BITCOIN E SCHEMI SEQUENZIALI DI HASHING

di Maria Letizia Perugini[1]

Resumen

Los motivos históricos y económicos que han llevado a programar el protocolo Bitcoin se encuentran en la actualidad con una interesante fase evolutiva de los algoritmos de encriptación para la identificación de datos y la transmisión de derechos, tratándose de un sistema que presenta aspectos jurídicos dignos de mención.

Palabras clave: Bitcoin, hashing, algoritmos de encriptación.

Abstract

Il tema di questo articolo richiama volutamente la definizione di analisi sequenziale propria delle scienze statistiche, nel cui ambito si procede formando un campione rappresentativo senza determinarne a priori l'ampiezza o la numerosità, che dipenderanno dai risultati ottenuti col progredire dell'osservazione o dell'esperimento. La ragione di questa scelta dipende 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 astratta del campione di studio. Le ragioni storiche ed economiche che, nel tempo, hanno portato alla programmazione del protocollo Bitcoin hanno conoscono oggi un'interessante fase evolutiva negli algoritmi di criptazione per l'identificazione di dati e il trasferimento di diritti, un sistema che presenta risvolti giuridici degni di nota.

Keywords: Bitcoin, hashing, algoritmi di criptazione.

Abstract

The theme of this paper is, on purpose, recalling the definition of sequential analysis typical of Statistics where the analysis goes on forming a representative sample with no predetermination of its magnitude or numerical amount, which will depend on the result gained as the observation or the experiment are going by. The reason for this choice is depending on the very nature of the topic we aim to analyse: a new subject matter, which effect are keeping on changing, thus making quite difficult the sample abstract determination. The historical reasons that, over time, have led to the Bitcoin protocol development are nowadays having an interesting implement in the encrypting algorithm for data identification and goods transferring, a system with remarkable legal effects.

Keywords: Bitcoin, encrypting algorithm, hashing.

PREMESSA[2]

Il campione digitale su cui si basa l'analisi svolta in questo articolo è il prodotto di uno specifico modello matematico, studiato per offrire una risposta efficiente a una determinata congiuntura di mercato e alle esigenze del momento storico che quella contingenza avevano determinato. Come spesso accade, le conseguenze di questa innovazione si sono rivelate ulteriori e diverse rispetto alle aspettative che nutrivano coloro che avevano preso parte alla creazione del modello e alla sua implementazione e diffusione. Ad oggi vi sono alcuni interessanti risvolti dei protocolli di Hashing che sembrano andare oltre le previsioni dei programmatori originari e che a nostro parere meritano di essere analizzate dal punto di vista scientifico dell'Informatica Giuridica.

---

[1] Dottoranda in Diritto e Nuove Tecnologie, *curriculum* in informatica forense, presso il CIRSFID (Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia, Sociologia del Diritto e Informatica Giuridica) dell'Alma Mater Studiorum Università di Bologna. http://www.unibo.it/SitoWeb/default.aspx?UPN=maria.perugini%40unibo.it.

[2] Bibliografía general sobre el tema: Bank of America Merrill Lynch: Bitcoin a first assessment, 2013, https://ciphrex.com/archive/bofa-bitcoin.pdf; Bitcoin Senate Hearing, 2013, http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies; Cesare Maioli: Questioni di Informatica Forense, 2015, Aracne Editrice.

Colored Coins whitepaper https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit.

David Yermack: Is Bitcoin a Real Currency? 2013,; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599; Eugenio Ruggiero, Moneta, Cambio, Valuta in Novissimo Digesto, Utet Torino 1995, vol X; Gavin Wood: Ethereum yellow paper, 2014, http://gavwood.com/Paper.pdf ; German Federal Financial Supervisory Authority: Trading in Bitcoins, 2014 http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Jahresbericht/2013/jb_2013_II_9_2_trading_in_bitcoins.html; 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.

Maria Letizia Perugini e Cesare Maioli 'Bitcoin: Between Digital Currency and Financial Commodity', 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2526472 ; Morgan Stanley, Commodity Book, 2007, http://www.morganstanleyiq.it/pdf/downloads/82_Commodity%20Book_Sett07.pdf; Nick Szabo: Formalizing and Securing Relationships on Public Networks, 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469 ; Nick Szabo: Secure Property Titles with Owner Authority, 1998, http://szabo.best.vwh.net/securetitle.html; Nick Szabo: The Idea of Smart Contracts, 1997, http://szabo.best.vwh.net/idea.html ; S. Capaccioli: Introduzione al trattamento tributario delle valute virtuali: criptovalute e bitcoin, in «Diritto e Pratica Tributaria Internazionale», CEDAM, – n. 1/2014; Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, http://bitcoin.org/bitcoin.pdf; Stalling W., Crittografia e sicurezza delle reti,2/ed Apogeo 2007 e Trappe W., Washinghton L. C. Crittografia con elementi di teoria dei codici, Pearson Ed. Italia 2009; Vitalik Buterin: Ethereum white paper, 2013, https://github.com/ethereum/wiki/wiki/. White-Paper ; Wei Dai: B-money, 1998, http://www.weidai.com/bmoney.txt.

