediato del valore agli aggiornamenti delle tariffe determinati dal gestore. Sempre in Italia, a metà degli anni '70 le monete erano state sostituite per un periodo dai c.d. miniassegni che facevano fronte alla temporanea scarsità del conio metallico rimpiazzando quelli che erano stati fino a quel momento i rimedi di pagamento 'fai da te' che avevano visto l'impiego di caramelle, francobolli, biglietti di autobus e tram; all'operazione di avvicendamento erano sopravvissuti solo i gettoni telefonici.

Figura 10: miniassegno del Banco San Paolo di Torino[196]

A nostro parere, per la definizione in termini giuridici dei *token* come *bitcoin* appare meglio adeguata l'espressione moneta virtuale che indica l'attitudine di questi strumenti alla produzione degli effetti della moneta, pur in mancanza delle tre funzioni legali di pagamento, fissazione dell'indice dei prezzi al consumo e risparmio. Un altra locuzione che troviamo adeguata alla descrizione della fattispecie è *digital currency* che viene spesso utilizzata per indicare l'uso dei metodi

[196] http://collezionieuro.altervista.org/blog/curiosita/i-miniassegni-perche-furono-emessi-1975/

di pagamento nativi digitali, facendo riferimento ai sistemi di *blockchain* e *DLT* in contrapposizione alla valuta elettronica.

Indipendentemente dalla loro appropriatezza sul piano del diritto, tutti i termini indicati in questo paragrafo possono essere utilizzati come punti di riferimento nel *semantic web,* un'evoluzione del W*orld Wide Web* ideata dallo stesso *Tim Berners-Lee,* in cui i documenti pubblicati in rete vengono associati ai metadati; questi dati aggiuntivi specificano informazioni sui dati oggetto di analisi, che in questo caso sono relative alla interoperabilità semantica e alle equivalenze dei descrittori, in modo tale da consentire ai motori di ricerca l'interpretazione e l'elaborazione automatica della *query* inserita in linguaggio corrente dall'utente[197].

[197] Tim Berners-Lee, James Hendler e Ora Lassila, "*The Semantic Web*", 2001: "*The Semantic Web will bring structure to the meaningful content of Web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users. Such an agent coming to the clinic's Web page will know not just that the page has keywords such as "treatment, medicine, physical, therapy" (as might be encoded today) but also that Dr. Hartman works at this clinic on Mondays, Wednesdays and Fridays and that the script takes a date range in yyyy-mm-dd format and returns appointment times. And it will "know" all this without needing artificial intelligence on the scale of 2001's Hal or Star Wars's C-3PO. Instead these semantics were encoded into the Web page when the clinic's office manager (who never took Comp Sci 101) massaged it into shape using off-the-shelf software for writing Semantic Web pages along with resources listed on the Physical Therapy Association's site.*"
http://www.cs.umd.edu/~golbeck/LBSC690/SemanticWeb.html

9. Profili economici

9.1. Resistenza alle procedure inflattive

Le monete virtuali a struttura decentralizzata rappresentano un'innovazione sotto molteplici profili, in particolare, molto si è scritto riguardo alla loro resistenza ad eventuali procedure inflattive. I sistemi analoghi a *Bitcoin* rimangono, infatti, estranei alle politiche monetarie delle Banche Centrali: la loro produzione è libera in rete, lo scambio passa tramite sistemi extraistituzionali e non vi è modo di influire dall'interno sul loro valore. La mancanza di un ente di emissione, differenzia nettamente questi strumenti dalle monete a corso legale: se è vero che manca un istituto centrale disposto a investire pesantemente nel tentativo di difenderne il valore, come accadde nel 1992 quando la Banca d'Italia intervenne per fare fronte all'attacco che lo speculatore Soros aveva portato alla Lira[198], si è comunque immuni dalle decisioni di politica economica che conducono alla svalutazione, procedure che hanno conosciuto il loro momento storico più critico nei casi di

[198] Il sole 24 ore, Le mosse disperate delle Banche centrali / Quando Soros il terribile affondò lira e sterlina (1992), 2016, http://www.ilsole24ore.com/art/notizie/2014-12-16/le-mosse-disperate-banche-centrali-quando-soros-terribile-affondo-lira-e-sterlina-1992-200339.shtml?uuid=ABt24iRC&refresh_ce=1

iperinflazione come quello del Marco della repubblica di Weimar, che arrivò ad essere stampato in banconote del taglio di 100.000 miliardi poco dopo il 1920, portando il prezzo del pane a 400 miliardi al kg[199].

Da un punto di vista formale, è proprio la struttura di queste *utility* che rende impraticabile la procedura di svalutazione: il numero di monete virtuali producibili è predeterminato dall'algoritmo adottato. *Bitcoin* ed *Ethereum* vedono la produzione organizzata secondo una frequenza definita in via matematica e non è possibile incrementare in maniera forzosa il numero delle unità in circolazione: il sistema adottato non consente politiche economiche in deroga. I sistemi analoghi a *Ripple* fanno invece eccezione alle considerazioni svolte in questo paragrafo: i *token* in *premining* sono già tutti in circolazione e sono assegnati ad alcuni soggetti in una percentuale talmente alta che la loro immissione in massa sul mercato sarebbe idonea a modificare il corso del valore di cambio.

Dal punto di vista pratico, esiste un altro fattore che rende il procedimento inflattivo estraneo alla fattispecie che stiamo esaminando: le monete virtuali non presentano di norma alcun valore sottostante. *Bitcoin, ether e Ripple xrp* sono composti di stringhe alfanumeriche; non c'è un bene di riferimento: le monete virtuali consistono piuttosto in un servizio. Se si pensa a un tradizionale servizio di trasferimento valori, le monete virtuali rappresentano il blindato su cui viene caricato l'oro, non l'oro medesimo: sono state progettate in questo modo proprio per ovviare ai problemi introdotti dall'interpretazione estensiva delle disposizioni *anti money laundering* contenute nel *Patriot Act*. La procedura inflattiva monetaria consiste in un'alterazione del rapporto numerico fra le monete emesse e la riserva aurea sottostante: aumentando il circolante si riduce il valore frazionale del denaro e, di conseguenza, il suo potere di acquisto. Quando si trasferiscono monete virtuali del genere dei *bitcoin* si cede il valore che il mercato riconosce a

[199] http://www.viaggio-in-germania.de/inflazione-1923.html

questo servizio, valore che consiste, principalmente, nel rendere anonima la transazione: questo schema non conosce una forma di alterazione legata al soprannumero di 'monete' eventualmente presenti sul mercato; ogni algoritmo di pagamento ha un numero finito di soluzioni ma gli algoritmi presenti sulla rete crescono ogni giorno senza che si riduca vicendevolmente il loro potere di acquisto. Allo stato dell'arte esistono alcune centinaia di strumenti analoghi ai *bitcoin* e ognuno di essi si basa sull'applicazione di un diverso algoritmo crittografico con un numero predefinito di *token*[200]; non risulta che alcuno di essi soffra decrementi di valore legati alla presenza degli altri: il valore di questi strumenti è determinato dall'uso della rete, dagli investimenti di mercato e da alcune decisioni di tipo istituzionale che ne condizionano l'esistenza, come accade quando vengono introdotte nuove disposizioni antiriciclaggio. I grafici che seguono evidenziano i movimenti storici di *bitcoin, Ripple xrp* ed *ether* mostrando mercati autonomi che non si recano danno a vicenda.

Figura 11: grafico valore storico *bitcoin*[201]

[200] *Vide http://coinmarketcap.com/*
[201] https://coinmarketcap.com/

Figura 12: grafico valore storico *Ripple xrp*[202]

Figura 13: grafico valore storico *ether*[203]

[202] https://coinmarketcap.com/
[203] https://coinmarketcap.com/

8.2. BCE *Virtual Currency Schemes*

Nell'ottobre del 2012 la BCE ha incluso i *bitcoin* nello studio *Virtual Currency Schemes*[204]*:* il documento analizza la natura di moneta virtuale di questa *utility*, considerando le caratteristiche che lo strumento presenta come moneta in senso economico, ed offre spunti di riflessione riguardo la sua natura di *commodity* finanziaria. Le pagine dedicate all'argomento ricordano il crollo del valore di cambio da $ 17.50 a $ 0.01 verificatosi in pochi minuti in occasione di un furto *on line* avvenuto il 20 giugno 2011 e le vicende della piattaforma speculativa *Bitcoinica*, liquidata dopo aver subito due pesanti *hacking attack*[205], mettendo in risalto quegli elementi di volatilità e rischio che caratterizzano lo strumento e ne costituiscono un elemento distintivo.

Il furto che aveva causato il crollo delle quotazioni era stato perpetrato ai danni della piattaforma di gestione *MtGox*. In quell'occasione si era parlato della sottrazione di 400.000 *bitcoin* ma leggendo le discussioni sui *forum* dedicati emerge che in realtà si sarebbe trattato di un attacco al sito con duplicazione dei *token* depositati che sarebbero poi stati rivenduti sul mercato a prezzo stracciato, con una serie di manovre speculative conseguenti; stando a questa ricostruzione, *MtGox* avrebbe risolto la situazione riportando il sistema a una versione precedente e offrendo ai clienti danneggiati

[204] BCE virtual currency schemes, 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[205]Megan Geuss, Bitcoinica users sue for $460k in lost Bitcoins: A complaint filed in SF accuses the trading platform of breach of contract, 2012, http://arstechnica.com/tech-policy/2012/08/*bitcoin*ica-users-sue-for-460k-in-lost-*bitcoin*s/

dall'attacco il rimborso delle perdite subite: il numero di *bitcoin* effettivamente sottratti si attesterebbe nell'ordine delle 2.500 unità[206].

Le vicende relative a *Bitcoinica* mettono in evidenza come la piattaforma, pur avendo precedentemente subito due attacchi in rete, non avesse provveduto alla messa in sicurezza del sito che aveva quindi subito il terzo attacco descritto nel report della *BCE*; ad esito delle operazioni il gestore si era reso disponibile a risarcire il 50% dei valori sottratti ma gli utenti avevano giudicato insufficiente la cifra offerta preferendo intentare una causa per il risarcimento dei danni subiti[207].

La stampa specializzata ha messo in luce che i fondi di *Bitcoinica* erano gestiti da *MtGox,* adombrando più di un sospetto sulla trasparenza delle operazioni di gestione: i fatti appropriativi descritti nel *report* mettono soprattutto in luce un problema relativo alla gestione dei due *exchange* che hanno potuto disporre liberamente dei valori depositati senza che le autorità esercitassero alcuna forma di controllo.

---

206 List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [Old], 2012, https://bitcointalk.org/index.php?topic=83794.0#post_june_2011_mt_gox_incident "*June 2011 Mt. Gox Incident. Mt. Gox, then the leading BTC/USD exchange service, suffered a severe breach as a consequence of an ownership change. The sale conditions involved a share of revenue to be remitted to the seller. To audit this revenue, the seller was permitted an account with administrator access. The seller's administrator account was hacked by an unknown process. The priveleges were then abused to generate humungous quantities of BTC. None of the BTC, however, was backed by Mt. Gox. The attackers sold the BTC generated, driving Mt. Gox BTC prices down to cents. They then purchased the cheap BTC with their own accounts and withdrew the money. Some additional money was stolen by non-attacking traders capitalizing on the dropping price and withdrawing in time, including toasty, a member of BitcoinTalk. Mt. Gox resolved the hack by reverting trades to a previous version. Many customers claim they have lost money from this reversion, but Mt. Gox claims it has reimbursed all customers fully for this theft. After the incident, Mt. Gox shut down for several days. The event's scale was widely disputed; some report a theft of almost 500000 BTC due to related account hacking. However, these reports are sparse and disreputable. Closer inspection puts the losses at closer to 2500 BTC. Aside from the direct damages of the theft, the hack involved a database leak. Some weaker passwords were used to conduct the relatively more severe Mass MyBitcoin Thefts.*"

207 John Weru Maina, Does Bitcoinica Founder Zhou Tong Have Some Explaining To Do?, 2015, https://www.cryptocoinsnews.com/bitcoinica-founder-zhou-tong-explaining/

Lo studio della BCE fa infine riferimento alle critiche formulate dalla moderna scuola economica austriaca riguardo alla possibilità dei *bitcoin* di divenire socialmente accettati come moneta[208]: la mancanza di un valore sottostante non consente a queste utilità di soddisfare il teorema della regressione di Von Mises che individua il fattore di accettazione sociale della moneta non nell'imposizione governativa ma nel valore a cui è agganciata, ad esempio l'oro, e di cui esprime il potere di acquisto. In conclusione, il report fa proprie le affermazioni di Gavin Andersen, *lead developer* di *Bitcoin*, riguardo alla natura di *internet start-up* di questo progetto e ai rischi che sono connessi a ogni forma di nuovo investimento[209]*:* entrambi i ragguagli devono essere letti in uno con la chiosa finale della BCE che avverte dei pericoli relativi alla sicurezza del sistema, privo di ogni forma di controllo istituzionale[210].

8.3. Rischio di bolla speculativa

Nella prospettiva ora delineata deve essere analizzato il problema ulteriore del mercato dei derivati: fin dal novembre 2012 la forte volatilità nel valore di cambio dei *bitcoin* ha indotto una società di investimento maltese a creare un *bitcoin hedge fund*[211] con base alle

[208] *BCE virtual currency schemes, 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf,* Ludwig Von Mises Italia, La moneta, http://vonmises.it/2014/04/30/la-moneta-v-parte/

[209] *BCE virtual currency schemes, 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*

[210] *BCE virtual currency schemes, 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf "All these issues raise serious concerns regarding the legal status and security of the system, as well as the finality and irrevocability of the transactions, in a system which is not subject to any kind of public oversight."*

[211] Un *hedge fund* è un fondo speculativo in cui si entra per grossi tagli: il forte rischio di investimento viene affrontato ripartendo la somma a disposizione fra alcuni prodotti alternativi, tutti ad elevata volatilità. Teoricamente la riuscita di almeno uno degli investimenti dovrebbe compensare le perdite subite sugli altri fronti. Per ulteriori informazioni, *vide*

Bermuda[212]; seguendo un piano di investimento analogo, a *New York* il progetto *Coinsetter* ha invece proposto la gestione da parte di alcuni *broker* di *Wall Street*: nonostante il crollo del 2014 i fondi in *bitcoin* hanno reso ottime prestazioni negli ultimi due anni e la prima metà del 2017 ha segnato quotazioni che hanno più che duplicato i massimi storici del 2013.

Nel tempo le scommesse sul valore dei *bitcoin* hanno condotto gli operatori ad assumere rischi talmente elevati[213] che già nel mese aprile 2013 gli analisti avvertivano che il mercato mostrava i segni aggressivi tipici delle bolle speculative[214]. Questa valutazione, che implica il forte rischio di un crollo verticale, è stata ripetuta ai più alti livelli[215]: in un intervista rilasciata all'*Huffington Post* nel 2013, Guido Rossi, già Presidente della CONSOB, si era riferito ai *bitcoin* come a un bene rifugio fasullo, affermando che essi rappresentano degli strumenti finanziari in grado di stravolgere le regole del capitalismo. L'insigne economista aveva fatto riferimento anche a *Ripple* asserendo che le *commodity* digitali ricordano da vicino il sistema dei derivati, al pari dei quali presentano rischi da non sottovalutare[216]. In senso analogo si era espresso anche Nout Wellink, ex governatore della Banca Centrale Olandese, che all'inizio di dicembre 2013, momento in cui le quotazioni registravano il massimo storico, aveva addirittura espresso la

---

http://www.finanzaonline.com/education/hedge_fund/index.php?=&folsession=ad2e917efcce4fbff7fed329047b6a81

[212]https://exante.eu/press/news/266/
http://www.hedgeweek.com/2013/11/25/193637/*bitcoin*-fund-best-performing-hedge-fund-year-date

[213]http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-*bitcoin*-via-derivatives-markets/ 2013

[214]Recenti studi accademici hanno messo in evidenza come l'ottica dei *broker* finanziari sia a volte improntata all'accettazione di un carico di rischi eccessivo. *Vide* Elmar Burchia, I *trader?* Più spietati degli psicopatici, 2011
http://www.corriere.it/economia/11_settembre_26/operatori_borsa_spietati_psicopatici_burchia_d1475624-e833-11e0-9000-0da152a6f157.shtml e Sherree Deconvy, *The financial psychopath next door*, 2012
http://www.cfapubs.org/doi/pdf/10.2469/cfm.v23.n2.20

[215]http://www.cnbc.com/id/100613010 2013.

[216]http://www.huffingtonpost.it/2013/04/16/*bitcoin*-parla-guido-rossi-e-uno-strumento-rischioso-e-come-i-derivati-puo-stravolgere-le-regole-del-capitalismo_n_3093273.html 2013.

preoccupazione che i *bitcoin* potessero rivelarsi una bolla peggiore di quella dei tulipani[217]; del tutto simile il giudizio di Alan Greenspan, ex governatore della *FED* che aveva etichettato l'intero fenomeno *e-money* in termini di bolla speculativa[218]. Per fortuna le previsioni degli economisti si sono rivelate sbagliate ma alla fine del 2013 i *bitcoin* sono stati realmente in pericolo di bolla come aveva evidenziato anche lo studio di *Merril Lynch* analizzato nel paragrafo successivo.

8.4. Merrill Lynch Bank of America 'Bitcoin: a first assessment'

Nello stesso periodo in cui gli economisti lanciavano un grido di allarme a più voci, *Merrill Lynch Bank of America* aveva pubblicato il documento '*Bitcoin: a first assessment'*[219]. L'analisi metteva in evidenza la necessità di una regolamentazione internazionale uniforme dei *bitcoin,* avvertendo peraltro che una normativa statale troppo stringente avrebbe incrementato in maniera significativa i costi di transazione, riducendo sensibilmente i vantaggi legati alla compravendita dello strumento.

Lo studio metteva altresì in guardia dalla mancanza sul mercato dei *bitcoin* delle forme di garanzia dei depositi tipiche del sistema bancario,

[217]http://www.businessinsider.com/dutch-banker-compares-*bitcoin*-to-tulips-2013-12 2013 In questo senso anche *David Groshoff: Kickstarter my heart: extraordinary popular delusions and the madness of crowdfounding constraint and bitcoin bubbles* 2013
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313396
[218]http://www.forexinfo.it/*Bitcoin*-valore-risale-sopra-1-000
[219]*Merrill Lynch Bank of America, Bitcoin: a first assessment, http://doc.xueqiu.com/142c5bad45a1f73fe6c865a4.pdf 2013*

un elemento di tutela degli investitori che i sistemi istituzionali considerano necessario e imprescindibile: tuttavia, gli analisti sottolineavano che l'ulteriore aggravio dei costi di transazione prodotto da questo strumento avrebbe eliminato la maggior parte dei benefici degli investimenti, specialmente se sommato a una normativa di dettaglio. *Rebus sic stantibus*, il giudizio conclusivo del documento prevedeva una quotazione massima dello strumento di $1300, assolutamente in linea con il prezzo raggiunto nella prima settimana di dicembre 2013[220].

Le considerazioni svolte nel documento prevedevano con due anni di anticipo gli eventi determinati nello stato di New York dall'introduzione della *BitLicense* del 2015, quando l'istituzione di controlli troppo stringenti ha portato a una riduzione del numero di imprese attive sul mercato delle monete virtuali. Un contemperamento delle opposte esigenze di mercato e sicurezza potrebbe portare all'introduzione di alcuni requisiti base che, mantenendo inalterata la garanzia per gli investitori, consentissero un accesso più ampio al settore: in particolare, riteniamo che potrebbe rivelarsi efficiente affiancare alle riserve e ai depositi obbligatori delle forme concorrenti di tutela degli investitori, come garanzie fidejussorie e assicurative rilasciate dagli istituti di credito (tradizionali) interessati a investire nelle iniziative digitali.

[220] *Ibidem,* pag. 10 si legge testualmente:*" Is Bitcoin a bubble? Assuming Bitcoin becomes (1) a major player in both ecommerce and money transfer and (2) a significant store of value with a reputation close to silver, our fair value analysis implies a maximum market capitalization of Bitcoin of $15bn (1BTC = 1300 USD). This suggests that the 100 fold increase in Bitcoin prices this year is at risk of running ahead of its fundamentals*".

8.5. European Bank Authority 'Warning to consumers on digital currencies'

Alla fine del 2013 il fermento attorno ai *bitcoin* era cresciuto al punto che nella seconda settimana di dicembre era intervenuta in argomento addirittura l'Autorità Bancaria Europea. In un'ottica di tutela degli investitori, l'Istituto aveva emesso un formale '*Warning to consumers on digital currencies*'[221] reagendo, con ogni probabilità, a dei movimenti di mercato particolarmente aggressivi: nei giorni precedenti infatti era stato registrato il valore massimo di quotazione mai raggiunto, seguito da un crollo verticale per cui, pur in assenza di riferimenti ufficiali, il valore dei *bitcoin* era passato in poche ore da oltre $1200 a poco più di $600.

Il documento adottava così un punto di vista forse fin troppo rigoroso, mettendo in rilievo unicamente gli aspetti di rischio legati all'utilizzo delle valute virtuali. Ribadito il monito, già formulato da *Merrill Lynch,* riguardo la mancanza di forme di assicurazione dei depositi, i cittadini europei venivano messi in guardia contro i rischi relativi alla volatilità e ai furti di *bitcoin.*

L'autorità ricordava quindi che occorre sempre tenere conto della tassazione applicabile agli investimenti sottolineando altresì i rischi di confisca delle intere somme impiegate nel caso di attività criminose svolte sulla piattaforma di gestione: in particolare, *l'EBA* invitava i cittadini a verificare sempre l'affidabilità del gestore, tenendo presente che, nel corso delle indagini su eventuali attività illecite, l'autorità

[221]http://www.eba.europa.eu/documents/10180/15971/EBA+Warning+on+Virtual+Currencies.pdf 2013

giudiziaria avrebbe potuto procedere al sequestro di tutte le somme presenti sul sito, senza possibilità di svincolo dei fondi su base personale.

Infine, gli investitori venivano invitati ad avere la massima cura dei loro portafogli virtuali e a tutelarsi impiegando nello strumento solo denaro nella loro effettiva disponibilità. Quest'ultimo avvertimento chiarisce il clima in cui è stato emesso il documento e appare volto a prevenire il tipico comportamento speculativo di bolla in cui si vendono immobili e si richiedono finanziamenti per partecipare in maniera decisiva alla 'corsa all'oro'[222]. Ciononostante, i toni del documento suonano forse un po' troppo allarmistici e hanno rischiato, proprio per questo motivo, di non essere presi nella dovuta considerazione dagli investitori che hanno continuato impassibili per la loro strada; in termini di *behavioral economics,* un esposizione ferma ma pacata dei rischi effettivi avrebbe forse potuto sortire effetti migliori.

[222]Per una valutazione delle bolle storicamente più importanti *vide* Charles Mackay: *Memoirs of Extraordinary Popular Delusions,* Londra 1841

9. Reazione all'allarme sociale

9.2. Silk Road

Il 2013 ha visto i *bitcoin* imporsi come fenomeno di massa: sotto il profilo bancario, in concomitanza con la crisi di Cipro si è avuto un forte incremento nelle quotazioni contro il dollaro statunitense, seguito da una serie di crolli e rimbalzi che hanno caratterizzato tutto il mese di aprile 2013[223]; Il successivo mese di maggio ha invece registrato una fase di crescita piuttosto regolare e si è chiuso con il cambio a $130.

Per quanto riguarda gli utenti della rete, in quel periodo si è avuta una forma molto intensa di impiego in funzione di criptomoneta (strumento di pagamento non rintracciabile), imposta nei *blackmarket* del *dark web* per mantenere segreta l'identità dei partecipanti: stando a quanto affermato dall'*FBI*, il sito di S*ilk Road,* posto sotto sequestro all'inizio del mese di ottobre 2013, accettava unicamente pagamenti in *bitcoin*[224].

[223]La prima settimana del mese di aprile il valore di cambio è salito da $100 a $240 per poi crollare nel giro di una settimana a un minimo di $60. Nei dieci giorni successivi si è avuto un rimbalzo a $140 seguito da un nuovo crollo a $100 alla fine del mese.

[224]http://www.scribd.com/doc/184579094/Virtual-Currency-Response-LettersFederal-Agencies-Respond-to-Homeland-Security-Committee-Questions-on-

La storia era salita alla ribalta in occasione di una clamorosa indagine: si stima che *Silk Road* gestisse compravendite di stupefacenti e altri articoli illeciti, come carte di identità contraffatte, armi, agenti biologici e servizi criminali di vario genere, per un ammontare giornaliero di 10.000 *bitcoin,* pari al 5% di quello che era il movimento complessivo dello strumento[225].

In occasione dell'azione di polizia, sul sito erano stati sequestrati anche 170.000 *bitcoin* appartenenti al gestore Ross Ulbricht, il quale aveva intentato un procedimento giudiziario per chiederne la restituzione, sostenendo che si sarebbe trattato di beni non sequestrabili secondo le leggi Federali; il procuratore incaricato del caso aveva opposto, peraltro, che nei casi di riciclaggio è previsto il sequestro di qualunque unità di valore e diversi giudici, intervistati in pendenza del processo, avevano avvalorato questa interpretazione[226].

Le utilità sequestrate rappresentavano i proventi di gestione delle transazioni concluse su *Silk Road* nel periodo compreso tra febbraio 2011 e luglio 2013 che si stima siano ammontate ad oltre 9.500.000 di *bitcoin*, su un totale di 11.000.000 di unità presenti in rete al momento del sequestro[227]. Le monete erano utilizzate come circolante, cambiate in denaro contante e ricevute nuovamente in pagamento dei prodotti commercializzati, ma il dato risulta particolarmente interessante se si considera che, secondo alcune stime, al tempo solo il 22% dei *bitcoin*

Digital-Currencies 2012 Quando il 3 di ottobre 2013 *l'FBI* ha oscurato S*ilk Road* il prezzo del *bitcoin* è crollato da $140 a $110 per poi rimbalzare in giornata a $124. http://www.theguardian.com/technology/2013/oct/03/*bitcoin*-price-silk-road-ulbricht-value

[225]http://www.businessinsider.com/senate-*bitcoin*-hearing-2013-11 2013.

