Alsindi, Wassim Zuhair; Lotti, Laura

Article

Mining

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Alsindi, Wassim Zuhair; Lotti, Laura (2021) : Mining, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-9, https://doi.org/10.14763/2021.2.1551

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Mining

Wassim Zuhair Alsindi *Massachusetts Institute of Technology* wassim@pllel.com
Laura Lotti *Independent*

DOI: https://doi.org/10.14763/2021.2.1551

Published: 20 April 2021
Received: 18 November 2020 **Accepted:** 27 November 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Alsindi, W. Z. & Lotti, L. (2021). Mining. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1551

Keywords: Blockchain

A draft of this article underwent open peer-review as an **Open Abstract**

Abstract: In the context of blockchain networks, mining describes a permissionless process intended to ensure the global consistency of a decentralised ledger. Mining requires the consumption of a costly computational resource to participate in a probabilistic competition that confers specific privileges to a node. These privileges typically relate to the proposal of a new block, including the identity and order of transactions contained within. Mining is incentivised via an algorithmically regulated provision of rewards, usually in the form of newly generated coins and/or transaction fees.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

In the context of blockchain networks, *mining* describes a permissionless process intended to ensure the global consistency of a decentralised ledger. Mining requires the consumption of a costly computational resource to participate in a probabilistic competition that confers specific privileges to a node. These privileges typically relate to the proposal of a new block, including the identity and order of transactions contained within. Mining is incentivised via an algorithmically regulated provision of rewards, usually in the form of newly generated coins and/or transaction fees.

Origin

Cryptocurrency mining was initially understood to refer to processes incorporating proof-of-work (PoW) (i.e., the spending of costly computational resources such as central processing unit (CPU) cycles via a mechanism originally developed to mitigate spam) (Dwork & Naor, 1992; Back, 2002). PoW is usually a permissionless process (i.e., anyone can partake) with miners' identities unknown (anonymous/pseudonymous). Precursor digital money projects such as Bit Gold and b-money (Szabo, 2005; Dai, 1998) proposed the use of PoW-type mechanisms to avoid resource exhaustion and message flooding attacks or Sybil attacks from large numbers of dishonest *sockpuppet* nodes (Douceur, 2002).

While the Bitcoin Whitepaper (Nakamoto, 2008a) did not refer to PoW explicitly as mining, reference was made to the gold mining analogy. The term was used colloquially in online forums and chatrooms including BitcoinTalk and IRC (Internet Relay Chat, a long-running instant messaging protocol) as far back as 2010. Indeed, the source code of the first version of the Bitcoin software referred to the process of generating coins as mining (Nakamoto, 2009).

The chain selection heuristic which uses PoW to ensure the eventual network-wide consistency of the Bitcoin ledger is referred to as Nakamoto Consensus. This requires a 51% majority of "work" to reach agreement on the latest valid block and a *"guarantee that all honest parties output the same sequence of blocks throughout the execution of the protocol"* (Kiffer et al., 2018, p. 1). Blockchains grow in height incrementally as new candidate blocks are constructed by miners and added to the

canonical chain. In PoW-based networks this takes place through the combination of nonces (i.e., an arbitrary variable which is progressively iterated) with the proposed block header to generate hashes which are then compared against the network-determined difficulty of finding a block. The miner chooses the identity and order of transactions contained within a proposed candidate block and this has potential economic implications including front-running and re-ordering of transactions (Daian et al., 2019).

The mining process is mediated by a *difficulty adjustment* feedback mechanism, which periodically recalibrates the effective probability of finding a valid block so as to maintain the network's target inter-block times. Should the hash of a candidate block be found that satisfies the network's difficulty requirements, the miner will announce it to the network and fellow network participants will confirm the validity of the block. Within the block, the miner may claim a so-called *mining subsidy* or *block reward* by including a transaction payable to themselves, in addition to any mining fees paid by transactions included.

The key cryptographic component of Bitcoin mining is the SHA-256 hash puzzle. Hashing refers to a one-way deterministic process that converts an input of arbitrary length to one of fixed length. An ideal cryptocurrency hashing algorithm must have the following properties (Narayanan a& Clark, 2017): (i) it is difficult to compute so that shortcuts or undue advantages are not available to participants; (ii) cost is parameterisable so that the energetic expenditure required to mine a valid block is not fixed over time; and (iii) it is trivially easy to verify the correctness of the hashed output from the input material. Since cryptographic hash functions are deterministic (i.e., given a fixed block with a fixed nonce—and a broad subset of possible hash values satisfying the difficulty requirements exist), it is entirely plausible that more than one valid candidate block may be found by competing miners at very similar times. In such an eventuality there begins a block propagation competition *per se* which allows the network to reach agreement on the latest state of the transaction ledger.