RUOLO DELLA NORMATIVA ANTIRICICLAGGIO

Si legge spesso che la storia dei bitcoin ha avuto inizio nel 2009, quando l'autore conosciuto con lo pseudonimo di Satoshi Nakamoto ha implementato un'idea che in ambito informatico era oggetto di attenzione da oltre un decennio[3]; non vengono però delineati i motivi per cui questi protocolli erano rimasti latenti per più di due lustri, un tempo infinito a livello digitale, o per quale ragione le scelte di programmazione effettuate nel 2009 abbiano riscosso tanto successo in rete.

Per comprendere la natura dei protocolli di moneta virtuale[4], occorre tenere presente che fra il 2001 e il 2009 l'ordinamento USA, punto di riferimento normativo dei Bitcoin, aveva apportato alcune radicali modifiche alla libertà economica dei cittadini, introducendo nelle disposizioni del Patriot Act[5] l'obbligo per i servizi di trasferimento valuta di procedere all'identificazione dei propri clienti (Know Your Customer Rule). La previsione aveva suscitato immediati dubbi interpretativi[6]: a termini di un primo report emesso dal dipartimento del Tesoro nel 2006, i servizi di trasferimento operanti in metalli preziosi non erano da considerare money transfer e sfuggivano perciò all'applicazione della normativa[7]; re melius perpensa, tra il 2006 e il 2008 il FinCen[8] e il Dipartimento di Giustizia hanno rivisto la propria valutazione, allargando progressivamente l'ambito di applicazione delle nuove regole fino a ricomprendervi il trasferimento di ogni genere di valore[9].

La nuova definizione delle regole anti money laundering, estesa dal 2012 anche alle compagnie straniere che consentono ai cittadini USA di aprire un account[10], ha comportato l'applicazione della KYCR a tutti i servizi value transfer, conducendo

---

[3] I lavori di maggiore riferimento sono: *B-money*, paper del 1998 di Wei Dai e *Bit Gold* di Nick Szabo, articolo del 2005 che rielabora i concetti espressi dal primo autore introducendo il concetto di proof of work; scartata l'idea presentata da Hal Finney (programmatore PGP) nel paper del 2004 *Reusable Proofs of Work,* in cui le possibilità di ottenere il risultato dipendono dalla potenza computazionale della macchina impiegata, Szabo definisce la funzione applicabile in termini meramente matematici. http://www.weidai.com/bmoney.txt. http://unenumerated.blogspot.kr/2005/12/bit-gold.html.http://cryptome.org/rpow.htm.

[4] L'analisi procede nel senso iniziato col lavoro *'Digital Currency*', capitolo del libro *'Questioni di Informatica Forense*', a cura di Cesare Maioli, Aracne Editrice. http://www.unibo.it/SitoWebDocente/default.aspx?UPN=cesare.maioli%40unibo.it. http://www.cirsfid.unibo.it/il-centro/le-aree-disciplinari/informatica-forense.

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

[6] http://www.venable.com/california-enacts-sweeping-new-law-targeting-money-transmitters-10-05-2010/, http://www.dgcmagazine.com/the-*E-Gold*-story/.

[7] 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.

[8] Financial Crimes Enforcement Network http://www.fincen.gov/.

[9] http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Cash-Intensive-Businesses-Audit-Techniques-Guide-Chapter-7.

[10] 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.

alla sospensione delle attività di alcune importanti piattaforme on line; vi è stato, peraltro, anche un risvolto inatteso, consistito in un incentivo alla riscoperta dei protocolli di moneta digitale e alla loro implementazione no asset backed.

I SERVIZI VALUE TRANSFER: IL CASO E-GOLD

E-Gold era un protocollo di trasferimento valori, fondato nel 1996 dall'oncologo Douglas Jackson e dall'avvocato Barry Downey, che, secondo un'opinione piuttosto diffusa, rappresenterebbe l'antesignano dei Bitcoin. Il sistema basava le proprie operazioni su un controvalore in lingotti d'oro del peso di 3.8 tonnellate: nella fase iniziale dell'attività, la scorta depositata era idonea alla copertura dei movimenti di trasferimento, concretizzando un sistema con funzioni di moneta aurea virtuale; nel corso del tempo la piattaforma era arrivata a gestire pagamenti per un controvalore di $20 miliardi l'anno la cui media di scambio giornaliera impegnava, da sola, l'intera riserva[11]. Le ragioni di questo successo erano molteplici: per un verso, il servizio offriva la sicurezza del gold standard; per l'altro, risultava decisivo l'anonimato offerto, con gli account registrabili sotto nomi di fantasia, senza che vi fosse verifica dei dati indicati. Quest'ultimo elemento aveva, purtroppo, attirato al servizio anche clienti oggetto di indagini finanziarie da parte dell'FBI: a seguito dell'interpretazione estensiva delle norme del Patriot Act, nel 2007 i gestori del sito erano stati incriminati per violazione della KYCR; secondo l'accusa, l'anonimato offerto da E-Gold si era rivelato strumentale a una serie di attività di money laundering che venivano loro imputate in via concorsuale[12];in conseguenza del processo, le attività del sito sono state congelate e nel 2009 è stato disposto un Value Access Plan per la restituzione dei fondi ai clienti identificati, con devoluzione al Governo USA dei valori non reclamati entro la fine del 2013[13].

