Appendice

Come nasce il progetto

Perché di tutti gli aspetti interessanti che orbitano intorno al mondo delle cryptovalute abbiamo deciso proprio di affrontare quello dei consumi di blockchain?

L'aspetto che più ci interessava analizzare di blockchain era in generale la sua trasparenza: quali contraddizioni si può portare dietro un protocollo all'apparenza così limpido? A quanto pare molte. in primo luogo, l'estrema trasparenza del protocollo stesso spinge chi vi si interessa a guardarvi attraverso e a concentrarsi su altro; l'attenzione non si ferma su quello che è in piena vista, ma si focalizza su quello che sta dietro: le cryptovalute. E in effetti in questo ambito le possibilità da analizzare erano molte: il boom improvviso del 2018, l'utilizzo delle cryptovalute per attività illegali di vario genere, l'enorme sommerso di transazioni fittizie, l'inerente contraddizione di un mercato che vuole essere libero e decentralizzato ma che in realtà è nelle mani di pochi eletti, e potremmo andare avanti. Le ragioni principali per cui abbiamo deciso di ignorare questi argomenti sono due: la prima, sono tutti problemi che vanno oltre blockchain, qualcosa che sta dietro le quinte, la terza faccia della moneta che elude la scienza dei dati; il secondo, e forse il più importante, è che questi argomenti contribuiscono a spostare ancora di più l'attenzione dalla trasparenza di blockchain che volevamo analizzare, e questo non poteva fare altro che stimolare la nostra curiosità sul punto iniziale.

Perché qualcosa di così trasparente non attira la nostra attenzione?

A guardare bene, forse qualcosa di interessante all'interno del protocollo stessa c'è, una contraddizione interna che spesso tende a passare inosservata. Ma per vederla dobbiamo ritornare ad osservare quel lato della moneta che sfugge alla scienza dei dati.

È il 2017, il valore di bitcoin, e con esso di tutte le altre crypto, inizia a salire vertiginosamente, attirando l'attenzione di investitori e speculatori in tutte le parti del mondo. Non sono solo le cryptovalute a volare in quel biennio: il mercato del mining impazzisce, un numero indefinito di acquirenti si getta in massa ad acquistare più hardware possibile per minare in fretta e furia, e i miner arrivano letteralmente a noleggiare Boeing 747 da riempire di ASIC e schede video per mettere le mani il più in fretta possibile su questi picconi digitali del 21esimo secolo. Ed è un aspetto legato a questa frenesia che attira la nostra attenzione: perché se ci sono così tanti miner, e se blockchain è così trasparente, non è possibile stabilire con precisione quanti di loro stanno operando nella rete? Considerando quanto consuma l'hardware destinato al mining, e considerando che un mercato del genere attira numerosissimi investitori e speculatori, un'informazione del genere è di importanza quantomeno non secondaria. Blockchain è così trasparente che spesso la nostra attenzione tende a ignorarla, a maggior ragione quella del miner che più che sul protocollo si concentra sul quanto gli costi minare una cryptovaluta. Ma che prezzo hanno i miner?

Una risposta precisa a questa domanda, come abbiamo visto, purtroppo non esiste. Quello che però è davvero peculiare è che un protocollo che si professa trasparente non dia neanche la possibilità di capire quanto una stima, che non sia una stima minima, sia lontana dalla realtà. Non speravamo di trovare dei dati riguardanti i consumi di tutte le risorse allocate per l'universo delle cryptovalute, non è possibile stabilire i costi relativi alla produzione e alla distribuzione dell'hardware dedicato al mining semplicemente perché l'hardware, una volta che esce dal produttore, non è più tracciabile. In molti casi non sappiamo nemmeno quanto hardware esista, i produttori di ASIC tendono a non condividere informazioni riguardo alle loro produzioni.

