On the effectiveness of blockchain against cryptocurrency attacks

Sayeed, Sarwar; Marco Gisbert, Hector

Published in:
The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies

Published: 18/11/2018

Document Version
Publisher's PDF, also known as Version of record

On the Effectiveness of Blockchain Against Cryptocurrency Attacks

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: {Sarwar.Sayeed,Hector.Marco}@uws.ac.uk

***Abstract*—Cryptocurrencies are being widely adopted to perform various online-based transactions; therefore, they are required to maintain a consensus to ensure a secured transaction. Blockchain comprises a distributed ledger, which holds digital records of individual crypto-transactions. Besides recording a particular activity, blockchain also ensures that the contents of the ledger are decided based on agreements of distinct participants. Various consensus mechanisms are followed by blockchain to ensure blocks are being summed up representing legitimate data on the network. However, the major consensus protocols comprise various limitations; and these are prone to different types of cyber attacks, such as Distributed denial-of-service, 51% attack, Double-spending, Long-range attack. In this paper, we analyze several attack vectors that can cause serious security threats due to the loopholes in the consensus mechanism. Our study involves examining 3 significant consensus mechanisms, which are followed by major cryptocurrencies. We also discuss the limitations of individual consensus mechanisms and demonstrate their robustness towards various attack vectors. We conclude that, although blockchain comprises proper consensus mechanisms to enhance secured crypto-transaction, unfortunately, it is not strong enough to defend against some cryptocurrency attacks which could discourage some users to adopt this technology.**

Keywords–Blockchain; Consensus; Cyber Attack.

I. INTRODUCTION

The blockchain is a medium of distributing digital information to users who are connected to the block. It uses a distributed system for verification and holds a record of every transaction that ever took place. Blockchain was first initiated in 2008 by a pseudonymous named Satoshi Nakamoto; however, it still remains a mystery about the founder of this technology. In the blockchain network, each block contains records of transactions and connected using cryptography. It is a secure and trustworthy platform, which can be used to produce applications, such as voting systems, games, online shops [1].

A cryptocurrency is a revolutionary growing technology that makes it possible for digital transactions to occur in just a few minutes. The transaction takes place in, an unidentified blockchain network; regardless of the network failure the transaction will still flow accordingly. In a blockchain network, every miner can keep their data and ensure that the chain is not corrupted. If an adversary tries to corrupt the block, then the whole system verifies every data for authenticity, and any corrupted finding gets restricted from the block.

Bitcoin is the first digital currency, which evolved in 2009 on blockchain platform. Data with several blocks in the chain cannot be altered without having every block changed; hence, making the whole process very secure and reliable. Beside Bitcoin, various other digital currencies, such as Ether, Litecoin, are currently being dominated in the crypto platform. Each cryptocurrency follows a consensus mechanism to make the transfer process secure and free from the attacks. However, recent attacks have questioned the reliability of the digital transactions and showed there is a loophole to bypass the security. Bitfinex and Dao incident are some of the recent incidents, which resulted in stealing millions of cryptocurrencies [2] [3]. Hence, it is essential to have a secure consensus mechanism in place.

Our major contributions in this paper are:

- We discuss ten cryptocurrency attacks, which not only can corrupt the cryptocurrencies but also can exploit the consensus mechanism.
- We assess three widely used blockchain consensus protocols, including their limitations.
- We evaluate the effectiveness of individual consensus mechanism by classifying towards discrete exploitation type.

This paper is organized as follows: Section II is the background section, which discusses the major cryptocurrencies. Section III presents the attack vectors that can be catastrophic to the blockchain network. In addition to that, phishing and scams are also discussed. Section IV summarizes the security enhancements in brief. Section V includes the discussion of 3 consensus mechanisms and limitations associated with each of the mechanisms. In Section VI, the consensus mechanisms are analyzed, in the context of attack vectors, and represented in a table. To conclude the paper, we discuss the findings from our analysis and future work to be undertaken.

II. BACKGROUND

In this section, we discuss five significant cryptocurrencies. Table I presents some cryptocurrencies that are classified according to the consensus mechanism. Figure 1 shows the recent market capitalization of 10 cryptocurrencies [4] that are dominating at the moment.

A cryptocurrency is a form of digital cash, which uses cryptography to process a secure and reliable transactions over a peer-to-peer (P2P) network. The transaction process is based on consensus, which means disagreement from any of the peers on the network will cause an interruption in the act. About 1662 cryptocurrencies exist at the moment and Bitcoin is the most widely used cryptocurrencies among all. The cryptocurrencies have limited supply as cash currencies do and they can be controlled by an algorithm process.

 ISBN: 978-1-61208-676-7

TABLE I. CRYPTOCURRENCIES BASED ON CONSENSUS MECHANISM

Consensus Mechanism	Cryptocurrencies
Proof of work	Bitcoin, Ether, Nimiq, Litecoin, Monero
Proof of stake	Linda, Neo, Pivx, Okcash, Stratis
Delegated proof of stake	Lisk, Ark, Rise, Oxycoin, BitShares

A. Bitcoin

Bitcoin was first proposed in 2008 and came into effect since 2009 [5]. It is an electronic based payment system where the authenticity is based on mathematical proof. The main concept of this cryptocurrency is to perform digital transactions and exchanges over a secured medium without having any central supremacy. Bitcoin is operated in a decentralized system, which can be considered as an alternative version of a bank. Once a transaction occurs, the sender is required to wait for the confirmations from the miners. The transactions get into the pool for authorizations. Mining computers then gather the unresolved transactions from the pool and switch them to a mathematical equation. Miners verify the transactions by solving the equation, and a new Bitcoin block gets added to the blockchain.

B. Ether

Ether is another popular cryptocurrency, which was launched in 2015. Ether, a crypto-fuel, is an important attribute to keep the Ethereum platform running [6]. Ether is used as an incentive for the application developers who develops efficient decentralized applications, a unique way of keeping the network active. Whenever a node validates a block on the Ethereum blockchain, 5 Ether is generated and rewarded as an incentive to the node. It normally takes 15-17 seconds for a new block to be publicized. Users wishing to utilize a decentralized application on the platform are required to pay in Ether as a service fee.

C. Ripple

Ripple came into effect in 2012. Ripple is a Real Time Gross Settlement system, which functions as a cryptocurrency and digital payment network [7]. Ripple relies on a common network, which is operated by a network autonomously validating server that can compare the transactions. The Ripple platform is decentralized and does not comprise proof of work (PoW) or proof of stake (PoS); instead, it relies on a shared public database. Since Ripple structure does not depend on mining; therefore, the cost of computing power and network latency is very low. A consensus protocol performs the validation of balances and transactions. The consensus process involves distinct nodes that determine the first transaction by going through a poll. The approval time from the poll is very fast and roughly takes 5 seconds.

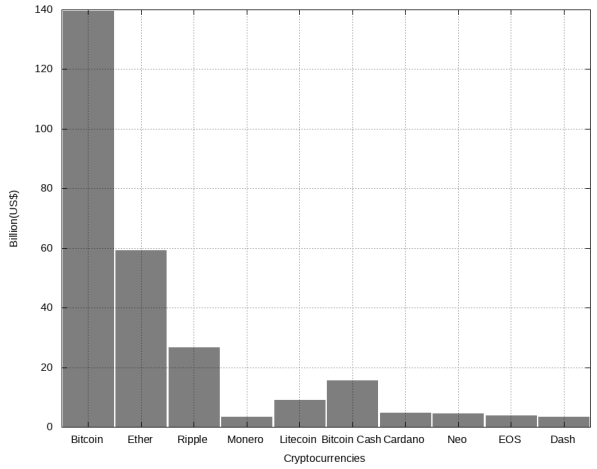

Figure 1. Market capitalization of cryptocurrencies (in billion) as of March 2018

D. Monero

Monero is a cryptocurrency, which was launched in 2014. It is privately based untraceable currency that focuses on decentralization [8]. The privacy is ensured by a special method called “ring signatures”. The method works by having a group of signatures, which involves a minimum of one genuine participant. Monero is dynamically scalable and comprises isolated features comparing to Bitcoin or Ether. For instance, Monero includes cryptography that protects all the potential transaction information, such as sender, receiver, transaction amount, from the outside world and giving the sender the ability to decide who will be allowed to view a particular transaction.

E. Litecoin

Litecoin is another cryptocurrency, which was developed by Charlie Lee and came into effect since 2011 [9]. Litecoin is one of the oldest cryptocurrencies that came into effect after Bitcoin. It is able to manage a large volume of transactions than other cryptocurrencies, such as Bitcoin. Litecoin generates the blocks more frequently; hence, it supports more transactions at a faster pace. The transaction fees are relatively low and determined based on the size of the block. It comprises much shorter blocks comparing to Bitcoin; therefore, the fee is low.

III. SECURITY THREATS

In this section, we discuss some of the important attacking techniques that can be dangerous in corrupting the cryptocurrencies as well as exploiting the blockchain.

A. 51% Attack

The 51% attack can be very critical in the blockchain network if exploited successfully [10]. The vulnerability starts by creating a corrupt version of the blockchain, which is isolated from the real version. Since blockchain policy complies with the longest chain to demonstrate the accuracy of the transaction, if the adversary manages to drive the longest chain, the corrupt version of blockchain will be predicted as a genuine chain. Therefore, the transactions that are not listed in the corrupted chain will be reversed. In the context of Bitcoin, once a transaction is approved by the sender it gets into the pool. It is then picked by individual miners to develop a block of transactions. The miner who gets first to solve the problem produces it to other miners to check the authenticity. In a 51% attack, a group of adversaries tries to solve the problem and then generate child of the blockchain so that they can avoid

 ISBN: 978-1-61208-676-7

showing the solution to other miners in the network. However, a large number of miners exist on the blockchain network, and it is nearly impossible to beat the hashing power of the network.

B. Sybil Attack

The Sybil attack comprises similar characteristics as 51% attack. This attacking method was first brought into attention by John Douceur, a researcher based on Microsoft [11]. In a Sybil attack, the adversary develops a vast amount of nodes in a sole network to cause disruptions over the network. This attack also involves corrupting a network to perform an unprivileged transaction or altering valid transactions. The network is unable to discover if multiple nodes are being controlled by a single attacker. In this attacking technique, the attacker may use several devices, virtual machines or Internet Protocol (IP) addresses. Normally in a centralized system, the monitoring process involves verifying if several requests are being made from the same device, but the blockchain does not possess such features. In blockchain technology, adversaries are restricted to the number of blocks they can produce. However, this attacking technique is very rare as the digital currency infrastructure was developed considering the restriction of the Sybil attack.

C. Distributed Denial-of-Service

Distributed denial-of-service (DDoS) is a type of cyber attack that exists from the past two decades to perform exploitation over various networks. DDoS is one of the most common attack vectors in the blockchain network, and the main objective of the adversary is to flood the network with a very high amount of traffic [12]. This attack is performed in the blockchain network so that authentic transactions could be stopped from being processed and invalid transactions could be accomplished. However, a DDoS attack over the blockchain network does not involve stealing the digital currency rather it just mitigates the network activity.

D. Mining Malware

In this attacking technique, the adversary takes advantage of cryptojacking malware to perform exploitation. It involves infecting miners system with malware to have the incentive directed to the attacker's wallet [13]. Regardless of the victim's location, mining malware can be exploited from any part of the world. Cryptojacking in mining malware comprises similar approach as ransomware. However, instead of having a good chunk of money within a short period, it focuses on achieving the targeted amount over a period. Cryptojacking works in stealth mode; hence, it is an attracting exploitation technique over ransomware. It may not require much effort to infect a system and can spread via corrupted websites or phishing campaigns.

E. P + Epsilon Attack

The PoW system is usually vulnerable to this type of attack [14]. It is a simple statical observation and based on the uncoordinated choice model. In an uncoordinated choice model, all the users are not inspired to engage with each other. Hence, they construct a group, which suddenly turns into big enough to dominate. Essentially when the network performs normal, the miners can never construct the miner group large enough to manipulate the network. It correctly assumes that the average miners will look after their interest.

F. Long-Range Attack

A long-range attack can occur due to the weak subjectivity model [15]. In the PoS chain, only a limited number of users participate at the beginning, and as the user increases, they form the chain as a pool of miners. Hence, users who staked at the chain, grow more prominent. Those limited number of users, from the beginning, can join together to maintain the previous chain back in action. In the following stages, they will be the one to dominate in mining blocks. PoS does not set a limit on the growth of the chain; hence, the chain can grow very long.

G. Eclipse Attack

In this attacking technique, an adversary manipulates the P2P network to control over the information that a node comprises. The exploitation may start when a peer communicates with other peers using gossip protocol [16]. An adversary can separate the target from the network chain so that the target could be diverted to misuse the computation power on invalid segment of the blockchain. In an eclipse attack, the adversary resides in between the nodes and the rest of the network by regulating the capacity of the node. It gives an attacker to perform a 51% attack with lot less mining power [17]. The attacker aims to manipulate the nodes to the attackers IP so that connections are made to their chosen destination. The attacking process goes through three phases. However, conducting this attack can be very expensive since the attacker is required to control the whole network system.

H. Border Gateway Protocol Hijacking

Border Gateway Protocol (BGP) hijacking is also known as routing attack. In this attacking technique, the Internet Service Provider makes false announcements over the routing system so that traffic could be diverted [18]. An investigation shows that the BGP attacks are increasing time to time over the Bitcoin network and a minimum of 100 BGP attacks are occurring on a monthly basis. The investigation also demonstrates that 447 nodes were hijacked in 2015. This attack vector can be performed to benefit from 2 attacking stages. Firstly, divide the network and secondly, obstruct the blocks by 20 minutes. Though the blockchain system is a decentralized network; however, when considering it from the routing perspective then it can be regarded as centralized as about 100 IP prefixes are managing about 20% of the Bitcoin hosts. Hence, this attacking technique can be proven fatal due to its centralization.

I. The Balance Attack

The Balance attack aims to focus on the nodes, which comprise balanced mining power. It mainly enforces double-spending on PoW consensus mechanism [19]. In this attacking technique, the adversary puts a delay between the legit subgroups of nodes. The next step involves the adversary mining as many blocks as possible in another subgroup confirming that other sub-tree puts importance on the transaction subgroups.

 ISBN: 978-1-61208-676-7

The adversary aims to exploit the ghost protocol by separating the blockchain branch from the other nodes in the network. At a later time, the separated branch will be furnished to other nodes to put an impact on the branch selection process.

J. Phishing and Scams

The number of scams occurs in the crypto-space is just remarkable, but not in a good sense. The main idea of the phishing and scams is to trick users to steal money from their wallet [20]. Phishing can spread from device to device, and technology-oriented people can easily fall for it without even noticing the influence. Scams can occur in many ways, for instance, an important email from the wallet asking to sync the account with a network which has just been hard-forked. Scams can also occur through social media by asking potential information from the user making it look like a legit request. Slack and forums attack can also occur by providing a corrupted link and asking the miners to log in through that link. Phishy wallets, fake ads are also some of the scam techniques being used to steal cryptocurrencies.

IV. Security Techniques

In this section, we summarize some of the security enhancements, which can be implemented to ensure a secured blockchain network.

A. SmartPool

SmartPool is a decentralized mining pool, which is based on Ethereum smart contracts [21]. SmartPool comprises various innovative data structures and design options, which have resulted in to be secure, efficient and reliable. SmartPool enhances probabilistic verification that helps to decrease the number of messages and cut down the expense for the miners. SmartPool provides a solution by ensuring a decentralized pool, mitigating transaction censorship threat, guaranteeing low variance.

B. Oyente

Oyente is a symbolic execution tool, which is used to find security bugs in smart contracts [22]. Oyente examines Ethereum smart contracts to figure out security loophole, which can cause potential threats. Oyente does not only detect unsafe bugs but also investigates every practical execution path. An experiment carried out by Oyente on 19,366 smart contracts, and it resulted in 8,833 of them are vulnerable.

C. Hawk

Hawk is a framework to develop privacy-preserving smart contracts [23]. Hawk does not require cryptography implementation, so it gives an opportunity to the non-programmers to write Hawk program. A Hawk compiler is in place to compile the Hawk program. One-chain privacy and contractual security are two security approaches guaranteed by Hawk to enhance security.

V. Blockchain Distributed Consensus Mechanisms

In this section, we analyze three blockchain consensus mechanisms, which are being utilized by the major cryptocurrencies such as Bitcoin, Litecoin, Ether and so on. We also put our focus on the limitations of each mechanism. Table II summarizes some of the main features of each consensus. The key point of the consensus mechanism is to ensure that the entire network agrees upon the contents of the ledger by following a set of rules. It also influences the security and economic guidelines of the blockchain network.

A. Proof of Work

Proof of work (PoW) is a consensus mechanism, which is based on solving a mathematical equation. PoW was first introduced by Bitcoin and currently implemented in many other cryptocurrencies [24]. The action involves mining where each node on the network is referred to as a miner. The process of rewarding miners ensures that it is running while establishing blocks. Miners are the foundation of PoW; hence, they are responsible for authorizing new transactions and recording them to the ledger. It usually takes 10 minutes to mine a Bitcoin block by solving strong mathematical equation based on a cryptographic hash algorithm. A successfully solved equation results in PoW; therefore, the transaction is considered as valid. Miners receive rewards for solving mathematical equation and transaction fees.

One of the major drawbacks of PoW is the cost of energy. The amount of energy the Bitcoin mining consumes per year is more than 159 countries individually. Research shows that Bitcoin to consume all the electricity of the world by February 2020 [25]. PoW for Bitcoin mining requires extensive hardware to make the mining process smooth and fast, which results in huge expenditures. Moreover, the effort in generating the blocks are useless as it can not be applied anywhere but takes a lot of time and energy to form the blocks.

B. Proof of Stake

Proof of stake (PoS) is another consensus mechanism, which has gained popularity in recent time. Peercoin was the first cryptocurrency to use this mechanism in 2012. In this consensus mechanism, a randomized system is applied to determine the creator of the following block [26]. The process involves giving information about the amount of cryptocurrency and the duration that cryptocurrency has been held for by a particular user. It does not need to meet any rigid hardware requirements and also abandons the high computation requirement. The possibility of obtaining the reward by developing a block entirely depends on the number of tokens possessed by potential users in the network. In PoS, each node is connected to an address and participants with a large number of coins likely to achieve the address, as well as involve in mining the

TABLE II. Main features of consensus mechanisms

Consensus	Energy Cost	Decentralization	Processing Speed
PoW	High	High	Low
PoS	Low	High	High
DPoS	Low	Low	High

 ISBN: 978-1-61208-676-7

next blocks. The advantage of PoS is that comparing to PoW; it is not energy intensive.

PoS suffers from weak subjectivity, and the implementation process is very complex and challenging. Another limitation of PoS system is that a large number of stakeholders have control over the network based on technical and economical aspects; therefore, making it a monopolized system.

C. Delegated Proof of Stake

Delegated proof of stake (DPoS) is another consensus mechanism that allows the shareholders to vote for witnesses [27]. One vote per share policy is performed giving the stakeholders the opportunity to have more votes if they own most coins. The witnesses get paid for building individual blocks, and failure to do so may result in being unpaid and voted out. They must obtain the largest number of votes from random stakeholders to perform the instructed task. The stakeholders also vote for the delegates to reform and make changes in the network which can be reviewed for an utmost decision. However, the rewards depend on the accomplishment of the DPoS mechanism. The voting power is endorsed by analyzing the number of tokens an account is holding. In a particular DPoS version, to prove dedication, the delegates may require to deposit funds in the time-locked security account and any corrupted behavior will result in money being seized. The version is called as deposit-based proof of stake [28].

Though DPoS enhances efficiency in the transactions; however, it comprises various limitations. The significant limitation of DPoS is that adequate decentralization cannot be obtained. An excessive amount of validators slow down the network. Moreover, delegates get penalized for not abiding with particular rules.

VI. Analysis

In this section, we evaluate the effectiveness of individual consensus mechanism. Our analysis does not involve discussing only the effectiveness rather it also classifies each mechanism towards distinct exploitation type and presents in a table. We assess three primary consensus mechanisms, and Table III shows that consensus mechanisms are vulnerable to various attack vectors.

The act of PoW method is too slow. Expensive hardware requirement and energy cost make it very costly. Some mining firms are dominating with enough mining power; hence, attacks to the mining firms can cause disruptions and also put massive impact over the cryptocurrency. PoW is vulnerable to the 51% attack, and a P + epsilon attack can also be carried out at no cost by having the required budget. Hence, the crypto-security level of the PoW based system towards P + epsilon attack can be considered as zero [29]. Our analysis indicates that the Sybil attack can exploit PoW as an adversary can interrupt the flow of the network by developing several malicious nodes. PoW is also vulnerable to the Balance attack. The Ethereum protocol and private blockchain are mainly vulnerable to this attacking technique. However, the adversary with much hashing power more likely to corrupt the Bitcoin blockchain network. In addition to that, our analysis also shows that the DDoS attack and BGP hijacking can corrupt the regular flow of this consensus mechanism.

Comparing to PoW, the significant advantage of PoS is the energy savings. However, in the context of security, it is not a fully secured mechanism. PoS is vulnerable to the 51% attack. To conduct a 51% attack, the adversary will have to achieve 51% of the cryptocurrency. Since it is quite tough to achieve 51% cryptocurrency; therefore, the threat of that attack can be very rare. However, PoS can be exploited by the long-range attack. PoS is not vulnerable to the P + epsilon attack since the adversary requires to produce a huge amount of budget to contribute as a security deposit for the participants when voting for the minority [29]. The Sybil attack can exploit PoS. A DDoS attack can also be carried out to disrupt the consensus mechanism. PoS can be an expensive option for novice attackers. It requires users to stake their own money first to validate transactions and produce blocks. Any corrupted activity in the network will confiscate the staked amount. Hence, the adversary will also lose their right to participate in future activities. This particular approach will demotivate potential attackers to carry out specific attack vectors; thus, it will enhance extra security.

Our analysis shows that comparing to PoS and PoW, DPoS comprises an entirely different consensus approach. Though the distinct approach holds advantages concerning energy cost, speed and processing time; however, in the context of security, DPoS is also not very secure. The adversary can convince the stakeholders to obtain 51% voting power and carry out a 51% attack [30]. It is also vulnerable to the other primary attack vectors, such as long-range attack, DDoS attack, P + epsilon attack, Sybil attack and the Balance attack. DPoS is not fully decentralized; therefore, it can always be the focal point of random attackers.

In the distributed network, a source entity can produce multiple entities from which some may not be reliable to perform particular tasks. Hence, a consensus algorithm is in place to ensure the reliability of the specific network. Cryptocurrencies in the blockchain network take advantage of the consensus algorithm to provide a secured transaction. Truechain is a blockchain platform, which comprises a hybrid consensus mechanism [31]. Proof of activity (PoA) is another hybrid consensus algorithm, which combines PoW with PoS [32]. Even though hybrid consensus ensures high security but PoA has been criticized due to the resources required for mining.

TABLE III. Consensus mechanisms that are vulnerable to various attacks

Consensus Mechanism	Long-Range Attack	51% Attack	DDoS	P + Epsilon Attack	Sybil Attack	The Balance Attack	BGP Hijacking
PoW	✗	✓	✓	✓	✓	✓	✓
PoS	✓	✓	✓	✗	✓	✗	✗
DPoS	✓	✓	✓	✓	✓	✓	✗

 ISBN: 978-1-61208-676-7

VII. CONCLUSION

The blockchain is a remarkable evaluation, and decentralization has made it a very reliable and secure medium for digital transactions. In this paper, we studied ten major attacking techniques. Our analysis indicated that some of the techniques could corrupt the consensus mechanism and also carry out crypto thefts. Major cryptocurrencies were discussed and presented in a table based on their consensus classification. We evaluated the effectiveness of 3 significant consensus mechanisms and pointed out that alongside various limitations, they are also vulnerable to different types of attack vectors.

Though blockchain consensus mechanism is a robust method conversely, it is visible that they are still vulnerable and can remarkably have an effect on particular cryptocurrency if successfully exploited. The vulnerability in the consensus mechanisms might discourage the miners to get involved in the mining process. Thus, we encourage the re-implementation of the mechanisms with robust security to mitigate the risks.

For our future work, we aim to analyze several other consensus mechanisms and develop a standard method, which can be used to relate various attack vectors and limitations to the consensus mechanisms. Our method will be used to determine particular exploitation class and constraints of individual consensus mechanism.

REFERENCES

[1] "What is Blockchain," 2018, URL: https://lisk.io/academy/blockchain-basics/what-is-blockchain [retrieved: July, 2018].

[2] S. FalKon, The Story of the DAOŁŁIts History and Consequences, 2017 (accessed April, 2018), https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

[3] C. Baldwin, "Bitcoin worth 72 million stolen from Bitfinex exchange in Hong Kong," 2016, URL: https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP [retrieved: July, 2018].

[4] M. Frankel, "15 largest Cryptocurrencies by Market Cap," 2018, URL: https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx [retrieved: July, 2018].

[5] "What is Bitcoin," 2018, URL: https://www.coindesk.com/information/what-is-bitcoin/ [retrieved: July, 2018].

[6] "What is Ether," URL: https://bitcoinmagazine.com/guides/what-ether/ [retrieved: July, 2018].

[7] J. Martindale, "What is Ripple," 2018, URL: https://www.digitaltrends.com/computing/what-is-ripple/ [retrieved: June, 2018].

[8] P. Bajpai, "The 6 Most Important Cryptocurrencies Other Than Bitcoin," 2018, URL: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/ [retrieved: July, 2018].

[9] J. Bushmaker, "What is Litecoin," 2018, URL: https://www.investinblockchain.com/what-is-litecoin/ [retrieved: July, 2018].

[10] J. S., "Blockchain: how a 51% attack works double spend attack," 2018, URL: https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 [retrieved: May, 2018].

[11] J. Risberg, "Yes, the Blockchain Can Be Hacked," 2018, URL: https://coincentral.com/blockchain-hacks/ [retrieved: June, 2018].

[12] S. Morgan, "Blockchain startup: 300,000 DDoS attacks will cause 150B in damages this year," 2017, URL: https://www.csoonline.com/article/3234775/security/blockchain-startup-300000-ddos-attacks-will-cause-150b-in-damages-this-year.html [retrieved: July, 2018].

[13] D. Palmer, "Cryptocurrency-mining malware: Why it is such a menace and where it's going next," 2018, URL: https://www.zdnet.com/article/cryptocurrency-mining-malware-why-it-is-such-a-menace-and-where-its-going-next/ [retrieved: June, 2018].

[14] V. Buterin, "The P + epsilon Attack," 2015, URL: https://blog.ethereum.org/2015/01/28/p-epsilon-attack/ [retrieved: June, 2018].

[15] A. Sharma, "Understanding Proof of Stake through its Flaws. Part 3 Long Range Attacks," 2018, URL: https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-part-3-long-range-attacks-672a3d413501 [retrieved: June, 2018].

[16] F. Wang, "Eclipse Attacks on Bitcoins Peer-to-Peer Network," 2015, URL: https://medium.com/mit-security-seminar/eclipse-attacks-on-bitcoin-s-peer-to-peer-network-e0da797302c2 [retrieved: May, 2018].

[17] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC'15. Berkeley, CA, USA: USENIX Association, 2015, pp. 129–144. [Online]. Available: http://dl.acm.org/citation.cfm?id=2831143.2831152

[18] P.-A. Vervier, "Why BGP Hijacking Remains a Security Scourge," 2018, URL: https://www.symantec.com/blogs/feature-stories/why-bgp-hijacking-remains-security-scourge [retrieved: July, 2018].

[19] C. Natoli and V. Gramoli, "The balance attack against proof-of-work blockchains: The R3 testbed as an example," CoRR, vol. abs/1612.09426, 2016.

[20] "Phishing in Cryptocurrency: How to Avoid Scams and Save Your Money," 2018, URL: https://medium.com/@Changelly/phishing-in-cryptocurrency-how-to-avoid-scams-and-save-your-money-d3d1b442a16a [retrieved: June, 2018].

[21] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "Smartpool: Practical decentralized pooled mining," in 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017, pp. 1409–1426. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/luu

[22] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 254–269. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978309

[23] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," Cryptology ePrint Archive, Report 2015/675, 2015, https://eprint.iacr.org/2015/675.

[24] A. Tar, "Proof-of-Work, Explained," 2018, URL: https://cointelegraph.com/explained/proof-of-work-explained [retrieved: June, 2018].

[25] "Bitcoin Mining," 2017, URL: https://powercompare.co.uk/bitcoin/ [retrieved: May, 2018].

[26] "Proof Of Stake," 2018, URL: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake [retrieved: July, 2018].

[27] B. Asolo, "Delegated Proof of Stake (DPOS) Explained," 2018, URL: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/ [retrieved: July, 2018].

[28] "Delegated Proof of Stake," 2018, URL: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake [retrieved: June, 2018].

[29] K. Wang, "Cryptoeconomics: Paving the Future of Blockchain Technology," 2017, URL: https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971 [retrieved: June, 2018].

[30] "Solving the Byzantine Generals Problem with Delegated Proof of Stake (DPoS)," 2018, URL: https://www.radixdlt.com/post/what-is-delegated-proof-of-stake-dpos [retrieved: August, 2018].

[31] "TRUE," 2018, URL: https://www.truechain.pro/ [retrieved: August, 2018].

[32] "Proof of Activity Explained: A hybrid Consensus Algorithm," 2018, URL: https://www.coinbureau.com/blockchain/proof-of-activity-explained-hybrid-consensus-algorithm/ [retrieved: August, 2018].

 ISBN: 978-1-61208-676-7