Data di pubblicazione: 28 febbraio 2017

Bitcoin e *distributed ledger technology*

di Ottavio Calzone

Abstract

La rete *Bitcoin* è il primo sistema di pagamento basato sul concetto di *distributed ledger technology* o *blockchain*: una rete di scambi in cui non vi è un'autorità incaricata di validare e registrare le transazioni. Ideata nel 2008, sta riscuotendo molto interesse, testimoniato anche dal fatto che negli ultimi due anni[1] si è passati da 50 milioni ad oltre 200 milioni di dollari[2] al giorno di transato, con punte di 500 milioni[3]. Il presente lavoro offre una panoramica del fenomeno, indicando anche dei siti utili per continuarlo a monitorare. Sono inoltre illustrate alcune delle realtà nate intorno al concetto di *blockchain* per sviluppare applicazioni non necessariamente legate agli scambi di moneta. In appendice è spiegato il funzionamento della rete *Bitcoin* da un punto di vista tecnico ma in modo per quanto possibile semplificato ed intuitivo.

Profilo

Ottavio Calzone svolge attività di *Marketing Intelligence* in ambito finanziario e bancario. Laureato presso l'Università di Siena dove ha conseguito anche il master in Economia Digitale ed E-Business che lo ha introdotto nello studio delle sinergie fra comportamenti sociali e tecnologie.[4]

Keyword Bitcoin, blockchain, distributed ledger technology, altcoin, Meta Coin

Sommario 1. Introduzione – 2. Il bitcoin – 3. Altre applicazioni della blockchain – 4. Prospettive future – 5. Conclusioni – Appendice. Funzionamento della rete Bitcoin – Note – Bibliografia

1. Introduzione

La rete *Bitcoin* è il primo sistema di pagamento basato sul concetto di *distributed ledger technology* o *blockchain*: una rete di scambi in cui non vi è un'autorità incaricata di validare e registrare le transazioni.

Per provare a visualizzare l'idea di fondo di un sistema di questo tipo, si può ricorrere ad un esempio tratto dal comportamento delle formiche[5]. Anche se il funzionamento della colonia del suo complesso non è banale, nella ricerca del cibo ogni formica esegue solo azioni semplici: girovagare a caso; verificare di aver trovato il cibo; tornare al nido; lasciare una scia di feromone lungo il ritorno; seguire una traccia di feromone già esistente. Le formiche che casualmente si trovano

vicino ad un percorso indicato con il feromone tenderanno a seguirlo e, ritornando al nido con il cibo, lasceranno a loro volta del feromone lungo la strada. Il percorso sarà così rafforzato e, con il passare del tempo, tutte le formiche convergeranno lungo la traccia che porta al cibo. Anche se non vi è un'autorità di controllo, nessuna formica può da sola creare un percorso falso, perché è il comportamento della maggioranza a stabilire la via migliore.

Nella rete *Bitcoin*, al posto delle formiche ci sono dei nodi collegati fra loro via internet per scambiarsi informazioni sui trasferimenti della valuta virtuale *bitcoin* con comunicazioni *peer-to-peer* (nodo a nodo). Ogni nodo[6] ha una copia del registro contabile dove memorizza i trasferimenti di valuta di tutta la rete, a partire dal primo avvenuto nel 2009. Le transazioni sono così pubbliche, note a tutti i nodi e conservate in una catena di blocchi (*blockchain*) in cui quelle avvenute nello stesso momento si trovano nello stesso blocco.

Come per il percorso verso il cibo delle formiche, non vi è un'autorità incaricata di stabilire le registrazioni contabili da effettuare, ma è il comportamento semplice dei singoli nodi a determinare il funzionamento della rete nel suo complesso. Un funzionamento tale che tutte le copie del registro si aggiornano automaticamente e in breve tempo.

In pratica, la rete *Bitcoin* è un sistema di pagamento:

- ad accesso libero e gratuito: per diventare un nodo della rete è sufficiente scaricare un client che implementi il protocollo *Bitcoin*;
- open-source: il client ufficiale Bitcoin Core è rilasciato anche in codice sorgente e chiunque può sviluppare applicazioni che si interfaccino con la rete
- scalabile: è facile aggiungere nuovi nodi
- robusto: la chiusura di un nodo non incide sul funzionamento complessivo del sistema
- a fiducia distribuita: non è necessario fidarsi di un'entità centrale che registri le transazioni o che controlli che tutte le copie del registro contabile siano identiche
- immediato: gli scambi di valuta avvengono nel giro di dieci minuti
- tracciabile: è possibile ricostruire tutte le transazioni a partire dalla prima avvenuta nel 2009;
- pseudo-anonimo: la rete non registra i dati sulla titolarità dei 'conti' sui quali avvengono i trasferimenti di valuta
- internazionale: il funzionamento della rete non dipende da dove viene utilizzata
- sicuro: fa ampio uso della crittografia per risolvere potenziali problemi come la registrazione di doppi pagamenti
- premiante: è previsto un meccanismo di ricompensa per chi usa la propria potenza di calcolo al servizio del buon funzionamento del sistema.

L'oggetto che viene scambiato nella rete è una valuta virtuale: il *bitcoin*. Quando si vuole parlare della valuta si usa in genere la lettera minuscola.

Una valuta virtuale è una rappresentazione digitale di un valore che, pur non essendo creato da una banca centrale, un'autorità pubblica o per mezzo di un legame con una valuta in corso legale, è

accettato da persone fisiche e giuridiche per effettuare dei pagamenti[7]. Questo valore può essere trasferito e conservato.