[226]Si noti che a causa delle oscillazioni di cambio il valore di questa somma si è fortemente apprezzato: al momento del sequestro i controvalore in dollari era nell'ordine dei 3 milioni mentre all'inizio di dicembre 2013 era decuplicato. http://nypost.com/2013/12/23/government-robbed-me-of-33m-in-*bitcoin*s-silk-road-pirate/ *et* http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-*bitcoin*s-from-ross-ulbricht-alleged-owner-of-silk-road/

[227]http://www.theguardian.com/world/interactive/2013/oct/02/silk-road-ross-william-ulbricht-criminal-complaint 2013. http://www.forexinfo.it/*Bitcoin*-valore-risale-sopra-1-000 2014.

sarebbe stato in circolazione. L'affermazione appare credibile, considerato che il basso valore iniziale delle monete aveva fatto si che i primi *miner* sottovalutassero l'opportunità di questa nuova forma di investimento: alcuni, come Hal Finney, avevano così interrotto il mining infastiditi dal funzionamento continuo delle ventole, altri avevano smaltito i vecchi PC senza salvare i bitcoin prodotti, altri ancora avevano perso i *cold wallet* su cui li avevano trasferiti.

Questo fatto introduce un elemento ulteriore nel mosaico delle indagini, fornendo di credibilità le affermazioni della difesa di Ulbricht che ha sostenuto la presenza di un *exchange*, nella fattispecie *MtGox*, dietro alle attività di *Silk Road.* La vicenda non ha avuto esito processuale, per cui non è possibile dare pieno credito a quanto affermato da Ulbricht, anche se la continua movimentazione di *bitcoin* su *Silk Road* ha richiesto con ogni probabilità l'intervento di un mediatore professionale. Subito dopo il sequestro Ulbricht aveva sporto un'altra denuncia, lamentando di aver subito il furto di $ 800.000 in bitcoin da parte di alcuni agenti *FBI;* inizialmente la segnalazione non aveva ricevuto grande credito ma successivamente il furto è stato accertato con sentenza definitiva[228].

Nel 2015 Ulbricht è stato riconosciuto colpevole di associazione per delinquere finalizzata al traffico di droga, cospirazione a fini di riciclaggio e *computer hacking,* il tutto aggravato dall'entità dei danni provocati, e condannato all'ergastolo. Stando a quanto affermato dalla difesa nel processo, l'anima dietro a *Silk Road* sarebbe però Mark Karpelès, *CEO* di *MtGox*[229]. Le affermazioni dell'avvocato di Ulbricht appaiono poco credibili nella parte in cui sostiene che il suo cliente dopo aver creato *Silk Road* lo aveva ceduto a terzi, rimanendo

[228] US federal agent investigating Silk Road admits $800,000 bitcoin theft https://www.theguardian.com/technology/2015/sep/01/us-federal-agent-investigating-silk-road-admits-800000-bitcoin-theft
[229]US investigated MtGox CEO as possible Silk Road mastermind, 2015, https://www.theguardian.com/technology/2015/jan/16/mtgox-ceo-silk-road-mark-karpeles-ross-ulbricht

invischiato in questa storia come capro espiatorio; dal canto suo Karpelès ha negato ogni addebito in una mail inviata alla Reuters e alle altre agenzie di stampa[230]. Peraltro, i numeri indicano che in un anno sono passati per *Silk Road* un numero di *bitcoin* pari a quattro volte il circolante di mercato del tempo: questo fatto rende altamente probabile che Ulbricht si appoggiasse a un sistema professionale di cambio.

Per quanto riguarda la posizione di Karpelès nella vicenda non sono intervenuti accertamenti giudiziari: uno degli agenti *FBI* incaricati delle indagini ha testimoniato che Karpelès era stato indagato e che il mandato di acquisizione della sua casella *Google-mail* era stato motivato proprio in base al suo presunto ruolo in *Silk Road*. In seguito, prosegue la testimonianza, la posizione di Karpelès sarebbe stata separata dall'indagine principale a seguito dell'incontro con un Procuratore Federale incaricato delle indagini su un traffico di denaro illecito[231].

Ad oggi, l'unico fatto accertato riguardo *MtGox* è che nel 2014 ha subito la perdita di 750.000 *bitcoin,* pari a circa un terzo del circolante dell'epoca, provocando la bancarotta della piattaforma e il crollo delle quotazioni della moneta virtuale.

In occasione del sequestro di *Silk Road,* il valore dei *bitcoin* era invece rimasto sostanzialmente stabile: si era infatti registrata una forte volatilità *intraday* ma subito dopo il cambio si era posizionato su un *trend* di crescita che era rimasto costante nel resto del mese con indifferenza alle sorti del sito di *blackmarket.* Storicamente, la volatilità dello strumento ha mostrato di risentire in maniera relativa delle vicissitudini della rete manifestando, piuttosto, maggiore sensibilità alle decisioni speculative e istituzionali.

---

[230] *Ibidem: "This is probably going to be disappointing for you, but I am not and have never been Dread Pirate Roberts," [...] "The investigation reached that conclusion already – this is why I am not the one sitting during the Silk Road trial, and I can only feel defense attorney Joshua Dratel trying everything he can to point the attention away from his client."*

[231] *ibidem*

Figura 14: grafico valore bitcoin ottobre 2013[232]

10.3. Udienza al Senato USA

Lo scalpore mediatico suscitato dal sequestro di *Silk Road* ha focalizzato l'attenzione sulle valute virtuali, conducendo all'udienza del Senato degli Stati Uniti del 18 novembre 2013[233] nel corso della quale hanno riferito in qualità di esperti Jennifer Shasky Calvery, capo dell'Agenzia *FinCEN*[234], Mythili Raman, *Assistant Attorney General* dello *U.S. Department of Justice*, *Criminal Division* e l'agente speciale Edward Lowery dello *U.S. Secret Service, Criminal Investigative Division, U.S Department of Homeland Security.*

Jennifer Calvery ha dichiarato che il *FinCEN* considera le monete virtuali nella loro qualità di servizi finanziari e coloro che le

[232] https://bitcoincharts.com/charts/bitstampUSD#rg60zczsg2013-10-01zeg2013-10-31ztgSzm1g10zm2g25zv
[233] *Bitcoin* Senate Hearing 2013
http://www.hsdl.org/?view&did=747209 e
http://www.businessinsider.com/senate-*bitcoin*-hearing-2013-11
[234] Financial Crimes Enforcement network – US Department of Treasury.

amministrano e le scambiano alla stregua delle istituzioni finanziarie: è perciò fondamentale che vengano posti in essere i controlli adeguati e che vengano predisposti i consueti *report anti money laundering*[235]. Secondo quanto dichiarato dalla Calvery, nel periodo ottobre 2012-ottobre 2013 il controvalore delle transazioni effettuate in *bitcoin* è stato di 8 miliardi di dollari statunitensi: una piccola realtà se paragonato agli oltre $ 800.000 miliardi dei movimenti legalmente effettuati da banche e intermediari di pagamento. Peraltro, il volume delle transazioni in *bitcoin* assume una dimensione di maggior rilievo se rapportato al movimento di *money laundering globale* che lo *United Nations Office on Drugs and Crime (UNODC)* stima sia stato di 1.600 miliardi di dollari nel solo 2009.

A propria volta, il Vice Procuratore Generale Mythili Raman ha informato il Senato che per rafforzare il contrasto ai traffici di riciclaggio è stata organizzata una collaborazione permanente con il *Virtual Currencies Emerging Threats Working Group*, un raggruppamento di contrasto agli usi illeciti delle valute virtuali fondato dall'*FBI* nel 2012 cui partecipano varie agenzie nazionali ed estere. In considerazione della grande attrattiva che l'efficienza dei *bitcoin* esercita sul mondo criminale, il Procuratore Raman ha invocato una costante attenzione al fenomeno sotto i profili legislativo, esecutivo e giudiziario per combattere gli usi illeciti delle valute digitali, confermando che l'adesione agli obblighi informativi *anti money laundering* costituisce la via legittima per l'uso delle valute virtuali.[236].

L'agente del *Secret Service* Edward Lowery ha, infine, posto l'accento sul carattere transnazionale delle valute digitali, sottolineando la necessità di un'attitudine cooperativa fra le istituzioni di paesi diversi in uno sforzo costante di armonizzazione della normativa antiriciclaggio,

[235] *Vide* http://www.hsdl.org/?view&did=747209 2013.
[236] *Ibidem*

senza dimenticare il potenziale delle valute digitali nello sviluppo di un commercio globale efficiente e trasparente.

Al momento in cui era stata programmata l'udienza al Senato *USA* si temeva che l'evento avrebbe fatto registrare riflessi pesantemente negativi sul cambio dei *bitcoin*; si è avuto invece l'effetto contrario: la valutazione positiva emersa dalle relazioni dei rappresentanti delle istituzioni ha portato a un incremento del 50% *nell'intraday* contro il dollaro, a conferma della nostra teoria secondo cui la volatilità dello strumento risente in maniera molto decisa dei provvedimenti istituzionali[237].

Le considerazioni svolte dai rappresentanti istituzionali indicano una possibile strada per l'integrazione nel sistema delle valute virtuali. Il problema sollevato con maggior frequenza dalle istituzioni consiste nella difficoltà di tracciare i pagamenti di valore ingente effettuati in *bitcoin*: la possibilità di creare un indirizzo nuovo per ogni transazione può rendere infatti questa attività molto complicata.

Per esemplificare i termini della questione si porta spesso il caso della transazione anonima di maggior valore effettuata fino ad oggi che è quella che il 22 novembre 2013 ha trasferito 194.993 *bitcoin* che al tempo valevano 155 milioni di dollari[238] e al valore raggiunto nel giugno 2017 oltre 560 milioni di dollari; la necessità di tracciare questi spostamenti *inest in re ipsa* e non occorre spendere parole per sostenere la fondatezza della richiesta.

Uno dei modi per risolvere, almeno in parte, il problema consiste nell'introduzione di un registro volontario di indirizzi agganciati a dati anagrafici, le cui transazioni sarebbero tracciabili e dunque accettabili

---

[237] *Regulators See Value in Bitcoin, and Investors Hasten to Agree* http://dealbook.nytimes.com/2013/11/18/regulators-see-value-in-*bitcoin*-and-investors-hasten-to-agree/?_r=0 2013.

[238] https://*blockchain*.info/tx/1c12443203a48f42cdf7b1acee5b4b1c1fedc144cb909a3bf5edbffafb0cd204?utm_source=buffer&utm_campaign=Buffer&utm_content=bufferf24ed&utm_medium=twitter

dall'ordinamento in via presuntiva, esattamente come accade nei trasferimenti del sistema bancario[239].

A nostro parere il metodo descritto appare preferibile a quello delle *key disclosure laws* proposto da alcuni ordinamenti di *Common Law* come Regno Unito, Australia e Sud Africa[240]. In base a queste disposizioni il rifiuto di rivelare le chiavi crittografiche alle autorità competenti viene sanzionato con la carcerazione preventiva, in deroga espressa al diritto di tacere, astenendosi da quelle dichiarazioni che potrebbero condurre alla propria incriminazione.

Il recente cambio di indirizzo politico degli *USA* ha reso attuale la questione anche in quell'ordinamento: se da un lato lo strumento contrasta apertamente con quanto stabilito dal quinto emendamento, dall'altro le cronache recenti riportano casi di imputati incarcerati per aver rifiutato di fornire *pin* e *password* dei loro *device*[241]. Per quanto riguarda l'ordinamento italiano l'argomento delle chiavi crittografiche deve essere inquadrato nel più ampio diritto di non auto-incriminarsi, pacificamente ritenuto applicazione della presunzione di non colpevolezza tutelata sia dalla Carta Costituzionale che dalla Convenzione Europea dei Diritti dell'Uomo.[242]

---

[239]Il sistema è proposto, fra gli altri, da *CoinValidation http://coinvalidation.com/*
Alla fine del 2013 anche JP Morgan aveva presentato richiesta di brevetto per un sistema di pagamento tracciabile basato sul sistema *bitcoin; l*o *US Patent Office* avrebbe, peraltro, rigettato la domanda per la carenza degli elementi di novità e non ovvietà previsti dal titolo 35 dello USC sez. 101 e 102
http://www.cryptonews.biz/jpmorgans-*bitcoin*-alternative-patent-rejected/
[240]http://www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-*bitcoin*-assets/ 2012.
[241] Wang Wei**,** Man Jailed 6 Months for Refusing to Give Police his iPhone Passcode, 2017, http://thehackernews.com/2017/06/unlock-iphone-passcode.html?m=1
[242] Giovanni Catalisano, Il libro verde sulla presunzione di non colpevolezza, Altalex, 2010, http://www.altalex.com/documents/news/2011/01/05/il-libro-verde-sulla-presunzione-di-non-colpevolezza

10.4. Mercato cinese

Per tutto il mese di novembre 2013 la quotazione dei *bitcoin* era rimasta in crescita costante, portando il cambio a oltre $ 1.200; di contrasto, il successivo mese di dicembre era stato caratterizzato da un crollo verticale che aveva dimezzato il prezzo della moneta virtuale, con una leggera ripresa verso la fine dell'anno. Nel bimestre indicato, un fattore di grande influenza era stato rappresentato da alcune vicende occorse sul mercato cinese: il picco di quotazione raggiunto nel mese di novembre si era verificato contemporaneamente alla decisione del portale *Baidu*, conosciuto anche come il Google cinese, e dei siti ad esso collegati di accettare pagamenti in *bitcoin*.

Alla fine di novembre 2013 la *People's Bank of China* aveva, infatti, diffuso un comunicato stampa in cui il vice governatore Yi Gang dichiarava che, pur non essendo la Cina intenzionata a riconoscere i *bitcoin* come moneta nel breve termine, i cittadini potevano sentirsi liberi di utilizzarli.[243] L'annuncio aveva segnato un deciso cambio di rotta rispetto alla politica precedente, in esecuzione della quale le valute virtuali erano state messe fuori legge fin dal 2009 allo scopo di contrastare il fenomeno *QQ*, la moneta virtuale del sito *Tencent,* che era arrivata a rappresentare il 13% del circolante.

In contrasto con queste dichiarazioni, all'inizio di dicembre 2013 la *PBoC* aveva però emesso un provvedimento di veto per le banche locali ad accettare *bitcoin* come moneta nonché per gli operatori del settore finanziario a realizzare attività ad essi collegate[244]. Per le compagnie che al momento del divieto avessero già in corso scambi in moneta digitale era stato sancito l'obbligo di procedere alla chiusura delle stesse e di

[243]http://www.forbes.com/sites/gordonchang/2013/11/24/a-china-triangle-*bitcoin*-baidu-and-beijing/ 2013.
[244]http://www.ilsole24ore.com/art/notizie/2013-12-05/la-cina-vieta-uso-moneta-elettronica-*bitcoin*-banche-e-finanza-120153.shtml 2013.

redigere i relativi bilanci entro la fine di gennaio 2014: i maggiori siti cinesi, compresi *Baidu* e *China Telecom,* avevano immediatamente sospeso le transazioni[245].

Se il comunicato di autorizzazione informale aveva contribuito in maniera decisa all'eccezionale rialzo del valore di cambio dei *bitcoin,* con l'emanazione del provvedimento di veto si era assistito a un crollo delle quotazioni che erano rimaste negative per tutto il 2014 anche in conseguenza degli eventi che analizzeremo nel prossimo paragrafo.

La decisione della Banca Centrale aveva comunque lasciato liberi gli scambi tra privati, consentendo così la prosecuzione delle transazioni in *bitcoin.* La scelta economica di produrre energia elettrica con centrali a carbone, aveva anzi contenuto il prezzo del *mining*, facendo si che nel tempo le *pool farm* si concentrassero proprio sul territorio cinese arrivando rappresentare oltre l'80% dell' *hash-power* totale[246].

I problemi di cambio in valuta erano stati apparentemente risolti dalla vendita diretta sul mercato dei *bitcoin* prodotti, alimentando più di una preoccupazione in ordine a una decisa riallocazione di capitali. Il 9 gennaio 2017 la *PBoC* ha così emesso un nuovo comunicato in cui ha chiarito che i *bitcoin* non possono circolare come moneta sul territorio cinese[247]. Il motivo di questa posizione sembra risiedere nel fatto che le transazioni in *bitcoin* sarebbero effettuate al 98% in *Yuan* per volumi complessivi annui di miliardi di dollari, superando ogni limite di tracciabilità ai fini del contrasto al riciclaggio.

---

[245]http://www.bloomberg.com/news/2013-12-07/baidu-stops-accepting-*bitcoin*s-after-china-ban.html 2013.

[246] Naveen Joshi, 3 things to know about Bitcoin Blockchain, 2017, https://www.linkedin.com/pulse/3-things-know-bitcoin-blockchain-naveen-joshi?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BSOk75Q3zYBSq8FXP8dtdSg%3D%3D

[247] Giuseppe Timpone, Bitcoin, crollo del 20% sul "warning" cinese, 2017, https://www.investireoggi.it/economia/bitcoin-crollo-del-20-sul-warning-cinese-perche-pechino-preoccupata/?refresh_ce

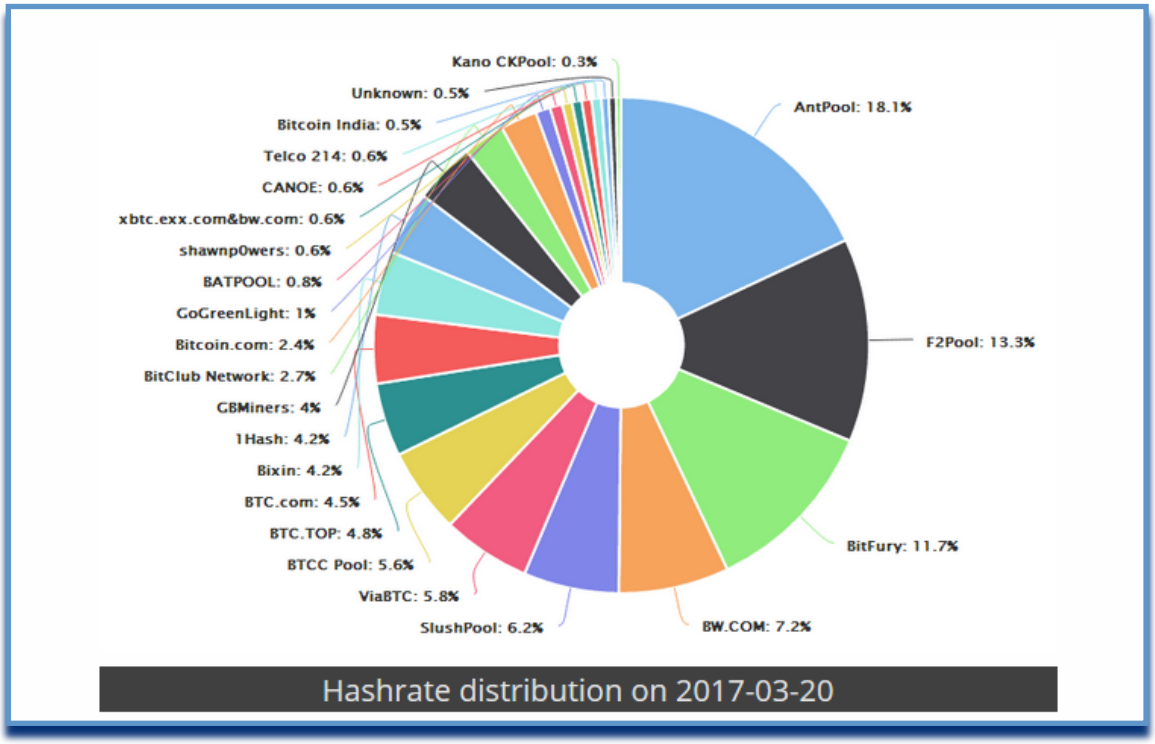


Figura 15: bitcoin hashrate distribution[248]

L'effetto immediato del comunicato della PBoC è stato quello di un ribasso del 20% nelle quotazioni *intraday* ma la fiducia degli investitori è rimasta inalterata e i *bitcoin* hanno ripreso la loro corsa verso l'alto.

10.5. Mercato russo

Nella prima settimana di febbraio 2014 la Russia aveva decretato la messa bando dei *bitcoin*, considerati fonte di rischio per i cittadini di essere coinvolti in attività illecite di vario genere, inclusi il riciclaggio e il finanziamento al terrorismo internazionale[249]. L'atto era stato emanato

[248] Jordan Tuwiner, Bitcoin Mining in China, 2017, https://bitcoinworldwide.com/mining/china/ , la maggioranza delle mining pool, fra cui Antpool, DiscusFish / F2Pool, BTCC , BW Pool, ha sede in Cina.
[249]http://www.reuters.com/article/2014/02/09/us-russia-*bitcoin*-idUSBREA1806620140209 2014.

il giorno dopo il *default* di *MtGox,* che analizzeremo nel prossimo paragrafo, e la risposta del mercato ai due gravi stimoli era consistita in una fuga decisa che aveva determinato un crollo di circa il 40% nel valore di cambio, ad ulteriore conferma della teoria esposta riguardo la forte influenza delle decisioni istituzionali e finanziarie sul valore di questa *commodity*.

Nei due anni successivi il contrasto russo alle monete virtuali aveva seguito un percorso costante: nel marzo 2016 era stata addirittura emanata una proposta di legge contro il cambio dei cc. dd. surrogati monetari, in cui il ministero delle finanze Russo proponeva l'applicazione di sanzioni comprese fra 3 e 5 milioni di rubli e la sospensione amministrativa di 90 giorni per le attività professionali che fossero state coinvolte in questo commercio. Il documento, comunicava inoltre che sarebbero stati presto formulati alcuni emendamenti al codice penale per la criminalizzazione della produzione e dell'uso dei surrogati monetari.

A un anno di distanza, il Governo russo sembra aver cambiato punto di vista e all'inizio del maggio 2017 è stato formalizzato un piano che dovrebbe portare alla legalizzazione delle monete virtuali nel 2018. Il motivo di questa decisione sembra risiedere nella trasparenza degli scambi di *blockchain* che consentirebbe di riorganizzare in maniera efficiente il sistema dei piccoli istituti di credito, attualmente parcellizzato nei territori di periferia. Il ministro delle finanze Alexey Moiseev ha dichiarato in un'intervista che la legalizzazione delle monete virtuali verrà effettuata allo scopo di contrastare il riciclaggio: la struttura dei trasferimenti di *blockchain* consentirà infatti di conoscere con certezza i soggetti che prenderanno parte alle transazioni, con azzeramento dei margini di manovra per le operazioni opache[250]. Le parole del ministro portano a ritenere che verrà messo allo studio un

[250] Arjun Carpal, Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency, 2017 http://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html

sistema di indirizzi dichiarati: anche se è ancora troppo presto per fare illazioni, è notizia dei primi di giugno che Vladimir Putin ha incontrato personalmente Vitalik Buterin, creatore di *Ethereum*[251], per discutere le opportunità offerte dal progetto.

10.6. *MtGox*

MtGox è stato uno dei maggiori *bitcoin exchange* e la sua storia si è intrecciata a doppio filo con quella delle monete virtuali. La piattaforma è stata progettata nel 2006 da Jed Mc Caleb come sito di scambio delle carte di un gioco on line, derivando il proprio nome dall'acronimo del nome del gioco, 'Magic: The Gathering Online', e della parola eXchange. Nel 2010 era stato trasformato in un *exchange* di *digital currency*; nel 2011 quando Mc Caleb era entrato a far parte della squadra di *Ripple* lo aveva venduto a Mark Karpelès, un programmatore francese che viveva in Giappone, mantenendo una quota del 12%[252]. Circa tre mesi dopo l'acquisto, Karpelès aveva subito l'attacco descritto nel *report* di *warning BCE*[253], e una volta ripreso il controllo del sito aveva disposto la più ingente transazione registrata finora, prelevando 424.242 *bitcoin* dai *cold wallet* e girandoli a un indirizzo *MtGox*, per dimostrare agli

[251] Michael del Castillo, Vladimir Putin and Vitalik Buterin Discuss Ethereum 'Opportunities', 2017 http://www.coindesk.com/vladimir-putin-vitalik-buterin-discuss-ethereum-opportunities-recent-forum/

[252] Cyrus Farivar , Original Mt. Gox founder: "I lost around $50,000" in site's collapse 2014, https://arstechnica.com/tech-policy/2014/05/original-mt-gox-founder-i-lost-around-50000-in-sites-collapse/

[253] Per comodità di lettura riportiamo in nota la descrizione degli eventi contenuta nelle pagine precedenti: Il furto che aveva causato il crollo delle quotazioni [da $ 17.40 a $ 0,01]era stato perpetrato ai danni della piattaforma di gestione *MtGox*. In quell'occasione si era parlato della sottrazione di 400.000 *bitcoin* ma leggendo le discussioni sui *forum* dedicati emerge che in realtà si sarebbe trattato di un attacco al sito con duplicazione dei *token* depositati che sarebbero poi stati rivenduti sul mercato a prezzo stracciato, con una serie di manovre speculative conseguenti; stando a questa ricostruzione, *MtGox* avrebbe risolto la situazione riportando il sistema a una versione precedente e offrendo ai clienti danneggiati dall'attacco il rimborso delle perdite subite: il numero di *bitcoin* effettivamente sottratti si attesterebbe nell'ordine delle 2.500 unità.

investitori che avevano a che fare con una solida realtà finanziaria[254]. L'operazione era stata molto rischiosa, perché l'alta visibilità dell'importo trasferito avrebbe potuto veicolare una serie di pesanti *hacking attack* ed aveva comunque dimostrato che Karpelès era in grado di muovere autonomamente i fondi ricevuti in gestione.

Nel 2011 *MtGox* aveva gestito i fondi di *Bitcoinica*, la piattaforma svaligiata da tre attacchi *hacker*. Dal 2012 al 2014 Karpelès era stato nel *board* della *Bitcoin Foundation,* dove sedeva anche Peter Vessenes CEO di *CoinLab;* i due imprenditori avevano così stipulato un contratto con cui *CoinLab* si impegnava all'acquisizione e alla gestione di nuovi clienti sul mercato nord americano per conto di MtGox in cambio di una commissione del 90%. La ragione dell'accordo stava nella necessità di una serie di licenze necessarie all'attività che *MtGox* non possedeva e la cui gestione sarebbe spettata a *CoinLab*[255].

