Bitcoin, altre criptovalute e tecnologia blockchain

di Umberto M. Meotto
Editor: Federico Forneris
Revisori Esperti: Luca Fumarco, Roberto di Lauro
Revisore Naive: Valentina Speranzini

Parole Chiave: Criptovalute, Bitcoin, Blockchain

Permalink: http://informa.airicerca.org/2018/02/19/bitcoin-criptovalute-blockchain/

Il clamore circa il Bitcoin è stato uno dei principali punti di discussione del 2017. Durante lo scorso anno, infatti, le criptovalute sono entrate a far parte del sistema finanziario globale ed hanno anche attratto l'attenzione dei media tradizionali. Il presente articolo intende mostrare vantaggi e punti critici dietro alla "Criptomania", sia nell'ambito della finanza che in quello informatico. Dal punto di vista economico, l'utilizzo di moneta elettronica può facilitare gli scambi, permettendo di risparmiare sul costo della singola transazione. Tuttavia, la possibilità di scambiare criptovalute con valute reali, come il dollaro americano, potrebbe incentivare una forte speculazione legata alle oscillazioni dei tassi di cambio. Dal punto di vista informatico, invece, le nuove valute hanno suscitato particolare interesse per via delle peculiari caratteristiche tecnologiche. Si tratta principalmente: dell'uso della crittografia, dell'approcio peer-to-peer, della tecnologia blockchain e del concetto di mining. Si mostreranno le ricadute etiche ed ambientali delle ultime tre. Una volta passata la bolla speculativa del Bitcoin, quale sarà il valore aggiunto che avremo ottenuto? Saranno in grado le blockchain di sostenere l'innovazione o invece la strangoleranno sotto una mole infinita di dati?

Nell'ottobre del 2008, un personaggio misterioso, rispondente al nome di Satoshi Nakamoto, pubblicò su una mailing list un articolo dal titolo "Bitcoin: un sistema di moneta elettronica peer to peer". Entro il gennaio dell'anno successivo (2009), Nakamoto rilasciò la prima versione del software bitcoin. Sebbene questa moneta non fosse supportata da banche o governi, esistesse puramente nel mondo virtuale e non possedesse alcun valore intrinseco, iniziò ad essere utilizzata per scambiare beni e servizi dotati di valore reale. Acquisì dunque un prezzo che per molti anni rimase sotto ai 10$; poi, nel corso del 2013, raggiunse dapprima i 100$ e quindi, verso la fine dell'anno, i 1.000$. Nel 2017 abbiamo visto il valore del bitcoin raggiungere quasi i 20.000$ (fig. 1). Inoltre, il rumore che si è fatto attorno al bitcoin ha portato all'attenzione del pubblico anche la tecnologia sulla quale si fonda questa valuta: la blockchain. Ad oggi non è chiaro chi sia veramente Nakamoto, si tratta probabilmente di uno pseudonimo utilizzato da una o più persone coinvolte nello sviluppo dell'algoritmo informatico alla base del Bitcoin. Diverse inchieste giornalistiche hanno tentato di svelarne l'identità: nessuna, tuttavia, ha permesso di dirimere i dubbi ed identificarlo univocamente.

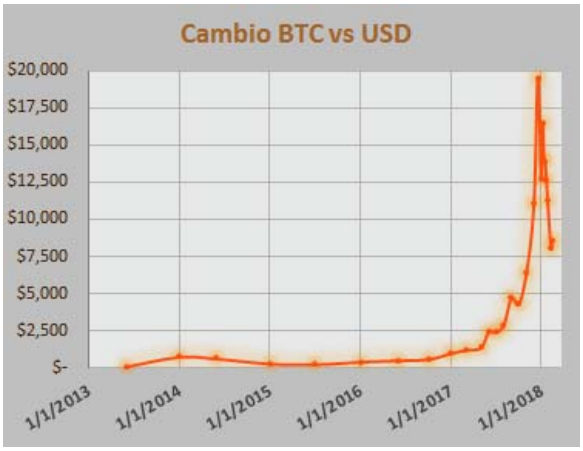


Figura 1 *- Andamento del cambio Bitcoin - dollaro americano negli ultimi 5 anni. Il massimo è stato toccato il 17.12.2017 superando i 20.000$, appena 50 giorni dopo il valore era sceso attorno ai 6.000$.*