2. Il *bitcoin*

Una valuta virtuale ha valore solo se è accettata da qualcuno in cambio di qualcosa: se esiste un mercato disposto ad acquistarla offrendoci dollari, altre valute o asset. Per il *bitcoin*, la prima proposta di questo tipo[8] è stata fatta il 5 ottobre 2009 dal sito New Liberty Standard[9]. Il cambio era di un dollaro ogni 1.309,03 *bitcoin*.

Stando ai dati riportati da Blockchain.info[10], il valore di un *bitcoin* è al 12 febbraio 2007 di circa mille dollari, che, moltiplicati per gli oltre sedici milioni in circolazione[11], fornisce una stima di sedici miliardi di dollari per la rete nel suo complesso. Negli ultimi due anni il numero di transazioni giornaliere è passato da circa 100 mila a quasi 350 mila e il volume degli scambi da circa 50 milioni ad oltre 200 milioni di dollari al giorno, con punte di 500 milioni[12].

Accettano pagamenti in *bitcoin* realtà come Microsoft, l'editore Bloomberg, il produttore di auto elettriche Tesla, fino ad arrivare a piccoli esercenti come librerie locali e *bed and breakfast*[13]. La 'banca' Bitbank.com[14] ha depositi per oltre 260 mila *bitcoin* e il sito Coinmap.org[15] visualizza, in stile Google Map, quasi 9.000 luoghi nel mondo dove è possibile usarli per i pagamenti.

I mercati (*exchange point*) recensiti dal sito Bestbitcoinexchange.io[16] sono oltre quaranta. In base al volume degli scambi, riportato su base giornaliera da Coinmarketcap.com[17] e su base mensile da Bitcoincharts.com[18], oltre il 90% dei cambi è con lo Yuan e i mercati principali sono i cinesi BTCC ed OKCoin.

Ogni mercato è organizzato da un *market maker* che propone le condizioni. Non esiste un listino ufficiale, anche se il sito Winkdex.com[19] propone il *Winklevoss Index*, basato sulle informazioni raccolte dai vari mercati. L'accettazione è su base volontaria: acquistando *bitcoin* ci si fida del fatto che anche in futuro ci siano dei mercati disposti a ricomprarli. Alla stregua di una valuta legale, sono stati creati un codice identificativo (BTC o XBT) e un simbolo: una B con una barra come la $ del dollaro. Esiste anche un mercato geograficamente distribuito (Localbitcoins[20]) dove chiunque può vendere la propria valuta virtuale proponendo un prezzo. Un altro modo per cambiare i *bitcoin* è usare dei mercati fisici: ATM che li comprano offrendoci la valuta del luogo in cui ci troviamo. Il sito Coinatmradar.com[21] elenca circa mille ATM di questo tipo in 55 paesi.

Il primo incremento significativo del valore del *bitcoin* è avvenuto in seguito alla crisi cipriota del marzo 2013[22]. Il piano di salvataggio dell'economia cipriota prevedeva anche un prelievo forzoso sui conti correnti, e i correntisti iniziarono ad acquistare valuta virtuale svuotando i propri conti. Il tasso di cambio passò così rapidamente da 80 a 260 dollari.

L'acquisto massivo da parte dei correntisti ciprioti era legato alla non confiscabilità e allo pseudo-anonimato delle transazioni[23]. La rete *Bitcoin* si basa sull'assenza di un'autorità di controllo e al suo

interno sono noti solo codici alfanumerici: gli indirizzi con i quali si riceve e spedisce valuta. Solo gli *exchange point*, per effettuare il cambio con dollari, altre valute o asset, sono tenuti a registrare informazioni sulla titolarità degli indirizzi, come il nome o la residenza di chi li possiede.

Con un client si possono creare più indirizzi. La moneta virtuale ricevuta può così essere spedita a un altro indirizzo di cui si dispone, ma la cui titolarità non è nota perché mai usata in un processo di registrazione, per poi essere ricambiata in un secondo momento, magari da un prestanome, in una nazione in cui sia in vigore una legge diversa sulla confisca dei beni. Per favorire le transazioni illegali o il riciclaggio di denaro sono nati anche dei servizi, di *mixing* o *tumblers*, per rendere più difficoltosa la ricostruzione dei vari passaggi di proprietà[24]. Parallelamente sono stati creati strumenti per l'analisi dei trasferimenti della valuta virtuale, come quelli offerti dal sito Chainalysis.com[25].

Quanto avvenuto a Cipro ha attirato l'interesse delle istituzioni e dei media e, in seguito alla diffusione delle prime notizie sull'apertura nei confronti della rete *Bitcoin* da parte dei governi di USA e Cina, il valore di un *bitcoin* aumenta fino a raggiungere i 1.132,26 dollari il 29 novembre 2013[26].

Dopo più di tre anni il fenomeno non si è esaurito, alimentato principalmente dall'uso della rete fatto in Cina come mercato valutario parallelo e come strumento per trasferire capitali all'estero al di fuori dei canali ufficiali. Per questi motivi recentemente la banca centrale People's Bank of China ha deciso di avviare un'inchiesta sui tre principali *exchange point* cinesi: BTCC, OKCoin e HUOBI[27].

Attualmente l'atteggiamento ufficiale delle istituzioni cinesi è considerato 'controverso': l'uso dei *bitcoin* è consentito solo alle persone fisiche. Il sito Bitlegal.io[28] indica per ogni paese il livello di apertura verso questa valuta virtuale e al momento gli unici paesi che hanno un atteggiamento considerato 'ostile' sono Islanda, Equador, Repubblica Domenicana e Bolivia. Il caso dell'Islanda è particolare: per difendere la propria moneta dal crollo del 2008, è vietato usare la Corona islandese per comprare *bitcoin*, visto come un modo per trasferire capitali all'estero, mentre è possibile fare il contrario[29].