Indipendentemente dai risvolti giudiziari, l'anonimato offerto da E-Gold era stato particolarmente apprezzato anche dagli utenti con fini leciti: le moderne tecnologie rendono infatti sempre più auspicabile di potere svolgere i propri acquisti in maniera riservata, evitando le procedure di raccolta dati a fini commerciali poste in essere dagli intermediari di moneta elettronica; la piattaforma costituiva uno strumento efficiente la cui regolamentazione avrebbe, a nostro parere, consentito l'attuazione di una valida alternativa nel sistema dei pagamenti, con incremento della concorrenza di settore e incentivo alle iniziative derivate, portando a risultati di mercato decisamente migliori rispetto a quelli prodotti dalla sua chiusura ex abrupto.

---

[11] http://www.wired.com/2009/06/*E-Gold*/all/.

[12] http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-*E-Gold*-of-helping-cybercrooks?lite.

[13] *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.

La posizione delle istituzioni USA nei confronti di E-Gold era stata particolarmente rigida: si era scelto di chiudere il servizio criminalizzandone l'attività, senza che fossero nemmeno poste in fase di studio le norme di diritto positivo idonee alla regolamentazione della materia: si era così aperto un vuoto di mercato, in cui lo spazio lasciato libero dalla piattaforma si rivelava idoneo ad accogliere una soluzione economicamente efficiente, vale a dire una protocollo implementato in modo da consentire il trasferimento anonimo nel rispetto delle disposizioni del Patriot Act, attuando le istanze di salvaguardia della privacy espresse dagli utenti della Rete.

Alla fine del 2008 un articolo a firma dello pseudonimo Satoshi Nakamoto[14] presentava alla rete i bitcoin, un sistema distribuito fra i nodi di una rete peer-to-peer[15], progettato allo scopo di mettere in sicurezza i pagamenti elettronici a prescindere dall'intervento di un garante esterno. L'utility applica un algoritmo di crittografia che procede al trasferimento elettronico sulla base di un protocollo gestito dai peer della rete, con verifica e convalida delle transazioni e conseguente garanzia di spendita unitaria. Il sistema crea una serie di monete virtuali che a differenza delle monete a corso legale, rimangono estranee alla regolamentazione generale dello scambio di beni e servizi essendo carenti delle tre funzioni tipiche di pagamento, unità di conto e riserva di valore[16]: nel caso delle monete virtuali non sussiste, infatti, alcun dovere generale di accettare il pagamento, come invece accade con la moneta avente corso legale nello Stato che deve essere accettata secondo il valore nominale[17]; mentre la funzione di unità di conto, ovvero la definizione dei valori di scambio in maniera idonea alla creazione di un indice di prezzi al consumo, viene ostacolata dalla volatilità del loro prezzo di mercato; la funzione di risparmio appare, infine, inconciliabile con questo genere di investimenti che richiedono piuttosto grande esperienza e propensione al rischio: si pensi che nel 2013 i bitcoin, punto di riferimento nel sistema delle monete virtuali, hanno mostrato un comportamento di mercato talmente aggressivo da indurre l'Autorità Bancaria Europea a emettere il documento 'Warning to consumers on digital currencies'[18]. Indipendentemente

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

[15] 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.

[16] Per la teoria classica della funzione monetaria, *vide*: Eugenio Ruggiero, Moneta, Cambio, Valuta in Novissimo Digesto, Utet Torino 1995, vol x, p. 5 SS.

[17] Nell'ordinamento italiano tale previsione è contenuta nell'art. 1277 cc.

[18] http://www.eba.europa.eu/documents/10180/15971/EBA+Warning+on+Virtual+Currencies.pdf. In quel periodo la volatilità media dei bitcoin si era attestata al 133%, con picchi intraday del 200%, quando, di norma, le valute tradizionali si muovono fra l'8% e il 12% e gli strumenti finanziari più scambiati hanno una volatilità compresa fra il 20% e il 30% mentre quelli più rischiosi raramente arrivano al 100% *Vide: Is Bitcoin a Real Currency?* by David Yermack, 2013, http://papers.ssrn.com/sol3/papers.

dalle considerazioni appena esposte, le monete virtuali differiscono dalla valuta per costituzione: le monete a corso legale sono, infatti, sempre soggette alla riserva di produzione dello Stato e degli Enti da esso autorizzati[19] e il loro valore dipende dalle politiche delle Banche Centrali; questi elementi sono estranei al sistema delle monete virtuali che rimangono espressione della più assoluta libertà di produzione, con variazioni di prezzo dettate dal mercato in maniera analoga alle commodity[20].

Il protocollo Bitcoin è stato di ispirazione a una lunga serie di monete virtuali: alcune sono state create ex novo implementando il progetto originario, come Litecoin, altre sono il risultato della riscrittura di algoritmi preesistenti, come il sistema Ripple: di seguito descriveremo il modello matematico originario e alcuni fra gli schemi derivati che riscuotono maggiore successo in rete.

BITCOIN [21]. ATTIVITÀ DI MINING

Nella produzione dei bitcoin, detta mining, alcuni nodi della rete, i miner, utilizzano la propria potenza di calcolo per individuare e verificare le soluzioni dell'algoritmo crittografico a base del sistema; questi complessi calcoli matematici devono essere convalidati da una proof of work, un dato particolarmente difficile da ottenere[22]: l'operazione genera in output un blocco di bitcoin[23] che viene attribuito al primo computer che ha risolto il problema e viene aggiunto alla catena logica (blockchain) insieme a tutte le transazioni associate. Il sistema è progettato per mantenere costante la velocità di produzione di un blocco ogni 10 minuti circa:

cfm?abstract_id=2361599; *et.,* 'Bank of America Merrill Lynch: Bitcoin a first assessment' 2013 https://ciphrex.com/archive/bofa-*bitcoin*.pdf.

