Blockchain Technical Report

180002209

Word count: 3634

Abstract

One of the most exciting new technologies to emerge in recent years has undoubtedly been blockchain. As with any new technology, it is important to be able to understand how it functions in order to fully engage with it and understand its strengths, weaknesses, applications, and future potential. This report provides a definitive overview of how blockchains work with additional attention paid to how cryptography and cybersecurity relate to the emergent technology.

Introduction

In a whitepaper published in 2008, the pseudo-anonymous figure Satoshi Nakamoto outlined for the first time the concept of a modern blockchain [Nak08]. The paper laid out a cryptographic framework for performing payments online without the need for a third party mediator (such as a bank or government), thereby solving the long standing double-spending problem (how can one guarantee a digital monetary token can only be spent once?) [Cho17]. A year later, the first Bitcoin network, based on previously released open source software, was begun and the digital currency became the first technology to be implemented using a blockchain network [Sar18], and arguably still remains the most well-known such technology today. The Bitcoin blockchain illustrated and exhibited the key features of a blockchain network; it was decentralised [FIN13], peer-to-peer [Dav11], and provided an immutable public record of each payment made using it [Ant14].

This report aims to explore and describe what blockchain is and how it works. This report also includes more in depth discussion of a particular aspect of blockchain technology, specifically the Proof of Stake consensus protocol and its relationship to the current standard Proof of Work protocol. Finally this report contains a review of some of the most important cybersecurity issues associated with blockchain technology, including discussion of historic failures, and concerns that have been raised with regards to the security of the emergent technology.

What is blockchain and how does it work?

Disambiguations

Throughout our discussion of blockchain, there are several terms which will often come up and which may seem interchangeable, however care should be taken to understand their specific meanings: Blockchain – the general technology being discussed, blockchain is an abstract protocol, not any single implementation; Bitcoin – the oldest blockchain based technology and often a convenient example. This report uses the convention that the abstract concept is capitalised, denominations of the currency are not (e.g. *"The Bitcoin network", "three bitcoins"*); Cryptocurrencies – a common application of blockchain, of which Bitcoin is an example. Currency based blockchain networks naturally incentivise peers in the network to behave as they should, although non-currency-based applications are viable, so long as the correct incentive structures are in place.

Overview of how blockchain works

As in the original whitepaper, we will motivate our explanation of blockchain by tying it to a real world money-based scenario. We will build our explanation by imagining a theoretical scenario wherein a group of individuals would like to digitally keep track of who in the group owes who money without having to rely on a bank or other panoptic institution. We will construct our explanation of blockchain as a means of allowing this group to accomplish this.

Anyone who has shared a house or flat with others has likely implemented a naïve version of such a system; when bills are paid, takeaways ordered, or shopping purchased, it is often easier to simply keep track of who has paid what and who is owed what in a system that can be tallied at a later time, such a system significantly reduces the number of times money needs to be exchanged physically, and if we are extremely committed to our system, has the potential to fully usurp the exchange of physical cash. This system, and others derived from it, we will call a "ledger", an entry (e.g. "Alice owes Bob £10") on the ledger a "transaction" or "line", and the individuals in the group "peers" or "nodes". A naïve ledger may rely wholly on trust, something hopefully ample among cohabiting housemates but which should be avoided at all costs if we want to extend this system to be used by people who don't know each other for larger payments and potentially even as the basis for a whole currency. On our naïve ledger, anyone can add a line, a better system would be one where when a line is added, the person spending money must verify they assent to the transfer. This can be done using a signature.

A digital signature scheme consists of three aspects: A way to generate public and private keys and two functions f (signing function) and g (verifying function) [Lys02] where

$$f(M, K_s) = S$$

and

$$g(M, S, K_p) = \begin{cases} \textit{True} & \text{if } f(M, K_s) = S \\ \textit{False} & \text{otherwise} \end{cases}$$

K_s is the private (secret) key of the signatory, K_p is the corresponding public key, M is the message or document being signed, and S is the resultant digital signature. A good digital signature system must be one such that given M and K_p (and any other knowledge except K_s) it is effectively impossible to find S such that $g(M, S, K_p) = \textit{True}$ [Lys02]. The Bitcoin blockchain network uses the Elliptic Curve Digital Signature Algorithm (ECDSA) [RG16], however different blockchains may use different algorithms [iot19], and there have been discussions about changing the algorithm used by the Bitcoin network [Sni19]. If, whenever a new line is added to the ledger, it is also signed by the person paying, we can be happy that it's genuine, and if we do have doubts, we can verify it ourselves and reject it if it does have an invalid signature.

The issue of trust in the system has now been addressed. Next we look at how the ledger can be decentralised. A decentralised system is one where every individual will keep their own record of the ledger and broadcast an update to everyone in the system when they receive updates. Blockchain provides a framework whereby mutual consensus as to who's ledger record is the correct one can be reached. In a scenario where a peer in the network receives updates from two different broadcasters, the definitive version of the ledger is taken to be the one where some quantity intrinsic to the ledger has been maximised [Zag18]. Blockchain networks generally use one of two different intrinsic quantities: Proof of work (PoW) and Proof of Stake (PoS) [Zag18]. PoS is generally considered as an alternative to the default PoW and will be covered in more detail later in this report.

To understand how a blockchain using PoW works, basic knowledge of cryptographic hash functions is necessary. A cryptographic hash function is a function f mapping messages of arbitrary size to a fixed length output, called the "hash" or "digest" [SAK11].

$$f(M) = H$$

Where M is the message and H the resultant hash. A good cryptographic hash function is one which is easy to compute, and where it is infeasible to, given an arbitrary hash H', find a message M' such that $f(M') = H'$. It should also be infeasible to find two different messages M_1 and M_2 such that $f(M_1) = f(M_2)$ [SAK11].

When new transactions need to be added to the ledger, certain peers in the network volunteer their computational power to verify transactions. These "verifiers" (or "miners") will gather a certain number of transactions, (for Bitcoin, 1MB worth [Nak10]) and group them into a "block". After a verifier has verified the block contains a valid set of transactions, some process is used to determine whether their block will be added to the ledger. In the case of a PoW network, this is determined by whether the verifier can also solve a computationally intensive problem: finding a bitstring to add to the bottom of the block such that the resultant hash of the block is less than a certain value (i.e. has a sufficient number of initial zeros). If a verifier can do this, they have permission to add their block to the ledger [Nie13][eth21]. On the Bitcoin network, verifiers will earn some number of bitcoins if they are the first to verify the transactions and solve the problem (or "mine the block") to compensate them for volunteering their computational power, other blockchains offer similar incentives [Ant14]. Once a block has been verified, the verifier can broadcast the new block to the rest of the network and it becomes part of the public ledger. On a PoW network, since the only way that block could have been verified was by using a large amount of computing power, the appended bitstring acts as a *proof of* the *work* done by the verifier, hence the name of the protocol. To provide a well-defined ordering for transactions, the hash of the previously verified block is included in the header of the block currently being verified, thus immutably placing it after the previous block. This linking of blocks is where the name "blockchain" arises.

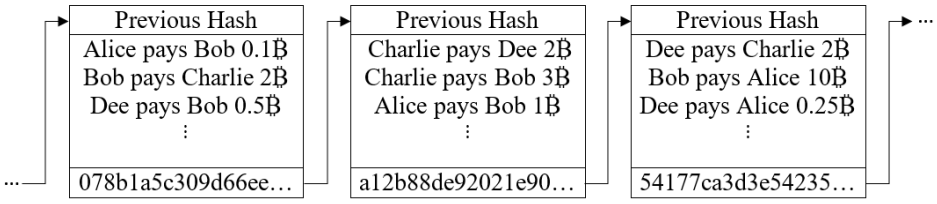

Figure 1: *The blockchain consists of blocks "chained" together by referencing the previous block in their header.*

We conclude this section with an example to understand how this system provides a reliable system for reaching mutual consensus, we imagine a scenario where a malicious individual (or group of individuals) Bob, wishes to send a fraudulent block to an individual (or group of individuals) Alice such that her understanding of the state of the blockchain differs from the rest of the network. Firstly, Bob verifies a fraudulent block and sends it to Alice. Alice adds the block to her blockchain and waits for more broadcasts, likely the next block she receives will be the true successor block that the fraudulent one tried to usurp, and that the rest of the network sees as the true successor block. After receiving this she keeps tabs on both branches of her blockchain. Unless Bob has control of a majority of the computational resources in the network (a scenario called a "51% Attack" discussed later in this report), the chances of the following blocks Alice receives also being fraudulent ones sent by Bob decreases as more blocks are verified, hence the branch of Alice's blockchain containing the most proof of work, and hence the one she will consider legitimate, will quickly become the one not including Bob's fraudulent block. Since it is in the best interests of the network members not to receive fraudulent blocks, they are motivated to listen for as many verified block broadcasts as possible and all reach the same conclusion about the chain with the longest number of blocks (or most total work invested) being the correct one.

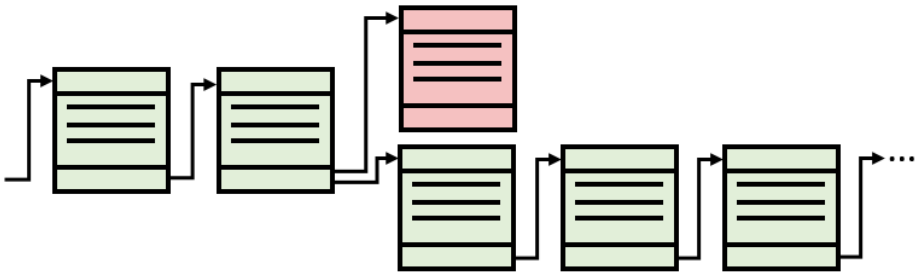

Figure 2: *Bob's malicious block might be added to Alice's version of the blockchain, but unless Bob can keep verifying blocks faster than anyone else, it will quickly be ignored once several more genuine blocks have been verified.*

We have now constructed a blockchain network, and have now seen how a blockchain system naturally answers the question of how to build a decentralised, immutable, peer-to-peer ledger where all of an individual's transactions have to be verified before being accepted, preventing so called double-spending exploits, where a user spends the same token twice. Now that a basic understanding of blockchain has been established, we use the next section to explore a specific aspect of blockchain technology in more depth.

Proof of Work versus Proof of Stake

While giving an overview of blockchain in the previous section, PoW was used as an example of how mutual decentralised consensus can be reached regarding the state of the blockchain, however there are alternatives; Proof of Stake (PoS) is one such option. In this section we discuss why an alternative to PoW is worth considering, what PoS is, and some security ramifications for networks which opt to use it.

Why consider alternatives to Proof of Work?

As blockchain technology has spread and become more widely adopted, the infrastructure required to keep it working has likewise expanded. A 2019 analysis of the carbon footprint of Bitcoin mining estimated a yearly footprint of between 22.0 and 22.9 million tons of CO2 per year [CS19]. The power consumption and footprint of the network also constantly increases, with recent estimates for the carbon footprint of bitcoin mining solely in China suggesting that in 2024 the nation could host miners generating around 130 million tons of CO2 annually [ea21b], which is *over a third* of the UK's *total* current annual CO2 emissions [gov21]. These colossal footprints are intrinsically tied to the nature of how blocks in the Bitcoin network are verified: Due to Bitcoin's current PoW protocol, at any given time, countless miners are racing to be the first to find the correct hash needed to verify a new block and receive their bitcoin reward, but once a block has been verified, there is no prize for second place, the computational energy of the vast majority of miners too slow to crack the hash first is effectively wasted. In a world being forced to more and more grapple with the adverse effects of climate change due to unsustainable global carbon emissions [ipc21], there is an obligation to consider more energy efficient alternatives to PoW.

What is Proof of Stake?

PoS is an alternative protocol for determining consensus across a blockchain network. In a PoW system, a verifier's chance of verifying a new block is proportional to the fraction of the system's computational power they control, in contrast, in a PoS system, a verifier's chance of verifying a new block is based on their stake in the network. Generally an individual's stake in the system simply refers to the volume of coins or network tokens the user owns, however the precise quantification of a user's stake can vary from implementation to implementation. PoS systems are exceedingly more energy efficient than PoW systems, with their energy usage per transaction being able to compete with the current non-blockchain industry standard, the VisaNet electronic payment network. [ea21a].

Security ramifications of Proof of Stake

This section explores some security vulnerabilities which can theoretically arise in PoS systems.

Firstly the so called *nothing-at-stake* problem: In a PoS system when a fork appears (two valid successor blocks are broadcast at similar times), since it costs nothing to verify blocks from both forks at the same time, there are twice as many chances to collect the block verifying reward for verifiers who verify on both forks rather than just one [YX20]. This incentive does not exist in PoW systems since splitting computational power between two forks will not increase the chance of verifying a block [Mar18]. In a scenario where all verifiers are fully committed to two (or more) branches, consensus may break down, and furthermore, an attacker who wishes to tip the balance in favour of a consensus to a certain branch may exert disproportionately large sway over which branch is considered legitimate, since adding a small stake to only one branch may be enough to increase the total stake invested in that fork by enough to have it be considered the legitimate main branch of the network, which can open the door to double spending exploits [Mar18].

PoS systems are theoretically susceptible to another group of attacks based on a principal called *Costless Simulation*, whereby attackers can build alternate histories of the blockchain by exploiting the fact that it does not cost any resources to simulate the verifying of many blocks successively. This fact has led to the outlining of several theoretical attacks which could be mounted against PoS networks [YX20].

These security vulnerabilities are generally considered theoretical and are relatively straightforward to safeguard against since they make very weak assumptions about the security protocols a network

might have in place [Mar18]. Although caution is a good policy, it should be noted there are no high profile cases of them being carried out. It is more important to consider how to mitigate the risk of feasible, known attacks. In the next section examples of some of the most important such risks and attacks are discussed, this will include brief discussion of how PoS can actually mitigate risks of a certain type of attack too.

Review of known feasible blockchain attacks and failures

Blockchain technology is often heralded as a technology poised to radically transform the security and trustworthiness of digital systems, and it certainly has the potential to do so. It is worth however also considering the potential risks and concerns associated with new emergent technologies, especially ones as potentially revolutionary as blockchain. We therefore consider some such blockchain issues here.

51% Attacks

Likely the most notorious and well known blockchain vulnerability, a 51% is an attack whereby an attacker controls, in the case of a PoW system, more than half of all the computational power in the system [Nah21]. As discussed earlier, a malicious agent attempting to add fraudulent blocks to the blockchain can only do so if they can keep verifying a majority of the network's new blocks. With a majority of the network's computational power, this becomes possible.

Although a 51% attack poses an unlikely threat to large established networks like Bitcoin due to the sheer magnitude of resources required to mount an attack, smaller cryptocurrencies, where the resources required to control a majority of computational power are more attainable, are more susceptible to the attack [SS19]. Krypton and Shift, two cryptocurrencies based on Etherium suffered 51% attacks in 2016 [Leu16] and it has been proposed that the rise of "mining marketplaces", where users can rent hashing hardware without buying it has lowered the bar for executing these attacks [Her18]. In 2018, five cryptocurrencies were attacked in the space of a single month [Her18].

It has been suggested that PoS systems may disincentivies 51% attacks more than PoW systems since an attacker attacking a PoS blockchain would need to have a large amount of value invested in the network, and since an attack would likely deflate the network's value, it would not be the attacker's best interest to do so [Bha18].

Smart contract exploits

An additional feature available in many blockchain networks are smart contracts. Smart contracts are relatively simple computer programs stored on the blockchain as bytecode [ibm]. Many cryptocurrencies support smart contracts, the largest smart contract ecosystem is possessed by the Ethereum blockchain network [cmc], however Bitcoin has also recently added support for smart contracts too [Sig21]. Smart contracts greatly increase the capabilities of a blockchain network, for example, Ethereum smart contracts have facilitated the recent boom in sales of digital art via NFTs (unique tokens linked to pieces of art immutably stored on the blockchain)[eth][bbc21]. However there are also security risks associated with smart contracts. Once a smart contract has been added to the blockchain, the blockchain's immutability means it cannot be changed, so if there is a vulnerability in the code stored in the smart contract, it is extremely difficult to fix, and the consequences can be disastrous. In 2016, The DAO, a decentralised venture capital fund aiming to pioneer a decentralised mode of operation was instantiated on the Ethereum blockchain. The fund, which was in control of over $100 million worth of ethereum raised through crowdfunding [Vig16a], implemented autonomous functionality through smart contracts. When a loophole in the behaviour of these contracts was found, which allowed an attacker to withdraw approximately $50 million worth of ethereum from the fund [Fin16], fixing the issue spawned a rift in the Ethereum community. While many members of the community, including Ethereum's founder, proposed a hard fork, whereby the network would be rolled back and funds returned, other members of the community maintained that such a decision went against the core principals of the blockchain, as such a fork would undermine the immutability of the network and disrepute the Ethereum project [Wil16].

A hard fork of the network was eventually greenlit and the blockchain was rolled back, with all funds invested in the DAO being returned to those who originally invested them. Despite this, the

original unmodified chain did not die off and was kept alive as Ethereum Classic by those for whom the preservation of the ideological purity of the blockchain was more important than the perceived moral duty to right the wrongdoing of the attacker [Vig16b].

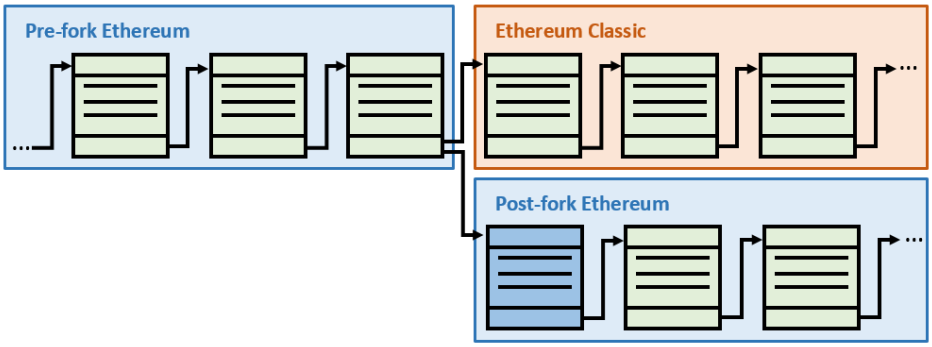

Figure 3: *The Hard Fork: The first block of the post-fork Ethereum chain was specially constructed to fix the DAO issue, however the original untampered-with chain is still recognised and maintained by the Ethereum Classic community.*

The DAO incident, which hasn't been the only one of its kind [GCD21][Bat21], raised pertinent legal, ideological, and technological questions regarding the security of blockchain technology in practice: Did reversing the attacker's transactions undermine the legal weight of smart contracts (the attacker merely exploited a loophole in the contract) which although analogous to real world legal contracts exist largely in a "jurisprudential vacuum" [All20]? How can Ethereum users have faith that the tenets of immutability and human non-intervention will be recognised in the future if they weren't in this instance? And how can smart contracts be safely constructed to guarantee similar attacks cannot take place in future? Although many a cryptocurrency and blockchain enthusiast will opine the airtight security of blockchain technologies, no technology is ever perfectly infallible and Ethereum's DAO incident proves blockchain is no exception – such attacks are only considered impossible until they happen.

Conclusion

This report has covered several different aspects of blockchain technology. Firstly an overview of what a blockchain is and how it functions was given. This was followed by a more in depth dissection of the Proof of Stake protocol for achieving blockchain consensus, an alternative to the standard but inefficient Proof of Work protocol. Finally an overview and discussion of two of the most pertinent security risks blockchain networks must face was included.

References

[All20] Kate Allass. The legal status of "smart contracts": a guide to the conclusions of the lawtech delivery panel. *Farrer & Co*, 2020. https://www.farrer.co.uk/news-and-insights/the-legal-status-of-smart-contracts-a-guide-to-the-conclusions-of-the-lawtech-delivery-panel/ [accessed 06-October-2021].

[Ant14] Andreas M. Antonopoulos. Mastering bitcoin: Unlocking digital crypto-currencies. 2014. O'Reilly Media. ISBN 978-1-4493-7404-4.

[Bat21] Tom Bateman. Comp crypto: Smart contract bug puts €134 million at risk as founder begs for tokens' return. *Reuters*, 2021. https://www.euronews.com/next/2021/10/04/comp-crypto-smart-contract-bug-puts-134-million-at-risk-as-founder-begs-for-tokens-return [accessed 06-October-2021].

[bbc21] What are nfts and why are some worth millions? *BBC*, 2021. https://www.bbc.co.uk/news/technology-56371912 [accessed 06-October-2021].

[Bha18] Dev Bharel. How proof of stake renders a 51% attack unlikely and unappealing. 2018. https://blog.qtum.org/how-proof-of-stake-renders-a-51-attack-unlikely-and-unappealing-ddebdc91a569 [accessed 06-October-2021].

[Cho17] Usman W. Chohan. The double spending problem and cryptocurrencies. 2017. https://ssrn.com/abstract=3090174 [accessed 06-October-2021].

[cmc] Top smart contracts tokens by market capitalization. *CoinMarketCap*. https://coinmarketcap.com/view/smart-contracts/ [accessed 06-October-2021].

[CS19] Ulrich Gallersdörfer Christian Stoll, Lena Klaaßen. The carbon footprint of bitcoin. *Joule*, 3(7):1647–1661, 2019. https://www.sciencedirect.com/science/article/pii/S2542435119302557 [accessed 06-October-2021].

[Dav11] Joshua Davis. The crypto-currency: Bitcoin and its mysterious inventor. *The New Yorker*, 2011. https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency [accessed 06-October-2021].

[ea21a] Moritz Platt et al. Energy footprint of blockchain consensus mechanisms beyond proof-of-work. *UCL Centre for Blockchain Technologies*, 2021. http://blockchain.cs.ucl.ac.uk/wp-content/uploads/2021/09/UCL_CBT_DPS_Q32021_updated-1.pdf [accessed 06-October-2021].

[ea21b] Shangrong Jiang et al. Policy assessments for the carbon emission flows and sustainability of bitcoin blockchain operation in china. *Nature Communications*, 12(1938), 2021. https://www.nature.com/articles/s41467-021-22256-3 [accessed 06-October-2021].

[eth] Non-fungible tokens (nft). *Ethereum.org*. https://ethereum.org/en/nft/ [accessed 06-October-2021].

[eth21] Proof-of-work. *Ethereum.org*, 2021. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow [accessed 06-October-2021].

[FIN13] FINCEN. Statement of jennifer shasky calvery, director financial crimes enforcement network united states department of the treasury. 2013. https://www.fincen.gov/sites/default/files/2016-08/20131118.pdf [accessed 06-October-2021].

[Fin16] Klint Finley. A $50 million hack just showed that the dao was all too human. *Wired*, 2016. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [accessed 06-October-2021].

[GCD21] Michelle Price Gertrude Chavez-Dreyfuss. Explainer: How hackers stole and returned $600 mln in tokens from poly network. *Reuters*, 2021. https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/ [accessed 06-October-2021].

[gov21] 2020 uk greenhouse gas emissions, provisional figures. *UK Department for Business, Energy & Industrial Strategy*, 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972583/2020_Provisional_emissions_statistics_report.pdf [accessed 06-October-2021].

[Her18] Alyssa Hertig. Blockchain's once-feared 51% attack is now becoming regular. *Coindesk*, 2018. https://www.coindesk.com/markets/2018/06/08/blockchains-once-feared-51-attack-is-now-becoming-regular/ [accessed 06-October-2021].

[ibm] What are smart contracts on blockchain? *IBM*. https://www.ibm.com/topics/smart-contracts [accessed 06-October-2021].

[iot19] Assuring authenticity in the tangle with signatures. *IOTA Blog*, 2019. https://blog.iota.org/assuring-authenticity-in-the-tangle-with-signatures-791897d7b998/ [accessed 06-October-2021].

[ipc21] Climate change widespread, rapid, and intensifying. *IPCC*, 2021. https://www.ipcc.ch/2021/08/09/ar6-wg1-20210809-pr/ [accessed 06-October-2021].

[Leu16] Angus Leung. Test attack on krypton, ethereum classic might be next. *Cointelegraph*, 2016. https://cointelegraph.com/news/test-attack-on-krypton-ethereum-classic-might-be-next [accessed 06-October-2021].

[Lys02] Anna Lysyanskaya. Signature schemes and applications to cryptographic protocol design. *MIT*, 2002. https://dspace.mit.edu/handle/1721.1/29271 [accessed 06-October-2021].

[Mar18] Julian Martinez. Understanding proof of stake: The nothing at stake theory. 2018. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027 [accessed 06-October-2021].

[Nah21] Pawan Nahar. What are 51% attacks in cryptocurrencies? *The India Economic Times*, 2021. https://economictimes.indiatimes.com/markets/cryptocurrency/what-are-51-attacks-in-cryptocurrencies/articleshow/85802504.cms [accessed 06-October-2021].

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. https://www.debr.io/article/21260.pdf [accessed 06-October-2021].

[Nak10] Satoshi Nakamoto. Bitcoin sourcecode via *Github*. 2009-2010. https://github.com/bitcoin/bitcoin/blob/41076aad0cbdfa4c4cf376e345114a5c29086f81/src/consensus/consensus.h#L10 [accessed 06-October-2021].

[Nie13] Michael Nielsen. How the bitcoin protocol actually works. 2013. https://michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ [accessed 06-October-2021].

[RG16] Arvind Narayanan Rosario Gennaro, Steven Goldfeder. Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security. 2016. https://link.springer.com/chapter/10.1007/978-3-319-39555-5_9 [accessed 06-October-2021].

[SAK11] Russell J. Bradford Saif Al-Kuwari, James H. Davenport. Cryptographic hash functions: Recent design trends and security notions. *University of Bath*, 2011. https://eprint.iacr.org/2011/565.pdf [accessed 06-October-2021].

[Sar18] Simanta Shekhar Sarmah. Understanding blockchain technology. 2018. https://www.researchgate.net/profile/Simanta-Sarmah/publication/336130918_Understanding_Blockchain_Technology/links/5d913eb9a6fdcc2554a69c7c/Understanding-Blockchain-Technology.pdf [accessed 06-October-2021].

[Sig21] MacKenzie Sigalos. Bitcoin just got its first makeover in four years. *CNBC*, 2021. https://www.cnbc.com/2021/06/12/bitcoin-taproot-upgrade-what-it-means.html [accessed 06-October-2021].

[Sni19] Stepan Snigirev. How schnorr signatures may improve bitcoin. 2019. https://medium.com/cryptoadvance/how-schnorr-signatures-may-improve-bitcoin-91655bcb4744 [accessed 06-October-2021].

[SS19] Hector Marco-Gisbert Sarwar Sayeed. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, 9(9):1788, 2019. https://www.mdpi.com/2076-3417/9/9/1788 [accessed 06-October-2021].

[Vig16a] Paul Vigna. Chiefless company rakes in more than $100 million. *The Wall Street Journal*, 2016.
https://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393 [accessed 06-October-2021].

[Vig16b] Paul Vigna. The great digital-currency debate: 'new' ethereum vs. ethereum 'classic'. *The Wall Street Journal*, 2016.
https://www.wsj.com/articles/BL-MBB-52061 [accessed 06-October-2021].

[Wil16] Jeffrey Wilcke. To fork or not to fork. *Ethereum Blog*, 2016.
https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/ [accessed 06-October-2021].

[YX20] W. Lou Y. T. Hou Y. Xiao, N. Zhang. A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2):1432–1465, 2020.
https://ieeexplore.ieee.org/document/8972381 [accessed 06-October-2021].

[Zag18] L. M. Bach; B. Mihaljevic; M. Zagar. Comparative analysis of blockchain consensus algorithms. *IEEE*, 2018.
https://ieeexplore.ieee.org/abstract/document/8400278 [accessed 06-October-2021].