Anche nei paesi in cui è legale, non tutti concordano se considerare o no il *bitcoin* come un semplice asset finanziario o una moneta a tutti gli effetti, uno strumento cioè con cui è possibile:

- esprimere il valore di beni e servizi (funzione di unità di conto)
- acquistare merci e servizi (funzione di mezzo di scambio)
- rimandare la spesa in un momento futuro non perdendo valore (funzione di riserva di valore).

La distinzione fra asset finanziario e moneta può avere delle implicazioni non banali, applicandosi in molti casi regole contabili diverse per rappresentare le due tipologie di asset in un bilancio e regole fiscali differenti a seconda che si consideri una moneta o un'altra tipologia di asset.

Oggi in Europa è prevalente la definizione data dall'Autorità Bancaria Europea (EBA), che considera il *bitcoin* una valuta virtuale, intesa come una rappresentazione digitale di un valore che, pur non essendo creato da una banca centrale, un'autorità pubblica o per mezzo di un legame con una valuta in corso legale, è tuttavia accettato da persone fisiche e giuridiche per effettuare dei pagamenti e pertanto può essere sia trasferito che conservato[30]. Questa accezione è la stessa che si ritrova nella risoluzione 72/E/2016 dell'Agenzia delle Entrate italiana che sancisce che le attività di cambio svolte dagli *exchange point* sono attività di intermediazione fra valuta reale e valuta virtuale, attività sulla quale non si applica l'IVA[31].

Anche se l'accezione dominante è quella di valuta virtuale e non di asset finanziario, da una ricerca dello SWIFT Institute emerge che, almeno fino a metà 2016, l'uso principale del *bitcoin* è come asset da detenere piuttosto che come mezzo di scambio in quanto considerato da molti *trader* come una riserva temporanea di valore a differenza di altri asset che si deprezzano facilmente[32]. Tuttavia l'EBA mette in guardia dai rischi connessi al detenere valuta virtuale e scoraggia le banche e gli altri intermediari vigilati dall'acquistare, detenere o vendere valute virtuali[33].

3. Altre applicazioni della blockchain

Il successo del *bitcoin*, a partire dal primo rilascio nel 2009 del software su cui si basa la rete, ha attirato l'interesse di numerose realtà. Oggi il sito Coindesk.com[34] registra oltre 250 start-up, nate intorno al concetto di *blockchain*, che hanno ricevuto investimenti da fondi di *venture capital* per un totale di circa 1.500 milioni di dollari. Il sito Angel.co[35] elenca poco più di 500 start-up operanti in questo campo che hanno attirato investitori 'Angel' con una valutazione media di 4,2 milioni di dollari a start-up. Sono inoltre censiti oltre 700 investitori 'Angel' attivi nel settore.

L'investimento in tecnologia *blockchain* non è realizzato solo tramite start-up, ma anche attraverso lo sviluppo in proprio o tramite consorzi. Alcune istituzioni finanziarie hanno registrato o inoltrato richieste di registrazione per brevetti riguardanti *blockchain*. Le realtà più attive in tal senso sono Bank of America, Goldman Sachs, JPMorgan, CitiBank e Bank of New York[36]. Il Consorzio R3[37] raggruppa oltre 75 delle principali istituzioni finanziarie mondiali per lo sviluppo di applicazioni finanziare che sfruttino la *distributed ledger technology* e la Linux Foundation ha creato il progetto Hyperledger[38], inteso come una cooperazione fra individui e aziende, comprese istituzioni finanziarie, per lo sviluppo della tecnologia *blockchain* in ottica *open source*. Lo sviluppo collaborativo è anche alla base del protocollo *Bitcoin*, portato avanti da una comunità di volontari riuniti intorno al sito Bitcoin.org[39].

È possibile segmentare il mercato delle soluzioni *blockchain* in base all'oggetto scambiato dalla rete di nodi: *bitcoin*, valute non virtuali, valute virtuali, contratti *smart*, altri asset, documenti.

Nella prima categoria possono essere inserite le varie realtà nate intorno alla rete *Bitcoin* per sfruttarne il successo offrendo servizi complementari. Rientrano in questo segmento società come Coinbase[40], che offre un servizio di cambio con altre valute, ma anche le realtà che sviluppano

sidechain: interfacce che permettono di collegare la rete *Bitcoin* ad altre reti che sfruttano protocolli differenti per lo scambio di valuta virtuale.

L'integrazione fra un servizio di cambio valute a una rete proprietaria simile a quella *Bitcoin* è alla base di un altro segmento di mercato, quello dei pagamenti in valute in corso legale su tecnologia *blockchain*, che garantisce la tracciabilità storica delle transazioni e l'aggiornamento delle varie copie del registro contabile senza necessità di meccanismi di audit. Rientra in questa categoria il servizio di pagamento via *app* offerto da Circle Internet Financial[41].

Abbiamo poi la categoria delle *altcoin* (*alternative coin*) composta da realtà nate per replicare il successo del *bitcoin* proponendo reti di scambio ognuna con la propria valuta virtuale. Il sito Coinmarketcap.com[42] elenca oltre 600 realtà di questo tipo, anche chiamate criptovalute poiché queste reti fanno ampio uso di algoritmi di criptografia. Appartengono al segmento realtà come Litecoin, Dogecoin, Monero, Peercoin, Namecoin. Fra queste, Monero ha quadruplicato nel 2016 in poco tempo il suo valore in seguito alla sua accettazione da parte di AlphaBay, sito illegale per la vendita di droghe[43]. L'accettazione da parte di AlphaBay è dovuta al fatto che, pur ispirandosi al *Bitcoin*, il protocollo di Monero rende non tracciabili le transazioni[44].