[19] Direttiva 2009/101/CE, attuata in Italia con d.lgs. n.45 del 16/04/2012. 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.

[20] Morgan Stanley, Commodity Book, 2007: «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.» http://www.morganstanleyiq.it/pdf/downloads/82_Commodity%20Book_Sett07.pdf.

[21] Questo paragrafo riprende l'analisi contenuta nell'articolo: *'Bitcoin: Between Digital Currency and Financial Commodity'*, 2014, scritto con Cesare Maioli e pubblicato in Social Science Research Network, id. 2526472, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2526472.

[22] *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.*» Per semplificare, si pensi all'operazione 2+X<5: si tratta di un calcolo che può essere eseguito facilmente inserendo al posto della x un valore qualunque che sia minore di 3. Nelle operazioni seguenti bisognerà però tenere conto del valore individuato precedentemente, che chiameremo K, e l'operazione diventerà (2+K)+X<5. Poiché non si conosce K, inserito da uno qualunque dei *miner,* la risoluzione dell'operazione richiederà sempre maggior tempo man mano che ci si avvicina alla soglia data di 5.

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

l'effetto è dovuto all'aumento della difficoltà di produzione della proof of work che cresce man mano che nuovi blocchi vengono generati; a propria volta, la consistenza dei blocchi va soggetta a un decremento del 50% ogni 4 anni circa di modo che, col passare del tempo, si riduca sempre più la produzione di bitcoin[24]. Il protocollo di Nakamoto stabilisce un numero massimo di 21.000.000 di unità da produrre entro l'anno 2140 e, allo stato dell'arte, ne sono state prodotte un numero superiore a 14.000.000[25]; il limite alla produzione non è costituito da un numero casuale: ogni bitcoin rappresenta uno dei possibili valori digitali ottenuti applicando l'algoritmo crittografico di base che prevede esattamente 20.999.999,9769 di soluzioni[26]. Col progredire delle operazioni, il mining richiede sempre maggior tempo ed energia: occorrono macchine dedicate[27] le cui spese di acquisto si sommano ai costi di estrazione, calcolati in elettricità e potenza di calcolo impiegate[28], fissando così un floor al valore di cambio dei bitcoin in moneta corrente.

VERIFICA DELLE TRANSAZIONI

La circolazione dei bitcoin implica ulteriori calcoli da parte dei nodi della rete i quali, in applicazione del protocollo crittografico adottato, procedono alla verifica e alla convalida dei pagamenti eseguiti, garantendo l'effettività delle transazioni: questa caratteristica peculiare evidenzia che il valore posto a base del bitcoin consiste non tanto in un bene, quanto nel servizio offerto. Ciascuna transazione viene convalidata dalla generazione di 6 blocchi di conferma, sottoposti a verifica dai peer che compongono la rete con un operazione che può richiedere fino a un massimo di 50 minuti di tempo; la verifica avviene tramite l'applicazione dell'algoritmo di hash, funzione non reversibile che genera una stringa alfanumerica, detta digest, che varia al variare di ogni singolo elemento del file. 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 produrrebbero infatti un digest differente. Ogni operazione sui bitcoin viene convalidata dall'applicazione di una marca temporale, una procedura informatica che consente di associare data e ora certe al file, al fine di verificare che le attività si siano svolte secondo l'ordine tempo-

[24] Originariamente ogni blocco consisteva di 50 *bitcoin* mentre allo stato dell'arte vengono prodotti dei blocchi unitari di 25 *bitcoin*: la consistenza si è ridotta in questo senso a far data dal 28/11/2012, *vide https://blockchain.info/block-index/322335/000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e*.

[25] https://blockchain.info/it/charts/total-*bitcoin*s.

[26] Il software di produzione ha dovuto essere riscritto nell'agosto 2010 quando, a causa di un *bug*, il sistema era incorso in *un integer overflow,* errore 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/.

[27] *https://en.bitcoin.it/wiki/Mining_hardware_comparison*.

[28] http://www.rischiocalcolato.it/2014/01/*bitcoin*-costi-del-mining.html.

rale dichiarato, evitando che il cedente possa procedere a una nuova transazione con unità che ha già trasferito in precedenza e con ciò offrendo una soluzione efficiente al problema del double spending.

SICUREZZA DEL SISTEMA

La sicurezza del sistema si basa sulla proof of work, un valore che, se da un lato riduce le possibilità dei miner di ricevere bitcoin in premio della loro attività, dall'altro rende particolarmente complesso invertire le operazioni eseguite sui bitcoin: ogni blocco contiene infatti la trascrizione della proof of work di tutti i blocchi precedenti e ogni modifica apportata su di esso si riflette su quelli successivi[29]. In questo senso il whitepaper di Nakamoto sottolinea che il trasferimento dei bitcoin si svolge in sicurezza se la maggioranza della CPU nella rete peer-to-peer è controllata da nodi onesti[30]; il sistema è, infatti, immune dagli attacchi con tecniche di forza bruta in cui si provano in sequenza tutti i codici possibili: l'applicazione dell'algoritmo SHA 256 genera in output un digest con una quantità esponenziale di chiavi di decifratura possibili, per la cui individuazione occorrerebbero secoli di lavoro di un supercomputer. La reversibilità delle transazioni in bitcoin può essere efficientemente portata a termine solo dall'interno: si tratta del così detto 51% attack che consentirebbe a un gruppo di nodi collusi di prendere il sopravvento sul

[29] 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/.