Date queste premesse, la nostra attenzione si è concentrata su questo aspetto abbastanza oscuro di blockchain, e per analizzarlo abbiamo deciso di concentrare la nostra attenzione sul luccichio dell'oro del nuovo millennio: bitcoin. Quanto ci costa collettivamente bitcoin in termini energetici? E quanto può inquinare una moneta digitale?

Blockchain e proof of work: come nasce l'oro del nuovo millennio?

Una cryptovaluta è un enorme registro di transazioni, un libro mastro dove vengono segnati i debiti e i crediti degli utenti che ne fanno parte.

A vuole inviare denaro digitale a B. Se il denaro è a conti fatti una stringa di bit, come si fa a rendere questa stringa non falsificabile, unica, e non duplicabile?

Una possibile soluzione consiste nel firmare una dichiarazione del tipo "A invia nX a B" con la chiave privata di A e, una volta che B ha controfirmato la dichiarazione, registrarla nel libro mastro. Come funziona una firma digitale?

Ogni utente possiede una coppia di chiavi: una pubblica e una privata. Una firma digitale, differentemente da una firma normale, non è un'entità fissa ma varia a seconda del documento firmato: il risultato della funzione che genera la firma dipende infatti sia dal documento da firmare, sia dalla chiave privata dell'utente che vuole firmare quel documento. Cambiare anche solo un bit del documento stravolge completamente la firma finale. La funzione di verifica prende invece in esame tre parametri: il messaggio, la firma del messaggio, e la chiave pubblica dell'utente che ha firmato il messaggio. Attraverso la funzione di verifica chiunque consulti il libro mastro può utilizzare le chiavi pubbliche di A e di B per verificare che le firme siano legittime e la transazione accettabile. Questa soluzione elimina il problema della creazione dal nulla di transazioni false, questa stringa può essere generata solo da A e controfirmata da B, ma non quello della duplicazione delle transazioni già esistenti (una volta creato il messaggio potrebbe essere copiato più volte sul libro mastro).

Per rendere una transazione unica si può assegnare ad essa un numero seriale univoco, ma per farlo c'è bisogno di un ente autorevole che assegni un numero di serie valido a ogni transazione. Questo ente dovrebbe occuparsi di controllare le transazioni, controllare i saldi di tutti gli utenti nel libro mastro, e fornire i numeri di serie univoci solo alle operazioni valide. In questo modo, una dichiarazione del tipo "A invia nX a B, codice seriale #123456" può essere registrata in maniera univoca e sicura sul libro mastro una volta che B, dopo essersi accertato con l'ente garante, decida di controfirmare la dichiarazione.

Sorgono due problemi: come fare a scegliere un ente autorevole? Fare in modo che i flussi di denaro vengano gestiti da un'entità centrale crea più vantaggi o svantaggi?

L'idea alla base della blockchain è quella di rendere tutti gli utenti del libro mastro l'ente di controllo stesso. In particolare, tutti gli utenti che utilizzano il libro mastro posseggono una copia del libro mastro stesso per controllare la validità delle transazioni. Questo libro mastro è appunto detto Blockchain.

All'interno della blockchain, quando A vuole inviare denaro a B, A firma il messaggio "A invia nX a B, codice seriale #123456" e invia questo messaggio a B; B può poi usare la sua copia della blockchain per controllare che la transazione sia legittima e, una volta confermata la validità della transazione, può controfirmarla per accettarla. Se la transazione viene accettata, B si occupa di trasmetterla a tutta la rete blockchain che viene riaggiornata con la nuova transazione, altrimenti la transazione viene ignorata e la blockchain non viene aggiornata.

Questo approccio però genera due problemi: 1) chi fornisce il codice seriale per la transazione? 2) come fare per impedire che A possa inviare la stessa dichiarazione, con lo stesso numero seriale, a più utenti diversi?