Nel 2013 *CoinLab* aveva fatto causa a *MtGox* e a *Tibanne KK*, un'atra società di Karpelès, chiedendo un risarcimento complessivo di 175 milioni di dollari per responsabilità contrattuale[256]; *MtGox* si era costituita eccependo la nullità dell'accordo, poiché *CoinLab* non aveva mai posseduto le licenze statali e federali per i servizi finanziari ivi dedotti e aveva formulato domanda per la costituzione di un *trust* giudiziario sulla somma di $ 5.315.210,79 che *CoinLab* aveva "*wrongfully converted*" dai depositi dei clienti *MtGox*[257].

---

[254] Alyson, Famous Bitcoin Transactions & The Stories Behind Them, 2016, https://blog.blockchain.com/2016/07/13/famous-bitcoin-transactions-the-stories-behind-them/

[255] Josef Young, Bitcoin Foundation: We're Trying to Recover from the Mess Peter Vessenes Made, 2015, http://www.newsbtc.com/2015/12/26/bitcoin-foundation-were-trying-to-recover-from-the-mess-peter-vessenes-made/

[256], Coinlab v. Mt. Gox Case 2:13-cv-00777, United States District Court for the Western District of Washinghton https://web.archive.org/web/20130518075639/http://www.scribd.com:80/doc/139160091/Coinlab-v-Mt-Gox

[257] Mt. Gox answer and counterclaim against CoinLab, United States District Court for the Western District of Washinghton at Seattle, 2013, https://www.scribd.com/doc/168517688/Mt-Gox-counterclaim-against-CoinLab

Nel 2013 lo *US Homeland Department* aveva sequestrato 5 milioni di dollari di fondi *MtGox* con l'accusa di esercizio abusivo dell'attività di *money transfer*[258]; la piattaforma aveva ottenuto la licenza *FinCEN* qualche mese dopo[259] ma il denaro non era stato svincolato. Nello stesso periodo l'*FBI* aveva indagato Karpelès per riciclaggio dei proventi di *Silk Road;* l'indagine, emersa dalle testimonianze degli agenti nel processo a carico di Ross Ulbricht, era stata archiviata, forse a seguito di un accordo con la Procura Federale[260]. Nel 2014 Charles Shrem, vice presidente della *Bitcoin Foundation,* si era invece dichiarato colpevole del favoreggiamento di *Silk Road*[261].

Il 6 febbraio 2014 *MtGox* aveva annunciato la sospensione dei prelievi dal sito, per una verifica di carattere tecnico; per comprendere appieno la portata dell'annuncio occorre considerare che, in quel momento, la piattaforma gestiva circa il 70% delle transazioni in *bitcoin*[262]. Alla fine di febbraio 2014 *MtGox* aveva invece avviato la procedura fallimentare, provocando un ulteriore ribasso nel valore di cambio dei *bitcoin* e rendendo sempre più attuale la questione dei controlli sulle piattaforme per la protezione degli investitori. Karpelès aveva denunciato la perdita di oltre 750.000 *bitcoin* a causa di un attacco *DDoS*[263] che, a suo dire, aveva sfruttato la c.d. 'malleabilità delle transazioni', un *bug* che in pendenza della convalida di una transazione in *bitcoin* consente di generare un secondo trasferimento di

---

[258] Raiman Dillet, Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It Of Violating Money Transfer Regulations, 2013, https://techcrunch.com/2013/05/16/mt-gox-dwolla-account-money-seizure/
[259] Vitalik Buterin, MtGox Gets FinCEN MSB License, 2013, https://bitcoinmagazine.com/articles/mtgox-gets-fincen-msb-license-1372534713/
[260] US investigated MtGox CEO as possible Silk Road mastermind, 2015, https://www.theguardian.com/technology/2015/jan/16/mtgox-ceo-silk-road-mark-karpeles-ross-ulbricht
[261] Alex Lawsom, Silk Road case: Bitcoin promoter Charlie Shrem pleads guilty, 2014, http://www.independent.co.uk/news/business/news/silk-road-case-bitcoin-promoter-charlie-shrem-pleads-guilty-9713563.html
[262] Anders Nilsson, The troublesome history of the bitcoin exchange MtGox, 2014, https://anders.io/the-troublesome-history-of-the-bitcoin-exchange-mtgox/
[263] French Press Agency, MtGox faced huge DDoS attack, 2014, https://www.dailysabah.com/economy/2014/03/09/mtgox-faced-huge-ddos-attack

quell'importo inserendolo nella *blockchain* prima di quello originario. In questo modo *l'attacker* avrebbe ottenuto conferma delle transazioni inserite in *double spending*, stornando indebitamente fondi[264]. Fin da subito erano sorti dei dubbi legittimi in merito alla ricostruzione prospettata da Karpelès, nonché alla docilità con cui *Mt.Gox* aveva effettuato gli invii di *bitcoin*, prelevando addirittura dai *cold storage*[265]. Le perplessità erano state rafforzate dalla pubblicazione in rete di un bilancio che evidenziava come *Mt.Gox* sarebbe stato ancora in possesso di 500.000 dei *bitcoin* di cui aveva denunciato la sottrazione[266].

Allo scopo di consentire una corretta classificazione delle operazioni in perdita sui *bitcoin,* alla fine di marzo 2014 lo *US Internal Revenue Service* aveva emesso una apposita circolare [267]. Per la corretta applicazione della normativa, ai possessori di *bitcoin* era richiesto di evadere una serie di obblighi dichiarativi[268], antesignani di quelli che nello Stato di New York sarebbero stati successivamente posti a base delle richieste di *Bitlicence*[269]. Karpelès, dal canto suo, aveva adottato una strategia difensiva a due facce, presentando domande distinte negli *USA* e in Giappone[270]. Sul fronte nipponico era stata così presentata domanda di ammissione alla procedura fallimentare con richiesta di

---

[264]Danny Bradbury, What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability, 2014,
http://www.coindesk.com/*bitcoin*-bug-guide-transaction-malleability/
[265]http://www.ibtimes.co.uk/what-transaction-malleability-did-it-kill-mtgox-1438411 2014.
[266]http://techcrunch.com/2014/03/09/mt-gox-hack-allegedly-reveals-*bitcoin*-balances-customer-account-totals/ 2014.
[267] Ai fini fiscali, i *bitcoin* venivano equiparati alla proprietà privata: per le operazioni svolte dai cittadini americani e dagli altri soggetti tenuti a rispettare le regole del fisco USA, le imposte sul reddito sarebbero state applicate facendo riferimento al valore di cambio del momento dell'operazione http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance 2014. Per la corretta applicazione della normativa, ai possessori di bitcoin era richiesto di evadere una serie di obblighi dichiarativi : la mancata o infedele dichiarazione avrebbe generato un caso di competenza federale, come ogni assunto in materia fiscale. http://www.irs.gov/pub/irs-drop/n-14-21.pdf 2014.
[268]http://www.irs.gov/pub/irs-drop/n-14-21.pdf 2014.
[269]Jeremy Quittner, lawsky and new virtual currency regulations for New York, 2014 http://www.inc.com/jeremy-quittner/lawsky-and-new-virtual-currency-regulations-for-new-york.html
[270]http://www.reuters.com/article/2014/03/07/us-*bitcoin*-mtgox-japan-idUSBREA2601Z20140307.

protezione pubblica dalle azioni personali dei creditori; negli *USA* la società aveva invece presentato domanda ai sensi del *chapter 15* del *Bankruptcy Act* che prevede l'inibizione delle azioni personali nel caso di fallimenti transfrontalieri, al fine contrastare la *class action* presentata in Illinois. Il successivo fallimento di *MtGox* ha prodotto la cessazione della materia del contendere in questo giudizio.

Nel 2015 Karpelès era stato arrestato in Giappone per falso in bilancio e appropriazione indebita; nel 2016 è stato rilasciato su cauzione in pendenza del processo, ma il giudice ha disposto il divieto di espatrio[271]. Le conseguenze del *default* sono state affrontate in maniera sistematica dal governo giapponese: nell'aprile 2017 è stato approvato il *Virtual Currency Act* in cui i *bitcoin* sono stati classificati come strumenti di pagamento, precisando che a fini fiscali devono essere trattati come *asset* e non come monete; è stata inoltre disposta esenzione IVA stabilendo che le variazioni del valore di cambio vadano soggette alla imposizione prevista per *capital gain* e reddito di impresa[272]. Allo scopo di contrastare il ripetersi di fenomeni analoghi a quello di *MtGox,* dal maggio 2016 la nuova regolamentazione prevede l'emissione di una licenza formale per i *virtual currency exchange*, in difetto della quale gli operatori non potranno esercitare. Ai fini di una regolamentazione efficiente il governo giapponese ha inoltre stretto accordi di cooperazione *fintech* con Singapore e Regno Unito[273].

Ad oggi la causa *CoinLab,* ancora pendente, ritarda il risarcimento dei creditori ammessi al passivo di *MtGox*[274] provocando ulteriori danni.

---

[271] Flora Drury, Former head of collapsed bitcoin exchange is arrested over disappearance of hundreds of millions of dollars of virtual currency, 2015, http://www.dailymail.co.uk/news/article-3182018/Former-CEO-collapsed-Mt-Gox-bitcoin-exchange-arrested-Japan-reports.html

[272] Japan exempts bitcoin from Consumption Tax http://www.vatlive.com/vat-news/japan-exempts-bitcoin-from-consumption-tax/

[273] The Japanese Times, Diet OKs bill to regulate virtual currency exchanges, 2017, http://www.japantimes.co.jp/news/2016/05/25/business/diet-oks-bill-regulate-virtual-currency-exchanges/

[274] Jon Southurst CoinLab Lawsuit Delaying Mt Gox Payouts: Trustee, 2016, https://news.bitcoin.com/coinlab-lawsuit-delaying-gox-payouts/

Il curatore fallimentare ha ottenuto uno sblocco parziale dei fondi sequestrati nel 2013 dallo *US Homeland Department*[275] e, in questo momento, liquidando i *bitcoin* in portafoglio si beneficerebbe della quotazione favorevole, con distribuzione di importi percentualmente più vicini al valore di insinuazione. A questo proposito, nel maggio 2017 Karpelès ha pubblicato su *Reddit* una lettera aperta a Peter Vessenes, in cui lo invita a trovare un accordo con il curatore fallimentare[276].

10.7. Questioni pratiche

Il sistema proposto da Satoshi Nakamoto prevedeva la creazione di unità di moneta virtuale del valore di $0,002: *rebus sic stantibus*, i *bitcoin* non esercitavano una particolare attrattiva al di fuori della nicchia dove erano stati concepiti e in cui venivano utilizzati, né gli attori interni al sistema avevano un incentivo al rovesciamento di questo sistema. Il forte incremento di valore cui è andato incontro lo strumento ha portato a un netto superamento dei costi di *mining*, offrendo di fatto un deciso incentivo ad una serie di attività illecite; l'effetto più importante della crescita esponenziale del valore di cambio è stato quello di un rischio generale di instabilità del sistema.

10.7.1. Attacchi interni

[275]Maria Nikolova, MTGOX's bankruptcy trustee updates on US seized funds release, 2017, https://financefeeds.com/mtgoxs-bankruptcy-trustee-updates-us-seized-funds-release/
[276]Mark Krpelès, Open letter to Peter Vessenes, 2017, https://www.reddit.com/r/mtgoxinsolvency/comments/6aj6eb/open_letter_to_peter_vessenes/

Il *Whitepaper Bitcoin* mette bene in chiaro che l'equilibrio della rete costituisce un valore fondamentale di questa architettura: se gruppi di nodi collusi prendessero il sopravvento con un *51% attack,* si potrebbero effettuare i calcoli necessari alla reversibilità delle transazioni con tutte le conseguenze di *double spending.* La sopravvivenza del sistema dipende dall'onestà dei nodi che rappresentano la maggioranza nella potenza di calcolo: poiché in *Bitcoin* manca un ente centrale di emissione e controllo, ogni alterazione del sistema passa, giocoforza, da condotte dei nodi della rete. In questo senso, il valore inizialmente ridotto del *bitcoin* costituiva di per sé una forma di garanzia: nello schema originale i costi dell'attività di *mining* venivano compensati 'alla pari' dai *bitcoin* guadagnati e i *miner* avevano un incentivo molto ridotto al rovesciamento del sistema. E' sempre stato chiaro che ogni intervento esterno di alterazione del valore di cambio avrebbe prodotto una forma di instabilità sostanziale, e in questo senso Satoshi Nakamoto si era opposto alla *partnership* con *wikileaks,* ritenendo *Bitcoin* un progetto ancora troppo acerbo per reggere una pressione di mercato che ne sarebbe derivata[277]. Quando il valore dei *bitcoin* ha superato i costi di *mining* e ha cominciato a confrontarsi con quello delle cc. dd. valute forti, la *commodity* è uscita dalla nicchia di rete in cui il suo creatore l'aveva collocata per entrare nel mondo degli investimenti di massa e il suo valore si è apprezzato in maniera tanto significativa da offrire una serie di nuovi incentivi agli attori in scena. In primo luogo, si è creato un grande incentivo alla produzione, finalizzata alla vendita sul mercato secondario, che ha creato nuove forme di ricchezza non solo fra i *miner* ma anche fra i produttori e i venditori di *hardware* dedicato. Vi sono poi stati una serie di incentivi all'attacco del sistema. Non si conosce ancora di attacchi interni, se pur essi vengano prospettati da più parti[278]; la

[277] http://www.wired.com/magazine/2011/11/mf_*bitcoin*/ 2011.

[278]Ittay Eyal e Emin Guen Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable, 2013, http://arxiv.org/pdf/1311.0243v1.pdf.* L'articolo dei due ricercatori del *Department of Computer Science* della *Cornell University* ha aperto il dibattito sul c.d. *bitcoin colluding problem.*

hard fork di *Ethereum,* la cui struttura ricordiamo nasce da una duplicazione di *Bitcoin,* ha rappresentato un fatto lecito, con adesione della maggioranza dei nodi a un progetto condiviso dalla community. Ad oggi, l'attività di interferenza illecita maggiormente simile a un 51% *attack* è stata quella che avrebbe sfruttato la c.d. malleabilità delle transazioni per sottrarre i depositi di *Mt.Gox*: si tratta però di un attacco che non prevede la collaborazione dei nodi impegnati nell'attività di verifica, i quali vengono anzi ingannati dal diverso *hash* assegnato alla transazione, e che può essere classificato fra gli attacchi esterni consistenti in truffe, falsificazioni e azioni appropriative di vario genere.

10.7.2. Attacchi esterni

Fra gli attacchi esterni, uno degli schemi più semplici che venivano attuati nei primi anni era quello del *mining* su *computer* altrui, tecnica che oggi ha perso di efficacia data l'altissima potenza computazionale che occorre per aggiungere blocchi alla catena. Nel mese di aprile 2013 aveva creato particolare scalpore il caso del sito *E-Sports Entertainment* contro cui era stato aperto un procedimento per aver infettato con un *malware* molti dei computer degli utenti al fine di creare una *botnet* di *mining.* Il caso si era chiuso con un accordo, senza che i fatti contestati venissero ammessi o verificati in giudizio[279].

Una variante di questa attività era quella in cui il permesso al *mining* veniva ottenuto con uno stratagemma basato su *social engineering,* lo studio del comportamento al fine di carpire informazioni utili che sta alla base di molti schemi di truffa. La società *We Build Toolbars LLC*, era la produttrice di *Your Free Proxy,* un *browser* di

[279]BBC News - E-Sports Entertainment settles *Bitcoin* botnet allegations http://www.bbc.co.uk/news/technology-25014477 2013.
http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-*bitcoin*-is-real-money/ 2013.

navigazione anonima che consentiva l'accesso anche ai siti bloccati per provvedimento dell'autorità: il pacchetto offerto in *download* era composto in maniera tale che quando l'utente installava il programma scaricava anche l'applicativo *monitor.exe* che, a propria volta, procedeva all'installazione del software *jhProtominer*, scaricandolo da un *server* remoto. In questo caso, la tecnica consisteva nello sfruttare l'abitudine dell'utente medio a muoversi in fretta quando installa un nuovo *software*, accettando le richieste della macchina in maniera acritica, senza leggere il loro contenuto. Accadeva così che il *software* scaricato minasse *bitcoin* sul *computer* ospite sulla base della licenza d'uso accettata per l'installazione di *Your Free Proxy;* l'accordo conteneva, infatti, una clausola in base alla quale l'utente consentiva alla WBT LLC il *mining* da remoto, cedendo alla società i blocchi eventualmente generati.[280]

Oggi gli attacchi di questo geere sono finalizzati alla creazione di monete che richiedono un impegno di potenza computazionale minore rispetto a *Bitcoin.* Nel maggio 2017 alcuni ricercatori impegnati nell'analisi del *worm WannaCry* hanno esposto una macchina in rete scoprendo l'esistenza di *Adylkuzz*, un virus che crea delle *mining bot* di *Monero*; come altri virus di questo genere ha un comportamento territoriale, sanificando la macchina infetta da altre applicazioni concorrenti e chiudendo le porte di accesso a nuovi attacchi, compresi quelli di *WannaCry* [281].

[280]Questo il testo dell'EULA: "*COMPUTER CALCULATIONS, SECURITY: as part of downloading a Mutual Public, your computer may do mathematical calculations for our affiliated networks to confirm transactions and increase security. Any rewards or fees collected by WBT or our affiliates are the sole property of WBT and our affiliates.*" http://www.tomshw.it/cont/news/minano-*bitcoin*-sul-vostro-computer-e-diventano-ricchi/51590/1.html 2013.

[281] Dan Goodin, Massive cryptocurrency botnet used leaked NSA exploits weeks before WCry
Campaign that flew under the radar used hacked computers to mine Monero currency, 2017, https://arstechnica.com/security/2017/05/massive-cryptocurrency-botnet-used-leaked-nsa-exploits-weeks-before-wcry/

La crescita di valore dei *bitcoin* ha invece fatto registrare la diffusione dei programmi dedicati alla loro falsificazione già utilizzati nell'attacco a *MtGox* del 2011: molti di questi programmi sono stati ritrovati dall'*FBI* in vendita su *Silk Road* dove, data la politica sui pagamenti adottata, venivano tariffati in *bitcoin* (!).

Uno schema ancora tipicamente utilizzato contro i possessori di *bitcoin* è quello di Ponzi[282]: applicando questo famoso raggiro, fra il 2011 e il 2012 il texano Trendon Shavers si era appropriato di 150.000 *btc* : perseguito giudiziariamente dalla *Security and Exchange Commission*, Shavers si era difeso facendo leva sulla natura indefinita dello strumento e affermando che la *SEC* non aveva alcuna competenza in materia, dato che i *bitcoin* non sono una vera moneta; il giudice federale Amos Mazzant, cui era stato affidato il caso, ha invece reso una delle prime pronunce sulla natura delle monete virtuali, dichiarando che, indipendentemente da ogni indagine più approfondita riguardo la loro natura, non vi è dubbio che i *bitcoin* costituiscano una *commodity* o

[282]Si tratta di uno schema truffaldino in base al quale un sedicente promotore finanziario propone a clienti normalmente poco versati nelle questioni economiche un investimento ad alto ritorno; in un primo momento vengono versati ingenti interessi che sono prelevati direttamente dal denaro raccolto; gli investitori, ignari della manovra pubblicizzano con il passaparola l'attività del truffatore che raccoglie così ulteriori investimenti: quando l'attività ha fruttato abbastanza denaro, l'impostore si dilegua. Lo schema porta il nome di Charles Ponzi, un italiano emigrato negli Stati Uniti che a Boston nel 1920 si accaparrò con questo sistema una cifra di quasi $ 30.000.000; al collasso dello schema gli investitori ricevettero solo 30 centesimi per dollaro investito con una perdita totale di oltre $20.000.000; Ponzi venne arrestato per truffa e, al rilascio, mise in atto lo schema nello Stato della Florida, venendo arrestato di nuovo; questi fatti si ripeterono più volte nel corso della sua vita finché morì in povertà a Rio de Janeiro nel 1949. In tempi recenti, Bernard Madoff, presidente del *NASDAQ (*il listino dei titoli tecnologici statunitensi), ha applicato lo Schema di Ponzi promettendo ai propri investitori un interesse del 10% e raccogliendo oltre $ 65.000.000.000; nel 2008, il collasso dello schema ha portato all'arresto per truffa di Madoff che, nel 2009 è stato condannato a 150 anni di prigione, il massimo della pena e il triplo rispetto a quanto richiesto dall'accusa: secondo quanto affermato dal Giudice Danny Chin della Distric Court of New York, la misura esponenziale dei danni provocati richiedeva l'intervento di una condanna esemplare. In http://www.nytimes.com/2011/06/29/nyregion/judge-denny-chin-recounts-his-thoughts-in-bernard-madoff-sentencing.html?pagewanted=all&_r=0

una forma monetaria e stabilendo la competenza della SEC in materia[283].

Un'altra tecnica *ever green* è quella del furto di *hot wallet* e *cold wallet*: solo i primi sono vengono commessi tramite tecniche di *hacking*, mentre i secondi sono furti comuni che hanno ad oggetto *hard drive,* chiavi *USB* e altri strumenti di archiviazione informatica. Fra i più importanti furti *on line* si ricordano quello ai danni di *BIPS (Bitcoin Internet Payment Services)*[284] che alla metà di novembre 2013 ha subito il furto di 1.295 *bitcoin* per un controvalore di $650.000 al momento della sottrazione e quello ai danni di *Sheep Marketplace*, il cui amministratore ha chiuso il sito a seguito del furto di 96.000 *bitcoin* per un controvalore di $100.000.000 al momento in cui è stato commesso l'illecito. La differenza fondamentale fra *BIPS* e *Sheep Marketplace* è data dal loro modo di porgersi sul mercato: *BIPS* era infatti il più grande sito europeo di cambio ed operava nella legalità; *Sheep Marketplace* era invece un sito di *black market* analogo a *Silk Road,* in cui l'anonimato garantito dalla rete *TOR*[285] veniva utilizzato per la compravendita di articoli illeciti. Se è vero che fuori dalla legalità non vi è alcuna garanzia, è altrettanto vero che, quando si tratta di *bitcoin*, il rischio di perdita del capitale incombe sull'investitore anche quando si rivolge agli intermediari autorizzati. In entrambi i casi i soggetti derubati hanno le medesime prospettive di recuperare il loro *bitcoin*, indipendentemente dal sito che avevano utilizzato per entrare su questo mercato: si tratta di un'eventualità piuttosto remota, dato che una delle tecniche maggiormente utilizzate in caso di furto consiste nel cambiare i *bitcoin* in valuta reale man mano che vengono sottratti; in questo modo la

[283]http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-*bitcoin*-is-real-money/ 2013.
[284]Ora acquisito da Coinfy https://coinify.com/
[285]Una rete TOR (*the onion router)* è strutturata secondo un'architettura di nodi paritari che consentono alla connessione di rimbalzare fra un certo numero *computer* compiacenti in modo tale che l'indirizzo IP del soggetto appaia diverso da quello effettivo: in questo modo si riesce a nascondere la propria posizione e a rendere anonima l'attività in rete. Per maggiori informazioni *vide* https://www.torproject.org/

ricerca si sposta dal piano virtuale, tracciato nel registro della *blockchain,* a quello reale del denaro contante, di per sé soggetto a difficile, se non impossibile, identificazione.

Parte III: Implementazioni

11. Sistemi derivati

11.1. *Soft Fork* e Implementazioni

Come abbiamo illustrato nella parte tecnica di questo lavoro, il sistema *Bitcoin* applica l'algoritmo di *hash* ad ogni *step* della *blockchain*, in modo da assicurare l'identità del prodotto ottenuto. Ciascun blocco reca in sé la traccia del *digest* che identifica il precedente: la catena logica è così rafforzata a ogni passaggio e un'eventuale manipolazione diviene immediatamente riconoscibile perché genera una biforcazione che da vita a un ramo di operazioni indipendente dal tracciato originario.

Il modello ha trovato applicazione iniziale ai pagamenti: per questa ragione i *token* di trasferimento vengono identificati nel parlare comune con il nome di monete. La *blockchain,* peraltro, ha uno spettro di applicazione molto più ampio essendo idonea all'identificazione di dati e al trasferimento di diritti in generale: utilizzando i sistemi di moneta virtuale oggi è possibile certificare digitalmente contratti, dichiarazioni sottostanti e dati relativi all'identità delle parti.

L'idea originaria è stata espressa nel 1998 da Nick Szabo e Wei Dai nei due *paper* indipendenti *Secure Property Titles with Owner Authority*[286] e *B-money*[287]: entrambi gli autori, considerati dalla rete gli ispiratori del lavoro di Satoshi Nakamoto, hanno teorizzato l'applicazione dei sistemi crittografici al trasferimento di diritti ulteriori rispetto al pagamento e, dunque, a uno schema contrattuale. Nick Szabo si era spinto oltre, predicendo addirittura degli esiti in cui la definizione computazionale delle clausole si sarebbe rivelata *self-enforcing*.

---

[286] Nick Szabo, Secure Property Titles with Owner Authority, 1998: "*A group, called a property club, gets together on the Internet and decides to keep track of the ownership of some kind of property. The property is represented by titles: names referring to the property, and the public key corresponding to a private key held by its current owner, signed by the previous owner, along with a chain of previous such titles. Title names may "completely" describe the property, for example allocations in a namespace. (Of course, names always refer to something, the semantics, so such a description is not really complete). Or the title names might simply be labels referring to the property. Various descriptions and rules -- maps, deeds, and so on -- may be included. [...]To implement a property club, we set up a replicated database so that the club members, hereafter "servers", can securely maintain titles of ownership, and securely transfer them upon the request of current owners. Actually getting end users to respect the property rights agreed upon by this system will be dependent on the specific nature of the property, and is beyond the scope of the current inquiry. The purpose of the replicated database is simply to securely agree on who owns what. The entire database is public".* http://szabo.best.vwh.net/securetitle.html

[287] Wei Dai, B-Money, 1998*: "3. The effecting of contracts. A valid contract must include a maximum reparation in case of default for each participant party to it. It should also include a party who will perform arbitration should there be a dispute. All parties to a contract including the arbitrator must broadcast their signatures of it before it becomes effective. Upon the broadcast of the contract and all signatures, every participant debits the account of each party by the amount of his maximum reparation and credits a special account identified by a secure hash of the contract by the sum the maximum reparations. The contract becomes effective if the debits succeed for every party without producing a negative balance, otherwise the contract is ignored and the accounts are rolled back. [...] 4. The conclusion of contracts. If a contract concludes without dispute, each party broadcasts a signed message "The contract with SHA-1 hash H concludes without reparations." or possibly "The contract with SHA-1 hash H concludes with the following reparations: ..." Upon the broadcast of all signatures, every participant credits the account of each party by the amount of his maximum reparation, removes the contract account, then credits or debits the account of each party according to the reparation schedule if there is one. 5. The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly."*
http://www.weidai.com/bmoney.txt

Nelle pagine che seguono esamineremo le *fork* di *Bitcoin* che hanno dato vita a *Namecoin* e *Litecoin* e le implementazioni *Colored Coins,* ripercorrendo l'evoluzione che ha condotto alla messa in atto degli *Smart Contract*, di cui ci occuperemo nel capitolo successivo.

11.2. *Namecoin*

La prima implementazione del sistema *Bitcoin* è stata attuata nel *2011 con la fork Namecoin*[288]*:* l'idea era apparsa in una serie di post, pubblicati sul forum *Bitcointalk.org* alla fine del 2010[289], che avevano messo in luce come il registro di *blockchain* potesse servire, oltre che per dare vita a un sistema di pagamenti, anche per la creazione di una struttura di assegnazione dei *top level domain* alternativa all'ICANN. La discussione, cui avevano preso parte, fra gli altri, Satoshi Nakamoto, Gavin Andersen e Hal Finney, nasceva dalla considerazione che il sistema *Bitcoin* sarebbe stato eccessivamente appesantito dalle registrazioni dei *domain name*; si era così ipotizzato di risolvere il problema con una *fork* del sistema, creando una blockchain nuova dotata di una moneta indipendente. Hal Finney aveva suggerito l'opportunità di inserire dei costi di transazione; Satoshi Nakamoto aveva aderito all'idea di riconoscere una ricompensa al lavoro dei *miner* suggerendo di calcolare la potenza di calcolo necessaria alla creazione dei *domani name* in maniera proporzionale alla domanda agganciando la quantificazione, e quindi la ricompensa, alla legge di Moore[290]. La

[288] https://namecoin.info/
[289]https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696
https://bitcointalk.org/index.php?topic=1790.msg22019#msg22019
https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917
[290] https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917
Hal Finney: "*The rules have to be that you have to spend a certain amount of bitdnscoins/DCCs in order to register your names and/or do other BitDNS transactions. That's the only way to make this alternative currency desirable and valuable.*"

discussione aveva preso in considerazione anche il mercato di questi nuovi prodotti: nella fase di *mining* i domini sarebbero stati generati con un nome in bianco e il primo acquirente avrebbe compilato questo campo liberamente, con il solo limite della disponibilità effettiva. Veniva quindi introdotta l'idea di un mercato secondario, con un sistema di cessione volontaria dei nomi dei domini[291], che avrebbe implicato transazioni nella moneta collegata, allargando gli orizzonti di mercato del progetto.

Namecoin, realizzazione pratica di quest'idea, è un sistema decentralizzato di registrazione e trasferimento dei *domain name,* basato sulla crittografia e su un sistema di indirizzi interno al *network*[292]*,* resistente ai tentativi di manipolazione esterna, inclusi quelli di censura. L'acquisto degli indirizzi è temporaneo, rinnovabile e strettamente collegato al possesso della moneta di riferimento che viene alterata nel codice, in modo da impedirne la spendita accidentale, dato che il sistema mantiene intatta la funzione di pagamento: infatti *Namecoin* nasce come *fork* di *Bitcoin* e il suo funzionamento è identico in tutto quello che non è stato modificato *ad hoc* per gli scopi del progetto. La chiave crittografica pubblica del *token* viene inserita nel registro di *blockchain,* per la verifica e l'esecuzione: per ragioni di protezione della *privacy,* gli amministratori del progetto stanno valutando di accettare in futuro le unità prodotte da *zerocash,* uno dei sistemi offuscati che abbiamo descritto nei paragrafi che precedono e che protegge la riservatezza delle transazioni utilizzando una dimostrazione a conoscenza zero per il trasferimento.

Satoshi: "*I agree. All transactions, IP changes, renewals, etc. should have some fee that goes to the miners. You might consider a certain amount of work to generate a domain, instead of a fixed total circulation. The work per domain could be on a schedule that grows with Moore's Law. That way the number of domains would grow with demand and the number of people using it.*"

[291]*Ibid.* Satoshi:"*Name change. A domain object could entitle you to one domain, and you could change it at will to any name that isn't taken. This would encourage users to free up names they don't want anymore. Generated domains start out blank and the miner sells it to someone who changes it to what they want."*

[292] L'intero elenco degli indirizzi viene scaricato su ogni *peer* del sistema.

Le caratteristiche di *Namecoin* consentono un uso tradizionale del sistema ma troviamo particolarmente interessante l'idea di inserire atti e documenti in questo registro di *blockchain,* con codifica crittografica in un'unità di moneta, per la validazione e l'esecuzione: ovviamente bisognerà rispettare i limiti di dimensione del campo[293] e questo comporta che in alcuni casi potrà rivelarsi maggiormente conveniente inserire il valore di l'*hash* del *file.* Si tratta di una caratteristica usufruibile anche in *Bitcoin* ma che appesantisce molto il registro, motivo per cui non è opportuno adoperarla in quel sistema che, ad oggi, ha già raggiunto una dimensione nell'ordine dei 120 *GB*. Inoltre considerato l'intenso traffico di *Bitcoin,* anche la transazione rischierebbe di essere ritardata: la composizione dei blocchi candidati è fatta in maniera da includere le *fee* più alte e, a meno di non inserire un valore cospicuo, i *miner* tenderanno a privilegiare transazioni di dimensioni minori così da cumulare più commissioni nel blocco[294].

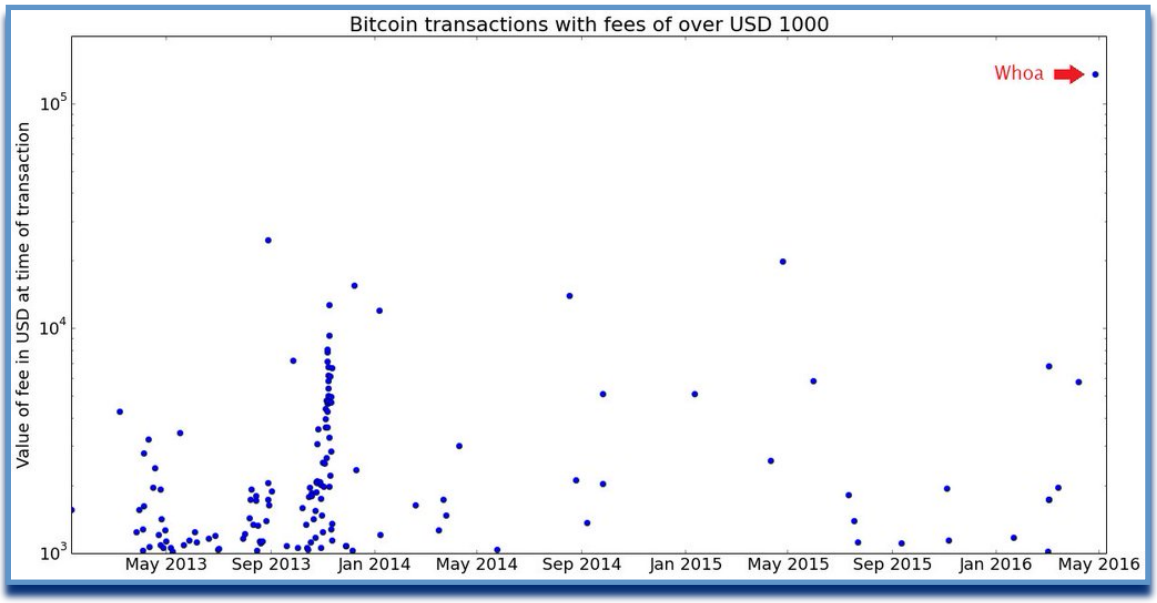


Figura 16: transazioni Bitcoin con commissioni oltre $1.000[295]

[293] Namecoin FAQ https://namecoin.org/docs/faq/

[294] http://btc.blockr.io/tx/info/4ed20e0768124bc67dc684d57941be1482ccdaa45dadb64be12afba8c8554537

[295] Arvind Narayan 2016
https://twitter.com/random_walker/status/729800710280335361

Il grafico che precede mostra una forte concentrazione delle transazioni con commissioni sopra $1.000 nei periodi di maggior valore dei *bitcoin:* aprile 2013 coincide con la crisi bancaria di Cipro e novembre 2013 rappresenta il periodo di maggior valore prima dei picchi del 2017; inserire i dati in una *blockchain* più leggera offre il vantaggio di una gestione dinamica e riduce i rischi legati alla volatilità. Le applicazioni pratiche di questa tecnica sono molteplici e consentono risparmi ingenti: la gestione di una *blockchain,* infatti, di per sé è un'attività costosa e impegnativa, per cui utilizzarne una pubblica ottimizza il rapporto fra prezzo e prestazioni. Inoltre, i sistemi storici come *Namecoin* godono di una reputazione di mercato solida che rappresenta un incentivo al'uso, consentendo ai *newcomer* di fruire di una credibilità già costruita.

11.3. *Litecoin*

Litecoin[296]*,* la seconda *fork Bitcoin* in ordine storico, è una delle monete virtuali più diffuse, con capitalizzazione di mercato[297] ai primi posti del *ranking*; il valore di queste *utilities* è molto più ridotto di quello dei *bitcoin,* rispetto cui si muove in maniera proporzionale, e si aggira attualmente sui $ 30, il che conferisce allo strumento una maggiore praticità d'uso, rendendolo dinamico sia in funzione di moneta virtuale che a in funzione di investimento.

[296]https://litecoin.org/it/

[297]"*Con riferimento ad una società, rappresenta il prodotto tra il numero di azioni in circolazione e il loro prezzo unitario; con riferimento ad un mercato rappresenta il valore complessivo - ai prezzi di mercato - di tutti i titoli quotati. La capitalizzazione di una società è data dal prodotto tra il numero di azioni in circolazione e il prezzo di mercato di ciascuna azione.*" Nel caso delle monete virtuali la capitalizzazione è data dal valore delle monete virtuali in circolazione moltiplicato per il loro prezzo.
http://www.borsaitaliana.it/bitApp/glossary.bit?target=GlossaryDetail&word=Capitalizzazione

Il sistema si basa su un'implementazione del progetto *Bitcoin* elaborata nel 2011 da Charles Lee, un programmatore MIT che nel 2013 ha lasciato il lavoro da Google per trasferirsi alla piattaforma di gestione *Coinbase*[298]. Pur mantenendo una struttura analoga alla previsione originaria, il nuovo sistema introduce alcune rilevanti modifiche:

- il limite di produzione delle monete virtuali viene elevato a 84 milioni di unità, quadruplicando i numeri del sistema *Bitcoin;*
- anche la velocità di esecuzione dei calcoli di generazione delle monete viene quadruplicata con produzione di un blocco ogni 2'.30'';
- vi è un incremento analogo anche nella velocità di esecuzione dei calcoli di convalida delle transazioni che nel sistema *Litecoin* richiede un tempo massimo di 15' circa;
- le transazioni *Litecoin* sono irreversibili: questo principio risolve in radice il problema della *transaction malleability* e del conseguente *double spending*;
- gli indirizzi *Litecoin* cominciano tutti con la lettera L per distinguerli da quelli *Bitcoin* che cominciano con il numero 1; poiché la modifica non è stata estesa agli indirizzi *multisignature, Litecoin* riconosce gli indirizzi *multisig Bitcoin* come validi. Disponendo a favore di uno di questi indirizzi, si rischia di perdere i *token* perché potrebbe trattarsi di indirizzi non assegnati, di cui nessuno gestisce e chiavi crittografiche.

Il 17 maggio 2017 *Litecoin* ha attivato *Segregated Witness (SegWit)* un servizio che consente di aggiungere al sistema funzionalità come *smart contract*, transazioni con importo confidenziale, *coin mixing* e

[298] http://www.coindesk.com/litecoin-creator-charles-lee-has-left-google-to-work-at-coinbase/

canali di pagamento reciproco che instaurano un rapporto analogo a quello di conto corrente di cui all'art. 1823 cc.[299].

Il 10 giugno 2017 Charles Lee ha lasciato il lavoro da *Coinbase* per dedicarsi a tempo pieno allo sviluppo di *Litecoin*.

11.4. Colored Coin

Colored Coin[300] è un sistema nato nel 2013 come integrazione del sistema *Bitcoin*, volta ad inserire meta dati in *blockchain:* la funzione originale consisteva nell'utilizzare le transazioni *bitcoin* per dare certezza e tracciabilità a informazioni ulteriori relative a dati personali, messaggi o diritti su beni. Oggi il sistema si è evoluto in un insieme di strumenti interattivi *blockchain agnostic* che opera su quel registro per conto degli utenti, consentendo loro di svolgere le operazioni di cui hanno necessità senza occuparsi personalmente delle transazioni e rappresenta una classe di metodi[301]. Il sistema originale è affine per certi versi a *Namecoin,* consentendo di inserire nella *blockchain* elementi digitali che vanno oltre lo scambio di *digital currency*. Le informazioni vengono computate nel codice di una moneta che viene 'colorata', cioè qualificata in maniera speciale così da impedirne la spendita accidentale, poiché il trasferimento della moneta comporta quello del

[299]Aaron van Wirdum, Litecoin Has Now Deployed Segregated Witness, 2017 https://bitcoinmagazine.com/articles/litecoin-has-now-deployed-segregated-witness/

[300] Yoni Assia, Vitalik Buterin, Lior Hakim, Meni Rosenfeld, Rotem Lev, The Colored Coins white paper https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit?pli=1

[301]nei linguaggi di programmazione ad oggetti, i metodi sono delle funzioni che svolgono un lavoro determinato sugli oggetti di una classe; a propria volta la classe è una struttura sintattica usata come modello per creare delle strutture dati che vengono appunto dette oggetti. In sintesi: vi sono dei dati aggregati che vengono chiamati oggetti, la classe che è il modello che consente di costruirli e i metodi sono le funzioni che lavorano su di essi.

diritto incorporato; funzionalmente si tratta del sistema *Bitcoin*, alla cui analisi facciamo riferimento per ogni ulteriore dettaglio.

Le *Colored Coin* possono contenere ogni genere di diritto digitalmente trasferibile: la circolazione avviene in base a una firma digitale che, nel rispetto dei limiti previsti dall'ordinamento, può anche avere carattere di pseudonimo tutelando così la riservatezza delle parti. Il contratto e il pagamento collegato vengono inseriti in *blockchain* con riferimento a una determinata chiave crittografica, rendendo certo il rapporto con il titolare del diritto che è anche il proprietario della moneta. Nello specifico, la chiave crittografica privata consentirà al sistema la verifica dell'identità informatica delle parti senza fornire dati ulteriori riguardo la loro identità.

Sotto il profilo istituzionale, i sistemi di questo genere contengono un forte potenziale di sviluppo dei registri della proprietà: una *blockchain* ad accesso riservato dei Pubblici Ufficiali competenti ben potrebbe digitalizzare i diritti sui beni registrati facilitando le iscrizioni e le trascrizioni e producendo come risultato un trasferimento rapido, sicuro ed economico. Anche nel settore privato le implicazioni sono di grande importanza: si pensi solo alla possibilità di digitalizzare in questi *token* azioni, obbligazioni e altri strumenti finanziari rendendo, in un prossimo futuro, le vicende collegate alla loro titolarità di rapida e sicura verificabilità, con conseguenze più che apprezzabili in termini di efficienza economica. In *Colored Coin* possono già essere digitalizzati i diritti trasferibili non soggetti a registrazione e la loro circolazione avviene secondo le regole di *blockchain*, nel rispetto dei limiti dell'ordinamento giuridico di riferimento.

12. *Smart Contract*

12.1. Clausole *self executing* e *Blockchain Log*

Gli *Smart contract* sono un'evoluzione del sistema *Bitcoin* in cui, al ricorrere di una condizione informaticamente verificabile, il sistema esegue in via automatica una determinata prestazione. Si tratta di un modello che è ancora in larga parte da definire ma che *de jure condendo* si rivela particolarmente interessante. L'obiettivo comune di informatici e giuristi all'opera su questa stimolante fattispecie consiste nell'individuazione di uno strumento, utilizzabile nella vita quotidiana, che risponda sia alle esigenze di completezza dell'ordinamento giuridico che a quelle matematiche del sistema binario. In altre parole, lo scopo della ricerca comune è di verificare se il giudizio ipotetico - prescrittivo (se c'è A ci deve essere B) tipico delle norme giuridiche possa essere applicato a un *target* di analisi molto particolare: la scrittura di un codice informatico che renda *self-executing* alcune clausole contrattuali, risolvendo in radice i problemi collegati al loro inadempimento.

L'idea di *smart contract* ha preso forma per la prima volta nel 1997 nei due *paper* a firma di Nick Szabo *Formalizing and Securing Relationships on Public Networks*[302]e *The Idea of Smart Contracts*[303], in cui l'autore prendeva spunto dal sistema di vendita dei distributori automatici per teorizzare il trasferimento di alcuni diritti in esecuzione di un algoritmo. Nel 1998 Nick Szabo formalizzava in un terzo *paper* intitolato *Secure Property Titles with Owner Authority*[304] i concetti già individuati nei due precedenti lavori. Nello stesso anno Wei Dai esponeva nell'opera *B-money*[305] l'idea di un sistema contrattuale indipendente da attuare in un *network* non tracciabile fra soggetti identificati da uno pseudonimo digitale (la chiave crittografica pubblica); il sistema prevedeva lo scambio di messaggi firmati digitalmente e crittografati e la predeterminazione delle regole di *enforcement*[306].

Pur nelle differenze logiche fra le due opere, gli schemi teorizzati dai due autori appaiono idonei ad esiti *self-enforcing* di quelle clausole che, essendo giuridicamente eseguibili, consentano altresì un'idonea determinazione computazionale.

12.2. Accordi e Contratti

Prima di procedere all'analisi degli s*mart contract* è opportuno tracciare i confini della nostra ricerca: la ricerca statunitense sul tema

[302]Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469
[303]Nick Szabo, *The Idea of Smart Contracts*, 1997, http://szabo.best.vwh.net/idea.html
[304]Nick Szabo, Secure Property Titles with Owner Authority, 1998, http://szabo.best.vwh.net/securetitle.html
[305]Wei Dai, B-Money, 1998, http://www.weidai.com/bmoney.txt
[306]Wei Dai, B-Money, 1998: "*5. The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly.*" http://www.weidai.com/bmoney.txt

viene condotta dal punto di vista informatico e considera gli smart contract come accordi eseguibili, distinguendo fra accordi giuridici e accordi semplici; in questo lavoro ci occuperemo unicamente degli accordi giuridici, limitando lo studio alle caratteristiche suscettibili di applicazione secondo la legge italiana.

Lo schema attuativo, di per sé è semplice: le previsioni contrattuali idonee vengono tradotte in un codice informaticamente eseguibile e inserite in un registro logico, per cui al verificarsi di una certa condizione (matematicamente accertabile) si produce l'evento digitalmente collegato. E' di fondamentale importanza che l'esecuzione automatica non sia giuridicamente contestabile, altrimenti si produrrebbe una litigiosità successiva di effetto opposto a quello che si vuole studiare.

Dal punto di vista giuridico, gli *smart contract* si propongono di intervenire in via preventiva in un ambito di inadempimento coercibile tramite esecuzione forzata. Il principio è analogo a quello degli accordi prematrimoniali che, in alcuni ordinamenti, prevengono l'insorgenza di una lite futura stabilendo in anticipo le condizioni economiche applicabili allo scioglimento di un matrimonio che deve ancora essere celebrato. Nella contrattazione *smart,* la scrittura di alcune clausole in codice informaticamente eseguibile consente di evitare alcune forme di litigiosità riguardo l'adempimento. Le parti concordano preventivamente sull'esecuzione automatica della clausola che avrà luogo secondo un *input* di sistema: eventuali dispute riguardo la validità del contratto o la puntualità dell'esecuzione potranno essere sottoposte alla valutazione del giudice in un momento successivo.

L'utilizzo delle funzioni di *blockchain* impone alcuni limiti di carattere tecnico: le prestazioni di commercio elettronico indiretto non sono infatti eseguibili in via informatica. Sono, così, escluse dall'applicazione tutte le clausole che abbiano riguardo a beni o servizi che, pur acquistati in rete, abbiano una consistenza tangibile o debbano essere eseguiti nel mondo materiale come, ad esempio, la consegna di

un libro o il servizio di pulizia di un locale. L'oggetto delle clausole *smart* è informaticamente circoscritto ai beni mobili di natura digitale, stante l'impossibilità materiale di inserire nel sistema informatico beni di natura differente; per quanto riguarda gli obblighi di fare, il paradigma *smart* risulterà applicabile nei casi in cui la prestazione sia erogabile direttamente, come accade in molti servizi *online.*

Nei casi di consegna di oggetti tangibili e prestazione di servizi materiali, esclusi per impossibilità pratica dall'esecuzione digitale automatica, il paradigma può comunque trovare applicazione indiretta nei casi in cui le parti abbiano preventivamente determinato un equivalente monetario da versare in via automatica alla verifica dell'inadempimento.

Quest'ultima evenienza è l'unica applicabile all'ipotesi di esecuzione automatica degli obblighi di non fare, in cui una prestazione negativa, quella di non fare, si trasforma in una positiva consistente nell'obbligo di eliminare ciò che è stato fatto in violazione del vincolo originario[307].

12.3. La proposta di Nick Szabo

La proposta formulata da Nick Szabo nel paper *Secure Property Titles with Owner Authority*[308] consiste in una *securitization* digitale

[307]Crisanto Mandrioli, Antonio Carratta, Diritto processuale civile vol. III, Giappichelli2015

[308] Nick Szabo, *Secure Property Titles with Owner Authority*, 1998: "*A group, called a property club, gets together on the Internet and decides to keep track of the ownership of some kind of property. The property is represented by titles: names referring to the property, and the public key corresponding to a private key held by its current owner, signed by the previous owner, along with a chain of previous such titles. Title names may "completely" describe the property, for example allocations in a namespace. (Of course, names always refer to something, the semantics, so such a description is not really complete). Or the title names might simply be labels referring to the property. Various descriptions and rules -- maps, deeds, and so on -- may be included. [...]To implement a*

all'interno di una rete *peer to peer*: uno specifico diritto di proprietà viene incorporato in un titolo destinato alla circolazione, assieme alle informazioni relative; il trasferimento è messo in sicurezza crittografica e il titolo di proprietà è inserito in una catena logica di titoli analoghi a garanzia della continuità delle operazioni. Alla codifica del titolo di proprietà possono essere aggiunti elementi ulteriori, come mappe o atti notarili, e l'intero *database*, che è pubblico, viene replicato su tutti i *computer* della rete in maniera da assicurare che la custodia e il trasferimento dei titoli avvengano correttamente.

Si tratta della rielaborazione delle idee presentate nei precedenti *paper Formalizing and Securing Relationships on Public Networks*[309]e *The Idea of Smart Contracts*[310] in cui l'autore proponeva di mettere a servizio della contrattualistica la crescente potenza computazionale, scrivendo l'attivazione di alcune clausole direttamente nel *software*, in maniera da rendere l'inadempimento scarsamente conveniente, se non addirittura proibitivo, in termini economici.

Lo schema, basato sulla crittografia, si articola in quattro punti fondamentali:

- La predisposizione di una chiave idonea a un ingresso selettivo dei contraenti e all'esclusione di terzi non autorizzati;
- La creazione di una *back door* che consenta sempre l'ingresso alla parte creditrice;

---

property club, we set up a replicated database so that the club members, hereafter "servers", can securely maintain titles of ownership, and securely transfer them upon the request of current owners. Actually getting end users to respect the property rights agreed upon by this system will be dependent on the specific nature of the property, and is beyond the scope of the current inquiry. The purpose of the replicated database is simply to securely agree on who owns what. The entire database is public". http://szabo.best.vwh.net/securetitle.html

[309]Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469

[310]Nick Szabo, *The Idea of Smart Contracts*, 1997, http://szabo.best.vwh.net/idea.html

- La possibilità per il creditore di attivare la *back door* se il pagamento viene meno per un determinato periodo di tempo; e
- La disattivazione permanente della *back door* come conseguenza automatica dell'ultimo pagamento.

A distanza di quasi vent'anni il sistema ideato da Nick Szabo appare ancora attuale e contiene in sé una serie di *input* utili per lo sviluppo del sistema di *smart contract* di cui ci stiamo occupando.

12.4. Il modello *smart*

Nell'era digitale molti contratti vengono gestiti in *Electronic Data Interchange,* un sistema standardizzato fin dal 1996[311]che consente lo scambio digitale automatico dei documenti amministrativi e contabili, relegando l'intervento dell'operatore ai casi di malfunzionamento, manutenzione e aggiornamento del sistema. In alcuni casi, server remoti gestiscono ogni fase del contratto: nel *web advertising*, ad esempio, vengono effettuate aste computerizzate a seguito delle quali il provider posiziona autonomamente i *banner* pubblicitari sulle pagine visualizzate dagli utenti *Internet*. Il servizio può posizionare effetti pubblicitari statici, che verranno retribuiti in base al numero di visualizzazioni, o dinamici, che contengano cioè un *link* al sito dell'inserzionista, e in questo caso il pagamento avverrà in base al numero di visite realizzate dagli utenti. Si tratta di forme contrattuali automatizzate che possono essere sospese o modificate in qualsiasi

[311] *Vide, inter alia,* http://www.nist.gov/ e http://www.unece.org/info/ece-homepage.html

momento: in caso di disaccordo fra le parti l'esecuzione forzata richiederà l'attivazione di una procedura giudiziaria.