[30] Satoshi Nakamoto: *Bitcoin A Peer-to-Peer Electronic Cash System,* 2008, p. 4: «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 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». http://*bitcoin*.org/*bitcoin*.pdf.

sistema compromettendone definitivamente la stabilità[31]; ad oggi non vi è notizia di attacchi di questo genere, peraltro l'aumentare del valore di mercato dei bitcoin rappresenta un incentivo al comportamento disonesto dei nodi da non sottovalutare.

CONSERVAZIONE E TRASFERIMENTO DEI BITCOIN

La conservazione dei bitcoin avviene alternativamente in portafogli on line, c.d. hot storage, o su supporti esterni scollegati dalla rete, c.d. cold storage, eventualmente 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 di accesso eventualmente installate.

Il trasferimento dei bitcoin si basa su un protocollo crittografico a chiavi asimmetriche[32] 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 a chiavi asimmetriche utilizza due chiavi alfanumeriche, una pubblica e distribuita di 34 caratteri e l'altra privata e strettamente personale di 51, 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 decrittare il messaggio[33]. Le parti vengono identificate tramite l'indirizzo IP, l'etichetta numerica che identifica in maniera univoca un dispositivo connesso a una rete che usa il protocollo internet, e un nome a loro scelta che può essere diverso per ogni transazione eseguita; quest'ultima caratteristica introduce la questione dell'anonimato, caratteristica permeante dei bitcoin: è l'utente che, impostando i parametri dell'indirizzo e variandoli a propria insindacabile valutazione, 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

[31] *Ibid*. p. 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».

[32] *Vide* Stalling W., Crittografia e sicurezza delle reti,2/ed Apogeo 2007 e Trappe W., Washinghton L. C. Crittografia con elementi di teoria dei codici, Pearson Ed. Italia 2009.

[33] 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 cambio della fine di novembre 2013 il prezzo in *bitcoin* delle due pizze sarebbe stato superiore a $ 12.500.000.

passaggi che la compongono[34]: ogni bitcoin è composto da 10.000.000 satoshi e può essere generato in blocco, secondo la procedura indicata, o acquistato sul mercato secondario dove tutte le unità e le loro frazioni possono essere spese.

ALTRI SCHEMI DI DIGITAL CURRENCY. LITECOIN

Litecoin[35] è una delle monete virtuali più diffuse, con capitalizzazione di mercato[36] 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 $ 3, il che conferisce allo strumento una maggiore praticità d'uso, rendendolo forse più adatto alla funzione di moneta virtuale richiesta dagli utenti dalla rete che a quella di investimento di banche e fondi istituzionali.

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 di monete virtuali Coinbase[37]. Pur mantenendo una struttura analoga alla previsione originaria, il nuovo protocollo introduce alcune rilevanti modifiche: il limite di produzione delle monete virtuali viene elevato a 85 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; l'innovazione più sensibile risiede, però, nella irreversibilità delle transazioni: questo principio risolve in radice il problema della doppia spendita dell'utility.

La maggiore frequenza di produzione dei blocchi ha però creato alcuni problemi a livello di generazione della proof of work: come evidenziato al paragrafo 3.1., l'hash di ogni blocco reca in sé la traccia del digest dei blocchi precedenti; nel sistema litecoin la computazione appare maggiormente complicata rispetto al modello bitcoin in ragione del fatto che il valore di convalida deve rimanere al disotto di una soglia che viene rideterminata con velocità quadrupla[38]. Per ovviare a questa

---

[34] http://blockchain.info/.

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

[36] «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.

[37] *Coinbase* è una società con base a San Francisco (Ca) che offre un servizio di gestione dei *bitcoin* che comprende compravendite agganciate a bonifici bancari, pagamenti, *wallet* di deposito e micro pagamenti gratuiti *user-to-user*. http://www.coindesk.com/litecoin-creator-charles-lee-has-left-google-to-work-at-coinbase/.

[38] *Vide* nota 21.

difficoltà, a partire dal mese di agosto 2014 Litecoin ha avviato un'attività di mining congiunto con Dodgecoin, la quinta moneta virtuale per capitalizzazione di mercato.

RIPPLE

Ripple[39] è un protocollo precedente a Bitcoin nato nel 2005 da un'idea di Ryan Fugger, un programmatore di Vancouver (CA) che ha sviluppato le teorie di Michael Linton riguardo ai LETS, local exchange trading system[40]; la struttura è gestita dai Ripple Labs, una società con base a San Francisco (Ca), fondata nel 2012 da Chris Larsen e Jed McCaleb con il nome originario di OpenCoin. Nel 2011, a seguito dell'interpretazione restrittiva delle disposizioni anti money laundering contenute nel Patriot Act, l'intero impianto di programmazione è stato ridisegnato in maniera da escludere ogni valore sottostante: ad oggi le monete no asset backed della piattaforma possono essere utilizzate con funzione solutoria user-to-user; come illustreremo meglio nel paragrafo 5.3., il protocollo consente anche degli interessanti risvolti in materia smart contract, non praticabili invece nel sistema Bitcoin, per via di un possibile sovraccarico della blockchain. La piattaforma Ripple funziona anche per il cambio fra valute di Paesi diversi, reperendo tra gli utenti coloro che sono disposti ad acquistare o a vendere una determinata valuta e mettendoli in contatto con chi intenda compiere l'operazione inversa; si può così immettere una moneta nel sistema che, eseguite le dovute operazioni, provvederà al pagamento in una divisa differente.