The class of hashing algorithms used in cryptocurrency mining today are considered to be potentially vulnerable to cryptographic attacks by quantum computers, resulting from the ability of quantum systems to search possibility spaces more efficiently than their classical counterparts. Increasingly sophisticated hardware and algorithms such as Shor's (1994) and Grover's (1996) collectively threaten the integrity of key mathematical assumptions for public-key cryptography such as the hardness of integer factorisation problem, the discrete logarithm problem and the elliptic-curve discrete logarithm problem. Quantum-resistant cryptographic

schemes have already been proposed for Bitcoin (Ruffing, 2019), however these would require contentious protocol upgrades.

Since there can only be one block with a particular height in a blockchain, should multiple candidates emerge the prospect of a persistent network partition known as a *fork* arises if subsets of the population of validating nodes do not overwhelmingly agree on the latest block. Such partitions may be short-lived in the case of *stale blocks* such as "orphans" and "uncles" (terms used with respect to Bitcoin and Ethereum mining respectively) [1] which represent discarded timelines as the canonical chain built upon another candidate block. In other cases, a fork can happen due to a malicious attack, such as a "51% attack"—when a nefarious actor manages to take control of the majority of hashing power and is able to modify the order of transactions or reverse the transactions that they themselves made, leading to double-spending (i.e., spending the same digital coins twice).

Combining these various elements, we can take the original meaning of cryptocurrency mining to be a *thermoeconomic*[2] process employing PoW and a parameterisable feedback mechanism (difficulty adjustment) with direct incentives provided by block rewards from an algorithmically regulated network-level issuance schedule alongside transaction fees.

Evolution

Since Bitcoin's PoW, the range of activities falling under the nominal banner of mining has broadened substantially over time.

A number of alternative PoW strategies have emerged in recent years, at first hypothetical and subsequently observed in the wild, which afford favourable game-theoretic outcomes by deviating from *honest* mining behaviour as originally intended by the Bitcoin protocol (Eyal & Sirer, 2018, Grunspan & Pérez-Marco, 2018). *Selfish mining*, also known as block withholding, may be conducted by a miner who finds a valid block but instead of immediately broadcasting to peers, the block is withheld and kept secret. The miner then begins to search for a valid block atop the previous clandestine block, with the aim of finding a valid second block (and then announcing the first secret block) before another participant finds an alternative

1. The term *uncle* is associated primarily with Ethereum-based networks, as a partial subsidy is allocated to orphaned blocks and therefore acts as a consolation prize for producing a valid block which does not become part of the canonical chain.

2. A portmanteau of *thermodynamic* and *economic*, not associated with the heterodox field of thermoeconomics.

valid first block. It has been claimed that this adversarial strategy is more beneficial than honest mining for a sufficiently well-resourced miner.

With the development of the field, the processes at the core of decentralised consensus have become unbundled and abstracted from the materiality of computational work, while at the same time capital and other exogenous resources have become more integrated. One popular approach to this virtualisation of work is *staking*, which involves locking (i.e., rendering illiquid) some form of collateral in a protocol and being rewarded for participating in network consensus proportionally to the amount staked. Since it extends and further virtualises the novelty of Bitcoin's consensus model, staking via proof-of-stake (PoS) has also been called "generalised mining" or "mining 2.0" (Brukhman, 2018). In fact, staking was initially proposed as a less computationally-intensive alternative to PoW to prevent double-spending in base layer chains such as Ethereum (King & Nadal, 2012), but the model has found broad application in 'layer-2' cryptoeconomic protocols (Brekke & Alsindi, 2021), made possible by smart contracts. An area in which staking has found significant application in layer-2 protocols is *Decentralised Finance* (DeFi), in which *liquidity mining* is currently (at the time of writing) a popular term used to describe the incentivised provision of collateral and liquidity for the most disparate financial activities: lending, borrowing, insurance, synthetic derivatives, and governance over the risk parameters of a decentralised bank.

Issues currently associated with the term

Critiques of the mining metaphor

The analogy between PoW-secured digital currency and gold has been widely discussed. In general it echoes the desirable commodity money characteristics prized by adherents to modern libertarian ideals or the Austrian School of Economics (Alsindi, 2019), among which is Szabo's concept of *unforgeable costliness* (Szabo, 2008) relating to the inelasticity of supply of Bitcoin (and most subsequent PoW cryptocurrencies). The strict resource scarcity that arises from Bitcoin's algorithmically regulated issuance schedule and the analogy with gold mining have become expressions of the *digital metallism* that characterises Bitcoin's discourse (Maurer et al., 2013).

Swartz (2018) further differentiates between *digital metallism* and *infrastructural mutualism*, that is, two techno-economic imaginaries stemming from the cryptoanarcho-libertarian and cypherpunk subcultures, respectively. Here mining, and the diverse meanings that emerged around this misnomer, illustrate the tensions be-

tween these two positions, which ultimately led to an ideological fork of the Bitcoin network in mid-2017: "*Digital metallists understood the act of mining as an opportunity to extract the greatest amount of Bitcoins to be used as a store of speculative value, whereas infrastructural mutualists saw mining as an act of collaboration to produce a shared privacy-protecting payment network*" (Swartz, 2018, p. 12).

These divergent ideologies profoundly influenced the development of the blockchain ecosystem beyond Bitcoin. Here we could argue that Satoshi Nakamoto and Hal Finney were much more in line with the infrastructural mutualism vision; early message logs exist where the two earliest known Bitcoin network participants were hopeful that solely altruistic behaviour could be encouraged as a community ethos (Nakamoto, 2008b). However, at the core of the process of mining is neither the minting of new coins, nor the access to decentralised economic flows *per se*, but the assurance of settlement through decentralised consensus (Antonopolous, 2018; Carter, 2019). In Bitcoin and other PoW chains, this assurance comes from the distribution of the computational power used to search for blocks, whereas in staking protocols it is a matter of economic distribution so that, in principle, no single actor is able to accumulate more than 51% of the *proving resource* (i.e., hashrate for PoW and token supply for PoS).

Ecological and thermodynamic critiques

As the term mining is now used to describe cryptoeconomic processes as well as thermoeconomic ones, the previously strained analogy now appears to be a pure simulacrum (Baudrillard, 1981). PoW mining is by necessity an energetically costly process, consisting of irreversible computation (Landuaer, 1961). At the time of writing, Bitcoin electricity consumption is estimated to be over 120 TWh per year, approximately equivalent to that of Norway or Pakistan (Cambridge Centre for Alternative Finance, 2021). Proofs-of-useful-work such as those used in cryptocurrencies such as Primecoin (King, 2013) have been proposed as more eco-friendly alternatives to Bitcoin-type PoW. In reality, useful work may not reduce the overall thermodynamic footprint of a cryptocurrency, as the effective worth of the useful work may simply be treated as a universal discount by all mining participants (Sztorc, 2015).

It has been proposed that Bitcoin liberates stranded, illiquid energy and the majority of PoW mining employs renewable energy from geothermal and hydroelectric sources far from population centres (Bendiksen & Gibbons, 2019). However, the insensitivity of PoW cryptocurrencies to the energy sources used to secure them has led to criticism as to their inability to mitigate their ecological externalities. PoS

systems are less resource-intensive but, by replacing a real (costly) resource with a virtual one, they become vulnerable to attack vectors leveraging costless simulation (i.e., "nothing-at-stake") of alternative malicious ledger timelines such as long-range attacks (Brown-Cohen et al., 2018).

Conclusion

In the context of blockchain networks, *mining* describes a permissionless process intended to ensure the global consistency of a decentralised ledger. Mining requires the consumption of a costly computational resource to participate in a probabilistic competition that confers specific privileges to a node. These privileges typically relate to the proposal of a new block, including the identity and order of transactions contained within. It is incentivised via an algorithmically regulated provision of rewards, usually in the form of newly generated coins and/or transaction fees. Initially understood to refer to processes incorporating PoW, over time the term mining has come to describe a wider array of mechanisms for achieving peer-to-peer consensus. One such "generalised mining" method is staking some form of collateral in a protocol and being rewarded for participating in network consensus. As more blockchains are adopting PoS and the term is used to describe cryptoeconomic processes as well as thermoeconomic ones, the original "gold mining" analogy has become increasingly exhausted.

ACKNOWLEDGEMENTS

The authors would like to thank Yuval Kogman, Anil Bawa-Cavia and Sam Hart for helpful feedback during the preparation of this article.