La teoria

Fino all'avvento del bitcoin, ed in gran parte ancora oggi, il commercio su internet è stato affidato a istituzioni finanziarie (come le banche) che gestiscono, come terze parti ed in modo affidabile, i pagamenti elettronici. Nell'abstract del suo articolo, Nakamoto, scrive tuttavia: "una versione puramente *peer to peer* di moneta elettronica potrebbe permettere di mandare dei pagamenti *online* direttamente da una persona ad un'altra, senza bisogno di passare attraverso un'istituzione finanziaria". Il *peer to peer* [1], letteralmente "da pari a pari", è un sistema di condivisione decentralizzata su internet: significa che ognuno dei computer che intervengono nel sistema paritario scarica, o condivide, informazioni (oggetto di scambio) senza il bisogno di una banca dati centralizzata (fig. 2).

Secondo Nakamoto, nel caso del pagamento elettronico, il compito fondamentale dell'istituto finanziario è quello di garantire che l'acquirente non possa spendere lo stesso denaro due volte cosicché il venditore non venga frodato. Per superare la necessità di un intermediario, egli propone quindi di utilizzare un sistema di pagamento che si basi su di una prova crittografata condivisa, tale prova garantirebbe l'ordine cronologico delle transazioni, evitando quindi il rischio di frode.

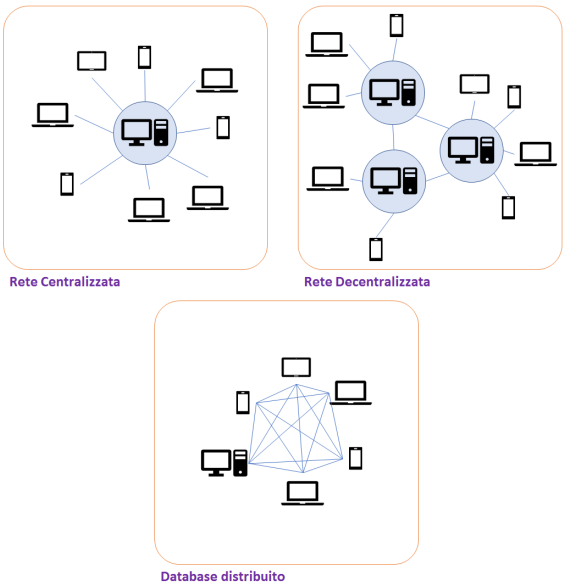
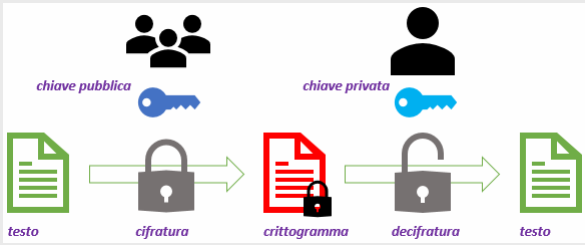


Figura 2 *- Varie tipologie di reti. In alto a sinistra la tradizionale "rete centralizzata": tutti gli utenti si connettono, ed affidano, ad una singola banca dati centrale. In alto a destra, una "rete decentralizzata": gruppi di utenti diversi possono fare affidamento su nodi diversi. In basso il "database distribuito", come quello del Bitcoin: non esiste una banca dati centrale, tutti i nodi sono connessi, e possono fare affidamento, tra di loro.*

Box1: Crittografia e moneta elettronica

La crittografia è una scienza che, per mezzo della matematica, consente di cifrare e decifrare dei dati. E' utile quando si vogliono proteggere delle informazioni private oppure trasmetterle a qualcuno in modo sicuro. Tramite la crittografia si può, ad esempio, trasformare un messaggio in una serie di caratteri, apparentemente privi di senso, di modo che soltanto i destinatari possano leggerlo una volta tradotto. Creare un "messaggio in codice" è in realtà molto semplice: si parte da un testo e per mezzo di una chiave (o cifra) ed un algoritmo matematico si ottiene il messaggio cifrato. Solo chi conosce la chiave può decifrare il messaggio. La crittografia viene anche utilizzata per le cosiddette "firme elettroniche" o "digitali". In questo caso le chiavi da utilizzare sono due: una pubblica (ad es. usata per cifrare) ed una privata (ad es. usata per decifrare). Tali chiavi sono legate tra di loro e garantiscono l'autenticazione. Ad esempio, un utente in possesso di una propria chiave privata è in grado di "firmare" un qualsivoglia dato o documento; per mezzo della chiave pubblica si può verificare che la sua firma sia valida.