Lo *smart management* del contratto rappresenta un passo ulteriore su questa strada, idoneo a consentire forme di gestione dinamica che riducano costi di un eventuale inadempimento: i servizi offerti dalle piattaforme *smart* sono infatti in grado di implementare la fattispecie contrattuale mettendo in atto il *self enforcement* di alcune clausole contrattuali. Il sistema varia in funzione dei diritti dedotti e dei diversi termini pattuiti, con l'inserimento nel registro di *blockchain* di *trigger point* come lo scadere di un termine, l'esercizio di una determinata opzione, o il verificarsi di uno specifico evento. Nel caso di contratto sottoposto a termine, la verifica sarà certa e immediata mentre nel caso di contratto condizionato potranno verificarsi due distinte ipotesi. L'evento *trigger* potrà infatti risultare da fonti pubbliche o istituzionali, come i siti *web* di aeroporti e ferrovie che riportano i ritardi dei collegamenti o i siti delle Borse Valori che riportano le quotazioni del giorno: in questo caso il codice del contratto farà discendere l'esecuzione da questa verifica che può essere considerata univoca. Negli altri casi invece, per la verifica dell'evento occorrerà una forma di conferma allargata: questo servizio viene normalmente fornito da un *internet oracle,* una piattaforma che esamina lo stato della rete avendo riguardo alla condizione da verificare e ne dà conferma al raggiungimento di un determinato numero di riscontri positivi.

Il *range* di applicazione della contrattazione *smart* è particolarmente ampio e, partendo dai semplici pagamenti, spazia dall'esecuzione delle clausole penali, alle clausole di tutela nei contratti dei consumatori, fino all'esecuzione di diversi contratti di borsa ma l'elencazione non è esaustiva. Al momento dell'inserimento in *blockchain* il sistema apporrà una marca temporale, associando data e ora certe al *file:* sarà così possibile verificare in ogni momento che le attività si siano svolte

secondo l'ordine temporale dichiarato, evitando contestazioni riguardo ai tempi della transazione.

12.5. Clausole *self executing* e tutela giudiziale

Nel paper del 2015 *The Ring of Gyges: Using Smart Contracts for Crime*[312], gli informatici Ari Juels, Ahmed Kosba ed Elaine Shi, mettono in guardia contro i possibili usi degli *smart contract* a fini criminali: i tre ricercatori esaminano forme di accordo abusivo, come il caso di scuola del contratto con il *killer*, che dal punto di vista del diritto civile costituisce una fattispecie nulla per illiceità dell'oggetto. Si tratta di un ordine di considerazioni molto interessante che sviluppa alcune delle ipotesi formulate nel da Tim May nel Manifesto Crypto-Anarchico[313] e nel *Cyphernomicon*[314]. Rinviando ad altra sede l'esame di questo genere di transazioni, la nostra analisi procederà con unico riguardo alle fattispecie lecite e giuridicamente possibili di *smart contract*.

[312]Ari Juels, Ahmed Kosba, Elaine Shi, 2015,The Ring of Gyges: Using Smart Contracts for Crime
http://www.arijuels.com/wp-content/uploads/2013/09/public_gyges.pdf

[313]Timothy C. May, The Crypto Anarchist Manifesto, 1988: "*The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.*"
http://www.activism.net/cypherpunk/crypto-anarchy.html

[314] Timothy C. May The Cyphernomicon, 1994.
16.3.2. "Do the views here express the views of the Cypherpunks as a whole?"
Several Cypherpunks who've thought about the issues of crypto anarchy have been disturbed by the conclusions that seem inevitable (markets for corporate information, assassianation made more liquid, data havens, espionage made much easier, and other such implications to be explored later in this section). So, take this section with these caveats.
https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html

Nel rispetto dei limiti funzionali individuati all'inizio di questo capitolo, l'ambito applicativo degli *smart contract* appare comunque molto ampio: in primo luogo, l'esecuzione automatica risulta congeniale a tutte le vicende contrattuali sottoposte a termine, un evento che il sistema è in grado di verificare con certezza in via immediata.

Analoghe considerazioni valgono per quanto riguarda quelle clausole che prevedono l'esercizio di opzioni o facoltà delle parti: si pensi al caso delle obbligazioni alternative, in cui è il creditore a scegliere la prestazione che desidera ricevere, o alle garanzie a prima richiesta scritta che invertono l'onere della prova riguardo l'inadempimento. Vi è poi l'esecuzione delle clausole che trasferiscono somme di denaro in relazione a eventi da verificare, come accade nel caso di premi, penali o *tranche* di pagamento.

L'accertamento avverrà, in via alternativa, tramite siti *web* istituzionali o attraverso i servizi di *internet oracle* descritti nel paragrafo precedente. Rientrano nel primo caso i contratti di borsa come i *future,* gli *swap* e le operazioni su derivati che prevedono unicamente flussi di cassa; mentre ricadono nella seconda ipotesi la verifica della qualità di un servizio o il riscontro di condizioni come lo stato di avanzamento lavori in un appalto o le condizioni meteo in un luogo determinato.

L'elenco dei contratti suscettibili di implementazione *smart* è meramente esemplificativo e non esaustivo: gli *smart contract* rappresentano l'evoluzione efficiente nella gestione dei flussi di cassa; si tratta di modelli ancora largamente da definire ma appare chiaro che il loro impiego consentirebbe la riduzione dei costi e i tempi giudiziari legati alla gestione dell'inadempimento. A livello informatico la procedura non è revocabile: una volta programmato il trasferimento della moneta virtuale non sarà possibile invalidarlo in alcun modo. La firma digitale avvia qui un procedimento irreversibile e, sotto l'aspetto tecnico, non c'è modo di annullarla o di limitarne gli effetti: eventuali

questioni relative alla validità o efficacia del contratto, dovranno essere gestite secondo il sistema delle rivalse tipico del diritto civile.

Recentemente gli *smart contract* hanno riscosso fiducia a livello istituzionale: nel mese di marzo 2017 lo Stato dell'Arizona (USA) ha disposto a favore della conformità ai requisiti di legge dei dati conservati in *blockchain*, formulando previsioni espresse in ordine alla legalità degli *smart contract*[315]; ancor più di recente, il 7 giugno 2017, lo Stato del Nevada (USA) ha disposto l'esenzione della *blockchain* da ogni forma di imposizione e licenza, stabilendo altresì che essa costituisce un'idonea forma legale di registrazione dei contratti[316]. Gli atti dell'Arizona e del Nevada vogliono dichiaratamente attirare *start up* sul territorio e fanno seguito alla legge del Vermont che dal 2016 riconosce valore di prova legale alle registrazioni contenute in *blockchain*[317]. Provvedimenti analoghi sono in discussione negli Stati di Hawaii, Maine, Delaware e addirittura al Congresso degli Stati Uniti che il 6 giugno 2017 ha richiesto, in due distinte udienze, il parere formale dei rappresentanti di *Coincenter*, l'associazione di ricerca *no-profit* che patrocina l'emanazione di *public policy* adeguate per monete virtuali e registri distribuiti[318].

[315] Arizona House bill 2417, 2017 https://legiscan.com/AZ/text/HB2417/2017
[316] Nevada Senate Bill 398, 2017, *https://legiscan.com/NV/bill/SB398/2017*
[317] Vermont General Assemby, 2016,
http://legislature.vermont.gov/bill/status/2016/H.868
[318] Neeraj Agrawal,We testified in Congress and advocated for your right to innovate with open blockchains, 2017 https://coincenter.org/

13. Piattaforme *Smart*

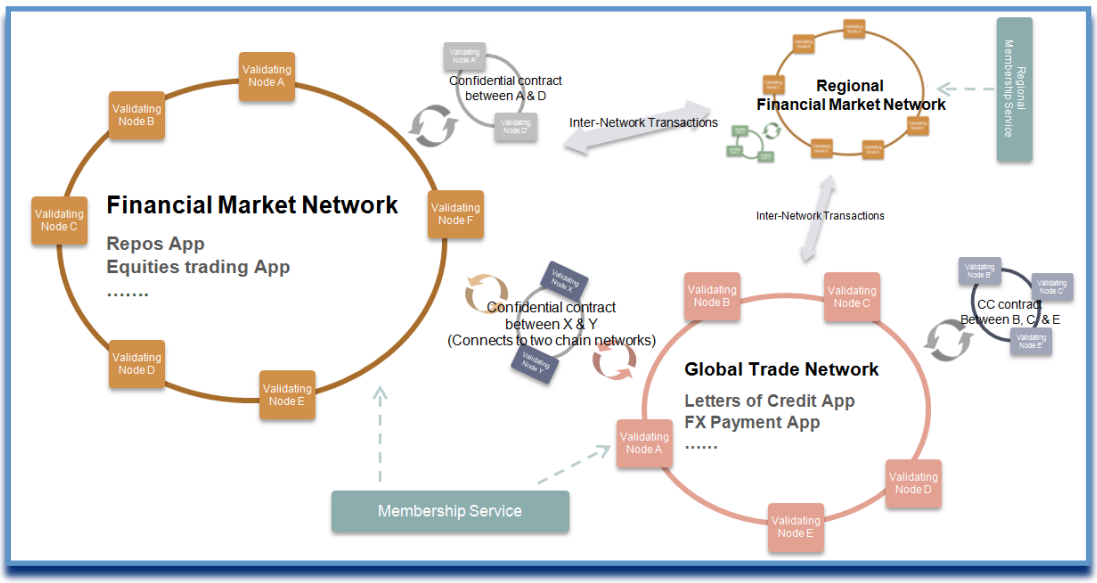
13.1. *Ruolo delle piattaforme*

Le piattaforme *smart* sono architetture *internet* evolute che consentono la conclusione di accordi vincolanti, applicando l'algoritmo di *hash* per l'individuazione univoca di dichiarazioni e intese. I *digest* così ottenuti vengono inseriti nel codice di una delle monete di riferimento, e i *miner* le eseguono quando aggiungono blocchi alla catena consentendo così la gestione tramite il registro logico di tutte vicende collegate.

13.2. *Hyperledger*

Hyperledger è un progetto della *Linux Foundation* per la creazione di una piattaforma di scambio fra sistemi per transazioni *business-to-business* (B2B) e *business-to-customer* (B2C) cui hanno aderito *stakeholder* di grande rilievo sul mercato come *IBM* e *Cisco*. L'idea alla base di questa proposta è che i sistemi specializzati siano maggiormente efficienti e che gli scambi di mercato possano ricevere un incentivo dal corretto scambio di informazioni fra i registri di *blockchain* che,

rimanendo autonomi nel modello prescelto per la verifica del consenso e la conservazione dei dati, siano in grado di offrire servizi interattivi per la gestione dell'identità, il controllo degli accessi e la contrattazione *smart*. Il fondamento del sistema è dato dall'applicazione di valori come fiducia, affidabilità e trasparenza al maggior numero di scambi possibile, allo scopo di ridurre i costi e la complessità delle transazioni in un ambiente *opensource* collaborativo. I modelli vengono sviluppati in collaborazione con le maggiori società del settore informatico in vista della loro adozione a livello generale[319].



[319] https://www.hyperledger.org/about *"Not since the Web itself has a technology promised broader and more fundamental revolution than blockchain technology. A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies. Together these can be used to build a new generation of transactional applications that establishes trust, accountability and transparency at their core, while streamlining business processes and legal constraints. Think of it as an operating system for marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly reduce the cost and complexity of getting things done in the real world. Only an Open Source, collaborative software development approach can ensure the transparency, longevity, interoperability and support required to bring blockchain technologies forward to mainstream commercial adoption. That is what Hyperledger is about – communities of software developers building blockchain frameworks and platforms"*

Figura 17: A world of many blockchain networks - Hyperledger Whitepaper[320]

Per consentire un'ampia varietà di partecipazione, la piattaforma permette l'uso di diverse *blockchain*: *Burrow*, un *client* compatibile con *Ethereum Virtual Machine* sviluppato da Monax e Intel; *Fabric* sviluppato da IBM; *Iroha*, implementazione di *Fabric* sviluppata da Soramitsu per il settore mobile; *Sawtooth* sviluppata da Intel, con il meccanismo di consenso '*Proof of Elapsed Time*' basato sull'azione di un gruppo di *trusted validators* a cui il sistema assegna casualmente un tempo di attesa per l'esecuzione delle operazioni di verifica, con inclusione nella catena logica del blocco validato dal nodo cui è stato assegnato l'intervallo temporale più breve.

13.3. *Ripple R3 Corda*

Ripple, di cui abbiamo già illustrato la cui struttura tecnica, aveva inizialmente preso parte allo sviluppo degli *smart contract* tramite la piattaforma *Codius,* un progetto abbandonato nel 2015 a causa delle dimensioni ridotte del mercato di riferimento[321]. Oggi, la ricerca *Ripple* è rivolta prevalentemente al sistema dei trasferimenti intercontinentali e a questo scopo è stato creato il consorzio R3, composto di gruppi bancari, *corporate* del settore tecnologico e istituzioni finanziarie, cui hanno aderito, fra le altre, *BNP Paribas*, *Credit Suisse*, *Deutsche Bank*, Intesa San Paolo, UBS e Unicredit.

[320]Hyper ledger whitepaper https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/pub

[321] Jeffrey Maxim, Ripple Discontinues Smart Contract Platform Codius, Citing Small Market, 2015, https://bitcoinmagazine.com/articles/ripple-discontinues-smart-contract-platform-codius-citing-small-market-1435182153/

L'obiettivo del consorzio è quello di sviluppare un struttura di pagamento che superi l'attuale frammentazione delle stanze di compensazione. La tecnologia sviluppata da *Ripple* viene utilizzata per dare vita a un sistema di scambi dove gli utenti possono collaborare in gruppi indipendenti, senza creare necessariamente un *network* aperto.

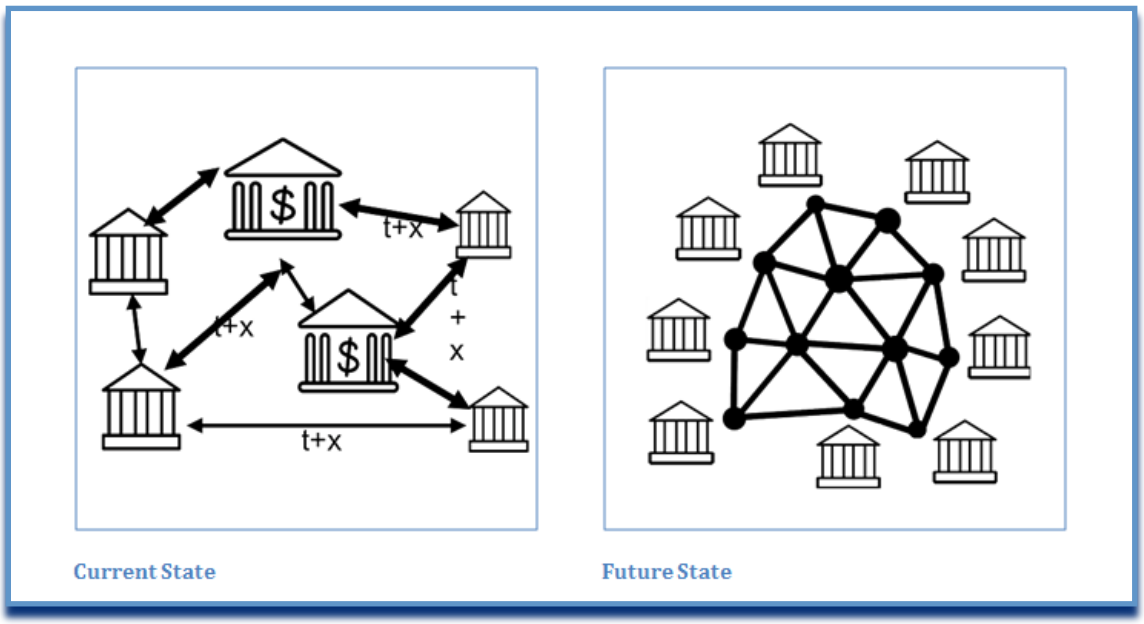


Figura 18: R3 - Impact to the Ecosystem [322]

Per l'attuazione del progetto, il consorzio R3 si serve della piattaforma Corda[323], sviluppata da in *DLT* per la registrazione, la gestione e la sincronizzazione degli accordi finanziari regolamentati. Il progetto adotta un registro distribuito largamente ispirato alla *blockchain*, di cui elimina però quelle caratteristiche che non sono adatte allo scopo perseguito. In particolare, l'adesione al gruppo è

[322] http://r3members.com/
[323] Richard Gendal Brown, Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services, 2016, http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

soggetta al requisito formale di appartenenza alle istituzioni regolamentate, cosa che rende superflua l'elaborazione della *proof of work* richiesta nei *network* aperti. La gestione dei gruppi avviene secondo la tecnologia del sistema di riferimento *Ripple,* alla cui precedente analisi rinviamo per ogni dettaglio.

Banche e *technology corporation* saranno così libere di interagire al livello che preferiscono, *rectius* al livello che consente gli scambi più efficienti, mantenendo per il resto la riservatezza imprescindibile per ogni modello finanziario. L'innovazione *DLT* riguarda anche le procedure di *audit*: l'identità dei dati è assicurata con algoritmo di *hash,* mentre la struttura del registro consente una verifica automatica e ininterrotta.

13.4. *Colu*

Colu è una *start up* nata nel 2015 a Tel Aviv, per la gestione delle *colored coin*; la progettazione comprendeva alcune funzionalità di *smart contracting.* La particolarità del sistema è data dalla sua interposizione tra la *blockchain* Bitcoin e gli utenti finali. In questo modo le transazioni vengono sganciate dal possesso di moneta virtuale: mancando un indirizzo *bitcoin,* gli effetti del trasferimento vengono inviati a numeri di telefono. Il servizio, *blockchain agnostic*, viene realizzato tramite l'acquisto e la gestione dei *bitcoin* necessari al trasferimento da parte di *Colu:* gli utenti finali compenseranno la prestazione ricevuta con il pagamento di una commissione.

Assecondando la richiesta degli utenti, nel 2016 gli amministratori hanno fatto delle *local currency* l'obiettivo principale del progetto. Il 7 giugno 2017 Colu ha annunciato ufficialmente la *release* del *software Bankbox,* dedicato alle banche centrali per l'emissione di valuta locale

su *blockchain*[324]. La prima adesione al progetto è arrivata dalla Banca Centrale di Barbados che, in collaborazione con la *start up Bitt* svilupperà il dollaro locale su *blockchain*. Il piano di lavoro prevede lo sviluppo in termini di *Lightning Network,* per la creazione di canali di pagamento bidirezionali fra *blockchain* di diversa natura, e l'interoperabilità con la piattaforma *HyperLedger*[325]

13.5. *Omni*

Omni, lanciata nel 2015, è la versione implementata di *Mastercoin*, piattaforma nota anche come 'il secondo sistema *Bitcoin'* che si propone la creazione di un sistema di cambi decentralizzato, l'implementazione della *smart property* e la gestione di depositi di risparmio. La piattaforma è basata su una *fork* del sistema *Bitcoin* e gestisce progetti come *Maidsafecoin*[326]*,* una moneta dedicata alla creazione e alla fruizione di servizi di *network*, *Tether*[327]*,* un *digital token* agganciato a parità fissa con il dollaro statunitense *rebrand* del sistema *Realcoin*, *e Factom*[328] un sistema che utilizza la *blockchain* per la conservazione di documenti e procedure aziendali. Nell'aprile 2017 la *Omni Foundation* ha annunciato la collaborazione con il Governo Armeno per l'emissione di azioni, obbligazioni e certificati di proprietà tramite *smart contract*[329].

[324] Mark Smargon, Open source banking—Announcing a new path for ColoredCoins, 2017, https://medium.com/colu/open-source-banking-announcing-a-new-path-for-coloredcoins-150f5066c232
[325] *Vide ultra*
[326]http://maidsafe.net/safecoin
[327]https://tether.to/
[328]*Business Processes Secured by Immutable Audit Trails on the Blockchain http://factom.org/*
[329]Richard Jacobs, Omni Foundation – A Platform for Utilizing the Bitcoin Blockchain for Diverse Transactions such as Issuing Bonds, 2017, https://www.bitcoin.com/podcast/omni-foundation-a-platform-for-utilizing-the-bitcoin-blockchain-for-diverse-transactions-such-as-issuing-bonds

13.6. *Stellar*

Stellar[330] è una piattaforma finanziaria creata nel 2014 da Jed Mc Caleb di *Ripple:* nata come *fork*, nel 2015 è stata dotata di un nuovo e diverso algoritmo di consenso poiché il co-sviluppatore Joyce Kim riteneva che quello adottato da *Ripple* fosse affetto da un *bug*[331]. Tramite la *Stellar Foundation* promuove la crescita dei piccoli servizi bancari e micro-finanziari nei paesi in via di sviluppo, offrendosi di supplire alla scarsa interoperabilità fra banche e sistemi di pagamento al fine di una riduzione dei costi di transazione delle operazioni collegate. Il sistema è gratuito e si propone lo scopo di creare strumenti e servizi finanziari per gli utilizzatori del *network* da rendere disponibili anche per enti senza scopo di lucro[332]. Il primo paese in cui è stata data attuazione alle attività di *Stellar* è la Nigeria, in collaborazione con la *start up Oradian*[333] che sviluppa *software* per la gestione di piccole realtà bancarie e per le operazioni di micro-finanza.

13.7. Zeronet

ZeroNet[334] è un *network opensource* decentralizzato con funzioni analoghe a quelle di *internet*: utilizza un *domain name system* proprietario cui si accede tramite un'applicazione che fa da *host* per le pagine ed è compatibile con i normali *browser.* Basato sulla tecnologia *blockchain*, il sistema utilizza la rete *BitTorrent* per la condivisione di

[330] https://www.stellar.org/
[331] Joyce Kim, Safety, liveness and fault tolerance—the consensus choices, 2014, https://www.stellar.org/blog/safety_liveness_and_fault_tolerance_consensus_choice/

[332] https://www.stellar.org/ https://www.stellar.org/about/mandate/
[333] https://oradian.com/
[334] https://zeronet.io/

contenuti soggetti a *copyright*: la replica del database su tutti i nodi della rete rende impossibile l'oscuramento delle pagine e dei contenuti condivisi.

13.8. Inter Planetary File Sistem

Inter Planetary File Sistem[335] è un *file system* multimediale alternativo al *world wide web.* Basato su una decentralizzazione *peer to peer,* scambia in *bit torrent file* identificati da un *hash* che il sistema utilizza per eliminare la ridondanza. Ogni nodo conserva solo le informazioni cui è interessato. Gli sviluppatori consigliano di applicare la funzione di *hash* ai file caricati inserendo i *digest* in *blockchain* in maniera da sfruttare la funzione di *timestamping* creando un indice univoco.

13.9. *CoinSpark* e *Multichain*

Coin Spark[336] e *Multichain*[337] sono piattaforme della società *Coin Science*[338] che offrono modelli gestibili in autonomia dall'utente.

Coin Spark è rivolta ai privati ed è finalizzata alla creazione di *digital asset e smart contract* che vengono trasferiti automaticamente in *wallet* creati per i sistemi operativi *Linux*, *Mac* and *Windows*: In questo modo

[335] https://ipfs.io/
[336] https://coinspark.org/
[337] http://www.multichain.com/
[338] http://www.slideshare.net/coinspark

la piattaforma consente la gestione diretta sul *pc* dell'utente anziché tramite *web wallet.*

Multichain è invece rivolta a banche e istituzioni finanziarie cui consente la creazione di *blockchain* private[339], creando un ambiente idoneo alla sperimentazione e allo sviluppo di caratteristiche specifiche con tutti i vantaggi tecnici esaminati nella prima parte di questo lavoro.

13.10. *Synereo*

Synereo[340] è un piattaforma creata da una società di Tel Aviv che, parallelamente al progetto base, sviluppa un *social network* basato su *blockchain* per la gestione di quegli elementi che hanno rilievo nella finanza decentralizzata come identità, reputazione *on line* e influenza generata dai *network*. Il sistema è *Turing complete* e si basa sulla *proof of stake;* analogamente ad *Ethereum,* di cui rappresenta un'implementazione, è collegato a una piattaforma autonoma che consente alle applicazioni di girare senza appoggiarsi su server centralizzati. Il progetto è entrato in fase *alpha* a settembre 2016 ed è stata annunciata una *beta release* per il 2017.

[339] http://www.multichain.com/download/MultiChain-White-Paper.pdf
[340] www.synereo.com/

14. Applicazioni e sistemi

14.1. *Interledger*

Uno dei maggiori problemi cui si cerca di porre rimedio è dato dalla difficoltà di trasferire fondi da una piattaforma all'altra: *Interledger* è un sistema di connessione fra *bockchain* rilasciato nel 2015 da Stefan Thomas ed Evan Schwartz di *Ripple*[341]. Il protocollo mette in comunicazione gli intermediari di valuta tradizionale, come le banche, con le piattaforme di gestione delle monete virtuali, consentendo trasferimenti incrociati fra i due mondi economici. Si tratta di un sistema di *escrow* crittografico *top-layer* in cui una serie di nodi dedicati, detti *connector,* gestiscono il flusso delle comunicazione secondo il metodo di funzionamento di Ripple. Nel dicembre 2016 il *report Distributed Ledgers in Payments* della *US Federal Reserve*[342] ha posto l'accento sul modo in cui queste tecnologie possono cambiare la conservazione, la tracciabilità e il trasferimento digitale, sottolineando la loro maggiore efficienza rispetto ai metodi attualmente impiegati. Nei

[341] Stefan Thomas ed Evan Schwartz, A Protocol for Interledger Payments, 2015, https://interledger.org/

[342] Finance and Economics Discussion SeriesDivisions of Research & Statistics and Monetary Affairs Federal Reserve Board Washington D.C, .Distributed ledger technology in payments, clearing, and settlement, 2016, https://www.slideshare.net/IanBeckett3/distributed-ledger-technology-in-payments-clearing-and-settlement-blockchain-fintech

soli *USA* vengono concluse circa 600 milioni di operazioni al giorno per un valore nell'ordine di 12.600 miliardi di dollari[343]: in considerazione di questi volumi di scambio, un protocollo di comunicazione fra registri diversi diventa imprescindibile.

14.2. Eternity Wall

Eternity wall[344] è una *start up* italiana che offre un servizio di *timestamping* per la certificazione su *blockchain Bitcoin:* gli utenti possono inserire l'*hash* di un *file* nel codice di una *moneta* ottenendo una marca temporale con effetti legali. Accanto al servizio di certificazione, il sito offre una attività di messaggistica pubblica che consente l'inserimento di brevi messaggi di testo nel campo della transazione. Al momento, l'offerta prevede un inserimento gratuito al giorno, di certificazione o di messaggistica, e sembra riscuotere il gradimento degli utenti che muovono la *dashboard* con vitalità. Le ingenti dimensioni raggiunte dalla *blockchain* rendono quanto mai attuale la proposta contenuta nel *Bitcoin whitepaper* di una riduzione secondo *Merkel Tree* dei blocchi più remoti, in modo da mantenere la certezza del registro alleggerendone il peso.