Caso ipotetico: A può inviare i messaggi "A invia nX a B, codice seriale #123456" a B e "A invia nX a C, codice seriale #123456" a C contemporaneamente; B e C controlleranno la validità della dichiarazione sulla loro blockchain che non è stata ancora aggiornata e, nel caso dovessero valutare la transazione nella stessa finestra d'aggiornamento temporale, entrambi controfirmeranno la transazione come valida e la trasmetteranno alla blockchain globale. Ma come fa la blockchain globale a decidere quale delle due transazioni con lo stesso numero seriale è valida? E anche se dovesse decidere, il codice seriale è univoco, quindi una delle transazioni verrebbe scartata.

Per evitare questa situazione l'utente che deve controfirmare una transazione non dovrebbe limitarsi a verificare la transazione da solo. Quando A invia il messaggio "A invia nX a B, codice seriale #123456", B dovrebbe come prima cosa controllare la validità sulla sua copia della blockchain, poi dovrebbe ritrasmettere il messaggio a tutta la rete e infine, una volta che la transazione è stata validato dalla rete, controfirmarla e ritrasmetterla a tutto il network. In questo modo, una situazione come quella precedente in cui A invia due pagamenti con lo stesso codice seriale a due persone diverse non potrebbe verificarsi, in quanto la rete stessa segnalerebbe ai due utenti che c'è un problema con la transazione prima che questi possano accettarla.

Come decidere però quanti utenti devono accettare una transazione prima che essa sia definita valida? Non possono essere tutti perché non è possibile conoscere a priori il numero di utenti della rete e, sempre per lo stesso motivo, non è possibile definire una porzione o comunque un numero fisso di utenti necessari per l'approvazione. Un possibile problema, inoltre, è che un utente potrebbe prendere il controllo del sistema di decisione creando un numero enorme di utenti fittizi che prendano il controllo della rete ogni volta che bisogna validare una transazione. È dunque necessario un sistema di consenso che non possa essere aggirato.

La rete blockchain utilizza un algoritmo di consenso basato sul protocollo *proof of work.* Il protocollo *proof of work* prevede la combinazione di due idee: 1) rendere artificiosamente costosa da un punto di vista computazionale la validazione delle transazioni e 2) premiare gli utenti che aiutano a validare le transazioni. Il vantaggio del rendere la validazione di una transazione complessa è che in questo modo non può essere influenzata dal numero di identità che un utente controlla all'interno della rete, bensì dalla potenza computazionale che può

utilizzare per influenzare l'esito della verifica. È possibile, con alcune accortezze, fare in modo che sia impossibile (o comunque *estremamente* sconveniente) avere la potenza computazionale necessaria per soverchiare il resto della rete.

La *proof of work* prevede il seguente scenario: A trasmette alla rete il messaggio "A invia nX a B, codice seriale #123456"; man mano che gli utenti della rete ricevono il messaggio lo aggiungono ad una coda di messaggi simili, ancora non approvati, che hanno ricevuto fino a quel momento; gli utenti che vogliono convalidare le transazioni in coda devono prima risolvere un puzzle complesso a livello di calcolo, la proof of work, perché la loro verifica possa essere considerata valida ed essere così trasmessa alla rete.

Il puzzle da risolvere consiste nel trovare, dato un blocco di transazioni e una funzione crittografica SHA-256, un numero x che, dato in input alla funzione insieme al blocco di transazioni, generi un hash che cominci con un numero di 0 consecutivi deciso in partenza. La difficoltà del puzzle dipende dal numero di 0 consecutivi che si devono trovare. La peculiarità che rende la risoluzione di questo puzzle difficile è che l'output di una funzione hash crittografica si comporta a tutti gli effetti come un numero casuale: cambiare anche solo di 1bit l'input della funzione stravolge l'output finale in maniera imprevedibile. Non appena un utente trova un numero che soddisfi i requisiti lo trasmette alla rete insieme al blocco di transazioni da approvare. Una volta verificata la legittimità della soluzione, tutti gli utenti della rete aggiornano la blockchain con l'ultimo blocco di transazioni.

Dal momento che l'unico modo per trovare un numero che soddisfi i requisiti consiste nell'andare per tentativi, e che la complessità dell'operazione è estremamente elevata (può essere manipolata in maniera arbitraria, ad esempio nel caso della rete bitcoin che è tarata per risolvere in media un blocco ogni 10 minuti), la potenza di calcolo necessaria per trovare quel numero è molto alta. È dunque necessario trovare un incentivo perché la gente sia spinta a usare potenza computazionale per validare questi blocchi di transazioni.

Il processo di validazione nella blockchain è chiamato mining. Per ogni blocco di transazioni validato, il primo miner che riesce a validarlo riceve come ricompensa una determinata quantità di credito, nuova valuta che viene generata all'interno della blockchain. La proof of work è insomma una sorta di gara a chi è più veloce ad approvare nuovi blocchi di transazioni: le chance di vincere il blocco dipendono dalla percentuale di potenza computazionale che può impiegare per risolvere il puzzle. Ad esempio, se un miner controlla l'1% della potenza globale della rete di validazione, la probabilità che vinca un blocco è di circa l'1%.

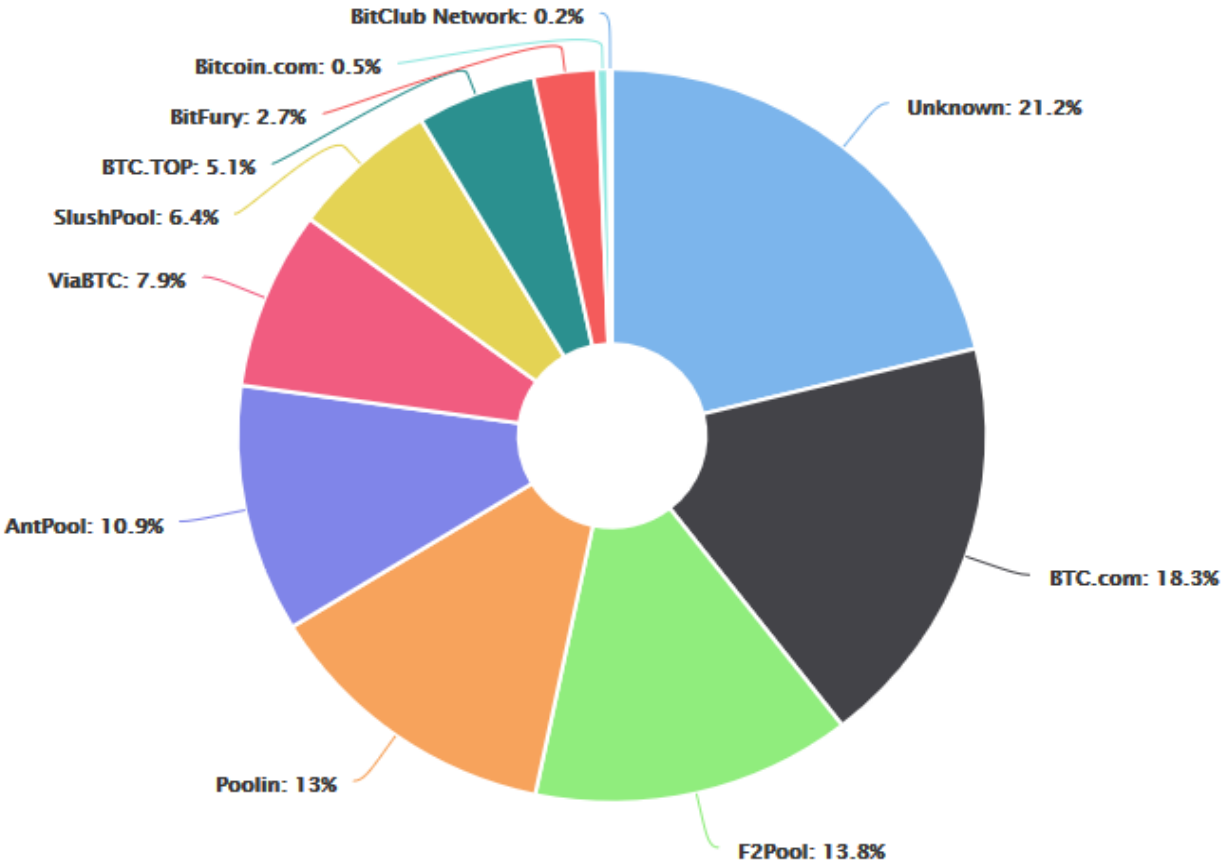
Un blocco è considerato valido solo se ha una proof of work valida, e per fare in modo che la blockchain sia ordinata in maniera cronologica ogni blocco contiene l'hash del blocco precedente. Dal momento che gli utenti della blockchain prendono come riferimento la catena con la maggior potenza computazionale spesa per generarla, quando un utente della rete riceve due blockchain diverse tra di loro, l'utente sceglierà quella con la catena più lunga; in caso di pareggio, aspetterà fino a quando una delle due non diventerà n blocchi più lunga dell'altra. In un sistema del genere, validare blocchi contenenti transazioni illegittime è estremamente

complesso. Se A invia a B un blocco non legittimo, B non lo accetterà subito perché allo stesso momento riceverà i blocchi legittimi trasmessi dagli altri miner; considerando che l'utente B sceglierà sempre la catena più lunga, per riuscire nel suo intento A dovrebbe continuare a generare da solo più blocchi rispetto a tutta la rete di miner. Per poter riuscire nel suo intento, A da solo dovrebbe avere più del 50% della potenza di calcolo dell'intera rete.

Quanto guadagnano i miner?

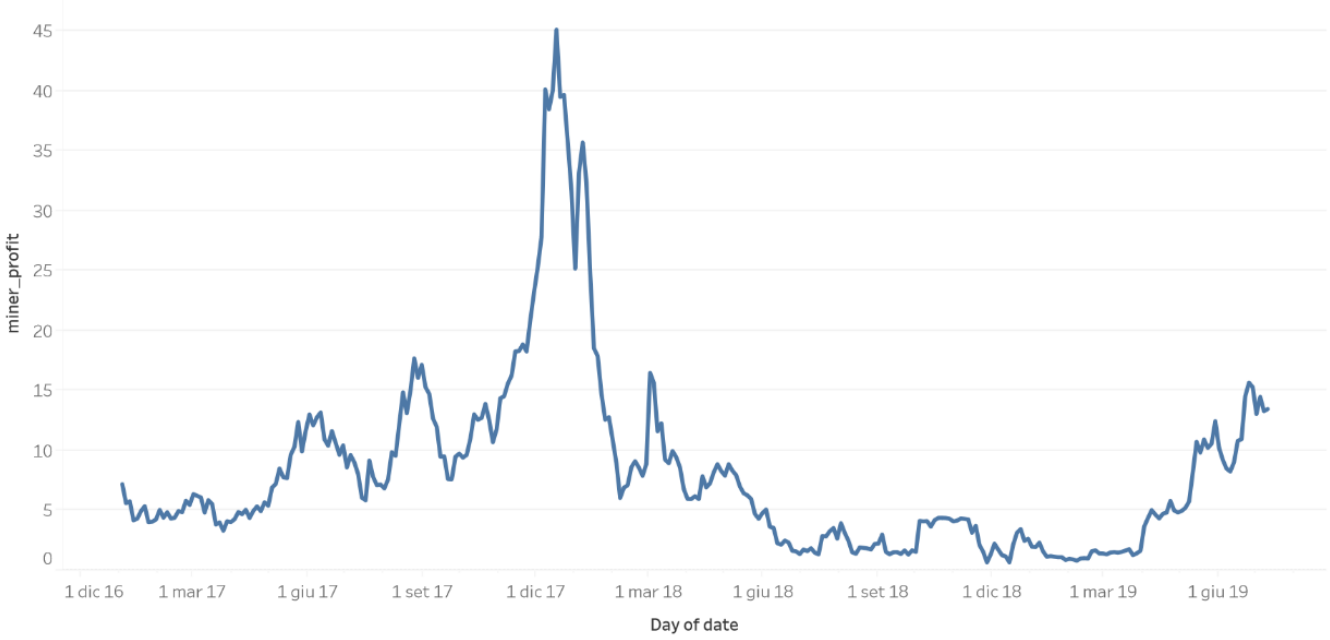
Il funzionamento di una blockchain dipende dalla sua fitta rete di validatori: utenti che mettono a disposizione una qualche risorsa per validare le transazioni e ottenere valuta in cambio. La risorsa messa a disposizione dipende dal tipo di blockchain, ma nel nostro caso l'attenzione si è focalizzata sulla potenza di calcolo, che è la risorsa utilizzata nelle reti proof of work.

Prendendo come riferimento la blockchain di bitcoin, la richiesta di potenza di calcolo attualmente necessaria per minare un blocco è estremamente onerosa, dunque anche il costo delle macchine per il mining risulta molto elevato (anche senza tenere conto dei costi di gestione come energia, raffreddamento e manutenzione). Questi alti costi di mining spingono gli attori della rete ad operare in gruppi detti pool: dei raggruppamenti in cui ogni miner mette a disposizione la propria potenza di calcolo che va a sommarsi con quella degli altri miner, aumentando così le probabilità che una pool vinca un determinato blocco. Una volta che una pool vince un blocco il guadagno derivato viene ridistribuito tra i miner che hanno partecipato nella pool stessa, con proporzioni che variano a seconda delle policy di ogni gruppo. La situazione attuale delle pool che operano su bitcoin è mostrata nel grafico seguente.



Il grafico ci dà un'idea di come sono divisi i guadagni complessivi della rete BTC tra le varie pool, ma purtroppo non ci dice come sono composti questi gruppi. L'hardware utilizzabile per minare bitcoin è praticamente infinito, e non tutti i miner operano in maniera legittima o razionale (ad esempio, per qualcuno che sta rubando potenza di calcolo è irrilevante tenere conto del rapporto guadagni/consumi dal momento che i costi legati all'utilizzo dell'hardware non lo riguardano). In sostanza, non è possibile sapere con certezza chi fa parte delle varie pool e quali e quante macchine operino al loro interno.

Quello che possiamo vedere però è un limite minimo di unità operative sotto al quale non si può scendere: dividendo la potenza di calcolo comprensiva della rete per la potenza della macchina più potente in commercio possiamo ottenere il numero minimo di macchine presenti in una determinata finestra temporale. Un altro dato interessante di cui tenere conto è che è possibile vedere quali sono i guadagni giornalieri del mining sull'intera blockchain Bitcoin. Con questi dati a disposizione, dividendo i guadagni complessivi per il numero minimo di miner presenti, assumendo che tutti i miner abbiamo le stesse probabilità di vincere un blocco (nello scenario ipotizzato tutte le macchine hanno la stessa potensa), è possibile ottenere il guadagno massimo in dollari per macchina sulla rete (tenendo conto anche di un costo in corrente giornaliero standardizzato di 0.12$ per kWh). Il grafico che si ottiene, partendo dal 2017, è il seguente:



Glossario

Altcoin: una valuta digitale alternativa a Bitcoin. Molte altcoin nascono come fork di bitcoin con qualche cambiamento rispetto alla versione standard (ad esempio Litecoin).

Asic: acronimo di "Application Specific Integrated Circuit", sono dei circuiti progettati per eseguire un unico compito (ad esempio, generare numeri casuali per un algoritmo di cifratura in particolare).