Le caratteristiche peculiari di Ripple rispetto al sistema Bitcoin consistono in premining: le monete virtuali, dette xrp, sono già tutte in circolazione nel numero di 100 milioni; di queste solo il 55% sono state messe 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%; irreversibilità dei pagamenti, fatto che, in maniera analoga a quanto accade nel sistema Litecoin, risolve in radice il problema della doppia spendita di queste monete virtuali; approvazione pressoché immediata dei pagamenti; 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 protocollo bitcoin.

Le monete virtuali di Ripple valgono pochi centesimi di dollaro e possono essere scambiate nel sistema senza che vengano applicati costi 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[41]; i costi

[39] https://ripple.com/.
[40] http://www.themoneyfix.org/interviewee/michael-linton.
[41] In questo tipo di attacco il server viene sommerso di richieste dall'esterno, fino ad impedirne il funzionamento.

di transazione richiesti non vengono, però, attribuiti a nessuno: gli xrp trasferiti a questo titolo vengono, infatti, annullati e rimossi dalla circolazione.

PROSPETTIVE ISTITUZIONALI E DI MERCATO

Prima di procedere all'illustrazione delle applicazioni derivate dai protocolli di moneta virtuale è bene fare un primo punto della situazione; gli studi giuridici ed economici sugli algoritmi di criptazione hanno avuto origine proprio da queste utility: nel 2013 il successo di mercato ottenuto dai bitcoin aveva addirittura fatto temere lo scoppio di una bolla speculativa; pur trattandosi di un'eventualità al momento scongiurata, la regolamentazione normativa del fenomeno rimane attuale, rispondendo a esigenze di garanzia dell'ordine sociale ed economico: il controllo dei flussi finanziari segue, infatti, l'evoluzione dei mezzi di pagamento e nel terzo millennio si sposta sul piano digitale.

De jure condendo, l'azione in un mercato globale prevede la creazione di regole di comportamento omogenee: gli algoritmi criptati di pagamento rappresentano un'interessante frontiera riguardo cui una regolamentazione di concerto internazionale ridurrebbe gli incentivi al free riding basati sulla scelta del'ordinamento più conveniente (c.d. forum shopping). Si pensi solo al dato fiscale, materia in cui ogni Stato dello Spazio Economico Europeo detta principi autonomi[42]: allo stato dell'arte, l'Autorità Danese opta per una completa esclusione del fenomeno dall'area di operatività della normativa fiscale[43]; la Banca di Finlandia propende per una definizione di commodity finanziaria; l'Ufficio delle Tasse Britannico, ritiene non si tratti di valuta ma di un bene e si interroga sull'applicabilità dell'Imposta sul Valore Aggiunto[44]; l'Autorità Federale Tedesca di Supervisione Finanziaria individua, invece, la natura dello strumento in dipendenza dell'uso che ne viene fatto[45]; dal canto proprio, l'autorità Norvegese si limita a considerare il fenomeno come estraneo all'alveo della moneta legale mentre la Svizzera potrebbe addirittura riconoscere i bitcoin come valuta straniera.

Per quanto riguarda la normativa sostanziale, bisognerà tenere conto che l'utilizzo della crittografia rende praticamente impossibile intervenire in via diretta sui protocolli, rendendo necessario agire sui meta-elementi, le caratteristiche della

---

[42] http://www.investireoggi.it/economia/*bitcoin*-leuropa-non-sa-che-fare-in-finlandia-aperto-il-primo-*bitcoin*-atm/.

[43] http://politiken.dk/oekonomi/dkoekonomi/ECE2244816/*bitcoin*-gevinster-kan-stikkes-direkte-i-lommen/ 2014 e., http://www.coindesk.com/denmark-declares-*bitcoin*-trades-tax-free/ 2014.

[44] http://www.bloomberg.com/news/2014-01-19/*bitcoin*-becomes-commodity-in-finland-after-failing-currency-test.html 2014. Per un'interessante disamina riguardo l'applicabilità del regime IVA *vide* S. Capaccioli: Introduzione al trattamento tributario delle valute virtuali: criptovalute e *bitcoin*, in «Diritto e Pratica Tributaria Internazionale», CEDAM, – n. 1/2014, pag. 27-68.