14.3. OpenBazaar

Openbazaar è un applicativo nato come risposta agli eventi di *Silk Road* per dimostrare che un *market peer-to-peer* ha effetti positivi ed

[343] Committee on Payment and Market Infrastructures
(2015), *Statistics on Payment, Clearing and Settlement Systems in the CPMI Countries*, http://www.bis.org/cpmi/publ/d142.htm
[344] https://eternitywall.it/

efficienti a livello economico e sociale. Accetta pagamenti nelle monete virtuali più diffuse ed è disponibile per Windows, Mac e Linux. A garanzia di venditori e acquirenti le transazioni vengono eseguite in *multisignature* con l'intervento del *market* in funzione di terzo garante per lo svincolo delle somme alla verifica dell'esecuzione. Il servizio, che non prevede commissioni, viene attuato tramite *Ricardian Contract*, accordi redatti sia in linguaggio umano che analizzabile da una macchina, firmati con chiavi crittografiche e inseriti in *blockchain* tramite *hash*[345]. All'inizio del 2017 il servizio era utilizzato da 300 inserzionisti, con un magazzino di 10.000 oggetti; mentre i contratti conclusi avevano generato 400.000 download[346]. Nei prossimi mesi il sistema integrerà *Inter Planetary File System* e *TOR* per una migliore protezione della riservatezza degli utenti.

14.4. *NXT*

NXT[347] è un sistema *plug-in* che utilizza la tecnologia *blockchain* per la realizzazione di un *network* di pagamento, un sistema di messaggistica e un *online market.* Le monete sono tutte emesse in *pre-mining* e l'aggiunta di voci al registro distribuito è basata sulla *proof of stake.* L'applicazione consente la creazione di *multi signature address,* vincolando l'esecuzione delle transazioni al consenso di un numero predeterminato degli aventi diritto. Tramite la funzione *phase* (lett. graduale) è possibile vincolare l'inserimento in *blockchain* di una transazione al verificarsi di determinate condizioni. Attivando questa opzione l'utente inserirà anche il lasso di tempo entro cui la condizione

[345] The Ricardian Financial Instrument Contract, 2012, http://www.systemics.com/docs/ricardo/issuer/contract.html#index
[346] Pete Rizzo, A New Version of OpenBazaar is Just Months Away, 2017, http://www.coindesk.com/blockchain-e-commerce-openbazaar-just-months-away/
[347] https://nxt.org/

si deve verificare. Allo scadere, se la condizione non si sarà verificata il sistema scarterà la transazione rendendo nuovamente disponibili le somme che erano state impegnate.

14.5. *IBM Adept* e *Watson IoT*

A conferma del grande fermento di mercato attorno alle applicazioni di *block chain* e *DLT,* un attore del calibro di *IBM* sta sviluppando diversi progetti per la messa in sicurezza delle informazioni *IoT*.

ADEPT (*Autonomous Decentralized Peer-to-Peer Telemetry*)[348] è un applicativo per la gestione di questi dati in un network *peer-to-peer* in cui l'aggiunta di dati alla *blockchain* è regolata da un sistema misto *proof of work* / *proof of stake*. Applica i concetti elaborati da sistemi *open* già presenti sul mercato, utilizzando *BitTorrent* per il *file sharing, Ethereum* per gli *smart contract* e il sistema di messaggistica cifrata *TeleHash*[349] per il *peer-to-peer messaging*. L'obiettivo è quello di istituire un registro dei device *IoT* che consenta lo scambio di informazioni per una comunicazione sicura ed economica[350].

Watson IoT[351] nasce invece con lo scopo di consentire ai device *IoT* l'esecuzione di alcune transazioni con invio dei dati a *blockchain* private e conseguente verificabilità pubblica, secondo lo schema di questa struttura dati. Watson è un analizzatore di linguaggio naturale impiegato nel *cognitive computing;* pur applicando lo schema di

[348] ADEPT: An loT Practitioner Perspective, Draft copy for advance review, 2015, https://archive.org/stream/pdfy-esMcC00dKmdo53-_/IBM%20ADEPT%20Practictioner%20Perspective%20-%20Pre%20Publication%20Draft%20-%207%20Jan%202015_djvu.txt
[349] http://telehash.org/
[350]Stan Higgins, IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things, 2015 http://www.coindesk.com/ibm-reveals-proof-concept-*blockchain*-powered-internet-things/
[351]IBM IoT and Blockchain project, http://www.ibm.com/internet-of-things/iot-news/announcements/private-*blockchain*/

blockchain il *focus* principale del sistema è l'apprendimento volto all'identificazione di dati rilevanti all'interno di più ampi flussi di informazioni. Per esempio, uno degli usi proposti riguarda il miglioramento delle applicazioni medicali in modo da correlare le informazioni raccolte a ricerche tecniche e mediche, ottenendo una diagnosi più completa.

14.6. *Slock*.it

Slock è un sistema di *smart lock* che consente di sospendere l'esecuzione di una prestazione *smart* finché non sia intervenuto il pagamento: *l'hash* della transazione viene infatti utilizzato come chiave *smart* per ottenere lo sblocco[352].

Viene proposto per gli *smart contract* del genere *Air B&B* allo scopo di garantire sia la fruizione del servizio che la prestazione e la corretta gestione del deposito cauzionale. Il servizio, che è *smartphone friendly*, al termine del contratto utilizza la piattaforma *Ethereum* per verificare se lo *smart contract* sottostante sia stato eseguito e stabilire se il depositario possa ritirare la cauzione o se la somma debba rimanere al proprietario.

Di recente il servizio è stato esteso al noleggio di *device IoT* e di automobili e costituisce un esempio di *sharing economy* particolarmente apprezzato in Germania, paese in cui la *start up* ha sede, dove a far data dal 2015 il 10% del Pil viene generato da applicazioni di *blockchain* [353].

[352] Ian Allison, Ethereum-based Slock.it reveals first ever lock opened with money, 2015, http://www.ibtimes.co.uk/ethereum-based-slock-reveals-first-ever-lock-opened-money-1527014
[353]Andreas Fisher, Das IoT in der Blockchain, 2017, http://www.onlinepc.ch/business/e-commerce/iot-in-blockchain-1228749.html

14.7. *Enigma*

Enigma è una piattaforma *cloud* decentralizzata sviluppata dai ricercatori degli *MIT Media Lab* per la gestione e la conservazione dei dati su *blockchain* [354].

Si tratta di un sistema *Ripple oriented* che divide le informazioni sulle transazioni in pacchetti di dati distribuiti a gruppi di nodi. Lavorando congiuntamente i nodi processano informazioni a cui nessuno ha accesso singolarmente. In questo modo le transazioni rimangono pubblicamente verificabili ma si protegge la riservatezza degli utenti: per questa ragione nel sistema *Enigma* gli *smart contract* sono denominati *private contract.*

Fra le applicazioni proposte nel *whitepaper* si segnalano quelle relative ai database aziendali, che impediscono agli utenti di estrarre dati completi dal singolo nodo, e quelle relative a *Internet of Things* che, in maniera analoga, mettono in sicurezza i dati contenuti negli *smart device* di uso domestico e quotidiano, affrontando una sfida più che attuale in ambito *privacy.*

14.8. *Everledger*

Everledger è un registro che sfrutta le caratteristiche di immodificabilità della *blockchain* per la tracciabilità dei diamanti e delle transazioni collegate al loro codice identificativo[355]. Il servizio di verifica

[354] http://enigma.media.mit.edu/ *«Enigma is a decentralized cloud platform with guaranteed privacy. Private data is stored, shared and analyzed without ever being fully revealed to any party. Secure multi-party computation, empowered by the blockchain, is the magical technology behind it.»*

[355] https://www.linkedin.com/company/everledger

è rivolto a privati, compagnie di assicurazione e forze dell'ordine[356] e consente di seguire la pietra attraverso l'intera sequenza commerciale. Uno degli scopi del progetto è il contrasto ai c.d. diamanti di sangue: l'inserimento delle informazioni in *blockchain* consente la formazione di *whitelist* o di *blacklist* ai fini di un mercato consapevole e lecito. E' però molto importante notare che *Everledger* registra informazioni eterodeterminate, ragion per cui diviene fondamentale che le pietre vengano correttamente identificate fino dalla fase dell'estrazione. Progetti analoghi si occupano della catalogazione delle opere d'arte, registrando i dati di quelle rubate per il contrasto al mercato nero.

14.9. Storj

*Storj (*pron. *storage)* è un *object storage* basato su *blockchain* che utilizza la crittografia *end to end* e si propone come alternativa a servizi come *Dropbox, Instagram e Spotify.* In un ottica di *share economy*, gli utenti mettono a disposizione lo spazio in esubero sui loro dischi e realizzano un compenso per l'attività di *hosting.* Le informazioni sono crittografate e vengono divise in pacchetti distribuiti fra vari nodi, riservando l'accesso unicamente al titolare delle chiavi crittografiche[357].

Per quanto si tratti di un'idea efficiente dal punto di vista economico, potrebbe essere fonte di alcuni problemi sotto il profilo giuridico. Nel caso di indagini contro uno degli appartenenti al *network,* l'autorità potrebbe infatti disporre il sequestro delle macchine su cui sono distribuiti i dati. Senza contare che indipendentemente dalle indagini in corso non c'è verifica sulla liceità e correttezza del materiale

[356] Jacob Donnelly, Everledger Plans Blockchain Database to Combat Art Fraud, 206, http://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/
[357] https://storj.io/

depositato che potrebbe essere l'oggetto o la prova di un reato. Analoghe considerazioni valgono per la sicurezza degli oggetti depositati che potrebbero sfruttare vulnerabilità della macchina per attivare virus o altri *malware*. Una valutazione ponderata di queste evenienze potrebbe scoraggiare molti dei possibili fornitori di spazio dall'aderire al progetto.

14.10. Torch

Alla fine del 2016 la banca olandese ABM AMRO ha annunciato il lancio di un progetto *blockchain* per la gestione delle transazioni immobiliari[358]. Le informazioni conservate nel registro verranno condivise fra tutti i partecipanti alla compravendita: le parti, il notaio, il perito incaricato della stima, il registro e l'agente immobiliare. Il progetto rappresenta una novità nell'Unione Europea ma non è il primo esempio di questo genere: Svezia, Honduras e la contea di Cook a Chicago (USA) hanno allo studio soluzioni analoghe. La Repubblica di Georgia ha già annunciato l'adozione della *blockchain* per la registrazione dei dati catastali: il progetto sarà operativo entro l'estate[359]. A propria volta lo stato del Kenia intende riformare in questo senso non solo il sistema catastale ma anche quello sanitario e la pubblica istruzione, allo scopo di promuovere la gestione trasparente della cosa pubblica[360]. Analoghe considerazioni sono state formulate dal governo di Dubai che intende mettere in atto la riforma completa dei

[358] Samburaj Das, Dutch Bank ABN AMRO Launches Blockchain Pilot in Commercial Real Estate, 2016, https://www.cryptocoinsnews.com/dutch-bank-abn-amro-launches-*blockchain*-pilot-commercial-real-estate/
[359] Laura Shin, The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project, 2017, https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#431f9e1b4dcd
[360] Muthoki Mumo, IBM eyes Blockchain technology deal for Kenya's public records, 2016

registri pubblici trasferendo tutte le informazioni su *blockchain* entro il 2020.

Conclusioni

15. Una trasformazione poliedrica

L'analisi che abbiamo svolto ha evidenziato che *blockchian* e *distrubuted ledger* sono in grado di trasformare sensibilmente molti dei contesti in cui si svolge la nostra vita interagendo in primo luogo con il sistema monetario ma anche con quello giuridico e con la conservazione dei dati: lo sviluppo di queste tecnologie crea un nuovo modello economico e apre nuove prospettive di ricerca. In considerazione dello sviluppo storico di questi sistemi, divideremo il capitolo in paragrafi che offrano rilievo a ognuna delle macro istanze delineate. La parte più ampia del discorso riguarderà la funzione di pagamento perché è il settore originario in cui si sono svolte la maggior parte delle vicende che hanno avuto ad oggetto questi sistemi: da qui ha preso avvio il settore del *fintech* e qui sono intervenuti la maggior parte dei provvedimenti autoritativi, sia di veto che di (parziale) regolamentazione. Seguirà una parte dedicata agli *smart contract* e alle possibilità di apertura del sistema giuridico che essi implicano, generando un nuova dimensione del diritto civile in larga parte ancora da scoprire. Infine, formuleremo

alcune riflessioni riguardo la funzione di conservazione dei dati e il modo in cui cambiano la gestione istituzionale, da un lato, e le prospettive di mercato dall'altro, rivolgendo lo sguardo alla *network security* che, anche in questo settore, costituisce una disciplina fondamentale.

15.1. Il mercato delle monete virtuali

Nel corso dell'analisi abbiamo evidenziato più volte l'influenza di provvedimenti economici e investimenti strutturati sull'andamento del valore di cambio: sicuramente vi è una parte degli utenti che mostra di considerare insostituibile la tutela della riservatezza, ma sono state le operazioni economiche su larga scala che hanno spronato in crescita il valore delle monete virtuali. In questo senso gli economisti e le istituzioni europee hanno messo in guardia i risparmiatori dal rischio di una bolla speculativa fino dal 2013: nonostante questi strumenti abbiano molto da offrire al *fintech* non si può sottovalutare l'eventualità prospettata, né si possono ignorare i rischi legati all'uso degli strumenti derivati. Nel 2013 gli investimenti ad alto rischio avevano trasformato i *bitcoin* in uno degli strumenti finanziari più rischiosi in circolazione[361] rendendo il loro valore troppo volatile per l'uso di massa; dopo un periodo di forti oscillazioni il cambio si è posizionato su un *trend* più costante e al giorno d'oggi le variazioni di prezzo conoscono un

[361]David Yermack, *Is Bitcoin a Real Currency?* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599 2013 :"*Bitcoin's exchange rate volatility since the start of 2013 has been 133%, an order of magnitude higher than the exchange rate volatilities of the other currencies, which fall between 8% and 12%. Gold, which is a plausible alternative to these currencies as a store of value, has had volatility of 22% since the start of 2013. For comparison purposes, most widely traded stocks have volatilities in the range of 20% to 30%, and even very risky stocks rarely exhibit volatility as high as 100%".*

movimento più contenuto. Cionondimeno, è opportuno tenere presente che le procedure di liquidazione dei cespiti ad alto prezzo e il conseguente rimbalzo tecnico possono produrre movimenti di mercato molto forti. Le monete virtuali non fanno eccezione a questa regola: nel mese di maggio 2017 le quotazioni raggiunte dalle varie divise hanno provocato vendite di massa che hanno fatto crollare i valori *intraday* anche di diverse centinaia di dollari, con perdite ingenti a carico degli investitori.

In questi anni il mercato delle monete virtuali ha espresso uno spettro di valori differenziato che va dai pochi centesimi degli *xrp* di *Ripple* alle migliaia di dollari dei *bitcoin.* Alcuni di questi strumenti, come gli *ether,* hanno conosciuto in pochi mesi un incremento di valore oltre il 5.000% passando da $8 nel gennaio 2017 a $410 il successivo 12 giugno[362]. Ad oggi i sistemi di pagamento basati su *blockchain* e *distributed ledger* rappresentano uno strumento efficiente che, in termini di riservatezza, ha effetti analoghi a quello del denaro contante: questo settore presenta ottime potenzialità di sviluppo nel mercato globale, come dimostra la decisione di *Paypal* che aveva consentito agli esercenti del nord America di accettare *bitcoin* già nel 2014[363].

15.2. Provvedimenti di veto

È proprio a causa della loro efficienza che i *bitcoin* sono stati largamente adottati a fini elusivi, inducendo Stati del calibro di Cina e Russia a intervenire con divieti all'uso di tipo drastico negli anni fra il 2013 e il 2016[364]. Questa prospettiva ha rappresentato, però, uno

[362] *Vide http://coinmarketcap.com/*
[363] Filippo Vendrame, PayPal introduce il supporto ai Bitcoin, 2014, http://www.webnews.it/2014/09/24/paypal-introduce-il-supporto-ai-bitcoin/
[364] Addirittura in Cina si è avuto un bando completo: alla fine di marzo 2014 la Banca Centrale ha imposto ai servizi terzi di pagamento di interrompere le transazioni con

spostamento del problema e non la sua soluzione: quando la Cina ha vietato a banche e imprese l'uso dei *bitcoin,* il mercato locale, che già raggiungeva volumi secondi solo agli *USA*, sembrava in un primo momento destinato a trovare accoglienza nella vicina Hong Kong, improntata alla tolleranza del libero mercato[365]. Invece i privati, che erano rimasti esenti dal provvedimento di veto, hanno sfruttato il basso costo locale dell'energia elettrica per dare sviluppo alle *mining pool,* costruendo così le basi di quello che è diventato il nuovo mercato di riferimento.

Bisogna, inoltre, considerare che anche mettendo al bando *bitcoin* e strumenti analoghi non si riesce comunque a risolvere il problema delle transazioni anonime, al cui contrasto mira invece questa previsione. Il veto autoritativo non può che svolgere effetti sulla fisiologia dello strumento, impedendo le transazioni alla luce del sole e con ciò precludendo lo sviluppo di una larga fetta di mercato; ma non esistono briglie legali applicabili alla matematica e tutto lascia prevedere che in caso di veto le monete virtuali continuerebbero a funzionare in *TOR* secondo i parametri originali. Se messe al bando, le *digital currency* si trasformerebbero effettivamente in criptomoneta, divenendo la divisa di scambio dell'*online blackmarket* e lo strumento privilegiato del *money laundering*[366] e di altre attività illecite: nel 2014, appena la Russia ha vietato l'uso dei *bitcoin,* un *ransomware* proveniente da San Pietroburgo

---

qualunque soggetto inserito nel commercio dei *bitcoin* mentre nel mese di aprile i *bitcoin dealers* hanno ricevuto una formale notifica che li invitava a ritirare quanto depositato nei dei conti loro intestati, destinati ad essere congelati dopo 15 giorni http://www.techinasia.com/china-banks-must-close-*bitcoin*-trading-bank1-accounts/ 2014.

[365]http://english.caixin.com/2014-03-27/100657518.html

[366]Nel 2013 il sospetto di riciclaggio ha indotto molti istituti di credito statunitensi al rifiuto dei bonifici provenienti da exchange non regolamentati per mancanza di tracciabilità. Anche Mt.Gox aveva avuto problemi di liquidità perché molte banche erano rifiutate di ricevere i bonifici effettuati dal sito con valuta di cui non si riusciva a individuare la provenienza: sotto questo profilo non era stata di aiuto la mancata dichiarazione a fini fiscali delle transazioni, per quanto lecitamente intervenute.
Sandro Iannacone, Mt. Gox è in rosso per oltre 10 milioni di dollari, 2013, http://daily.wired.it/news/economia/2013/09/17/mt-gox-*bitcoin*-rosso-oltre-10-milioni-dollari-564654.html

ha infettato via *mail* i *computer* di molti Comuni, anche italiani, chiedendo un riscatto di €400 da pagare in *bitcoin*[367]. Lo stato delle cose non è certo migliorato nel 2016 quando è stata proposta l'adozione di sanzioni criminali contro i produttori e gli utilizzatori di 'surrogati monetari'.

Nel novembre 2016 il dibattito sul veto ha trovato eco anche nell'Unione Europea, facendo seguito alle dichiarazioni del *senior officer* ESMA (*European Securities and Markets Authority*) Patrick Armstrong alla conferenza londinese '*Blockchain Technology: The Future for Financial Services'*. Il funzionario ha ricordato che dal gennaio 2018 la Direttiva sui Mercati Finanziari MIFID II consentirà l'emanazione di provvedimenti di messa al bando di *blockchain* e *DLT*[368]. Armstrong ha specificato che si tratta solo di un'ipotesi, poiché al momento l'Agenzia non vede nelle *DLT* una fonte di pericolo e preferisce rimanere in attesa per valutare quelli che saranno gli effettivi sviluppi di mercato; ciononostante, la sola prospettazione di provvedimenti restrittivi ha messo in subbuglio gli addetti ai lavori.

Nel febbraio 2017 la *vexata quaestio* ha trovato soluzione quando l'ESMA ha presentato il report '*The Distributed Ledger Technology*

---

[367] Giusepe Guastella, La mail pirata attacca i Comuni E il riscatto va pagato in bitcoin, 2014,
http://www.corriere.it/tecnologia/economia-digitale/14_ottobre_20/phishing-comuni-hacker-bitcoin-ricatto-c457694c-5831-11e4-9d12-161d65536dad.shtml
Gli hacker offrivano anche un servizio di *help desk,* nel caso si fossero verificati problemi di installazione del *software* di decrittazione: per quanto possa sembrare una beffa, questo atteggiamento risponde a una precisa strategia di mercato. In un contesto come quello in cui si è svolta la trattativa, caratterizzato dall' extralegalità, la mancanza di regole attivabili in giudizio viene compensata dalla reputazione del venditore: se, ottenuto il pagamento, egli adempirà scrupolosamente a quanto promesso, in futuro ulteriori soggetti si determineranno all'acquisto; viceversa, si spargerà la voce che inviare denaro è inutile e i malcapitati destinatari del *malware* non prenderanno in considerazione la richiesta ricevuta. *Vide*: Gregory Mankiw, Mark Taylor,: Principi di microeconomia, Zanichelli, Bologna 2012.

[368] https://www.esma.europa.eu/sites/default/files/library/2016-1613_1.pdf

Applied to Securities Markets'[369] con queste testuali parole: '*ESMA believes that DLT could bring a number of benefits to financial markets, including more efficient post-trade services, enhanced reporting capabilities and reduced costs*'[370].

Nella primavera 2017 anche la Russia ha invertito rotta dichiarando che le monete virtuali saranno legalizzate a fini di contrasto al riciclaggio.

La scelta di integrare questo mercato è di per sé efficiente: *PWC* ha stimato che tra febbraio e ottobre 2016 *blockchain* e *distributed ledger* abbiano procurato investimenti per $ 1.400.000.000[371], e attualmente il *trend* è positivo, come dimostra la *IPO* di *Bancor*, un sistema di ispirato alla moneta bancaria proposta da John Maynard Keynes, che il 13 giugno 2017 ha raccolto 153.000.000 in *crowdfunding*[372].

Allo stato dell'arte, c'è grande attesa per la regolamentazione cinese che dovrebbe vedere la luce entro la fine del mese di giugno 2017: il Governo e la *PBoC* hanno infatti dichiarato in più occasioni che le monete virtuali, e in particolar modo i *bitcoin,* costituiscono uno strumento di fuga dallo *Yuan* cui occorre porre un freno e questi *warning* ufficiali sono spesso stati la causa di crolli delle quotazioni di mercato[373]. Gran parte delle perplessità che sono state manifestate a livello istituzionale troverebbe, a nostro parere, soluzione adottando una

[369] https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
[370] https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt%E2%80%99s-potential-and-interactions-eu-rules
[371] John Kennedy, $1.4bn investment in blockchain start-ups in last 9 months, says PwC expert, 2016, http://linkis.com/Ayjzj
[372] Blockchain : la fondation du protocole Bancor lève 153 millions de dollars, 2017, http://www.linformaticien.com/actualites/id/44234/blockchain-la-fondation-du-protocole-bancor-leve-153-millions-de-dollars.aspx
[373] Giuseppe Timpone, Bitcoin, crollo del 20% sul "warning" cinese: ecco perché Pechino è preoccupata, 2017, https://www.investireoggi.it/economia/bitcoin-crollo-del-20-sul-warning-cinese-perche-pechino-preoccupata/

costruzione normativa che tenga in considerazione i valori che costituiscono il fondamento delle scelte dei consociati[374].

15.3. Soluzione istituzionale

Gli ordinamenti si confrontano quotidianamente con esigenze di garanzia dell'assetto sociale ed economico attuate tramite il controllo dei flussi finanziari: una delle possibilità di regolamentazione consiste nel dare rilievo alle caratteristiche monetarie che questi strumenti sicuramente rivestono sul piano economico, considerandoli come monete elettroniche ai sensi di legge e riservandone emissione e intermediazione alle sole Banche Centrali e istituti autorizzati.

Questa decisione decreterebbe la fine delle monete virtuali così come le conosciamo adesso o, meglio, decreterebbe la fine del sistema decentralizzato che perderebbe la natura libertaria che lo ha caratterizzato fino dagli inizi per divenire uno strumento a servizio degli enti centrali. Una volta istituzionalizzata la rete, verrebbero con ogni probabilità imposti dei costi di transazione di tipo burocratico riducendo così i vantaggi economici dei privati. Si tratta di una prospettiva in cui un sistema di pagamento nato per consentire agli utenti di scrollarsi di dosso le pastoie e i costi di istituzioni considerate troppo pesanti a livello burocratico, verrebbe assunto, per l'efficienza dimostrata, a strumento di punta nella moneta istituzionale del nuovo millennio.

---

[374] *Vide* Guido Calabresi, Of Tastes and Values, 2014, Yale Law & Economics Research Paper No. 500: *" The relationship between values and legal rules is admittedly highly complex. Sometimes promulgation of a legal rule furthers the values that it seeks to espouse; sometimes it brings forth a backlash and a growth of counter-values; sometimes it does a little of both. Accordingly, lawmakers must be more than wary in pushing laws in order to bring about what they deem desirable values. But that does not mean that such a lawmaker would not benefit, and benefit immensely, from scholarly analyses of what tastes and values, and sub-tastes and values, are worth pursuing."* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483947

A nostro parere, questa soluzione si rivelerebbe di scarsa efficienza, venendo con ogni probabilità a creare un problema di bipartizione del mercato: la funzionalità delle monete virtuali è tale da offrire agli utenti un incentivo a forzare le regole piuttosto che ad adattarsi pacificamente ad esse e a fianco della gestione istituzionale si verrebbe verosimilmente a generare un'attività di *dark web* analoga a quella prodotta da una procedura di veto.

15.4. Soluzione di mercato

Più che nella creazione di un monopolio istituzionale, riteniamo che una soluzione efficiente del problema potrebbe consistere nel mantenere il sistema delle monete virtuali inalterato, intervenendo invece sui presupposti di liceità del pagamento e sui comportamenti devianti. Nell'esercizio della funzione solutoria le monete virtuali non differiscono concettualmente dalla valuta e le medesime norme antiriciclaggio che consentono il pagamento in denaro contante al disotto di un determinato ammontare, si rivelano idonee a stabilire i limiti entro cui è ammissibile l'anonimato digitale.