Attacco 51%: un attacco su blockchain in cui un agente controlla più del 50% del consenso della rete. Il consenso può tradursi in potenza di calcolo in caso di blockchain proof of work, valuta per la proof of stake, etc.

Bitcoin: la cryptovaluta più conosciuta, il gold standard delle crypto, creata nel 2009 da Satoshi Nakamoto. Utilizza una blockchain proof of work ed è la valuta con più miner.

Blockchain: una ledger distribuita, composta da pacchetti di transazioni immutabili detti blocchi. I blocchi rappresentano lo storico delle transazioni nella rete, e ognuno di essi è agganciato al blocco precedente tramite una firma digitale cifrata.

Crypto/Cryptovaluta: una forma di valuta digitale protetta, generata, e distribuita attraverso tecniche crittografiche varie.

Decentralizzazione: il trasferimento dell'autorità da un'organizzazione o ente centralizzato ad un network distribuito in cui l'autorità è divisa tra I vari nodi.

Difficoltà: un indice della potenza di calcolo necessaria, in hash, per vincere un blocco

Fork: una versione alternativa di una blockchain

Gpu: acronimo di "graphics processing unit". Le gpu sono volgarmente delle schede video che, per ragioni di architettura, si prestano a minare alcune cryptovalute meglio di altri tipi di hardware.

Hash: una funzione che converte un input di numeri e lettere in un output criptato di lunghezza finita. Nel caso del mining, l'output di una funzione hash è l'elemento che serve per validare un blocco.

Hashrate: il numero di funzioni hash eseguite da un hardware, per un algoritmo specifico, in un determinato intervallo di tempo

Ledger: un registro in cui le informazioni possono essere solamente aggiunte, mentre I record precedenti restano immutati. Generalmente usato per immagazzinare transazione, può contenere anche informazioni di altro tipo.

Market Cap: il valore totale del mercato di una determinata cryptovaluta

Miner: l'entità singola che effettua il mining. Utilizzato sia per indicare il possessore delle macchine, sia la macchina stessa singolarmente

Mining: il processo attraverso il quale le transazioni vengono validate in una blockchain proof of work. Il mining prevede l'utilizzo di potenza di calcolo per risolvere problemi crittografici, validare blocchi, e attraverso la validazione generare nuova valuta.

Proof of stake: un sistema di consenso alternativo alla proof of work in cui la risorsa utilizzata per gestire il consenso è la valuta stessa.

Proof of work: un algoritmo di consenso in cui la risorsa utilizzata per gestire il consenso della rete è la potenza di calcolo impiegabile dai miner.

SHA 256: la funzione criptografica alla base della proof of work della blockchain bitcoin

Whitepaper: un documento in cui vengono definite le specifiche tecniche di una cryptovaluta.

Bibliografia

De Vries, Alex. “Bitcoin Energy Consumption Index.” *Digiconomist*, https://digiconomist.net/bitcoin-energy-consumption

De Vries, Alex. “Bitcoin Electronic Waste Monitor.” *Digiconomist*, https://digiconomist.net/bitcoin-electronic-waste-monitor

Nielsen, Michael. “How the Bitcoin protocol actually works.” *DDI: Data-driven intelligence*, 06/12/2013, http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 18/08/2008, https://bitcoin.org/bitcoin.pdf

Buterin, Vitalik, and Virgil Griffith. “Casper the Friendly Finality Gadget.” 29/10/2017, https://github.com/ethereum/research/blob/master/papers/casper-basics/casper_basics.pdf

Rauchs, Michel and Blandin, Apolline and Klein, Kristina and Pieters, Gina C. and Recanatini, Martino and Zhang, Bryan Zheng, “2nd Global Cryptoasset Benchmarking Study”, 12/12/2018, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf

Stoll, Christian, and Klaaßen, Lena, and Gallersdörfer, Ulrich. “The Carbon Footprint of Bitcoin.” Joule, 12/06/2019, https://www.cell.com/joule/fulltext/S2542-4351(19)30255-7

Fortney, Luke. “Blockchain Explained” *Investopedia*, 25/06/2019, https://www.investopedia.com/terms/b/blockchain.asp

Acronis, “Acronis Notary.” *Acronis*, Acronis, https://www.acronis.com/it-it/blockchain-data-authentication

Simply vital health, “Healthcare Safe Blockchain Infrastructure.” *Simply vital health*, https://www.simplyvitalhealth.com

Zago, Matteo Gianpietro. “Essentia to become first blockchain based solution from Finnish Government through collaboration with MTK” *Medium*, Medium, 13/04/2018, https://medium.com/essentia_one/essentia-to-become-first-blockchain-based-solution-from-finnish-government-through-collaboration-4ae326126c13

Press Release. “PR: Essentia.One in Talks with the Netherlands Government for Blockchain Solutions to Border Control.” *Bitcoin.com*, 06/03/2018, https://news.bitcoin.com/pr-essentia-one-in-talks-with-the-netherlands-government-for-blockchain-solutions-to-border-control

IBM. “IBM Verify Credentials: transforming digital identity into decentralized identity.” *IBM Blockchain*, IBM, https://www.ibm.com/blockchain/solutions/identity

Jenkinson, Gareth. “Ethereum Classic 51% Attack — The Reality of Proof-of-Work.” *Cointelegraph*, 10/01/2019, https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work

Orcutt, Mike “Nearly all Bitcoin trades are fake, apparently.” *MIT Technology Review*, 26/03/2019, https://www.technologyreview.com/f/613201/nearly-all-bitcoin-trades-are-fake-apparently

Danova, Helga. “Official statement on 51% threat and closed round table.” *CEX.IO*, 16/07/2014, https://blog.cex.io/news/official-statement-on-51-threat-and-closed-round-table-6619

Interviste

Di Francesco Maesa, Damiano. Intervista via Skype 09/07/2019.

De Vries, Alex. Intervista via Skype 10/07/2019.

Fonti Dati

CoinMarketCap. “Top 100 Cryptocurrencies by Market Capitalization.”, dati consultati in data 13/07/2019, CoinMarketCap, https://coinmarketcap.com

Blockchain. “Hash Rate.”, dati consultati in data 13/07/2019, Blockchain.com, https://www.blockchain.com/it/charts/hash-rate

Blockchain. “Miners Revenue.”, dati consultati in data 13/07/2019, Blockchain.com, https://www.blockchain.com/charts/miners-revenue

Blockchain. “Hashrate Distribution.”, dati consultati in data 13/07/2019, Blockchain.com, https://www.blockchain.com/pools?timespan=4days

De Vries, Alex. “Bitcoin Energy Consumption Index”, dati consultati in data 13/07/2019, Digiconomist, https://digiconomist.net/bitcoin-energy-consumption

De Vries, Alex. “Bitcoin Electronic Waste Monitor.”, dati consultati in data 13/07/2019, Digiconomist, Digiconomist, https://digiconomist.net/bitcoin-electronic-waste-monitor

Edgar. “Fossil CO2 & GHG emissions of all world countries, 2017.”, European Commission: EU Science Hub, https://edgar.jrc.ec.europa.eu/overview.php?v=CO2andGHG1970-2016&sort=des8

International Energy Agency. “World energy outlook 2017 (Annex A).”, International Energy Agency, https://www.iea.org/weo2017/

Cryptocompare. “Mining Equipment (ASIC).”, dati consultati in data 20/06/2019, https://www.cryptocompare.com/mining/#/equipment

Bitcoin Wiki. “Non-specialized hardware comparison”, dati consultati in data 23/06/2019, https://en.bitcoin.it/wiki/Non-specialized_hardware_comparisonAuthor

United States Energy Information Administration. “Total Electricity Net Generation.”, EIA Gov, https://www.eia.gov/beta/international