Le **criptovalute** si chiamano così perché utilizzano esattamente questi principi per verificare l'autenticità delle transazioni. Quando un nuovo utente crea il proprio portafoglio elettronico di Bitcoin viene generata una coppia di chiavi pubblica-privata tramite un algoritmo noto. Tale coppia di chiavi, opportunamente elaborata, verrà utilizzata ogni qual volta si effettui una transazione. Risulta chiaro, quindi, come le firme digitali siano un ingrediente fondamentale per il funzionamento degli scambi in moneta elettronica, e perché queste prendano il nome di criptovalute.

Il bitcoin in pratica

Questi presupposti permettono di comprendere fin da subito che le criptovalute, come il bitcoin, sono molto diverse dalle valute tradizionali, innanzitutto poiché non ci sono istituti bancari o governi che le emettono o le controllano, ma soltanto la collettività dei suoi utilizzatori (fig. 3). All'atto pratico, il bitcoin è una moneta virtuale con un valore intrinseco nullo, emessa da un codice computerizzato in portafogli elettronici: essa ha un valore effettivo semplicemente perché le persone che la scambiano ne accettano una determinata quantità in cambio di un servizio o di una merce. Il suo "cambio" è dunque puramente definito dalla leva di domanda e offerta.

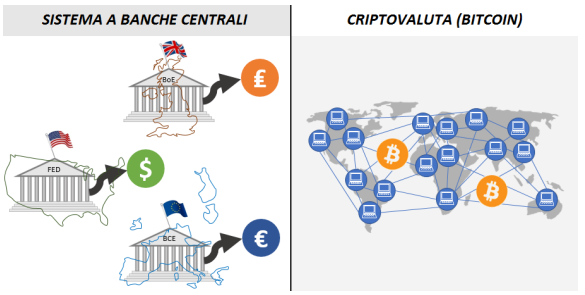


Figura 3 *- Differenza tra sistemi bancari a banche centrali (sinistra) e rete Bitcoin (destra).*

Il fatto che il Bitcoin abbia, o meno, un valore intrinseco è un argomento controverso e dibattuto: basandosi sulla definizione data da Adam Smith ne "La ricchezza delle nazioni", una moneta non ha altri scopi fuorché permettere l'acquisto di beni. Dunque, le valute sono beni strumentali che debbono fungere da mezzi di scambio ed accumulo della ricchezza. Se da un lato le criptovalute sembrano funzionare molto bene come mezzi di scambio, d'altra parte l'alta volatilità cui sono soggette, ed il fatto di non essere legate a nessuna riserva o *commodity*, non permette di riconoscerle come strumenti affidabili per l'accumulo di ricchezza. La discussione per ora rimane aperta.

Bitcoin ed inflazione

Diversamente da quanto accade per le valute a corso legale, la quantità di bitcoin è definita a priori. L'algoritmo di generazione ne prevede infatti un numero massimo di 21 milioni di pezzi. Questo limite, combinato ad una richiesta sempre crescente da parte del mercato, potrebbe far subire al bitcoin la cosiddetta *deflazione* ovvero l'aumento del valore della moneta (e quindi il calo dei prezzi espressi in quella valuta). La deflazione è un problema rilevante che non limita i suoi effetti ai meccanismi di creazione della moneta. Si immagini, ad esempio, il disagio che deve affrontare un'impresa non potendo vendere i propri beni -o servizi- al prezzo preventivato, bensì ad uno più basso. Essa potrebbe avere difficoltà a ripagare gli investimenti fatti o, peggio ancora, non essere in grado di erogare gli stipendi ai dipendenti, con una chiara ricaduta sociale. Inoltre, in un sistema deflazionistico la ricchezza viene redistribuita a favore di chi presta il denaro causando diseguaglianze economiche e un generale indebolimento del processo democratico.

Anche per queste ragioni, la politica monetaria delle banche centrali tende ad adattarsi alle circostanze dell'economia reale. Prendiamo ad esempio l'ultima crisi finanziaria, in parte dovuta a politiche di combattimento dell'inflazione combinate a riduzioni dei salari portate avanti da vari governi. In questa occasione, per correre ai ripari, la Federal Reserve americana (FED), la Bank of England (BoE) e la Banca Centrale Europea (BCE), hanno attuato delle politiche monetarie espansive (rispettivamente su Dollaro, Sterlina ed Euro) proprio al fine di mitigare il rischio di spirali deflazionistiche. I vari strumenti utilizzati (bailout, quantitative easing) comportano quindi un aumento della base monetaria con l'obiettivo di stimolare gli istituti di credito a prestare denaro alle imprese.