[45] 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'.

fattispecie che non dipendono in senso stretto dal sistema di pagamento utilizzato. Non è dato prevedere nel dettaglio i contenuti dei testi normativi che gli Stati adotteranno ma le linee di intervento con maggiori probabilità di applicazione sono quelle che riguardano una forma di equiparazione delle monete virtuali alla valuta: come evidenziato alla Bitcoin USA Senate Hearing del 2013, è in predicato la stabilità stessa del sistema finanziario[46]. Si potrebbero, dunque, stabilire i presupposti di liceità delle transazioni, come la provenienza da indirizzi correttamente agganciati a dati reali; si potrebbe, altresì, intervenire sul valore delle transazioni stabilendo sotto quale cifra gli uffici finanziari perdano interesse all'accertamento delle transazioni intervenute, senza preclusione alcuna per le indagini di polizia, come avviene con gli acquisiti in contante: norme di questo genere presenterebbero il vantaggio di consentire un uso legittimo secondo parametri prestabiliti e avrebbero maggiori probabilità di essere accettate dagli utenti. Riteniamo che sarebbe inoltre opportuno intervenire a tutela degli investitori, introducendo l'autorizzazione istituzionale degli intermediari e la garanzia obbligatoria dei depositi: i furti on line a carico delle piattaforme BIPS (Bitcoin Internet Payment Services)[47] e Mt.Gox[48] hanno reso evidente che gli Stati non possono rimanere ai margini di un fenomeno che ha ormai assunto contorni di raccolta del risparmio. Un intervento di regolamentazione organica della materia offrirebbe un incentivo di mercato efficiente: la predisposizione di regole di concerto riguardo i termini e gli oneri delle nuove utility ridurrebbe sensibilmente gli incentivi al forum shopping; i controlli istituzionali sugli intermediari, l'assicurazione obbligatoria dei depositi e l'applicazione delle procedure di sicurezza standard compenserebbero, forse, in termini di costo alcuni dei vantaggi derivanti dall'uso delle monete virtuali ma la loro attuazione sarebbe in grado di offrire dei termini di garanzia, a nostro parere, particolarmente graditi agli investitori.

PROTOCOLLI DERIVATI

Come illustrato al paragrafo 3., il sistema Bitcoin applica l'algoritmo di Hash ad ogni passaggio della blockchain, in modo da assicurare l'identità del prodotto ottenuto: ogni blocco reca in sé la traccia del digest che identifica il precedente; la catena logica è 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 trova applicazione anche all'esterno del sistema dei pagamenti: gli algoritmi oggetto di questo studio sono, infatti, idonei all'identificazione di dati e al trasferimento di diritti in generale; utilizzando i protocolli derivati dal sistema

[46] http://www.hsdl.org/?view&did=747209.

[47] Ora acquisito da Coinfy https://coinify.com/.

[48] http://www.ilsole24ore.com/art/finanza-e-mercati/2014-02-28/piattaforma-bitcoin-mt-gox-dichiara-bancarotta-persi-345-milioni-euro-160351.shtml?uuid=ABXu8tz&refresh_ce=1.

BItcoin, è oggi 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 [49] di e B-money[50], entrambi gli autori, considerati dalla rete gli ispiratori del lavoro di Satoshi Nakamoto, che hanno teorizzato l'applicazione dei protocolli crittografici allo schema contrattuale predicendo addirittura degli esiti in cui la definizione computazionale delle clausole si sarebbe rivelata self-enforcing.

WOIN

Il primo sviluppo del sistema Bitcoin in questa direzione è stato attuato nel 2011 con la fork Namecoin[51]: la prima idea del progetto era contenuta in una serie di post, apparsi sul forum Bitcointalk.org alla fine del 2010 [52], che avevano messo

---

[49] 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.

[50] 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.

[51] https://namecoin.info/.

[52] https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696 . https://bitcointalk.org/index.php?topic=1790.msg22019#msg22019. https://bitcointalk.org/index.

in luce come il registro di blockchain potesse servire, oltre che per implementare 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 protocollo Bitcoin sarebbe stato eccessivamente appesantito dalle registrazioni dei domain name; si era così ipotizzato di risolvere il problema con una fork dell'algoritmo base: in un interessante scambio di vedute fra Satoshi Nakamoto e Hal Finney riguardo l'opportunità di inserire dei costi di transazione, era stato delineato uno degli elementi distintivi del modello ipotizzando che ogni protocollo fosse dotato di una propria moneta[53]; la proposta conteneva anche l'idea di un sistema di cessione volontaria dei nomi dei domini, con il solo limite della disponibilità effettiva[54], 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[55], 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; la chiave crittografica pubblica della moneta viene inserita nel registro di blockchain, consentendo una verifica analoga al quella del sistema Bitcoin. Per ragioni di protezione della privacy, gli amministratori del progetto stanno valutando di accettare in futuro le unità prodotte da zerocash, un protocollo che implementa l'anonimato del progetto Bitcoin introducendo il trasferimento basato su una dimostrazione a conoscenza zero[56]. Per quanto le caratteristiche di Namecoin consentano un uso tradizionale del sistema, la proprietà che troviamo maggiormente interessante consiste nella possibilità di inserire atti e documenti nel registro di blockchain con codifica crittografica in un'unità di moneta. Le implicazioni di questo protocollo sono molteplici e si rivelano particolarmente interessanti anche

---

php?topic=1790.msg28917#msg28917.

[53] 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.*»

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.*»

[54] *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.*»

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

[56] 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; v*ide:* 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, p. 628-631.

sotto il profilo istituzionale: adottando una soluzione di questo genere, infatti, gli enti che in ragione del proprio funzionamento rilasciano documenti potrebbero creare delle catene crittografate di emissione che renderebbero più agevole e maggiormente sicura la creazione dei titoli. Come già evidenziato, ogni eventuale manomissione del protocollo creerebbe una biforcazione della catena logica, rendendo immediatamente individuabili eventuali corpi estranei: si pensi all'emissione dei documenti di identità personale, caso in cui la possibilità di individuare digitalmente ogni falso si rifletterebbe positivamente sulla sicurezza nazionale, senza contare che l'applicazione di un algoritmo unico risulterebbe vantaggiosa anche in termini economici.