Alcune delle realtà incluse nella categoria *altcoin* rientrano invece più propriamente nel concetto di *Meta Coin*[45]. Dove per 'meta' si intende qualcosa che supera l'idea di moneta che abbiamo. La moneta è infatti un qualcosa di inanimato, ma grazie ad internet è possibile trasformarlo in qualcosa di autonomo, dinamico, intelligente e veloce. In una parola in qualcosa di *smart*. Gli *smart contract* sono contratti scritti usando delle piattaforme informatiche ad hoc in modo che le transazioni previste avvengano in maniera automatica e controllata dalla piattaforma al verificarsi di determinati eventi. La piattaforma Ethereum[46] usa il concetto di *blockchain* per la creazione e lo scambio di contratti *smart* in cui i pagamenti avvengono nella valuta virtuale 'ethereum' (in codice ETH). L'applicabilità del concetto di *smart contract* spazia dal *crowdfunding*, al *commercial paper* delle banche, ai derivati, e a tutti quei casi in cui un trasferimento di denaro è legato al verificarsi di un evento o ad una determinata scadenza temporale.

Le realtà considerate fino ad ora sono reti che permettono lo scambio, anche attraverso contratti *smart*, di una valuta, virtuale o meno. Tuttavia un database distribuito basato sul concetto di *blockchain* può registrare e permettere lo scambio di informazioni di varia natura. Sono state sviluppate così applicazioni che permettono di registrare e trasferire la titolarità di asset di vario tipo (oro, azioni, ecc.). Rientrano in questo segmento realtà come Counterparty[47].

Anche l'informazione riportata in un documento è un asset. È questa l'idea alla base del prodotto Harmony della società Factom[48], che sfrutta la tecnologia *blockchain* per la gestione documentale (*document management*). L'uso di una *distributed ledger technology* in questo campo ha numerosi vantaggi. In particolare permette di avere tutto lo storico dei trasferimenti di informazione fra i vari partecipanti alla rete, riducendo così potenziali dispute legali dovute all'accusa di non condivisione di dati. Si possono creare anche dei meccanismi di ricompensa legati allo sviluppo di 'nuova

conoscenza', creando consorzi per lo sviluppo di brevetti in cui le percentuali di titolarità degli stessi siano legate alla contribuzione data da ognuno. Contribuzione che è possibile ricostruire da tutti i partecipanti alla rete in base alla propria copia del registro degli scambi di documenti.

Proprio perché tutti possiedono una copia del registro, soluzioni di *document management* possono andare incontro a problemi di privacy, specie quando le informazioni sono sensibili, come potrebbero essere le cartelle cliniche dei pazienti di più ospedali, o quando i partecipanti della rete operano in giurisdizioni diverse con norme differenti per quanto riguarda la privacy. In questi casi è possibile studiare soluzioni tecnologiche per preservare la riservatezza dei dati sensibili o soluzioni giuridiche come la realizzazione di consorzi con regole comuni sulla gestione della privacy.

Il concetto di informazione come asset che è possibile trasferire è alla base anche della *Internet of Things*, in cui a scambiare dati non sono persone fisiche ma dispositivi 'intelligenti', hardware e software, che cooperano fra loro per realizzare uno scopo condiviso, come tracciare i vari passaggi di una merce fra i diversi punti di una *supply chain*. La *distributed ledger technology* è considerata dagli esperti una tecnologia abilitante per lo sviluppo di applicazioni in questo campo[49].

4. Prospettive future

David Schatsky e Craig Muraskin, in un'analisi pubblicata dalla Deloitte University[50], evidenziano come prima del 2015 ci si focalizzava principalmente nel realizzare soluzioni che offrissero servizi completi basati sulla tecnologia *blockchain*, come Circle Internet Financial[51], che propone servizi di pagamento via *app*, o la stessa rete *Bitcoin*. A partire dal 2015 il focus si è spostato verso l'offerta di servizi per la realizzazione di reti *blockchain* personalizzate (es. BlockCypher[52] e Chain[53]) e verso lo sviluppo di nuovi protocolli informatici basati sul concetto di *distributed ledger technology* (ad esempio, Ripple[54] e Blockstream[55]).

Questa evoluzione nasce dalla considerazione che la tecnologia *blockchain* può essere applicata in numerosi campi. Tuttavia oggi la vera sfida da cogliere sembra essere quella di sfruttare la *distributed ledger technology* non come una tecnologia fine a se stessa, da usare per lo scambio di asset, ma come una soluzione che, attraverso gli scambi, consente di realizzare reti sociali per la creazione di valore. Un tentativo in tal senso è stato fatto da 21 Inc.[56], sito di profili professionali, tipo LinkedIn, in cui la risposta ai messaggi ricevuti è incentivata attraverso la ricezione di *bitcoin*. Lo scambio di denaro non è quindi la finalità della rete, ma un mezzo per incoraggiare un comportamento sociale. Stesso principio su cui si basa Solarcoin.org[57] in cui la produzione di energia solare è incentivata con pagamenti in valuta virtuale 'solarcoin'.

Anche la piattaforma Augur[58] usa la tecnologia *blockchain* per creare una rete di comportamenti sociali. In questo caso la finalità è stimare la probabilità di eventi futuri. In maniera molto semplificata, i partecipanti alla rete Augur possono acquistare o vendere quote di una scommessa. Il prezzo degli scambi è una stima della probabilità che i partecipanti danno a un determinato evento. Anche se la finalità dei singoli individui è vincere la scommessa, il loro comportamento

determinerà una stima sul verificarsi di un evento. L'idea di fondo è che la probabilità calcolata sulla base del comportamento di molti sia più accurata della stima che può fare un singolo individuo. La tecnologia *blockchain* è usata in questo caso per consentire gli scambi delle quote ed effettuare i pagamenti al verificarsi degli eventi su cui si è scommesso.