Detto in modo semplice: se c'è un'ampia offerta di moneta, il valore del denaro diminuisce e quello dei beni sale (inflazione), se invece c'è scarsità nell'offerta della moneta, il valore del denaro sale e di conseguenza i beni si deprezzano (deflazione), rallentando la crescita economica.

Se da un lato i sostenitori del Bitcoin ritengono che la deflazione non sia un impedimento, d'altro canto molti economisti di stampo keynesiano lo considerano un problema serio poiché risulta chiaro che la politica monetaria di questa criptovaluta non considera lo stato dell'economia reale [2]. In risposta a tale rischio sono state sviluppate criptovalute con sistemi di regole leggermente differenti: Primecoin (200 milioni di $ di capitalizzazione al 15.1.2018) e Peercoin (30 milioni di $ di capitalizzazione al 15.1.2018), ad

esempio, modificano l'algoritmo Bitcoin al fine di garantire una fornitura di moneta illimitata.

Come si creano i bitcoin: il mining

Non tutti i 21 milioni di bitcoin sono stati generati in principio: gli algoritmi che stanno alla base di questa criptovaluta sono studiati in modo da introdurre nuova moneta fino al raggiungimento del suddetto limite nel 2033. Infatti, il numero di bitcoin attualmente disponibili viaggia attorno ai 16-17 milioni. L'attività attraverso la quale vengono creati i nuovi bitcoin si chiama *mining* (in analogia al lavoro di miniera), e viene effettuata per mezzo di calcoli svolti dai computer che fanno parte della rete. Inizialmente la regola prevedeva che ogni 10 minuti circa venissero generati 50 nuovi bitcoin (un blocco). Tale numero è programmato per dimezzarsi ogni 4 anni, per cui oggi vengono creati 12,5 BTC per blocco.

Una delle caratteristiche più innovative ed interessanti del bitcoin risiede proprio nel concetto di *mining* dei blocchi e nella tecnologia che gestisce la "catena dei blocchi", ossia, la *blockchain*.

Blockchain

Si può immaginare la *blockchain* come un "libro mastro" nel quale sono archiviate, criptate, tutte le informazioni relative alle transazioni ed alla proprietà del denaro. Poiché, come abbiamo detto in principio, la moneta elettronica è *peer to peer*, tutti i computer nel mondo che fanno parte della rete bitcoin sono in grado di accedere e leggere la *blockchain*, ossia il "libro mastro". E' facile comprendere che ogni nuova transazione introduce dei cambiamenti nello stato della *blockchain*, infatti, nel momento in cui la transazione è validata e verificata, essa entra a far parte di un blocco che si dovrà aggiungere alla catena. Tramite un protocollo di lavoro collaborativo (consenso), i computer/nodi della rete decidono se il blocco è valido e può essere aggiunto alla *blockchain*. I *miners* (minatori) che trovano i blocchi validi da aggiungere alla catena sono ricompensati con la nuova moneta generata (fig. 4).

Di fatto, l'attività di *mining* consiste nel risolvere un *puzzle* che richiede molta capacità computazionale e la registrazione del nuovo blocco di transazioni può avvenire soltanto se il *puzzle* viene risolto.L'evidenza che il *mining* sia stato effettuato è detta "*proof of work*" o "prova del lavoro", concetto informatico definito già durante gli anni '90, quindi molto prima dell'invenzione del bitcoin.

E' importante quindi dare i giusti incentivi economici a chi si impegna a risolvere il *puzzle*, ossia i *miners*, poiché questo è l'unico modo in cui le nuove transazioni possono essere aggiunte al libro mastro. La ricompensa, come si è detto in precedenza, può consistere in nuovi bitcoin oppure in una commissione per la registrazione della transazione. Poiché la somma di ricompensa tenderà a ridursi negli anni fino a sparire, l'unico modo di ricompensare i *miners* in futuro sarà per mezzo delle commissioni.