COLORED COIN

Colored coin[57] è una seconda implementazione del protocollo Bitcoin che consente di inserire nella blockchain elementi come l'identificazione di dati personali, messaggi o diritti digitali su beni: gli elementi indicati vengono computati nel codice di una moneta che anche questo sistema qualifica in maniera speciale, in maniera da impedirne la spendita accidentale; nel caso dei diritti trasferibili, il trasferimento della moneta comporta quello del diritto collegato. Funzionalmente, la piattaforma replica la struttura del protocollo Bitcoin, cui fa riferimento per ogni ulteriore dettaglio: per questa ragione le piattaforme analoghe a Colored Coin vengono anche identificate come Bitcoin 2.0.

Sotto il profilo istituzionale, i protocolli 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 illustrate al paragrafo 3, nel rispetto dei limiti dell'ordinamento giuridico di riferimento.

Hashing platform e smart contract

[57] http://coloredcoins.org/.

Il passo successivo, conosciuto anche come Bitcoin 3.0, è quello delle hashing platform come Ethereum[58], Omni[59] e Ripple, architetture internet la cui funzione consiste nell'individuazione univoca di dichiarazioni e accordi tramite applicazione dell'algoritmo di Hash: i digest così ottenuti vengono inseriti nel codice di una delle monete di riferimento consentendo la gestione tramite registro di blockchain di tutte vicende collegate. Ethereum e Omni sono applicazioni derivate dal protocollo Bitcoin, di cui replicano il registro logico tramite chainfork, mentre, come indicato nel paragrafo 3.2.2., Ripple costituisce un protocollo autonomo.

Una delle più interessanti innovazioni delle hashing platform consiste nella possibilità di dare attuazione ai c.d. smart contract: la categoria è stata teorizzata da Nick Szabo nel 1997[60], prendendo spunto dallo schema di vendita dei distributori automatici; la proposta dell'autore mette a servizio della contrattualistica la crescente potenza computazionale scrivendo alcune clausole direttamente nel software e rendendo così l'inadempimento di scarsa convenienza, se non addirittura proibitivo, in termini economici.

Lo schema, fondato sulla crittografia, consiste di quattro elementi base:

Una chiave idonea a un ingresso selettivo dei contraenti e all'esclusione di terzi non autorizzati; Una back door che consenta sempre l'ingresso alla parte creditrice;

L'attivazione della back door del creditore in dipendenza del mancato pagamento per un determinato periodo di tempo; e Il pagamento finale a disattivazione permanente della back door.

Nell'era digitale molti contratti vengono gestiti in Electronic Data Interchange, un protocollo che, in alcuni casi, rende addirittura automatica la loro conclusione ed esecuzione: si pensi, ad esempio, alle aste computerizzate per il posizionamento di banner pubblicitari sulle pagine visualizzate dagli utenti Internet. Lo smart management del contratto rappresenta un passo ulteriore su questa strada, idoneo a consentire forme di gestione dinamica che negli altri casi restano impraticabili per via dei costi di transazione: i servizi offerti dalle hashing platform sono in grado di implementare la fattispecie contrattuale aggiungendo alla caratteristica della veri-

---

[58] La creazione di questo protocollo è valsa al giovane programmatore Vitalik Buterin il premio World Technology 2014 http://www.wtn.net/summit-2014/2014-world-technology-awards-winners; il *white paper* https://github.com/ethereum/wiki/wiki/White-Paper del 2013 è stato implementato da uno *yellow paper* http://gavwood.com/Paper.pdf scritto da Gavin Wood nel 2014 e il progetto è stato finanziato con un *bitcoin crowdfunding* che ha realizzato un controvalore di oltre $18.000.000 http://www.reddit.com/r/ethereum/comments/2fhmzm/ethereum_was_second_largest_crowdsale_in_history/.

[59] Omni, lanciata nel 2015, è la versione implementata di Mastercoin, hashing platform nota anche come 'Il secondo protocollo *Bitcoin*' https://github.com/OmniLayer/spec.

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

The Idea of Smart Contracts, 1997, http://szabo.best.vwh.net/idea.html.

ficabilità matematica il self enforcement di alcune clausole contrattuali; il sistema varia in funzione dei diritti dedotti e dei diversi termini pattuiti, con l'inserimento di trigger point osservabili in via immediata nel registro di blockchain, come l'esercizio di una determinata opzione.

Si tratta di un modello suscettibile di sviluppi interessanti che riduce i costi di gestione del contratto rendendo automatici alcuni eventi che si realizzano in conseguenza di fatti matematicamente accertati: riteniamo che questo schema soddisfi pienamente le esigenze della società contemporanea, offrendo rapidità e speditezza ai traffici giuridici. Resta aperta l'interessante questione della riferibilità a persona certa, un elemento che de jure condendo sarà imprescindibile chiarire se, come auspichiamo, le istituzioni decideranno di percorrere questa strada innovativa anche per il trasferimento dei beni registrati; negli altri casi essa degrada a mera utilità, lasciando le parti libere di contrattare nel modo che preferiscono.

CONCLUSIONI

Lo studio delle potenzialità di mercato degli algoritmi di criptazione è soltanto all'inizio: l'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. E' 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 protocolli 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; a conclusione della nostra analisi non possiamo che 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.