5. Conclusioni

La rete *Bitcoin* è il primo sistema di pagamenti basato sul concetto di *distributed ledger technology* o *blockchain*: una rete di scambi in cui non vi è un'autorità incaricata di validare e registrare le transazioni. Oltre al suo successo, sono da registrare quelli di altre reti che hanno applicato la stessa tecnologia in campi molto diversi fra loro.

Lo sviluppo di queste reti ha attirato l'interesse di molti e uno degli interrogativi odierni è se tale successo possa essere replicabile e duraturo. Per rispondere a queste domande sarebbe forse opportuno usare Augur e prevedere, attraverso una rete *blockchain*, il futuro delle reti *blockchain*. Anche se questo può sembrare solo un gioco di parole, nasconde una verità più profonda. Nei fenomeni di rete spesso il successo è autoreferenziale: il fallimento determina ulteriore fallimento ed il successo ulteriore successo.

Appendice. Funzionamento della rete *Bitcoin*

L'idea di base del protocollo *Bitcoin* è stata pubblicata il 31 ottobre 2008 nell'articolo *Bitcoin: A Peer to Peer Electronic Cash System* firmato da Satoshi Nakamoto, pseudonimo di uno o più ricercatori[59]. La prima implementazione pratica è avvenuta il 3 gennaio 2009 con il rilascio del software Bitcoin Core, arrivato alla versione 0.13.2 e disponibile gratuitamente ed in modalità *open source* per le piattaforme Windows, Mac e Linux sul sito Bitcoin.org[60].

Installando il client Bitcoin Core, o un altro client che implementi il protocollo, si diventa un nodo della rete ed è possibile ricevere e spedire *bitcoin*, valuta frazionabile fino alla 10^{-8}. Alcune frazioni hanno dei nomi propri: 1 mbtc = 0,001 BTC, 1 bits = 0,000001 BTC, 1 satoshi = 0,00000001 BTC.

Con il client si possono creare coppie di chiavi, pubbliche e private. La chiave pubblica è l'indirizzo da usare per ricevere i *bitcoin* e può essere comunicata a tutti[61]. Quella privata permette di autorizzare i pagamenti in uscita e non deve essere resa nota. Il sito Blockchain.info[62] stima ad oggi l'esistenza di circa 450 mila indirizzi univoci.

La chiave privata è una sequenza di caratteri creata in maniera casuale. Da questa chiave, il client usa l'algoritmo crittografico ECDSA (*Elliptic Curve Digital Signature Algorithm*) per calcolare un'altra sequenza di caratteri, la chiave pubblica, univocamente associata a quella privata. Ciò che è criptato con la chiave privata può essere decifrato solo con quella pubblica e viceversa, ma a partire dalla chiave pubblica non è possibile ricostruire la chiave privata che l'ha generata.

L'ECDSA non è l'unico algoritmo di crittografia usato dal protocollo *Bitcoin*, che fa ampio uso delle *funzioni di hash* SHA-256 (*Secure Hash Algorithm* 256) e RIPEMD-160 per creare codici univoci[63]. Le funzioni di *hash* calcolano una stringa di caratteri di lunghezza fissa da un messaggio, un documento o una sequenza di caratteri di lunghezza variabile. Il codice generato è il *message digest* o *digital fingerprint*, anche impropriamente chiamato *hash* del messaggio. SHA-256 e RIPEMD-160 differiscono nella lunghezza del *digest* generato.

Nella creazione del codice sono garantite:

- efficacia e velocità: tutti i partecipanti alla rete possono calcolare facilmente il *digest* di un messaggio ottenendo rapidamente sempre lo stesso risultato
- resistenza alle contro-immagini: da un *digest* non è computazionalmente possibile calcolare il messaggio che lo ha generato
- resistenza forte alle collisioni: impossibilità computazionale di trovare due messaggi diversi che generino lo stesso *digest*.

Il calcolo di un *digest* è usato, fra le altre cose, per eseguire un trasferimento di valuta. Se si hanno dei *bitcoin*, esiste almeno una transazione verso la propria chiave pubblica. Volendo inviarli tutti, creiamo un *digest* inserendo in input: la transazione dalla quale li abbiamo ricevuti e la chiave pubblica del destinatario del pagamento. I due input testimoniano che siamo in possesso della valuta è che la vogliamo inviare ad un determinato indirizzo.

Usando la nostra chiave privata per criptare il *digest* della transazione creiamo una firma della stessa. La transazione sarà propagata nella rete con comunicazioni *peer-to-peer*, cioè nodo a nodo, insieme alla firma e alla nostra chiave pubblica. Ogni nodo potrà verificare, usando la nostra chiave pubblica, che siamo stati noi a firmare il *digest*. Anche se il *bitcoin* è chiamato *cryptocurrency*, l'uso della crittografia a chiave pubblica non serve a nascondere i trasferimenti di valuta ma a certificarne l'autenticità e l'integrità, evitando inoltre che l'autore di una transazione ne rinneghi in seguito la titolarità. Solo chi è a conoscenza della chiave privata può aver firmato il *digest* della transazione, che non è possibile modificare una volta incluso nella firma.

Le transazioni, oltre ad esse pubbliche, sono registrate in blocchi cronologicamente ordinati (*blockchain*). Quelle inserite in uno stesso blocco sono considerate avvenute nello stesso momento. Tutte le copie della *blockchain* conservano in memoria la successione dei blocchi a partire dalla prima transazione avvenuta nel 2009. È così possibile ricostruire tutti i passaggi di titolarità dei *bitcoin*.