Il ritorno di mercato delle monete virtuali suggerisce di adottare soluzioni normative tese alla definizione dell'ambito di legittimità e dei requisiti identificativi per gli utenti di questi schemi, in modo che gli Ordinamenti possano beneficiare degli effetti di un sistema di scambi pubblici e tracciati. L'integrazione presenterebbe il vantaggio di consentire l'uso legittimo del denaro virtuale secondo parametri prestabiliti e, permettendo agli utenti della rete di fruire di tutti i benefici relativi allo strumento, avrebbe maggiori probabilità di essere effettiva. Riteniamo, inoltre che dovrebbero essere oggetto di regolamentazione anche i provvedimenti di tutela degli investitori.

De jure condendo, è auspicabile una regolamentazione armonizzata a livello internazionale*:* l'azione in un mercato globale prevede la creazione di regole di comportamento omogenee, in modo da ridurre gli incentivi al *free riding* basati sulla scelta del'ordinamento più conveniente (c.d. *forum shopping*). Il panorama dei mercati finanziari è radicalmente cambiato negli ultimi tre anni e le applicazioni di *fintech* sono diventate all'ordine del giorno*:* solo per citare alcuni esempi, le banche riunite nel consorzio R3 studiano ogni possibile applicazione al mercato finanziario, Barbados ha già all'attivo un piano di emissione del dollaro locale, mentre la Palestina pianifica di emettere nel medesimo modo la moneta di cui dovrebbe essere dotata nel prossimo futuro[375]. Nelle vicende legate al mercato dei capitali, è il diritto che plasmandosi segue l'evoluzione della società: diventa fondamnetale emettere regole armonizzate, per ridurre al minimo l'evenienza di casi come quello della piattaforma *Mt.Gox* che ha richiesto negli *USA* la protezione dalle azioni personali dei creditori, in modo da eludere le conseguenze del *default* cui era andata soggetta in Giappone[376].

Gli Stati potrebbero, ad esempio, stabilire al verificarsi di quali presupposti ricorra una presunzione uniforme di liceità delle transazioni, ad esempio quando esse provengano da un indirizzo correttamente agganciato a dati anagrafici reali: questo consentirebbe di risolvere, almeno in parte, i problemi di natura fiscale che finora sono

---

[375] Alex Lielacher, Palestine May Launch Its Own Cryptocurrency as Sovereign Legal Tender, 2017, https://bitcoinmagazine.com/articles/palestine-may-launch-its-own-cryptocurrency-sovereign-legal-tender/

[376]Il caso è significativo di quanto possa essere deleterio prendere decisioni normative locali riguardo fenomeni globalizzati: la società era stata costituita in un sistema che, allo stato attuale considera i *bitcoin* come un fenomeno diverso dalla moneta, anche se, in circostanze da specificare, si riserva di introdurre tassazione e controlli antiriciclaggio, v*ide* http://www.reuters.com/article/2014/03/07/us-*bitcoin*-mtgox-japan-idUSBREA2601Z20140307. Prendendo le mosse proprio da questo caso, il *New York State Department of Financial Services* ha disposto che nel prossimo futuro le piattaforme di cambio saranno soggette a una regolamentazione analoga a quella di Banche e servizi di intermediazione finanziaria; si tratta però di legge statale, e non federale, argomento che ripropone il problema della discrasia normativa *vide* http://www.inc.com/jeremy-quittner/lawsky-and-new-virtual-currency-regulations-for-new-york.html

stati sollevati da più parti. Si potrebbe, inoltre, stabilire di concerto la soglia di valore al di sotto della quale gli uffici finanziari perdono interesse oggettivo all'accertamento delle transazioni intervenute, senza preclusione alcuna per le indagini di polizia, disponendo in maniera analoga al tetto di valore massimo degli acquisiti che possono essere effettuati in contante.

La predisposizione di forme di garanzia obbligatoria dei depositi rappresenta un punto nevralgico e dovrebbe godere di un adeguato livello di attenzione: il fenomeno ha assunto contorni troppo ampi perché gli Stati possano concedere l'autorizzazione ad operare alle piattaforme di cambio prescindendo da questa forma di tutela dei risparmiatori. Il problema sollevato nel tempo dai furti ai danni degli *exchange* è consistito proprio nella loro diretta riferibilità agli investitori, senza l'interposizione di alcun filtro da parte delle piattaforme.

Non è dato prevedere nel dettaglio i contenuti dei testi normativi che verranno adottati ma la IV Direttiva Antiriciclaggio ha introdotto il concetto di valuta virtuale come '*mezzo di scambio per l'acquisto di beni e servizi*'. Poiché l'utilizzo della crittografia rende praticamente impossibile intervenire in via diretta sulle monete virtuali, riteniamo che la normativa di armonizzazione manterrà con ogni probabilità questa equivalenza alla base dei futuri interventi.

15.5. Gli *Smart Contract*: verso una nuova forma di espressione della libertà contrattuale

Il trasferimento di diritti tramite registro distribuito individua una nuova frontiera del diritto, in maniera analoga a quello che accadde quando venne formulato il concetto di proprietà spazio-temporale, la c.d. multiproprietà, dando vita a un'espansione dell'istituto classico e consentendo un modo nuovo di fruizione del diritto[377]; rispetto a quell'innovazione che ha ad oggetto diritti reali, retti dal principio del *numerus clausus*, l'ambito di applicazione della nuova disciplina incide su un'area regolata dal principio di atipicità: i consociati saranno perciò liberi di formulare il regolamento contrattuale con il solo limite di realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico, ex art 1322 c.c..

La declinazione delle clausole in termini informatici consente di prevenire i problemi legati all'inadempimento, mettendo in esecuzione automatica tutte le prestazioni digitalizzabili: gli *script* associati al contratto vengono inseriti in un *token* e i nodi li processando eseguendo l'attività come previsto sul sistema.

Negli *smart contract*, la tutela giudiziale cede così il passo all'esecuzione automatica mantenendo, tuttavia, inalterata la capacità

[377] Decreto legislativo 9 novembre 1998, n. 427: Attuazione della direttiva 94/47/CE concernente la tutela dell'acquirente per taluni aspetti dei contratti relativi all'acquisizione di un diritto di godimento a tempo parziale di beni immobili sostituito dal Decreto legislativo 6 settembre 2005 n. 206 e successive modifiche, c.d. Codice del Consumo

di intervento a correzione delle eventuali patologie: l'irreversibilità informatica delle operazioni di *blockchain* trova una forma di bilanciamento nel sistema delle rivalse tipico del diritto civile. Indipendentemente dal metodo digitale di espressione, il contratto rimane regolato e tutelato dalla legge e le parti saranno comunque libere di adire le istanze giudiziarie per porre rimedio all'esecuzione automatica di un contratto invalido o la cui attuazione sia affetta da un malfunzionamento provocato da *bug* di sistema.

A differenza dei sistemi di trasferimento di moneta virtuale basati su *blockchain*, ormai ampiamente funzionali, gli *smart contract* sono in fase di realizzazione e la loro elasticità implementativa non consente ancora di formalizzare un sistema univoco. Si tratta di un modello nuovo, ancora da regolamentare a livello giuridico. Lo studio delle potenzialità di mercato dei sistemi basati su *blockchain* è soltanto all'inizio: questo interessante modello matematico è stato sviluppato per fare fronte alle necessità libertarie sollevate dall'interpretazione restrittiva delle regole *anti money laundering USA;* la loro dimostrazione di efficienza li ha resi oggetto di attenzione in ambito istituzionale ed economico, contesti lontani più che mai dal principio che eleva la libertà totale di pensiero e di azione a massimo valore nella vita.

È proprio la razionalità del sistema binario che rende il dato digitale maggiormente idoneo di altri alle operazioni di governo del mercato e il diritto, in questo contesto, si limita a seguire l'evoluzione della società, ponendo regole di confine che, almeno in linea teorica, dovrebbero sostenere l'iniziativa privata, senza imbrigliarla. Inglobare i sistemi di *hashing* nelle regole di diritto generali rappresenta, a nostro parere, un vantaggio per i consociati: inserendo i dettagli delle transazioni nel registro di *blockchain* si potrebbe fruire di maggiore certezza nei traffici giuridici, con riduzione dei costi di gestione: l'introduzione di clausole *self-enforcing* renderebbe questi modelli ancora più efficienti; troviamo opportuno ribadire che la corretta attuazione di questi schemi

innovativi passa imprescindibilmente per la messa in opera di regole di concerto internazionali che sottraggano ogni incentivo al *forum shopping*. La ricerca futura volta alla costruzione del modello non potrà prescindere dalla considerazione che lo schema di *blockchain* è espressione di una scuola di pensiero che eleva a valore di vita l'esercizio della libertà in un sistema trasparente, un principio applicato costantemente dalla corrente del *software Open Source*. Si tratta di una gamma di argomenti ampia e interessante la cui analisi dovrà tenere conto anche delle istanze manifestate dalla comunità *Bitcoin* che ha espresso e continua a implementare il paradigma di *blockchain.*

15.6. La funzione di certificazione: vantaggi istituzionali dei nuovi sistemi

Alcuni Governi locali hanno già preso in considerazione i vantaggi offerti dai registri distribuiti: lo scorso anno la Repubblica di Georgia ha avviato la riforma in questo senso del registro catastale e si prevede che le nuove iscrizioni saranno possibili a partire dal mese di luglio 2017. Si tratta di una modifica particolarmente efficiente che porterà una gestione trasparente e più economica della cosa pubblica. Le operazioni che fino ad oggi sono state registrate nei registri separati di uffici analoghi ai nostri Catasto e Conservatoria verranno unificate in un *database* distribuito: dall'aprile del 2016 sono già stati registrati oltre 100.000 atti e una volta entrato a regime il sistema gestirà anche mutui, demolizioni e servizi notarili. A seguito della disgregazione dell'URSS molti registri della proprietà georgiani erano andati distrutti e la ricostruzione in termini digitali consente un risparmio sulle spese di

attività e di gestione, dando vita a un servizio innovativo in cui la prova dell'identità del titolare e della proprietà del bene possono essere offerte senza rivelare dati personali. Modifiche analoghe sono allo studio in Svezia e nel Regno Unito[378].

Anche lo stato del Kenia ha allo studio una riforma analoga ma su scala maggiore: il progetto qui riguarda anche il servizio sanitario e la pubblica istruzione, allo scopo di consentire una gestione rapida ed efficace dei dati, salvaguardando la riservatezza del titolare. I registri distribuiti creano un sistema di *identity trust* in cui al posto dell'identità reale viene inserita quella digitale, idoneamente protetta da crittografia; il servizio sanitario organizzato in *DLT* amministrerà così i dati relativi a vaccini, malattie, cure, interventi, medicinali, dispositivi biomedicali, procedure *cross trial* e simili con assoluta precisione e tutela della *privacy* dei pazienti, fornendo un registro immodificabile delle attività da cui risulteranno accessi e prescrizioni.

Analogo discorso vale per il sistema scolastico, dove la corretta registrazione dei traguardi raggiunti dagli studenti consentirà di rendere più efficiente la gestione delle qualifiche, specialmente nei casi in cui abbiano valore di titolo di stato, e ne agevolerà il riconoscimento internazionale facilitando la mobilità nella società globalizzata. Anche in questo caso il registro parteciperà dei benefici della *blockchain* divenendo inalterabile e fornendo prova legalmente valida di tutte le attività inserite.

A propria volta, l'emirato di Dubai darà inizio alla riforma dei registri pubblici, che intende completare entro il 2020, emettendo i primi passaporti su *blockchain*. L'uso di questo modello consentirà la gestione efficiente delle istanze relative alla certificazione dell'identità: infatti, considerato che ogni manomissione del sistema crea una biforcazione

[378] Lester Coleman, U.K. Land Registry Looks to Register Property on a Blockchain, 2017, https://www.cryptocoinsnews.com/u-k-land-registry-looks-register-property-blockchain/

della catena logica, eventuali corpi estranei saranno immediatamente riconoscibili. La possibilità di individuare digitalmente ogni falso nell'emissione dei documenti di identità si rifletterà positivamente sulla sicurezza nazionale, senza contare che l'applicazione di questo modello risulterà vantaggiosa anche in termini economici: utilizzando *Bitcoin* i 2.800.000 cittadini di Dubai potranno essere identificati inserendo in *blockchain* una transazione da 1 *satoshi* per ognuno, con una spesa complessiva di 28 *millibitcoin*[379]; ma esistono registri come quello di *Ripple* che offrono monete molto più economiche[380]. Le spese generate dalla predisposizione e dalla gestione del nuovo registro sono comunque inferiori a quelle richieste dalla sola amministrazione dei registri tradizionali, che richiedono impiegati, uffici e dotazioni, e la modifica apporta dei vantaggi indiscutibili dal punto di vista della sicurezza.

15.7. Progetti per *IoT*

A livello sociale i registri distribuiti godono di un discreto successo fino dal 2011: la novità di un sistema decentralizzato, privo di imposizioni da parte dell'autorità, ha destato velocemente l'interesse degli utenti della rete, da sempre sostenitori della più ampia forma di libertà. Probabilmente nel successo iniziale del progetto ha giocato un ruolo anche la curiosità accesa da un progetto che in qualche modo tornava alle origini, consentendo a ognuno di creare la propria ricchezza in maniera analoga a quella in cui i minatori dell'*old west* estraevano l'oro dalle miniere. Ad ogni modo, l'evoluzione del sistema ha portato novità interessanti in molti settori del quotidiano estendendo la tutela della *privacy* a settori che inizialmente non sembravano avere punti in comune con il piano di Satoshi Nakamoto.

[379] pari, al cambio attuale, a poco meno di $ 90
[380] In questo caso la spesa sarebbe di $0,9

Ad oggi uno dei settori in maggiore fermento è quello dell'*Internet of Things* che rappresenta un mercato del valore di miliardi di dollari, destinato a incrementarsi nel tempo: i progetti attuali stanno studiando un modo di sfruttare la messaggistica sicura della *blockchain* per la gestione delle comunicazioni fra oggetti *smart*. Tenuto presente che larga parte dei dati rappresenta la c.d. lista della spesa, è molto probabile che per l'archiviazione di queste comunicazioni verranno sviluppate delle *sidechain* o dei metodi analoghi a quello adottato da *NXT* con le *prunable transaction* che consentono di mantenere i dati in una copia locale della *blockchain* per un tempo determinato, procedendo poi alla loro cancellazione.

Considerati i volumi di denaro in gioco, l'argomento *IoT* introduce un'istanza della massima importanza, espressa in termini *network security:* infatti, spostare i dati su *blockchain* per garantire la comunicazione sicura fra *device* che possono nascere privi di *password* è un *nonsense*. Le recenti vicende di *Mirai* hanno messo in evidenza che gli utenti spesso non hanno modo di intervenire nella gestione delle credenziali, preimpostate da molte aziende tutte coi medesimi valori.

La *network security* è, fondamentalmente, una questione di scelte opportune e la struttura dati prescelta, per quanto efficiente, non può supplire a carenze dal lato umano: la situazione non sarebbe molto diversa da quella in cui dopo aver installato una serie di dispositivi di sicurezza in casa, si lasciassero porte e finestre aperte al mondo.

Inoltre spesso la struttura di registro distribuito non è compatibile con quella dei *device* IoT: molti di questi strumenti sono costruiti in maniera incompatibile con il *download* , si pensi ai sensori che possono caricare dati in rete ma non archiviarli; altri strumenti, pur avendo capacità di *storage,* non sono in grado di processare quantità di informazioni elevate come quelle richieste per la partecipazione alle operazioni di *blockchain.*

I progetti per *IoT* sono ancora in fase di studio e riteniamo che allo stato dell'arte l'analisi sarebbe prematura; per il momento ci limitiamo a formulare un invito alla riflessione sul fattore sicurezza, suggerendo un uso ponderato di queste strutture.

15.8. Prospettive di ricerca

I registri distribuiti costituiscono una grande innovazione sotto molteplici profili: il settore originario di intervento è stato quello dell'informatica dove la ricerca è cominciata per prima e che oggi conosce i traguardi più avanzati.

Ogni giorno vengono esplorate nuove possibilità e i confini di questa materia continuano ad allargarsi verso la linea del'orizzonte. Ad oggi i sistemi nati per il pagamento vengono utilizzati anche per il trasferimento di diritti, la certificazione e la conservazione documentale: sono allo studio i sistemi di voto e molte altre implementazioni.

Questo fermento creativo si è riverberato sul mercato, facendo del settore economico il secondo ambito di ricerca in ordine temporale: l'ambito *fintech* conosce già la contrattazione di derivati tramite *blockchain*[381] e i grandi gruppi bancari stanno lavorando per riorganizzare il sistema dei pagamenti intercontinentali su registro distribuito.

I movimenti economici hanno chiamato in causa il terzo settore della ricerca, rappresentato dal diritto: ai giuristi spetta il compito di individuare la normativa idonea a sostenere le nuove attività produttive

[381] Arjun Kharpal, Barclays used blockchain tech to trade derivatives, 2016, http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html

senza imbrigliarle, tenendo conto anche della vocazione internazionale della materia.

Lo studio della normativa applicabile ai sistemi distribuiti non è che all'inizio e le previsioni sono favorevoli a un'analisi approfondita in ognuno dei settori interessati da questa importante novità. Dal canto nostro, troviamo adeguata la scelta di un metodo basato sulla interdisciplinarità: l'organizzazione del percorso accademico proposto dal CIRSFID dell'Università di Bologna ci ha portato a un confronto costante con esperti di settori diversi dal nostro, tutti ugualmente importanti nella determinazione del nostro pensiero: riteniamo che non sarebbe stato possibile conseguire risultati altrettanto approfonditi in un ambiente monodisciplinare e suggeriamo l'adozione di questo approccio per la ricerca futura.

BIBLIOGRAFIA E SITI

1) 1923 - quando un chilo di pane costava 400 miliardi di marchi http://www.viaggio-in-germania.de/inflazione-1923.html
2) Accenture Newsroom, Prototype of editable blockchain, 2017, https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm
3) Accenture, Top 10 challenges for investments banks 2017, Blockchain moves to early adoption https://www.accenture.com/us-en/insight-investment-bank-challenge-10-distributed-ledgers
4) Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuill, Enabling Blockchain Innovations with Pegged Sidechains, 2014, https://blockstream.com/sidechains.pdf
5) ADEPT: An loT Practitioner Perspective, Draft copy for advance review, 2015, https://archive.org/stream/pdfy-esMcC00dKmdo53-_/IBM%20ADEPT%20Practictioner%20Perspective%20-%20Pre%20Publication%20Draft%20-%207%20Jan%202015_djvu.txt
6) Agenzia delle Entrate, Risoluzione 02/09/2016 n° 72 www.agenziaentrate.gov.it/
7) Alyson, Famous Bitcoin Transactions & The Stories Behind Them, 2016, https://blog.blockchain.com/2016/07/13/famous-bitcoin-transactions-the-stories-behind-them/
8) Andrea Bai, Bitcoin: è la moneta del futuro? 2013, http://www.businessmagazine.it/articoli/3710/bitcoin-la-moneta-del-futuro_4.html.
9) Andreas Fisher, Das IoT in der Blockchain, 2017, http://www.onlinepc.ch/business/e-commerce/iot-in-blockchain-1228749.html
10) Ari Juels, Ahmed Kosba, Elaine Shi, The Ring of Gyges: Using Smart Contracts for Crime, 2015, http://www.arijuels.com/wp-content/uploads/2013/09/public_gyges.pdf
11) Arizona House bill 2417, 2017 https://legiscan.com/AZ/text/HB2417/2017
12) Arjun Carpal, Bitcoin value rises over $1 billion as Japan, Russia move to legitimize cryptocurrency, 2017 http://www.cnbc.com/2017/04/12/bitcoin-price-rises-japan-russia-regulation.html
13) As Certain as Death and Taxes: Consumer Considerations of Bitcoin Transactions for When the IRS Comes Knocking by Jennifer Isom, University of New Mexico - School of Law, 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2365493
14) Baidu Stops Accepting Bitcoins After China Ban, 2013 http://www.bloomberg.com/news/2013-12-07/baidu-stops-accepting-bitcoins-after-china-ban.html
15) Bailey Reutzel, Disruptor Chris Larsen Returns with a Bitcoin-Like Payment System, 2012, https://www.americanbanker.com/news/disruptor-chris-larsen-returns-with-a-bitcoin-like-payment-system
16) Bank of America Merrill Lynch: Bitcoin a first assessment, 2013 http://cryptome.org/2013/12/boa-bitcoin.pdf

17) Bank of America ve al bitcoin como “un serio competidor” 2013 http://tecnologia.elpais.com/tecnologia/2013/12/06/actualidad/1386326468_153216.html
18) BBC News - E-Sports Entertainment settles Bitcoin botnet allegations 2013 http://www.bbc.co.uk/news/technology-25014477
19) BCE virtual currency schemes, 2012, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
20) BIPS Bitcoin exchange cleaned out in $990K virtual heist 2013 http://siliconangle.com/blog/2013/11/26/bips-bitcoin-exchange-cleaned-out-in-990k-virtual-heist/
21) Bitcoin and Money Laundering: Mining for an Effective Solution by Danton Bryans 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317990
22) Bitcoin Apple riapre la App Blockchain, 2014 http://www.ansa.it/sito/notizie/tecnologia/internet_social/2014/07/29/bitcoin-apple-riapre-ad-app-blockchain_70d554ee-c079-474c-a94a-f832bb5cdc37.html
23) Bitcoin becomes commodity in Finland after failing currency test, 2014 http://www.bloomberg.com/news/2014-01-19/bitcoin-becomes-commodity-in-finland-after-failing-currency-test.html
24) Bitcoin crashes after warning from China, 2013 http://www.businessinsider.com/bitcoin-falls-after-china-warning-2013-12
25) Bitcoin Forenscs http://www.bitcoinforensics.it/
26) Bitcoin Forum, List of bitcoin heists, 2014, https://bitcointalk.org/index.php?topic=576337
27) Bitcoin gevinster kan stikkes direkte i lommen, 2014 http://politiken.dk/oekonomi/dkoekonomi/ECE2244816/bitcoin-gevinster-kan-stikkes-direkte-i-lommen/
28) Bitcoin Hivemind http://bitcoinhivemind.com/
29) Bitcoin Network Shaken by Blockchain Fork, 2013 http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/
30) Bitcoin Roma arriva primo bancomat la moneta elettronica, 2014 http://www.ilsole24ore.com/art/tecnologie/2014-03-14/bitcoin-roma-arriva-primo-bancomat-la-moneta-elettronica-212147.shtml?uuid=ABUKTC3
31) Bitcoin Senate Hearing 2013 http://www.hsdl.org/?view&did=747209
32) Bitcoin Showing Typical ‘Aggressive Bubble’ Behavior, 2013 http://www.cnbc.com/id/100613010
33) Bitcoin wiki https://en.bitcoin.it/wiki/Main_Page
34) Bitcoin, parla Guido Rossi è uno strumento rischioso, è come i derivati, può stravolgere le regole del capitalismo, 2013 http://www.huffingtonpost.it/2013/04/16/bitcoin-parla-guido-rossi-e-uno-strumento-rischioso-e-come-i-derivati-puo-stravolgere-le-regole-del-capitalismo_n_3093273.html
35) Bitcoin, the nationless electronic cash beloved by hackers, bursts into financial mainstream, 2013 http://www.foxnews.com/tech/2013/04/11/bitcoin-electronic-cash-beloved-by-hackers/

36) Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto, 2009 http://bitcoin.org/bitcoin.pdf
37) Bitcoin: what you need to know, 2013 http://www.theguardian.com/technology/2013/oct/04/bitcoin-what-you-need-to-know-silk-road
38) Bitcoin's roller-coaster ride gets wilder as Wall Street, China climb on , 2013 http://arstechnica.com/tech-policy/2013/12/bitcoins-roller-coaster-ride-gets-wilder-as-wall-street-china-climb-on/
39) Bitcoin-Paypal,2014 http://www.wired.it/attualita/tech/2014/05/20/bitcoin-paypal/
40) Bitcoins are private money in Germany, 2013 http://www.webcitation.org/6JJIqfMJn
41) Block Apps http://blockapps.net/
42) Blockchain Technologies http://www.blockchaintechnologies.com/blockchain-definition
43) Building Better Bitcoins - by Stephen L Carter, 2013 http://www.bloomberg.com/news/2013-11-29/building-better-bitcoins.html
44) Business Processes Secured by Immutable Audit Trails on the Blockchain ,2014, http://factom.org/
45) Canada Says Bitcoin Isn't Legal Tender - Canada Real Time - WSJ, 2013 http://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal-tender/
46) CGUE sentenza 22 ottobre 2015, causa C-264/14 http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=IT
47) Chain of Things http://www.chainofthings.com/
48) Charles Mackay: Memoirs of Extraordinary Popular Delusions, 1841 http://pinkmonkey.com/dl/library1/digi346.pdf
49) China bans banks from bitcoin transactions, 2013 http://www.smh.com.au/business/markets/currencies/china-bans-banks-from-bitcoin-transactions-20131206-2yugy.html
50) China Bans Payment Firms from Working With Bitcoin Exchanges, 2013 http://forexmagnates.com/china-bans-payment-firms-from-working-with-bitcoin-exchanges/
51) China Restricts Banks' Use of Bitcoin, 2013 http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html?_r=1&
52) Cloud Security Alliance Blockchain/Distributed Ledgers Working Group https://cloudsecurityalliance.org/group/blockchain/
53) Cloud Security Alliance https://cloudsecurityalliance.org/
54) Coin Market Cap http://coinmarketcap.com
55) Coin Science http://www.slideshare.net/coinspark
56) Coin Spark https://coinspark.org/
57) Coinlab v. Mt. Gox Case 2:13-cv-00777, United States District Court for the Western District of Washinghton, 2013, https://web.archive.org/web/20130518075639/http://www.scribd.com:80/doc/139160091/Coinlab-v-Mt-Gox
58) Colored Coin http://coloredcoins.org/
59) Colu project https://www.colu.co/

60) Committee on Payment and Market Infrastructures (2015), Statistics on Payment, Clearing and Settlement Systems in the CPMI Countries, http://www.bis.org/cpmi/publ/d142.htm
61) Congresso USA: Regulation of Bitcoin in Selected Jurisdictions, 2014 http://www.loc.gov/law/help/bitcoin-survey/2014-010233%20Compiled%20Report_.pdf
62) Corte di Giustizia UE, Quinta Sezione, sentenza 22 ottobre 2015, causa C-264/14 http://www.dirittoegiustizia.it/allegati/17/0000071427/Corte_di_Giustizia_UE_Quinta_Sezione_sentenza_22_ottobre_2015_causa_C_264_14.html
63) Court officially declares Bitcoin a real currency, 2013 http://rt.com/usa/bitcoin-sec-shavers-texas-231/
64) Crisanto Mandrioli, Antonio Carratta, Diritto processuale civile vol.III, Giappichelli 2015
65) Crypto currency, 2011 http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html
66) Cryptonote Technology, Ring signatures: Untraceable payments https://cryptonote.org/inside
67) Cyrus Farivar "Taming the bubble" investors bet on Bitcoin via derivatives markets http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/ 2013
68) Daniel Forrester, Mark Solomon, Bitcoin Explained - Today's Complete Guide to Tomorrow's Currency, Grassroot Books, 2013
69) David Chaum, Achieving Electronic Privacy, Scientific American, 1992, http://www.chaum.com/publications/ScientificAmerican-AEP.pdf
70) David Chaum, "Blind signatures for untraceable payments" in Advances in Cryptology Proceedings of Crypto 82 (3): 199–203 http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
71) David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, vol. 24 no. 2, February, 1981, http://www.chaum.com/publications/chaum-mix.pdf
72) David Chaum, Amos Fiat, Moni Naor, Untraceable Electronic Cash , Advances in Cryptology CRYPTO 1988, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327, http://www.chaum.com/publications/Untraceable_Electronic_Cash.pdf
73) David Chaum, Eugene van Heyst, Group signatures, Advances in Cryptology EUROCRYPT 1991, D.W. Davies (Ed.), Springer-Verlag, pp. 257-265
74) David Chaum, Online Cash Cecks, 1989 https://w2.eff.org/Privacy/Digital_money/?f=online_cash_chaum.paper.txt
75) David Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, vol. 28 no. 10, October 1985, http://www.chaum.com/publications/Security_Wthout_Identification.html
76) David Patterson, MIT running a ripple validator, 2016, https://ripple.com/insights/mitvalidator/

77) Decreto MEF 9 maggio 2016
http://www.gazzettaufficiale.it/eli/id/2016/08/22/16A06123/sg
78) Defense Pentagon bitcoin terrorism, 2014 http://rt.com/usa/157552-defense-pentagon-bitcoin-terrorism/
79) Définition de Preuve de travail,
https://fr.bitcoin.it/wiki/Preuve_de_travail
80) DEFT, http://www.deftlinux.net/it/
81) Deloitte USA, Blockchain's future in oil and gas: Transformative or transient?, 2017
https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-future-in-oil-and-gas.html
82) Denmark declares bitcoin trades tax-free, 2014
http://www.coindesk.com/denmark-declares-bitcoin-trades-tax-free/
83) DUTCH CENTRAL BANKER: Bitcoin Hype Is Even Worse Than Tulip Mania, 2013
http://www.businessinsider.com/dutch-banker-compares-bitcoin-to-tulips-2013-12#ixzz2mdocOcYK
84) EBA Warning to consumers on virtual currencies, 2013
http://www.eba.europa.eu/documents/10180/15971/EBA+Warning+on+Virtual+Currencies.pdf
85) E-health – Estonian Digital Solutions for Europe https://e-estonia.com/e-health-estonian-digital-solutions-for-europe/
86) Eiichiro Fujisaki e Koutarou Suzuki, Traceable ring signature, In Public Key Cryptography, 2007, https://eprint.iacr.org/2006/389.pdf
87) Electronic Data Interchange standard, http://www.nist.gov/,
http://www.unece.org/info/ece-homepage.html
88) Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), 2014, http://zerocash-project.org/paper
89) Ente di Normazione Italiano http://www.uni.com/
90) ESMA assesses DLT's potential and interactions with EU rules, 2017,
https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt%E2%80%99s-potential-and-interactions-eu-rules
91) ESMA report The Distributed Ledger Technology Applied to Securities Markets, 2017,
https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
92) Ethereum Design Rationale, 2016,
https://github.com/ethereum/wiki/wiki/Design-Rationale#uncle-incentivization
93) Ethereum Glossary, 2016,
https://github.com/ethereum/wiki/wiki/Glossary
94) Ethereum https://www.ethereum.org/
95) Ethereum whitepaper – ghost implementation, 2015
https://github.com/ethereum/wiki/wiki/White-Paper#modified-ghost-implementation
96) Ethereum whitepaper, 2013,
https://github.com/ethereum/wiki/wiki/White-Paper

97) Ethereum yellowpaper, 2014, http://gavwood.com/paper.pdf
98) Eugenio Spagnuolo, Addio Bitcoin, nel deep web ora si paga con Monero e Zcash, 2017, https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash/
99) European Central Bank - Virtual Currency Schemes, 2012 http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
100) FBI Says It's Seized $28_5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road, 2013 http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/
101) FBI, Bitcoin Virtual Currency: Unique Features Present Distinct Challenges, 2012 http://cryptome.org/2012/05/fbi-bitcoin.pdf
102) Federal judge rules bitcoin is real money, 2013 http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/
103) Feds stole my $33M bitcoins booty Silk Road 'pirate', 2013 http://nypost.com/2013/12/23/government-robbed-me-of-33m-in-bitcoins-silk-road-pirate/
104) Finance and Economics Discussion SeriesDivisions of Research & Statistics and Monetary Affairs Federal Reserve Board Washington D.C, .Distributed ledger technology in payments, clearing, and settlement, 2016, https://www.slideshare.net/IanBeckett3/distributed-ledger-technology-in-payments-clearing-and-settlement-blockchain-fintech
105) Firestartr, Blockchain-Hackathon-at-London-Fintech-Week-2015, http://www.firestartr.co/events/2015/9/18/blockchain-hackathon-at-london-fintech-week-2015
106) Franco Angeloni Horribilia juridica (quando ci si mette il legislatore), Contratto e impresa, 1993, 3 , CEDAM Padova
107) Gavin Wood Ethereum yellow paper, 2014, http://gavwood.com/Paper.pdf
108) Gideon Greenspan Blockchains vs centralized databases, 2016, http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/
109) Global Bitcoin Nodes Distribution https://bitnodes.21.co/
110) GNU Privacy Guard https://www.gnupg.org/
111) Gordon G. Chang, A China Triangle Bitcoin, Baidu And Beijing, 2013 http://www.forbes.com/sites/gordonchang/2013/11/24/a-china-triangle-bitcoin-baidu-and-beijing/
112) Grace Caffyn, IPO and Insurance Projects Win £2,000 at Blockchain Hackathon, 2015 http://www.coindesk.com/ipo-and-insurance-projects-win-2000-at-blockchain-hackathon/
113) Greg Maxwell, Confidential Transactions, 2013 https://www.weusecoins.com/confidential-transactions/
114) Hal Finney Bitcoin and me (Hal Finney) , 2013, https://bitcointalk.org/index.php?topic=155054.0
115) 'Horribilia Juridica' D.O.C. (raccolte, garantite e proposte alla rinfusa da Lina Bigliazzi Geri), Contratto e impresa, 1993, IX/3, CEDAM Padova

116) http://arstechnica.com/tech-policy/2012/08/bitcoinica-users-sue-for-460k-in-lost-bitcoins/
117) http://telehash.org/
118) https://ipfs.io/
119) https://zeronet.io/
120) Hyperledger whitepaper https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/pub
121) I trader? Più spietati degli psicopatici, 2011 http://www.corriere.it/economia/11_settembre_26/operatori_borsa_spietati_psicopatici_burchia_d1475624-e833-11e0-9000-0da152a6f157.shtml
122) Ian Allison, Ethereum-based Slock.it reveals first ever lock opened with money, 2015, http://www.ibtimes.co.uk/ethereum-based-slock-reveals-first-ever-lock-opened-money-1527014
123) Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2011, zerocoin.org/media/pdf/ZerocoinOakland.pdf
124) IBM IoT and Blockchain project, http://www.ibm.com/internet-of-things/iot-news/announcements/private-blockchain/
125) IDESG https://www.idesg.org/
126) IEFT https://www.ietf.org/
127) Insur ETH, 2015, https://github.com/bertani/insurETH
128) Is Bitcoin a Real Currency? by David Yermack, 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599
129) Is Bitcoin Money: What Economists Have To Say, 2013 http://www.economicpolicyjournal.com/2013/10/is-bitcoin-money-what-economists-have.html
130) ISO http://www.iso.org/iso/home.html
131) ITU-T http://www.itu.int/en/ITU-T/Pages/default.aspx
132) Jacob Donnelly, Everledger Plans Blockchain Database to Combat Art Fraud, 206, http://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/
133) Japan exempts bitcoin from Consumption Tax http://www.vatlive.com/vat-news/japan-exempts-bitcoin-from-consumption-tax/
134) Jeff John Roberts Why Accenture's Plan to 'Edit' the Blockchain Is a Big Deal, 2016, http://fortune.com/2016/09/20/accenture-blockchain/
135) Jim Edwards, 18-Year-Old Reports $1 Million Bitcoin Theft From 'Bank' He Controlled — And Says He Can't Call The Cops, 2013 http://www.businessinsider.com/1-million-bitcoin-theft-in-australia-2013-11
136) John F. Nash, Equilibrium Points in n-Person Games, Procedings of the National Accademy of Science of the United States of Amenrica 1950, http://web.mit.edu/linguistics/events/iap07/Nash-Eqm.pdf
137) John Weru Maina, Does Bitcoinica Founder Zhou Tong Have Some Explaining To Do?, 2015, https://www.cryptocoinsnews.com/bitcoinica-founder-zhou-tong-explaining/
138) JP Morgan lancia la sfida a Bitcoin, 2013 http://america24.com/news/jp-morgan-lancia-la-sfida-bitcoin

139) JPMorgan's "Bitcoin-Alternative" Patent Rejected - Bitcoin & Cryptocurrency , 2013 http://www.cryptonews.biz/jpmorgans-bitcoin-alternative-patent-rejected/
140) Kickstart my heart:extraordinary popular delusions and the madness of crowdfunding costraint ant bitcoin bubbles, David Groshoff, 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2313396
141) Kim Zetter, Bulion and Bandits, the Improbable raise and fall of E-Gold, 2009 http://www.wired.com/2009/06/E-Gold/all/
142) Kimberley Process https://kimberleyprocessstatistics.org/
143) Kyle Torpey, 5 Ways Bitcoins Could Be Transferred to a Sidechain, 2017, https://news.bitcoin.com/5-ways-bitcoins-transferred-sidechain/
144) La autoridad bancaria europea alerta de los peligros del bitcoin 2013 http://tecnologia.elpais.com/tecnologia/2013/12/13/actualidad/1386926648_816453.html
145) La Cina vieta l'uso della moneta elettronica Bitcoin a banche e finanza, 2013 http://www.ilsole24ore.com/art/notizie/2013-12-05/la-cina-vieta-uso-moneta-elettronica-bitcoin-banche-e-finanza-120153.shtml
146) Lester Coleman, U.K. Land Registry Looks to Register Property on a Blockchain, 2017, https://www.cryptocoinsnews.com/u-k-land-registry-looks-register-property-blockchain/
147) LETSystem portal http://www.gmlets.u-net.com/
148) List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [Old], 2012, https://bitcointalk.org/index.php?topic=83794.0#post_june_2011_mt_gox_incident
149) List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses, 2013 https://bitcointalk.org/index.php?topic=83794.0
150) Litecoin https://litecoin.org/
151) Ludwig Von Mises Italia, La moneta, http://vonmises.it/2014/04/30/la-moneta-v-parte/
152) magoo Blockchain Graveyard, 2017, https://magoo.github.io/Blockchain-Graveyard/
153) Maidsafehttp://maidsafe.net/safecoin
154) Majority is not Enough Bitcoin Mining is Vulnerable, 2013 http://arxiv.org/abs/1311.0243
155) Mance Harmon Choosing the Right Distributed Ledger Algorithm, 2017, https://www.pingidentity.com/en/blog/2017/01/18/choosing_the_right_distributed_ledger_algorithm.html
156) Maria Apostolaki, Aviv Zohar, Laurent Vanbever , Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, 2016, https://arxiv.org/abs/1605.07524v2
157) Maria Nikolova, MTGOX's bankruptcy trustee updates on US seized funds release, 2017, https://financefeeds.com/mtgoxs-bankruptcy-trustee-updates-us-seized-funds-release/
158) Mark Stone, The Tiny European Country That Became A Global Leader In Digital Government, 2016, https://www.forbes.com/sites/delltechnologies/2016/06/14/the-tiny-

european-country-that-became-a-global-leader-in-digital-government/#6e2ef90ae13a
159) Megan Geuss, Bitcoinica users sue for $460k in lost Bitcoins: A complaint filed in SF accuses the trading platform of breach of contract, 2012,
160) Michael del Castillo, The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem, 2015, http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html
161) Michael del Castillo, Vladimir Putin and Vitalik Buterin Discuss Ethereum 'Opportunities', 2017 http://www.coindesk.com/vladimir-putin-vitalik-buterin-discuss-ethereum-opportunities-recent-forum/
162) Michele Spagnuolo, Federico Maggi, Stefano Zanero , BitIodine: Extracting Intelligence from the Bitcoin Network , 2014, fc14.ifca.ai/papers/fc14_submission_11.pdf
163) MimbleWimble https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt
164) MIT license http://opensource.org/licenses/MIT
165) Mt. Gox answer and counterclaim against CoinLab, United States District Court for the Western District of Washinghton at Seattle, 2013, https://www.scribd.com/doc/168517688/Mt-Gox-counterclaim-against-CoinLab
166) Multichain Whitepaper, 2015 http://www.multichain.com/download/MultiChain-White-Paper.pdf
167) Multichain http://www.multichain.com/
168) Namecoin https://namecoin.info/
169) Naveen Joshi, 3 things to know about Bitcoin Blockchain, 2017, https://www.linkedin.com/pulse/3-things-know-bitcoin-blockchain-naveen-joshi?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BSOk75Q3zYBSq8FXP8dtdSg%3D%3D
170) Nell'arcipelago delle monete virtuali i paradisi fiscali puntano sui bitcoin, 2014 http://espresso.repubblica.it/affari/2014/07/31/news/nell-arcipelago-delle-monete-virtuali-i-paradisi-fiscali-puntano-sui-bitcoin-1.175140
171) Nevada Senate Bill 398, 2017, https://legiscan.com/NV/bill/SB398/2017
172) New Money Laundering, 2013 http://www.forbes.com/sites/timothylee/2013/03/19/new-money-laundering-guidelines-are-a-positive-sign-for-bitcoin/ 2013
173) Nick Szabo, Contracts with Bearers, 1998, http://szabo.best.vwh.net/bearer_contracts.html
174) Nick Szabo, Formalizing and Securing Relationships on Public Networks, 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469
175) Nick Szabo, Secure Property Titles with Owner Authority, 1998, http://szabo.best.vwh.net/securetitle.html
176) Nick Szabo, The Idea of Smart Contracts, 1997, http://szabo.best.vwh.net/idea.html
177) Novissimo Digesto, Utet Torino, 1995

178) NXT https://nxt.org/
179) NY Department of Financial Services, "Regulations of the Superintendent of Financial Services, part 200: virtual currencies", Retrieved April 13, 2017, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf
180) OASIS https://www.oasis-open.org/
181) Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC by Shawn J. Bayern, 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366197
182) Oraclize https://www.oraclize.it/home/features
183) Paolo Dal Checco, Bitcoin Forensics, http://www.bitcoinforensics.it/
184) ParsnipCommander, Ethereum was second largest crowdsale in history, 2014 http://www.reddit.com/r/ethereum/comments/2fhmzm/ethereum_was_second_largest_crowdsale_in_history/
185) Pastebin http://pastebin.com/CcGUBgDG
186) Payman Mohassel, One-Time Signatures and Chameleon Hash Functions, 2010, https://www.researchgate.net/publication/221274662_One-Time_Signatures_and_Chameleon_Hash_Functions
187) Post Satoshi Nakamoto, Gavin Andersen, Hal Finney 1/3 https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696
188) Post Satoshi Nakamoto, Gavin Andersen, Hal Finney 2/3 https://bitcointalk.org/index.php?topic=1790.msg22019#msg22019
189) Post Satoshi Nakamoto, Gavin Andersen, Hal Finney 3/3 https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917
190) Press release, MIT Adopts Ripple Validator to Advance Consensus and Blockchain Research, 2016 http://www.businesswire.com/news/home/20160412005403/en/MIT-Adopts-Ripple-Validator-Advance-Consensus-Blockchain
191) Qiong Wei, Yansheng Lu , Qiang Lou, Privacy-Preserving Data Publishing Based on De-clustering, 2008, http://ieeexplore.ieee.org/document/4529813/figures
192) Raiman Dillet, Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It Of Violating Money Transfer Regulations, 2013, https://techcrunch.com/2013/05/16/mt-gox-dwolla-account-money-seizure/
193) Reddit ,IMPORTANT WARNING to those who want to use Monero/ShapeShift and NOT end up in jail, 2016 https://www.reddit.com/r/DarkNetMarkets/comments/4zf25q/important_warning_to_those_who_want_to_use/?compact=true
194) Reddit, OPSEC Electrum, 2016 https://www.reddit.com/r/DarkNetMarkets/comments/3353ae/opseccomputer_folks_gotta_stop_saying_use/
195) Reddit, Planning to place a first order with Monero, what should I know? 2016 https://www.reddit.com/r/DarkNetMarkets/comments/4zc96n/planning_to_place_a_first_order_with_monero_what/
196) Renato Di Lorenzo, Emilio Cuomo; Le parole del trader di borsa. Breve dizionario dei termini finanziari; ed. Gruppo 24 Ore, 2011

197) Richard Chirgwin Evil ISPs could disrupt Bitcoin's blockchain, 2017, https://www.theregister.co.uk/2017/04/11/evil_isps_could_disrupt_bitcoins_blockchain/
198) Richard Gendal Brown, Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services, 2016, http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services
199) Richard Kastelein Accenture Releases Patented Blockchain Editing Tool for Banks, 2016, http://www.the-blockchain.com/2016/09/20/accenture-releases-patented-blockchain-editing-tool-banks/
200) Ripple consensus process https://ripple.com/build/ripple-ledger-consensus-process/
201) Ripple consensus whitepaper, 2014, https://ripple.com/files/ripple_consensus_whitepaper.pdf
202) Ripple https://ripple.com/
203) Rohas Nagpal Build a private blockchain ecosystem in minutes with this open source project, 2017, https://www.linkedin.com/pulse/build-private-blockchain-ecosystem-minutes-open-source-rohas-nagpal?trk=v-feed&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BqyDSGRJCP%2BSAVlgmHJy5%2Bg%3D%3D
204) Rootstock http://www.rsk.co/
205) RPOW - Reusable Proofs of Work, 2004, http://nakamotoinstitute.org/finney/rpow/
206) Russian E-Money Association, Overview of the legal proposals to ban the usage of 'monetary surrogates' (incl. Bitcoin) in the Russian Federation, 2016, http://npaed.ru/en/home-en/releases/290-overview-of-the-legal-proposals-to-ban-the-usage-of-monetary-surrogates-in-the-russian-federation
207) Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts, 2013 http://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation/
208) Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, http://bitcoin.org/bitcoin.pdf
209) Scott Shorter https://www.linkedin.com/in/scott-shorter-24575a2
210) Senate Bitcoin Hearing, 2013 http://www.businessinsider.com/senate-bitcoin-hearing-2013-11
211) Sheep marketplace goes offline and up to 44 million in bitcoins disappears, 2013 http://www.businessinsider.com/sheep-marketplace-goes-offline-and-up-to-44-million-in-bitcoins-disappears-2013-12
212) Shen Noether, Adam Mackenzie and Monero Core Team , Ring Confidential Transactions, 2016, https://www.ledgerjournal.org/ojs/index.php/ledger/article/download/34/61
213) Showroomprive. com è il primo in Europa ad adottare i bitcoin, 2014 http://www.ninjamarketing.it/2014/10/09/showroomprive-com-e-il-primo-in-europa-ad-adottare-i-bitcoin/
214) Stalling W., Crittografia e sicurezza delle reti,2/ed Apogeo, 2007
215) Stan Higgins, IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things, 2015 http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/

216) Standards Australia, Australia to lead international blockchain standard committee
http://www.standards.org.au/OurOrganisation/News/Pages/Australia-to-lead-international-blockchain-standards-committee.aspx
217) Standards Australia, blockchain information sheet
http://www.standards.org.au/OurOrganisation/Events/Documents/Blockchain%20NFTA%20Information%20Sheet.pdf
218) Stateless Virtual Money in the Tax System by Aleksandra Bal 2013
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298537
219) Stefan Thomas, Evan Schwartz, Smart Oracles: A Simple, Powerful Approach to Smart Contracts, 2014,
https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts
220) Stellar https://www.stellar.org/ e https://www.stellar.org/
https://www.stellar.org/about/mandate/
221) Tails https://tails.boum.org/
222) Tether https://tether.to/
223) TFUE http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12012E%2FTXT
224) The Economist, The fintech revolution, 2015,
http://www.economist.com/news/leaders/21650546-wave-startups-changing-financefor-better-fintech-revolution
225) The financial psychopath next door Sherree Deconvy, 2012
http://www.cfapubs.org/doi/pdf/10.2469/cfm.v23.n2.20
226) The Japanese Times, Diet OKs bill to regulate virtual currency exchanges, 2017,
http://www.japantimes.co.jp/news/2016/05/25/business/diet-oks-bill-regulate-virtual-currency-exchanges/
227) The Kantara Initiative https://kantarainitiative.org/
228) The Money Fix documentary, 2011,
http://www.themoneyfix.org/interviewee/michael-linton
229) The Omnilayer http://www.omnilayer.org/
230) The Rise and Fall of Bitcoin Wired Magazine, 2011
http://www.wired.com/magazine/2011/11/mf_bitcoin/
231) The rise of the bitcoin: Virtual gold or cyber-bubble? 2013
http://articles.washingtonpost.com/2013-04-04/world/38280106_1_bitcoin-satoshi-nakamoto-monetary-policy 2013
232) The USA PATRIOT Act: Preserving Life and Liberty, 2001
http://www.justice.gov/archive/ll/highlights.htm
233) Timothy C. May, The Crypto Anarchist Manifesto, 1992
http://www.activism.net/cypherpunk/crypto-anarchy.html
234) Today, we are all money transmitters… (no, really!), 2013
https://bitcoinfoundation.org/blog/?p=152
235) Trappe W., Washinghton L.C. Crittografia con elementi di teoria dei codici, Pearson Ed. Italia, 2009
236) US Financial Crimes Enforcement Network: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, 2013 http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

237) US federal agent investigating Silk Road admits $800,000 bitcoin theft https://www.theguardian.com/technology/2015/sep/01/us-federal-agent-investigating-silk-road-admits-800000-bitcoin-theft
238) US govt clarifies virtual currency regulatory position, 2013 http://www.finextra.com/News/FullStory.aspx?newsitemid=24645
239) US Internal Revenue Service , Virtual Currency Guidance, 2014 http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance 2014
240) US Internal Revenue Service http://www.irs.gov/pub/irs-drop/n-14-21.pdf, 2014
241) US investigated MtGox CEO as possible Silk Road mastermind, 2015, https://www.theguardian.com/technology/2015/jan/16/mtgox-ceo-silk-road-mark-karpeles-ross-ulbricht
242) US regulator: Bitcoin exchanges must comply with money-laundering laws, 2013 http://arstechnica.com/tech-policy/2013/03/us-regulator-bitcoin-exchanges-must-comply-with-money-laundering-laws/
243) USA Department of Justice, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges, 2008, http://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
244) USA Internal Revenue Service (IRS), Cash Intensive Businesses Audit Techniques Guide - Chapter 7, Digital Cash and Electronic Money,rev. 2010 http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Cash-Intensive-Businesses-Audit-Techniques-Guide-Chapter-7
245) Vermont General Assemby, 2016, http://legislature.vermont.gov/bill/status/2016/H.868
246) Virtual Currency Response Letters - Federal Agencies Respond to Homeland Security Committee Questions on Digital Currencies, 2013http://www.scribd.com/doc/184579094/Virtual-Currency-Response-LettersFederal-Agencies-Respond-to-Homeland-Security-Committee-Questions-on-Digital-Currencies
247) Vitalik Buterin Ethereum white paper, 2013, https://github.com/ethereum/wiki/wiki/White-Paper
248) Vitalik Buterin On Public and Private Blockchains, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
249) Vitalik Buterin, MtGox Gets FinCEN MSB License, 2013, https://bitcoinmagazine.com/articles/mtgox-gets-fincen-msb-license-1372534713/
250) Wang Wei, Man Jailed 6 Months for Refusing to Give Police his iPhone Passcode, 2017, http://thehackernews.com/2017/06/unlock-iphone-passcode.html?m=1
251) Wei Dai, B-Money, 1998, http://www.weidai.com/bmoney.txt
252) Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering by Catherine Martin Christopher, 2013 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312787
253) What is a Bitcoin Tumbler ? 2014 https://bitcoin.stackexchange.com/questions/17807/what-is-a-bitcoin-tumbler
254) World Technology award winners 2014 http://www.wtn.net/summit-2014/2014-world-technology-awards-winners
255) Xgate, How Ripple Works, 2017, http://xagate.com/#topbar

256) XRP Chat, Japan initiated the operation of the Validator node of digital asset (virtual currency) "XRP" at the Tokyo data center, contributing to a highly reliable currency system, 2017, https://www.xrpchat.com/topic/3117-japan-initiated-the-operation-of-the-validator-node-of-digital-asset-virtual-currency-xrp-at-the-tokyo-data-center-contributing-to-a-highly-reliable-currency-system/
257) Yoni Assia, Vitalik Buterin, Lior Hakim, Meni Rosenfeld, Rotem Lev, Colored Coins white paper, 2012 https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit?pli=1
258) Zerocash project http://zerocash-project.org/
259) Zerocash project http://zerocash-project.org/
260) Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), Eli Ben-Sasson, Alessandro Chiesay Christina Garmanz Matthew Greenz, Ian Miersz Eran Tromerx Madars Virzay, 2014, http://zerocash-project.org/paper