Sicurezza

Per un non esperto, il concetto di *blockchain* può apparire ad un primo approccio decisamente complesso. La tecnologia, poi, essendo estremamente informatizzata, potrebbe altresì sembrare poco sicura rispetto alla cara vecchia carta. E' questo, tuttavia, un mito da sfatare. Le *blockchain* stanno prendendo piede in molte applicazioni e nel corso del 2017 hanno creato un giro d'affari di 150 miliardi di dollari in tutto il mondo.

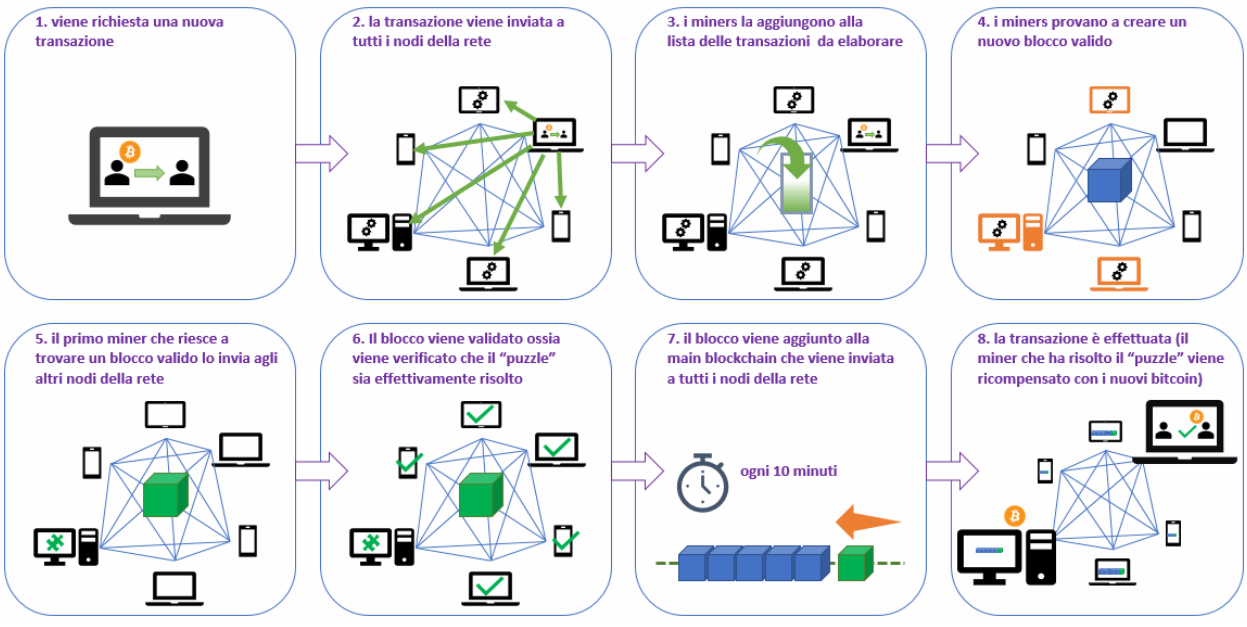


Figura 4 *- Schema di funzionamento di una blockchain. Per semplicità e leggibilità si è scelto di non approfondire il metodo di soluzione del "puzzle".*

La ridondanza dei dati (ogni nodo ha una copia della catena), il controllo della transazione prima della convalida, la registrazione della transazione in blocchi ordinati in base ad un algoritmo a consenso e l'utilizzo della crittografia sono caratteristiche che fanno della tecnologia *blockchain* uno strumento sicuro. Al punto che tutto il mondo dell'economia e della finanza vi si sta interessando [7].

Il criterio applicato al bitcoin è facilmente estendibile ad obbligazioni (*bond*) e azioni (*stock*), tant'è che esistono consorzi creati dalle più grandi banche mondiali al fine di sviluppare database distribuiti di questo tipo.

Semplificando, il sistema di sicurezza sviluppato da Nakamoto per il bitcoin prevede che la catena più lunga sia quella giusta. Un eventuale *hacker* che volesse annullare una transazione, o crearne una alternativa a suo vantaggio, dovrebbe generare una catena più lunga di quella corretta. Tuttavia, per fare questo, avrebbe bisogno del consenso, ossia, dovrebbe essere in grado di manipolare la catena sul 51% dei nodi della rete (fig. 5).

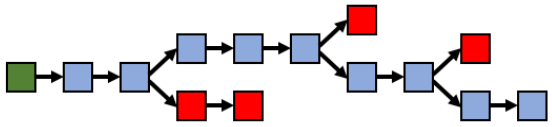


Figura 5 *- Schema semplificato di una blockchain.*

Box2: Influenza della tecnologia sul sistema mondiale degli scambi finanziari

La storia dei mercati borsistici affonda le sue radici nell'età antica: in mesopotamia e nell'agorà greca esistevano già agenti che operavano in attività di tipo economico. E' però a partire dal XV secolo che si fondano le prime borse, precorritrici degli attuali mercati finanziari. Per molti anni, le borse valori sono stati luoghi fisici dove acquirenti e venditori si incontravano ed effettuavano le negoziazioni. Tipicamente, gli scambi avvenivano in opportune sale tra traders vestiti in divise dai colori sgargianti; ciò permetteva di identificare rapidamente per quale casa d'investimento essi lavorassero. La negoziazione si realizzava grazie ad un particolare metodo di comunicazione (detto "*open outcry*") fatto di grida e gesti prestabiliti.

Durante gli anni '80 e '90 il trading telefonico ed i sistemi informatici hanno rimpiazzato questo metodo di negoziazione nella gran parte delle borse mondiali. Ad oggi pochissimi mercati (ad es. NYSE) mantengono sale dedicate al trading di persona. Ma come ha fatto la telematica a pervadere l'ambito finanziario così rapidamente? La risposta è semplice: gli scambi gestiti dai computer possono avvenire a velocità incredibili, inavvicinabili persino dal trader più esperto. L'avvento dei computer, non solo ha accelerato i movimenti, ma ha anche permesso di superare il problema dei fusi orari, rendendo gli scambi praticamente continui. Il Forex, ad esempio, venne creato dalle più grandi istituzioni bancarie al fine di scambiare centinaia di milioni in valuta nel giro di pochi istanti. Ciò ha modificato notevolmente il mercato, al punto che oggi la maggior parte delle transazioni non è finalizzata all'acquisto o alla vendita di beni bensì alla speculazione.

Citando un articolo del New York Times, la nuova velocità dei soldi sta rimodellando i mercati. Immense stanze piene di computer hanno sostituito il fracasso dei broker dalle giacchette sgargianti, le macchine effettuano ormai qualsiasi tipo di scambio richiesto dalle banche, dai gestori di fondi e dalle compagnie di brokeraggio su valute, azioni, obbligazioni, fondi, futures e chi più ne ha più ne metta. E in tempi che si misurano in frazioni di millisecondi. Le aziende informatiche che gestiscono i sistemi combattono sul terreno del trading ad Alta Frequenza ("High Frequency Trading"), rosicchiando microsecondi quà e là, attendendo l'avvento dell'Intelligenza Artificiale anche in questo settore.

Altre criptovalute

Oggigiorno il bitcoin, sebbene rimanga la principale criptovaluta in circolazione, deve affrontare l'assalto di numerose piattaforme alternative: tra tutte le più promettenti sembrano essere Ethereum e Ripple (fig. 6). Il sito web coinmarketcap.com riporta ben 1372 criptovalute esistenti al 31/12/2017 di cui una buona trentina supera il miliardo di dollari di capitalizzazione. Non tutte però funzionano allo stesso modo: Ethereum [3], ad esempio, si basa sulla pubblicazione *peer to peer* di contratti (*smart contract*) mentre Ripple è un sistema di trasferimento fondi utilizzato anche da grandi banche.

Figura 6 *- Principali criptovalute al 31.12.2017 ed al 29.01.2018. Il mercato complessivo delle criptovalute è sceso da 700 a 570 miliardi di dollari in un solo mese (mostrando l'alta volatilità di questi prodotti). Dati da* http://www.coinmarketcap.com/.

Ciò che accomuna tutte è il fondarsi su alcuni concetti base quali l'utilizzo di algoritmi di criptazione, la presenza di database distribuiti per mezzo del peer to peer su reti i cui nodi sono i computer degli utenti e diversi standard di *blockchain*.

Possibili applicazioni della tecnologia blockchain

Le *blockchain* non sarebbero mai potute esistere senza le reti informatiche come, ad esempio, internet. Tuttavia qualsiasi rete può essere utilizzata: un'*intranet* (rete privata) potrebbe sostenere una *blockchain* utile ad un'azienda o a qualsivoglia organizzazione. Infatti, questa tecnologia è interessante non solo per il tracciamento ed il controllo delle attività finanziarie ma potenzialmente anche per qualsiasi transazione che richieda l'identificazione personale, la *peer-review* o un processo democratico di presa di

decisione (come ad esempio il voto elettronico). Secondo alcuni studi [4-5], un sistema altamente decentralizzato e basato sulle *blockchain* potrebbe migliorare la qualità stessa dell'informazione; se ben concepito, potrebbe limitare altresì la diffusione di *fake news*, aumentando la trasparenza e riducendo le asimmetrie nell'accesso all'informazione da parte delle persone.

Sebbene la tecnologia sia molto più accessibile oggi di quanto non fosse qualche anno fa è necessaria ancora molta ricerca e sviluppo per trasformare il potenziale della tecnologia *blockchain* in un vero valore per le industrie e la società.

Altre implicazioni: PoS contro PoW

Abbiamo visto che l'attività del *mining* è per sua natura competitiva (il primo minatore che risolve il *puzzle* riceve la ricompensa) e che essa è quindi una fonte di profittabilità economica per i partecipanti. Oggigiorno tuttavia, la potenza di calcolo necessaria a trovare il nuovo blocco da aggiungere alla *blockchain* è tale che i minatori debbono unirsi in "gilde" (*mining pool*) per mettere in condivisione le proprie risorse. Questo perché la rete degli utilizzatori è sempre più vasta, la produzione dei nuovi bitcoin procede ad una velocità costante (e ad un tasso decrescente) ed il numero di calcoli per blocco aumenta. Non è più possibile, quindi, fare *mining* con un semplice computer o laptop di uso comune. L'attività, dunque, non è a costo nullo, ma richiede un impegno economico sia in termini di *hardware* (servono macchine specializzate) che di energia elettrica consumata.

Tali condizioni permettono di inquadrare l'attività del *mining* all'interno di quella teoria dei giochi [6] che vede come figure fondamentali John von Neumann (matematico, fisico e pioniere della scienza dei computer) ed il matematico John Nash. Il quesito è: quali strategie possono adottare i *miners* affinché la loro attività permanga redditizia? come possono aumentare l'efficienza dei loro sistemi per mantenere un bilancio positivo?

Sebbene la questione del consumo energetico possa sembrare un punto secondario, in realtà la potenza richiesta per effettuare i calcoli non è indifferente: molti autori si stanno interrogando sulla "sostenibilità" del bitcoin e sul suo impatto nel consumo dei combustibili fossili. Diverse fonti riportano che il fabbisogno annuo necessario a generare i bitcoin è dell'ordine di decine di TWh (terawattora), quanto una nazione di medie dimensioni.

Esistono, dunque, un certo numero di problemi con l'attuale implementazione della *blockchain* per il bitcoin. Molta ricerca e sviluppo si sta dedicando a trovare metodi alternativi per il *mining* dei blocchi [8]. Una soluzione che pare molto promettente è l'utilizzo della tecnica *proof of stake* (PoS) al posto dell'attuale *proof of work* (PoW) (fig. 7). Ethereum, ad esempio, ha già proposto di passare a questo nuovo tipo di algoritmo, decisamente più efficace dal punto di vista energetico.

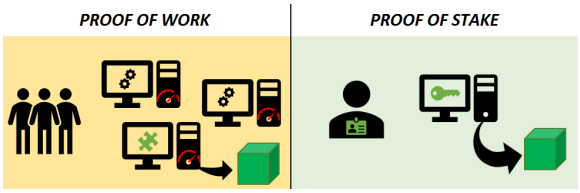


Figura 7 *- Schemi esemplificativi della Proof of Work (PoW) e Proof of Stake (PoS).*

Mentre la PoW si basa fondamentalmente sul consumo di energia di tutti i *miners*, la PoS (prova di chi ha la posta in gioco) funziona sul fatto che il creatore del nuovo blocco viene scelto in modo deterministico tra chi possiede la maggior quantità di ricchezza o partecipazione (*stake*, in inglese). Sebbene questo metodo sia meno sicuro, poiché la base del consenso è ridotta, l'efficienza è centinaia, se non migliaia, di volte migliore. Ciò apre ad un interrogativo che è innanzitutto etico: verrà mai il momento in cui dovremo, in nome dell'efficienza energetica, sacrificare il consenso democratico?

Box3: Aggiornamenti finali

Data la spiccata attualità dell'argomento trattato, si riportano di seguito alcune salienti novità provenienti dalla galassia delle criptovalute. La notizia che, in questo inizio 2018, ha senz'altro dato uno scossone al Bitcoin è stata la messa al bando delle valute digitali da parte di alcuni governi asiatici, in primis Cina e Corea del Sud. Questi paesi hanno praticamente dichiarato guerra al **Bitcoin**, chiudendo le piattaforme di scambio, bloccando le app per la telefonia mobile e, addirittura, censurando le pubblicità delle criptovalute sui social network. Tali contromisure sono giustificate dalla necessità di evitare effetti indesiderati sul cambio delle valute interne, nonché lo spostamento di grossi capitali verso altre nazioni. Discorso differente quello della criptovaluta **NEM** che a fine gennaio ha subito un furto equivalente a circa 500 milioni di dollari sulla piattaforma giapponese Coincheck. Questo dimostra che la tecnologia blockchain può essere affidabile, ma se chi la utilizza non dà il giusto peso alla sicurezza, è possibile che sorgano dei problemi. Rapporto contrastato anche quello con il mondo islamico: se da un lato Egitto ed Arabia Saudita hanno preso provvedimenti, anche sul piano religioso, atti a contrastare il trading di criptovalute, in Malesia ed Indonesia queste sono sempre più diffuse.

In questi giorni molti commentatori si domandano se il crollo del Bitcoin non sia altro che lo sgonfiarsi dell'ennesima "bolla" speculativa; altri parlano di un elaborato schema di Ponzi. Le istituzioni internazionali vedono le criptovalute come una minaccia alla stabilità finanziaria e mettono in guardia sulla possibilità che la discesa dei prezzi possa in alcuni casi portare a zero il valore di alcune di esse. Un caso emblematico è quello del **Bitconnect**, criptovaluta che ha perso (tra il 7 gennaio ed il 7 febbraio) ben 2.5 miliardi di capitalizzazione, ovvero il 97% del suo valore.

Bibliografia

[1] Satoshi Nakamoto - Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore - Bitcoin: Economics, Technology, and Governance - Journal of Economic Perspectives—Volume 29, Number 2—Spring 2015—Pages 213–238
[3] Jamal Bouoiyour and Refk Selmi - Ether: Bitcoin's competitor or ally?
[4] Morgan C. Benton and Nicole M. Radziwill - Quality and Innovation with Blockchain Technology
[5] Janze, C. (2017, June). Towards a Decentralized Information Systems Success Model. In Atas da Conferência da Associação Portuguesa de Sistemas de Informação (Vol. 17, No. 17, pp. 42-59).
[6] Nicola Dimitri - Bitcoin mining as a contest ISSN 2379-5980 (online) doi: 10.5195/LEDGER.2017.96
[7] Bano at al. - SoK: Consensus in the age of Blockchains
[8] S. Porru, A. Pinna, M. Marchesi, R. Tonelli - Blockchain-oriented Software Engineering: Challenges and New Directions

Autore: Umberto M. Meotto
Da sempre interessato alla divulgazione scientifica, Umberto Maria Meotto lavora come Senior Process Integration Engineer nel dipartimento di Ricerca e Sviluppo della Micron Technology, multinazionale americana leader globale nel settore dei semiconduttori. Nato nel 1978 a Torino, si laurea nel 2003 in Scienza dei Materiali con una tesi sui diodi in Carburo di Silicio condotta principalmente presso i laboratori del Politecnico di Torino. Dopo pochi mesi viene assunto da STMicroelectronics dove si occupa di Memorie Flash NOR a 90 e 65nm. Dal 2008 al 2010 lavora per Numonyx, spin-off delle divisioni memorie di STM ed Intel, su tecnologie Flash NAND a 52nm. Ha al suo attivo alcune pubblicazioni e 4 brevetti negli Stati Uniti inerenti memorie ad intrappolamento di carica (CTF) e a cambiamento di fase (PCM), suo attuale campo di ricerca.

Info sui Revisori di questo articolo

- **Luca Fumarco**, PhD in economia, si occupa di benessere economico come postdoc presso l'istituto di statistica lussemburghese STATEC.
- **Roberto di Lauro** è Software Engineer presso London Stock Exchange Technology. In particolare si occupa di Sistemi di High Frequency Trading.
- **Valentina Speranzini** è laureata in biologia e lavora come ricercatrice postdoc in biologia strutturale presso lo European Molecular Biology Laboratory (EMBL) di Grenoble.