Installando Bitcoin Core si può decidere di scaricare la *blockchain* e occuparsi del suo aggiornamento diventando così un *nodo full*. Non tutti i client possono diventare *nodi full*[64]. Si deve infatti garantire alla rete il rispetto di alcune regole, ad esempio che il proprio computer sia acceso e collegato ad internet per almeno sei ore al giorno per aggiornare costantemente la copia della *blockchain*. Il sito Bitnodes.21.co[65] analizza caratteristiche e distribuzione geografica dei *nodi full*. Oggi ne esistono oltre 5.900, concentrati principalmente in USA, Germania e Francia. Ognuno di

questi nodi conserva in memoria una *blockchain* di oltre 65GB. La registrazione dei blocchi avviene su tutte le copie del registro.

Le transazioni non ancora incluse nella catena sono inviate in broadcast ai vari nodi della rete. Ogni nodo le raccoglie in un blocco da registrare. L'ultimo blocco della *blockchain* ha un proprio *digest* ed è calcolato anche quello del blocco da registrare. Il protocollo *Bitcoin* regola il funzionamento di una gara computazionale fra nodi il cui obiettivo è trovare una stringa di caratteri che, inserita nella funzione di *hash* SHA-256 insieme ai due *digest*, produca un output con un determinato numero di zeri iniziale.

Il numero di zeri determina la difficoltà del compito: più zeri iniziali ci sono, più è difficile. Il protocollo fissa, ogni 2016 blocchi aggiunti alla catena (circa due settimane), la difficoltà della gara sulla base del tempo medio di risoluzione registrato a partire dall'ultimo aggiornamento della difficoltà. Lo scopo è garantire che la risoluzione avvenga in media ogni dieci minuti.

Per le proprietà delle funzioni di *hash*, l'unico modo per vincere la gara è generare quante più sequenze possibili e inserire in *hash* ogni sequenza insieme al *digest* dei due blocchi. Se il *digest* calcolato ha il giusto numero di zeri iniziale, ci si ferma, altrimenti si continua con i tentativi. Non esistono scorciatoie ed è 'più bravo' chi è più veloce nel generare sequenze e verificarle. Per questo si dice che la gara può essere vinta solo usando 'forza bruta'. Intendendo per 'forza' la velocità di calcolo, misurata nell'ecosistema *Bitcoin* in *hash rate*, cioè in numero di funzioni di *hash* che possono essere calcolate al secondo. Si stima che la potenza di calcolo dell'intera rete *Bitcoin* sia oggi di oltre 3,5 milioni di miliardi di *hash* al secondo[66].

Non tutti i nodi partecipano alla gara e quelli che vi prendono parte sono chiamati *miner*. Il *miner* cha ha trovato per primo la soluzione al problema di calcolo ha diritto di proporre la registrazione del nuovo blocco ai nodi full della rete ricevendo in cambio un premio. Il codice trovato costituisce una prova del lavoro svolto, una *proof-of-work*. La verifica della vittoria può essere fatta da ogni nodo ricalcolando l'*hash* dai digest dei due blocchi, quello da registrare e l'ultimo registrato, insieme alla stringa individuata dal *miner*. Se il problema è effettivamente risolto, il nodo accetta la registrazione proposta e aggiunge il blocco di transazioni alla *blockchain*.

Il meccanismo di gara garantisce che la registrazione sia temporalmente corretta: uno dei tre input usati è il *digest* dell'ultimo blocco registrato e quindi le nuove transazioni saranno memorizzate dopo questo anello della *blockchain*. Inoltre, perché la difficoltà è stabilita in modo che la vittoria avvenga in media ogni dieci minuti, anche le registrazioni delle transazioni richiedono lo stesso periodo di tempo.

Può avvenire che due *miner* trovino contemporaneamente la soluzione della gara. In questo caso ogni nodo che riceve le due proposte di registrazione continuerà ad aggiungere blocchi a partire quella che ha ricevuto per prima. Questo crea una biforcazione della catena e lo sforzo computazionale della rete sarà suddiviso fra i vari rami: i *miner* usano per risolvere la gara anche il

digest dell'ultimo blocco registrato e in questo caso alcuni *miner* lavoreranno a partire da un *digest* ed alcuni a partire dall'altro.

Ad un certo punto avverrà che uno dei due rami avrà più nuovi blocchi inseriti rispetto all'altro. Questo perché la potenza di calcolo che ha lavorato su una catena sarà stata maggiore rispetto a quella dedicata allo sviluppo dell'altro ramo. Il protocollo è fatto in modo che in breve tempo tutti i nodi aggiorneranno il proprio registro accettando di memorizzare solo la catena più lunga, annullando così la biforcazione che si era creata. Per questo motivo in genere si aspettano almeno sei blocchi successivi a quello in cui è inserita la propria transazione prima di considerarla confermata dalla rete. In questo tempo, di circa un'ora, i nodi avranno avuto modo di annullare l'eventuale biforcazione[67].

La catena più lunga è quella con la maggiore potenza computazionale spesa dalla rete. Per falsificare la *blockchain* bisogna quindi falsificarne il futuro, sviluppando una catena di blocchi falsi che sia sempre più lunga di quella su cui stanno lavorando tutti gli altri. Per come è organizzata la gara computazionale, la 'falsificazione del futuro' è possibile solo se si ha a disposizione maggiore potenza di calcolo rispetto a tutti gli altri *miner* messi insieme. Un attacco alla rete di questo tipo è detto 'attacco al 51%', intendendo che chi è in grado di farlo ha a disposizione almeno il 51% della potenza di calcolo della rete.

Un altro attacco possibile è legato alle collisioni della funzione di *hash*. Un 'attacco a collisione' sfrutta il fatto che in realtà l'indirizzo su cui si ricevono i *bitcoin* è il *digest* di una chiave pubblica. Una collisione della funzione di *hash* genererebbe due indirizzi identici per due persone diverse, che avrebbero così lo stesso 'conto' sul quale ricevere la valuta. In pratica un attacco a collisione non è possibile perché, con la potenza di calcolo attuale, ci vorrebbero quasi 40 mila anni per individuare due input diversi che producano lo stesso *digest*[68].