References

Alsindi, W. Z. (2019). *TokenSpace: A Conceptual Framework for Cryptographic Asset Taxonomies*. Parallel Industries. https://doi.org/10.21428/0004054f.ccff3c19

Antonopolous, A. (2018). The Bitcoin Network. In *Mastering Bitcoin* (2nd ed.). https://github.com/bitcoinbook/bitcoinbook

Back, A. (2002). *Hashcash—A denial of service counter measure*. http://www.hashcash.org/papers/hashcash.pdf.

Baudrillard, J. (1981). *Simulacra et Simulation*. Éditions Galilée.

Bendiksen, C., & Gibbons, S. (2019). *The Bitcoin Mining Network: Trends, Average Creation Costs,*

Electricity Consumption & Sources [White Paper]. CoinShares Research. https://coinshares.com/research/bitcoin-mining-network-december-2019

Brekke, J. K., & Alsindi, W. Z. (2021). Cryptoeconomics. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1553

Brown-Cohen, J., Narayanan, A., Psomas, C., & Weinberg, S. M. (2018). Formal Barriers to Longest-Chain Proof-of-Stake Protocols. *ArXiv*. https://arxiv.org/abs/1809.06528

Brukhman, J. (2018, October 30). *Generalized Mining and the Third-Party Economy: An Introduction & Primer* [Talk]. Prague Blockchain Week, Prague. https://youtu.be/ceex9CN2YZU

Cambridge Centre for Alternative Finance. (2021). *Cambridge Bitcoin Electricity Consumption Index*. University of Cambridge, Judge Business School, Cambridge Centre for Alternative Finance. https://www.cbeci.org/

Carter, N. (2019). It's the settlement assurances, stupid! [Blog post]. *Medium, Nic Carter*. https://medium.com/@nic__carter/its-the-settlement-assurances-stupid-5dcd1c3f4e41

Dai, W. (1998). *B-money*. Wei Dai. http://www.weidai.com/bmoney.txt

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. *2020 IEEE Symposium on Security and Privacy (SP)*, 910–927. https://doi.org/10.1109/SP40000.2020.00040

Douceur, J. R. (2002). The Sybil Attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Eds.), *Peer-to-Peer Systems* (pp. 251–260). Springer. https://doi.org/10.1007/3-540-45748-8_24

Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In E. F. Brickell (Ed.), *Advances in Cryptology—CRYPTO' 92* (pp. 139–147). Springer. https://doi.org/10.1007/3-540-48071-4_10

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95–102. https://doi.org/10.1145/3212998

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

Grunspan, C., & Pérez-Marco, R. (2018). On profitability of selfish mining. *ArXiv*. https://arxiv.org/abs/1805.08281

Kiffer, L., Rajaraman, R., & Shelat, A. (2018). A Better Method to Analyze Blockchain Consistency. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18*, 729–744. https://doi.org/10.1145/3243734.3243814

King, S. (2013). *Primecoin: Cryptocurrency with Prime Number Proof-of-Work* [White Paper]. Primecoin. https://primecoin.io/bin/primecoin-paper.pdf

King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* [White Paper]. Peercoin.

Landauer, D. (1961). Irreversibility and Heat Generation in the Computing Process. *IBM Journal*, *5*(3), 183–191. https://doi.org/10.1147/rd.53.0183

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The

practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277. https://doi.org/10.1080/10350330.2013.777594

Nakamoto, S. (2008a). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2008b, November 14). *Cryptography Mailing List "Bitcoin P2P e-cash paper"*. https://satoshi.nakamotoinstitute.org/emails/cryptography/12/

Nakamoto, S. (2009). *Bitcoin* (0.1.5 Alpha) [Computer software]. https://github.com/bitcoin/bitcoin/tree/4405b78d6059e536c36974088a8ed4d9f0f29898

Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36–45. https://doi.org/10.1145/3132259

Ruffing, T. (2019). *Cryptography for Bitcoin and Friends* [PhD Thesis]. Universität des Saarlandes.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/SFCS.1994.365700

Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies*, *32*(4), 623–650. https://doi.org/10.1080/09502386.2017.1416420

Szabo, N. (2005). Bit gold [Blog post]. *Unenumerated*. https://unenumerated.blogspot.com/2005/12/bit-gold.html

Sztorc, P. (2015). Nothing is Cheaper than Proof of Work [Blog post]. *Truthcoin*. https://www.truthcoin.info/blog/pow-cheapest/

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya