Security of Blockchain Consensus Protocols

Austine Onwubiko, Sarwar Sayeed, Hector Marco-Gisbert
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
High St, Paisley PA1 2BE, UK
Email: {Austine.Onwubiko, Sarwar.Sayeed, Hector.Marco}@uws.ac.uk

***Abstract*—The blockchain is a decentralised technology distributing digital information through peer-to-peer, where the consensus protocol remains the most significant part ensuring the integrity of the recorded information. The consensus works as an agreement among the network nodes determining the authenticity of the network peers and also puts forward a set of rules. Nodes that do not comply with the consensus rules, fail to take part in the network activities. However, the major consensus protocols comprise severe weaknesses allowing malicious parties to conduct activities that are against the network rules. Although blockchain is based upon a sturdy structure solving many security issues, the robustness of it is still severely affected by various attack techniques. Most of the attacks were possible due to the weaknesses in the adopted consensus protocol. Many security proposals evolved to defend against the vulnerability but fully failed to minimise the attacking possibilities encouraging attackers even more to conduct such exploitation. In this research, we analyse 19 important consensus protocols that are adopted by major cryptocurrencies. We also discuss the most dreadful consensus-based attacks and major defense mechanisms. Our analysis shows that the weaknesses in the consensus protocol result in significant attacks.**

Keywords–Blockchain; Consensus; Cyber Attack.

I. Introduction

The blockchain is a supreme technology of the current era that stores transactional records in a block-like structure [1]. The block storage are databases, often referred to as Distributed Ledger Technology (DLT), chained to its adjacent blocks forming a secure chain of blocks. The whole process is done through a Peer-to-Peer (P2P) network where every node comprises a copy of the ledger. Blockchain is not concentrated on a centralised system; therefore, it requires an adversary to exploit the majority of network nodes to conduct an attack.

The blockchain-primarily relies on three of its main components that include the nodes, miners, and the blocks [2]. Every node in the network contains the same data blocks, where the miners are responsible for generating and validating new data blocks. The mining process requires every network participant to agree on a single state so that a malicious party can not influence the integrity of the network. And, the above can only be accomplished with the help of a consensus [3].

Although the decentralised aspects of blockchain are a solution to various baneful attack techniques; however, it still comprises severe weaknesses within the consensus protocol resulting in many attacks, such as 51% attack, Sybil attack, etc. [4] [5] [6]. 51% attack is considered to be one of the most fatal attack techniques as a successful attack can impact over the entire blockchain network significantly.

A majority of the cryptocoins comprise only a limited number of nodes making them vulnerable to the attacks as the likelihood of a 51% attack entirely depends on the total hashing ability of an adversary. Although it requires an extensive amount to execute a 51% attack, the attack can be executed as low as $500 on the low hashing coins. Hence, it remains a tremendous challenge for the cryptocoins with minimal nodes. In the case of bitcoin, each hash comprises a double Secure Hash Algorithm 256 (SHA-256) hash calculation. The miners use their hardware devices to calculate the hashes for solving the mathematical puzzles. The miners that comprise more powerful machines have more chance of solving the puzzle than other miners in the network.

Blockchain solves various security challenges that exist in the current centralised system. However, being one of the many ingenious technologies of the current time, blockchain is always one of the prime targets where attackers put into practice unique attacking techniques to exploit its vulnerability. Attackers apply different methods to execute successful attacks that may include exploiting the vulnerability in the P2P network, application bugs, malicious activities, or leveraging the weakness in the consensus protocol. In most recent attacks through the consensus protocols remain a serious challenge as most of the adopted security techniques remain vulnerable.

This paper is organised as follows: Section II discusses some of the most important factors of blockchain technology. In Section III we present 19 major consensus protocols that are adopted by various blockchain networks. Section IV reviews 5 major security attacks that occur due to the weaknesses in the consensus protocol. In Section V, we discuss the available protection techniques to mitigate blockchain attacks. Finally, the concluding Section VI discusses the overall research work. It also indicates the future challenges and future work.

II. Background

In this section, we discuss some of the important features of blockchain technology. The review of the literature includes significant contexts of blockchain technology.

A. *Blockchain: A Summary*

The blockchain is a trustless system where each party holds a common digital history [2]. It is an immutable ledger technology where a single modification invalidates all the blocks it is connected with [1]. Bitcoin is the first blockchain application that came into effect in 2009. Many cryptocurrencies follow a different approach to be produced, whereas the bitcoin and other major cryptocurrencies comprise a mining process that requires powerful systems to conduct the mining tasks.

ISBN: 978-1-61208-811-2

B. Asymmetric Key

Asymmetric Key is an advanced level of encryption method that uses keypairs of a public key and a private key. The public key is open and can be shared with a third party in the bitcoin network. However, it is attached to the private key and it is impossible to retrieve the private key through the public key. A private key is in place to perform authorization activities. In a normal scenario, a sender requires to encrypt a message using the public key of the recipient. Once the message is sent through a safe medium, the receiver can only obtain it by decrypting it using his private key. The private key works as a password; hence, attackers in possession of a private key can drain all the coins from users' wallets.

C. Consensus Protocol

A consensus protocol is a common agreement in the blockchain network about the present state of the distributed ledger. There is no central authority or a third party involved in the blockchain network. To verify and validate transactions in the network, the network must agree that every new block that is added to the blockchain is verified and valid. The agreement establishes a trust among unknown nodes in a distributed computing environment. This can be achieved by the consensus protocol, which is the core part of blockchain network.

D. The Significance of Network Hashing

The hash rate of a blockchain network is the method to determine the processing power of the network [7] [8]. The hash rate has significant effects on cryptocoins that are primarily based on Proof of Work (PoW) protocol. In the case of bitcoin, all the transaction data get hashed to a single hash data. The miner needs to solve a mathematical puzzle to prove to the network that his work is valid. The hash rate plays a significant role as the more hashing power a miner comprises the more attempts he can make to solve the puzzle. Hence, the chances go higher to solve the next blocks.

E. Blockchain Mining

The mining involves verifying the authenticity of the network data [9]. It is the core responsibility of the network miners to get involved with the mining process to validate the presented data. Different blockchain network comprises a different approach to perform the verification process. In Bitcoin blockchain, usually, the network miners form a pool, often referred to as the mining pool to get involved in the process. The more miners join the group, the more chance they have in solving the puzzle; thus, more reward for the miners.

III. Blockchain Consensus Protocols

In this section, we discuss the most important consensus protocols that are adopted by various cryptocoins. Figure 1 shows the functionality of PoW protocol. Three miners involve in solving a mathematical puzzle, where one of the miners has been able to solve it first. The network verifies it and processes rewards for the winner. The network also sets the difficulty level and sends another new puzzle for the network to solve.

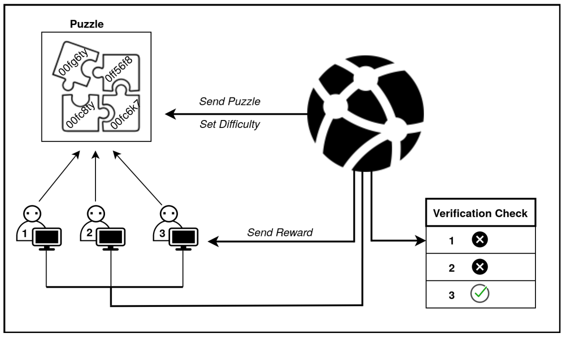

Figure 1. The functionalities of Proof of Work consensus protocol.

A. Proof of Work (PoW)

PoW was an idea to stop junk emails by Dwork and Naor in the year 1992 according to [10]. The purpose was to prevent attackers from sending junk emails, as this will require them to do some difficult work of forwarding junk emails that will not be beneficial for them. In Blockchain, a distributed consensus algorithm is applied as a method of protecting the blockchain. This form of consensus protocol is used by the cryptocurrency bitcoin and other applications in the blockchain network, without any central authority, the only way to verify the transaction in the blockchain network is by mining.

B. Proof of Stake (PoS)

PoS is another form of a consensus protocol that was implemented in 2012 [11]. This protocol was first used by the cryptocurrency PeerCoin. The PoS protocol was implemented to solve the huge computational power and expensive hardware usage in PoW [10]. In this consensus protocol, verifying transactions is done by validation. Unlike the PoW protocol, the process requires the validators to stake their economic share, in the form of cryptocurrency, in order to add the next block to the blockchain. The block is added to the blockchain by the node with the highest amount of stake, and the user is rewarded with a transaction fee.

C. Delegated Proof of Stake (DPoS)

DPoS is a convenient consensus protocol that is similar to PoS enabling miners to generate the next block according to their stake. DPoS is representative democratic in nature as the name implies, while PoS is direct democratic that brings the major difference between DPoS and PoS [12]. This protocol utilises the stakeholders to vote for their delegates or witnesses. The stakeholders vote to elect any number of witnesses to generate the next block. Once elected and a witness fails to produce a block, the witness may be voted out in future elections [11].

D. Leased Proof of Stake (LPoS)

LPoS is another version of PoS consensus protocol that uses the cryptocurrency WAVE [13]. In a PoS protocol, the users with the highest amount of stake are eligible to add the next block to the blockchain network, whereas in LPoS the users can lease their stake to a full node and earn a percentage of the payout as a reward. The reward amount is determined by the amount of stake the user is willing to stake. The higher the amount, the higher chance the full node has to add the next block in the network.

E. Proof of Burn (PoB)

PoB is proposed as an alternative of PoW and PoS, and was invented by Lain Stewart. This protocol shows that miners have done something hard, but with a reduced rate of energy consumption. PoB allows miners to invest in a mining rig or virtual mining power. The process of PoB involves burning the coins or currency and sending it to a public address that can be verified and is inaccessible [14].

F. Proof of Capacity (PoC)

PoC is a consensus protocol that is also known as Proof of Space (PoSP). It was proposed to handle the issue of expensive mining hardware and computational power of PoW, and to improve the inefficient mining in the PoW protocol [15]. Miners are expected to invest their disk space to be able to mine the next block in the network, instead of consuming more power and expensive hardware. Therefore, the more disk space a miner comprises, the higher likelihood for the miner to mine the next block.

G. Proof of Elapsed time (PoET)

PoET is based on a lottery consensus, in which nodes complete a designated waiting time to be selected. PoET operates in a protected enclave Trusted Execution Environment (TEE) [16], where nodes have to wait for a random amount of time. The node with the least wait time will be able to add the next block to the network. PoET has three main steps for adding blocks to the blockchain network. First, the nodes require to register their pair keys and waiting time. Second, the waiting time of the nodes is calculated by applying an equation. Third, other nodes need to verify the nodes generated block before it can be accepted into the network.

H. Proof of Weight (PoWeight)

PoWeight is an upgrade version of the PoS consensus protocol [17]. Poweight tries to solve the problem where the more token a user has in the network, the better chance the user has to find the next block in the PoS. PoWeight uses weight value as a selection method to assign a weight to users on the network as part of their contributions. The weight value can be any value, not just a token, that will be used to determine the weight of the user. This protocol uses cryptocurrency like filecoin [18], which considers the quantity of Interplanetary File System (IPFS) information that a user has to determine the weight factor.

I. Proof of Importance (PoI)

PoI is a type of protocol that uses the concept of accounts to validate and adds new blocks to the network [15]. PoI does not make use of expensive hardware for mining rather, it makes use of the account known as harvesters. These harvesters are responsible for validating the network and must hold at least 10,000 vested coins to be eligible to participate in the network. PoI uses cluster as a way of clustering nodes to analyse and utilise the quantities and balances of the individual nodes that determines the importance of each node [19].

J. Proof of Activity (PoAc)

PoAc is a consensus protocol that is the combination of PoW and PoS [18] [20]. The PoAc mining process first starts with the PoW, where the miners mine to produce the next block. Once the block is found, it follows the PoS process as the new block only contains the header information and address of the miner. The PoS process starts by selecting a group of validators with the highest amount of stake by random, as these validators are required to sign the new block found.

K. Proof of Ownership (PoO)

Proof of Ownership (PoO) is an approach that secures information on the blockchain ensuring proof of the ownership of that particular information [21]. It leverages the bitcoin ledger to trace the ownership of significant data. PoO can be utilised for enterprises to validate the integrity and other confidential information. It comprises enhanced security comparing to the existing centralised repository as such centralised approaches are prone to be comprised that may include tampering of data, removal of data, etc.

L. Proof of Retrievability (PoR)

PoR includes a compact proof enabling a client to rescue a file [22]. A file system is considered as a prover, whereas the client is a verifier. This method is a proof by the prover to the client that a particular file is authentic. PoR comprises the Byzantine adversarial model. The protocol enables a client to encode a file prior to being transferred for archiving. It then triggers bandwidth-efficient challenge-response protocols to ensure the availability of the file to the other end, which is a remote storage supplier.

M. Proof of eXercise (PoX)

PoX is a consensus approach associated with the cryptocurrency mining [23]. It is mainly focused on bitcoin-through solving a practical eXercise that involves a scientific computation matrix-based issue. In order to overcome the issues, PoX consists of a down-top presentation approach.

N. Proof of Luck (PoL)

PoL is a consensus protocol that is based on TEE [24]. In PoL, the nodes request for a random number from the TEE and the node with the highest luck gets elected to validate a block. The nodes that are selected to add a new block to the blockchain network depended on its luck value, which is generated by the PoL protocol. Nodes that are participating in this network require to try several numbers until they reach the lucky number, as this process requires some processing power that is similar to the current problem of PoW.

O. Proof of Trust (PoT)

PoT is designed for the hybrid blockchain architecture [25]. This protocol operates in four phases. The first phase is the leader election for the ledger management, where the protocol elects a leader for the consortium ledger management group. In the second phase, the ledger management leader nominates a service transaction validation group using a voting mechanism.

In the third phase, the transaction validation group members vote for the transactions that should fill in the next block. The fourth and last phase is ledger management voting and bookkeeping, where the validated transactions are put into a block and linked to the blockchain network.

P. Proof of Vote (PoV)

PoV is an efficient version of PoW that uses the voting mechanism for the verification of new blocks in the network [18]. Different security identities are created for participating nodes that are the main criteria of this protocol. These identities are responsible for producing new blocks and these blocks are submitted to the appropriate entities for verification and voting. There are four roles in the protocol to ensure safety, efficiency, and reliability for the consortium network model.

Q. Proof of Authority (PoAu)

PoAu is a consensus protocol that is suitable for permissioned blockchain [26]. PoAu does not require the use of miners to validate and authenticate blocks. This helps to reduce the limit of power usage due to low computational power used in validating blocks in the network. The PoAu protocol relies on a set of trusted validators for validation and authentication instead of the use of miners. The set of validators consists of a leader with the highest priority for block confirmation than the other validators.

R. Proof of Reputation (PoR)

PoR has recently been proposed by various researcher and companies, and it is an extension of the PoAu consensus protocol [27]. In PoR, validation nodes are selected based on their reputation and the reputation is established in advance with accumulated and calculated formula. The validating nodes are voted into the network as an authoritative node once it passes verification and proves its reputation, then the nodes act like the PoAu consensus protocol.

S. Tendermint

Tendermint is based on the concept of Practical Byzantine Fault Tolerance (PBFT) [27]. All the processed transactions made are broadcast to a group of validators. The validators are selected through a voting mechanism by the protocol involving the participants in the network. The validators ensure that blocks are added to the blockchain in the correct order and blocks will only be added when 2/3 signatures from the validator nodes are received. The problem of computational power in the PoW protocol is solved as this process ensures that there is less number of nodes that will be acting as validators.

IV. Attack Strategies

In this section, we discuss various attack techniques that are executed due to the flaws in the consensus protocol.

A. 51% Attack

The 51 percent attack is also known as the majority hash rate attack where the attacker is able to defy the rule of the blockchain. In this attack, an attacker with the mining power above 50 percent will be able to control more than half of the network. Such an attack allows the attacker to double-spend coins, forcing miners to accept fake transactions and adding it to the network [28]. For example, in PoW an attacker creates a corrupt version of the blockchain transactions when they control 51 percent of the network hash. The corrupt version of the transaction has to be longer than the current version in order to reverse the transaction and perform a double spend attack.

B. Selfish Mining Attack

The Selfish Mining Attack is an attack on the consensus protocol that is similar to the Long Range Attack. The purpose of this attack is for the attacker to obtain rewards from honest miners and also waste the computing power of the miner [29]. In this process, the attacker attempts to fork the blockchain network, to form a private chain from the public chain (original chain). The attacker continues to mine the newly created chain and try to maintain a longer chain than the public chain, as the new chain from the attacker holds new information and transaction from the old one.

C. Goldfinger Attack

The Goldfinger Attack is an attack with the goal of compromising a given cryptocurrency system, as this attack may not have any direct economic benefit to the attacker [30]. The reason for this type of attack can be for economic interest where the attacker exploit the short market positions and taking out other competitors of the cryptocurrency market, and also it can be for a political or ideological reason. This attack can be effective by the means of renting, bribing, and buying computational power from others that are called the hostile take over attack.

D. Balance Attack

The Balance Attack is a recent theoretical generalisation of the Delay Attack against PoW blockchain [31]. This Attack is performed by identifying a network of subgroup miners, with this subgroups maintaining a balance in mining power to achieve double spending. This aims to delay network communications between these subgroups of nodes for the attacker to issue a transaction in one subgroup and then the attacker mine as many blocks as possible in another, so that the sub-tree of another subgroup exceeds the subgroup of the transaction issued by the attacker. The attacker splits the whole blockchain network by exploiting the ghost protocol with the aim of balancing the mining power of the subgroups.

E. Long Range Attack

The Long Range Attack is an attack when an attacker goes back and fork the genesis block of the blockchain network [32]. This attack splits the blockchain from the main chain as shown in Figure 2, and is successful when the new chain created by the attacker is longer than the main chain. The attacker's chain is accepted as the main chain, as this chain is populated with a completely different transaction and history than the main chain. Long Range Attack in the PoS protocol and Selfish mining Attack in the PoW are related in a way, as the attacker aims to create the fake chain in secret.

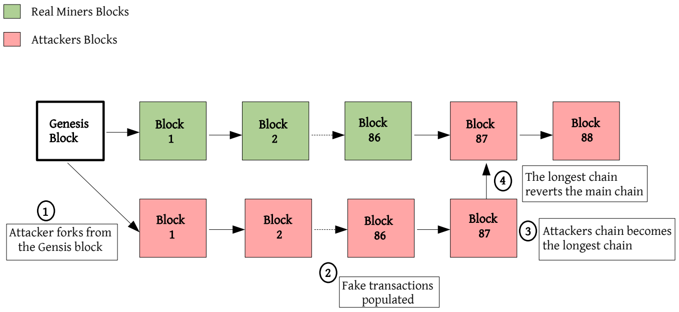
Real Miners Blocks
Attackers Blocks
Genesis Block
Block 1
Block 2
Block 86
Block 87
Block 88
4
The longest chain reverts the main chain
1
Attacker forks from the Gensis block
Block 1
Block 2
Block 86
Block 87
3
Attackers chain becomes the longest chain
2
Fake transactions populated

Figure 2. A Long Range Attack in a blockchain network.

This attack is unlikely to occur in bitcoin that uses the PoW protocol, but can be destructive to the PoS and DPoS protocols since PoS process of operation that does not define a limit on the chain; hence, the chain can be extended [33].

V. Protection Techniques

In this section, we discuss major protection techniques that are in place to mitigate blockchain attacks.

A. Historical Weighted Difficulty based Proof of Work

Historical Weighted Difficulty based Proof of work (HW D-PoW) protocol is a technique proposed by [34], with the intentions of setting a 51% defense mechanism against attack. The supposition is that in a genuine blockchain branch, new blockchain miners will undoubtedly be the same people who mined the past blocks and will be reflected in the distribution history. In a malicious blockchain branch, dispersion of miners of new blocks will probably be constrained by the assailants, which will be not the same as the ordinary conveyance of miners in history.

B. Random Mining Group Selection

Random mining group selection technique proposed by [35] that reduces computing power and defends against 51% attacks. Here, the essential thought is to distribute the miners into different gatherings. Note that not all miners are constantly engaged with the mining cycle, and just miners having a place with a specific gathering are allowed to mine future blocks. Each peer hub decides its mining bunch utilising a hash function Hg(-) and its wallet address. Moreover, when a block is made, its hash esteem is utilised with Hg(-) to figure out which mining bunch should locate the following block. Just peer hubs having a place with the mining bunch are approved to mine the following block and rival one another.

C. Indegree and Outdegree

Indegree and Outdegree is a countermeasure against an Eclipse attack as described by [36]. Indegree implies the number of direct routes coming into a hub and outdegree implies the number of direct routes leaving a hub. The plan to protect against Eclipse assault is to bound both indegree and outdegree of the assailant hubs. This strategy can be depicted as follows. To start with, a defensive mechanism is applied to the Sybil assault. This cycle guarantees there is no chance of Eclipse assault dependent on a Sybil assault. At that point, the main focus can be on the most proficient method to manage the indegree and outdegree of the aggressor hubs.

D. Self-Registration

The countermeasure is an identity registration procedure called Self-Registration [36] to defend against Sybil Attack. The registration process of a new node requires the node to calculate its identifier by hashing its IP address and port, and then register its identifier at another node that has been registered already. The new node will then request to join the P2P network. Other registered nodes on the network can identify a fake node once a new node joins the network. The new node will not be accepted by the P2P network if the node is a fake.

E. Backward-Incompatible Defense

Backward-Incompatible Defense is a countermeasure against Selfish Mining [37]. The defense is a fork punishment rule where competing blocks receive no block reward. The first miner receives half of the forfeited rewards in the blockchain for adding proof of the block forked. This process; however, creates another kind of attack, as miners suffer collateral damage due to the defense. A certain number of signatures and dummy blocks should be associated with each solved block to prove the absences of competing block, and that the block is witnessed by the network to allow miners to work on it. There is no mechanism provided to evaluate the number of proofs to know if it is sufficient to continue working.

F. Tie Breaking Defense

Tie Breaking Defense is a countermeasure against Selfish Mining attack [37]. The defense techniques can also be referred to as the `Uniform tie break`, as the name implies. A miner chooses what chain to be mined on as long as the chain is uniformly at random in a tie. The profit threshold that is the minimum mining power share to earn an unfair block rewards are raised by the defense techniques, and the profit threshold can rise to 25% within their selfish mining strategy.

G. Dynamic and Auto Responsive Approach

Gupta et al. proposed dynamic and auto responsive approach for defending against DDoS attack [38]. A wide range of flooding DDoS attacks have been highlighted with various design principles and evaluation results to accurately detect these characterised attacks for the proposed framework. The low volume-based approach is used to detect these attacks that observes unexpected changes in the network traffic in the ISP domain.

VI. Conclusion And Future Work

Blockchain, the record keeping-technology has brought vast advancements in various sectors transforming the method of conventional actions adopted in a centralised system. However, our research has revealed that there are severe weaknesses that exist in the blockchain technology and proving to be a barrier for this technology to be adopted. We have shown that consensus protocols are the most significant factors of this technology as weaknesses in the protocol results in various attacks. We have also analysed the most pernicious attack techniques that can exploit the consensus protocol. Furthermore, our analysis of the protection techniques indicates that the protection techniques are not robust enough to defense; hence, a strong protection approach required to mitigate the attacks.

The research has revealed various future research scopes to ensure a secure blockchain network. For our future work, we aim to perform a deep analysis of the limitations of the major consensus protocol to propose a robust security approach to mitigate the attacks.

References

[1] L. Mearian, “What is blockchain? The complete guide,” 2019, URL: https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html [retrieved: March, 2020].

[2] CBINSIGHTS, “What Is Blockchain Technology?” 2020, URL: https://www.cbinsights.com/research/what-is-blockchain-technology/ [retrieved: August, 2020].

[3] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A survey of distributed consensus protocols for blockchain networks,” IEEE Communications Surveys & Tutorials, vol. 22, 2020, pp. 1432–1465.

[4] S. Sayeed and H. Marco-Gisbert, “Assessing blockchain consensus and security mechanisms against the 51% attack,” Applied Sciences, vol. 9, 04 2019, p. 1788.

[5] S. Sayeed, H. Marco-Gisbert, and T. Caira, “Smart contract: Attacks and protections,” IEEE Access, vol. 8, 2020, pp. 24 416–24 427.

[6] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, “Dns-idm: A blockchain identity management system to secure personal data sharing in a network,” Applied Sciences, vol. 9, no. 15, 2019, p. 2953.

[7] D. Chowles, “51% Attacks and Double Spending in Cryptocurrencies,” 2018, URL: https://www.chowles.com/51-percent-attacks-and-double-spending-in-cryptocurrencies/ [retrieved: March, 2020].

[8] M. Beedham, “Hash rate is at an all time high, here’s what it’s all about,” 2019, URL: https://thenextweb.com/hardfork/2019/08/05/ugh-this-is-what-bitcoins-hash-rate-means-and-why-it-matters/ [retrieved: March, 2020].

[9] ITPro, “What is cryptocurrency mining?” 2020, URL: https://www.itpro.co.uk/digital-currency/30249/what-is-cryptocurrency-mining [retrieved: March, 2020].

[10] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, “Study of blockchain based decentralized consensus algorithms,” in TENCON 2019-2019 IEEE Region 10 Conference (TENCON). IEEE, 2019, pp. 908–913.

[11] L. Bach, B. Mihaljevic, and M. Zagar, “Comparative analysis of blockchain consensus algorithms,” in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018, pp. 1545–1550.

[12] H. Wang, Z. Zheng, S. Xie, H.-N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” International Journal of Web and Grid Services, vol. 14, 10 2018, pp. 352 – 375.

[13] P. Marchionni, “Distributed ledger technologies consensus mechanisms,” Available at SSRN 3389871, 2018.

[14] A. Baliga, “The blockchain landscape,” Persistent Systems, vol. 3, no. 5, 2016, pp. 1–21.

[15] Q. Deng, “Blockchain economical models, delegated proof of economic value and delegated adaptive byzantine fault tolerance and their implementation in artificial intelligence blockcloud,” Journal of Risk and Financial Management, vol. 12, no. 4, 2019, p. 177.

[16] W. Zhao, S. Yang, and X. Luo, “On consensus in public blockchains,” in Proceedings of the 2019 International Conference on Blockchain Technology, 2019, pp. 1–5.

[17] D. A. Gol, “An analysis of consensus algorithms for the blockchain technology,” International Journal for Research in Applied Science & Engineering Technology, vol. 7, 2019.

[18] K. Sharma and D. Jain, “Consensus algorithms in blockchain technology: A survey,” in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2019, pp. 1–7.

[19] N. Chalaemwongwan and W. Kurutach, “Notice of violation of ieee publication principles: State of the art and challenges facing consensus protocols on blockchain,” in 2018 International Conference on Information Networking (ICOIN), Jan 2018, pp. 957–962.

[20] G. Bashar, G. Hill, S. Singha, P. Marella, G. G. Dagher, and J. Xiao, “Contextualizing consensus protocols in blockchain: A short survey,” in 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2019, pp. 190–195.

[21] Unblock, “What does PoO/Proof of Ownership mean?” 2020, URL: https://unblock.net/glossary/poo-proof-of-ownership/ [retrieved: September, 2020].

[22] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: Theory and implementation,” in Proceedings of the 2009 ACM Workshop on Cloud Computing Security, ser. CCSW ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 4354. [Online]. Available: https://doi.org/10.1145/1655008.1655015

[23] A. Shoker, “Sustainable blockchain through proof of exercise,” in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 2017, pp. 1–9.

[24] Q. He, N. Guan, M. Lv, and W. Yi, “On the consensus mechanisms of blockchain/dlt for internet of things,” in 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), 2018, pp. 1–10.

[25] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, “A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services,” IEEE Transactions on Services Computing, vol. 12, no. 3, 2019, pp. 429–445.

[26] M. Cash and M. Bassiouni, “Two-tier permission-ed and permission-less blockchain for secure data sharing,” in 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018, pp. 138–144.

[27] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, “Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review,” IEEE Access, vol. 7, 2019, pp. 43 622–43 636.

[28] S. Sayeed and H. Marco-Gisbert, “Proof of adjourn (poaj): A novel approach to mitigate blockchain attacks,” Applied Sciences, vol. 10, no. 18, 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/18/6607

[29] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, 2017.

[30] A. Meneghetti, M. Sala, and D. Taufer, “A survey on pow-based consensus,” Annals of Emerging Technologies in Computing, vol. 4, 01 2020, pp. 8–18.

[31] P. Ekparinya, V. Gramoli, and G. Jourjon, “Impact of man-in-the-middle attacks on ethereum,” in 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS). IEEE, 2018, pp. 11–20.

[32] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, “A survey on long-range attacks for proof of stake protocols,” IEEE Access, vol. 7, 2019, pp. 28 712–28 725.

[33] H. M.-G. Sarwar Sayeed, “On the effectiveness of blockchain against cryptocurrency attacks,” The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2018, pp. 9–14.

[34] X. Yang, Y. Chen, and X. Chen, “Effective scheme against 51% attack on proof-of-work blockchain with history weighted information,” in 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 261–265.

[35] J. Bae and H. Lim, “Random mining group selection to prevent 51% attacks on bitcoin,” in 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE, 2018, pp. 81–82.

[36] Y. Yang and L. Yang, “A survey of peer-to-peer attacks and counter attacks,” in Proceedings of the International Conference on Security and Management (SAM), 2012, p. 1.

[37] R. Zhang and B. Preneel, “Publish or perish: A backward-compatible defense against selfish mining in bitcoin,” in Cryptographers Track at the RSA Conference. Springer, 2017, pp. 277–292.

[38] S. Bhatia, S. Behal, and I. Ahmed, “Distributed denial of service attacks and defense mechanisms: current landscape and future directions,” in Versatile Cybersecurity. Springer, 2018, pp. 55–97.