Il fatto che i *miner* agiscano per il bene della rete è inoltre incoraggiato dal meccanismo di ricompensa: la rete premia il *miner* vincitore emettendo nuova valuta attraverso transazioni chiamate *coinbase*. Il numero di *bitcoin* che si ricevono è stabilito dal protocollo. Oggi la ricompensa è di 12,5 *bitcoin*[69]. Questo valore è dimezzato ogni 210 mila blocchi registrati (circa quattro anni) in modo che l'emissione di valuta sia decrescente nel tempo fino a raggiungere il tetto massimo 21 milioni di *bitcoin* in circolazione per il 2140. Quando questo limite sarà raggiunto i *miner* saranno retribuiti esclusivamente dai partecipanti alla rete. Il momento in cui avviene il dimezzamento della ricompensa attraverso transazioni *coinbase* è chiamato *halving* (dimezzamento).

Per ricevere il premio in *bitcoin*, sono stati creati software e hardware dedicati per ottimizzare la potenza di calcolo cercando di minimizzare al contempo l'uso di energia elettrica. Sono nati così anche dei circuiti integrati dedicati esclusivamente all'attività di *mining*. Circuiti di questo tipo sono indicati con il termine di ASIC: *Application-Specific Integrated Circuit*. Un'altra strategia intrapresa è stata quella di condividere fra più persone la potenza di calcolo e le ricompense

ottenute. Sono stati così sviluppati dei software che permettono di partecipare via internet con altri computer all'attività di *mining*. Una strategia di questo tipo è chiamata di *pooled mining*. Il sito Blockchain.info[70] pubblica delle stime sulla potenza di calcolo dei *mining pool*. I principali sono una ventina ed i primi quattro (AntPool, F2Pool, BitFury, ViaBTC) hanno la stessa potenza di calcolo di quella ottenuta dalla somma degli altri *pool*.

Note

(ultimo accesso ai link segnalati: 12 febbraio 2017)

[1] Tutti i dati riportati nel documento sono aggiornati al 12 febbraio 2017.

[2] Per *dollaro* si intenderà sempre quello statunitense, indicato anche con il codice USD.

[3] Stima in USD del volume di transazioni, https://blockchain.info/it/charts/estimated-transaction-volume-usd?timespan=2years.

[4] https://21.co/ottaviocalzone.

[5] Spiegazione del funzionamento dell'algoritmo delle colonie di formiche, ispirato a quanto avviene in natura, https://it.wikipedia.org/wiki/Algoritmo_delle_colonie_di_formiche.

[6] *Nodi full*; maggiori informazioni tecniche in appendice.

[7] EBA, *EBA Opinion on 'Virtual Currencies'*, EBA/Op/2014/08, Londra 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[8] Sito dedicato alla storia del *bitcoin*, http://historyofbitcoin.org.

[9] New Liberty Standard, http://newlibertystandard.wikifoundry.com.

[10] Informazioni sul cambio fra *bitcoin* e dollaro, https://markets.blockchain.info.

[11] Informazioni sui *bitcoin* in circolazione ed altri dati statistici, http://www.bitcoinblockhalf.com.

[12] Statistiche e grafici sulla rete *Bitcoin*, https://blockchain.info/it/stats.

[13] J. CHOKUN, *Who Accepts Bitcoins as Payment?*, 7 febbraio 2017, https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.

[14] BitBank, https://bitbank.com.

[15] Mappa degli esercenti che accettano *bitcoin*, https://coinmap.org.

[16] Sito di recensioni sui principali *exchange point*, https://www.bestbitcoinexchange.io/.

[17] Volumi giornalieri di cambi nei principali *exchange point*, http://coinmarketcap.com/currencies/volume/24-hour/#.

[18] Volumi mensili di cambi nei principali *exchange point*, http://bitcoincharts.com/charts/volumepie.

[19] *Winklevoss Index*, http://winkdex.com.

[20] LocalBitcoins, https://localbitcoins.com.

[21] Mappatura degli ATM *Bitcoin*, https://coinatmradar.com.

[22] L. CICCONE, *Il protocollo Bitcoin: analisi storica trasversale*, Luiss Guido Carli, Roma 2015, http://tesi.eprints.luiss.it/15725/1/178431.pdf.

[23] N. PASSARELLI, *Bitcoin e antiriciclaggio*, Il Mondo dell'Intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/11/Bitcoin-e-riciclaggio-Passarelli.pdf.

[24] NOVETTA, *Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins*, McLean (Virginia, USA) 2015, https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.

[25] Chainalysis, https://www.chainalysis.com.

[26] Ciccone, *Il protocollo Bitcoin*, cit.

[27] L. BATTANTA, *La Cina contro i bitcoin*, in «Il Sole 24 Ore», 12 gennaio 2017, http://www.ilsole24ore.com/art/finanza-e-mercati/2017-01-11/la-cina-contro-bitcoin-usati-attacco-speculativo-yuan--224504.shtml?uuid=AD9pKXVC.

[28] Mappatura della legalità del *bitcoin* nel mondo, http://bitlegal.io.

[29] Ciccone, *Il protocollo Bitcoin*, cit.

[30] EBA, *EBA Opinion on 'Virtual Currencies'*, cit.

[31] AGENZIA DELLE ENTRATE, *Risoluzione 72 /E: trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali*, Roma 2016, http://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/documentazione/provvedimenti+circolari+e+risoluzioni/risoluzioni/archivio+risoluzioni/risoluzioni+2016/settembre+2016+risoluzioni/risoluzione+n.+72+del+02+settembre+2016/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf.

[32] D. G. BAUR, K. HONG, A.D. LEE, *Virtual Currencies: Media of Exchange or Speculative Asset?*, Working Paper No. 2014-007, SWIFT Institute, Londra 2016, https://www.swiftinstitute.org/wp-content/uploads/2016/06/Bitcoin-Baur-et-al_-2016-SWIFT-FINAL.pdf.

[33] EBA, *EBA Opinion on 'Virtual Currencies'*, cit.

[34] Analisi degli investimenti *venture capital* in tecnologia *blockchain*, http://www.coindesk.com/bitcoin-venture-capital.

[35] Analisi delle start-up e degli investimenti 'Angel' nel settore *blockchain*, https://angel.co/blockchains.

[36] T. MACHEEL, *Crypto Colonizing: B of A's Blockchain-Patent Strategy*, in «American Banker», 1 febbraio 2016, https://www.americanbanker.com/news/crypto-colonizing-b-of-as-blockchain-patent-strategy.

[37] Consorzio R3, http://www.r3cev.com.

[38] Progetto Hyperledger della Linux Foundation, https://www.hyperledger.org.

[39] Sezione del sito Bitcoin.org dedicata allo sviluppo del protocollo, https://bitcoin.org/it/sviluppo.

[40] Coinbase, https://www.coinbase.com.

[41] Circle, https://www.circle.com/it.

[42] Mappatura delle cripto-valute, http://coinmarketcap.com/currencies/views/all.

[43] *Ciao bitcoin, la nuova moneta online è Monero*, in «La Repubblica», 04 settembre 2016, http://www.repubblica.it/tecnologia/2016/09/04/news/ciao_bitcoin_la_nuova_moneta_online_e_monero-147159445.

[44] Sito ufficiale della valuta virtuale Monero, https://getmonero.org.

[45] ABI LAB, *Le banche e la blockchain: quali opportunità?*, Versione 1.1, Roma 2016.

[46] Sito ufficiale della piattaforma Ethereum, https://www.ethereum.org.

[47] Counterparty, http://counterparty.io.

[48] Factom, https://www.factom.com.

[49] ABI LAB, *Le banche e la blockchain*, cit.

[50] D. SCHATSKY E CRAIG MURASKIN, *Beyond Bitcoin: Blockchain is Coming to Disrupt Your Industry*, Deloitte University Press, 2015, https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html.

[51] Circle, https://www.circle.com.

[52] Blockcypher, https://www.blockcypher.com.

[53] Chain, https://chain.com.

[54] Ripple, https://ripple.com.

[55] Blockstream, https://blockstream.com.

[56] 21 Inc., https://21.co.

[57] SolarCoin, https://solarcoin.org.

[58] Augur, https://augur.net.

[59] N. SATOSHI, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009, https://bitcoin.org/bitcoin.pdf.

[60] Bitcoin Core, https://bitcoin.org/it/scarica.

[61] In realtà, come vedremo, l'indirizzo da comunicare è un *hash* della chiave pubblica.

[62] Statistiche e grafici sulla rete *Bitcoin*, https://blockchain.info/it/stats.

[63] B. BERTANI, *La crittografia nel sistema di moneta digitale Bitcoin*, Università di Bologna, Bologna 2013-2014, http://amslaurea.unibo.it/7934/1/bertani_beatrice_tesi.pdf.

[64] Come diventare un *nodo full*, https://bitcoin.org/en/full-node.

[65] Mappatura dei *nodi full*, https://bitnodes.21.co.

[66] Statistiche sulla potenza di calcolo della rete *Bitcoin* e sulla difficoltà della gara computazionale, https://blockchain.info/it/charts.

[67] Bertani, *La crittografia nel sistema di moneta digitale Bitcoin*, cit.

[68] Bertani, *La crittografia nel sistema di moneta digitale Bitcoin*, cit.

[69] Spiegazione dell'emissione controllata di nuovi *bitcoin*, https://en.bitcoin.it/wiki/Controlled_supply.

[70] Distribuzione della capacità di *hash* fra i principali gruppi di *miner*, https://blockchain.info/it/pools.

Bibliografia

•

ABI LAB, *Le banche e la blockchain: quali opportunità?*, Versione 1.1, Roma 2016

B. BERTANI, *La crittografia nel sistema di moneta digitale bitcoin*, Università di Bologna, Bologna 2013-2014, http://amslaurea.unibo.it/7934/1/bertani_beatrice_tesi.pdf

C. VALMORRA, *Funzioni di hash e sicurezza crittografica*, Università di Bologna, Bologna 2012-2013, http://amslaurea.unibo.it/6300/1/Valmorra_Camilla_tesi.pdf

D. SCHATSKY E C. MURASKIN, *Beyond Bitcoin: Blockchain is Coming to Disrupt Your Industry*, Deloitte University Press, 2015, https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html

D.G. BAUR, KOHOON HONG, Adrian D. Lee, *Virtual Currencies: Media of Exchange or Speculative Asset?*, SWIFT Institute, Londra 2016, https://www.swiftinstitute.org/wp-content/uploads/2016/06/Bitcoin-Baur-et-al_-2016-SWIFT-FINAL.pdf

L. CICCONE, *Il protocollo bitcoin: analisi storica trasversale*, Luiss Guido Carli, Roma 2015, http://tesi.eprints.luiss.it/15725/1/178431.pdf

N. SATOSHI, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009, https://bitcoin.org/bitcoin.pdf

N. PASSARELLI, *Bitcoin e antiriciclaggio, Roma*, Il Mondo dell'Intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/11/Bitcoin-e-riciclaggio-Passarelli.pdf

NOVETTA, *Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins*, McLean, Virginia, USA 2015, https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf