Review of Blockchain, Challenges and Solutions

Ojasvi Aggarwal
Indraprashtha Institute of
Information and Technology
New Delhi, India
Email: ojasvi17033@iiitd.ac.in

***Abstract*—The blockchain is a latest concept in the field of digital currency. Unlike traditional centralized approaches in databases, it supports decentralization. It serves multiple purposes. For example it acts as a distributed database, provides incorruptible storage etc. Recently, blockchains are facing a lot of challenges. Some of these challenges are data tampering, the anonymity of users, network speed, transaction costs etc. Some solutions have been proposed for these problems, like alternate chains, secure multiparty communication in bitcoin network etc. In this review paper we would explore purposes of the blockchain, why is it a good research area. In the upcoming sections, paper analyzes persisting challenges to blockchain and their solutions.**

***Index Terms*—Blockchain, ledger, decentralisation, multiparty, peer to peer network, bitcoin, anonymity, tamper-free, transaction.**

I. Introduction

Till date, people used physical currency in exchange for any product. Cryptocurrency is a new evolution in this area. Cryptocurrency is a virtual currency designed to work as a medium of exchange. It uses cryptography to secure transactions over the internet. A number of cryptocurrencies have been introduced in past few years. Some of these are bitcoin, ethereum, ripple, bitcoin cash. The blockchain is the backbone of these cryptocurrencies. The blockchain is an undeniable invention by Satoshi Nakamoto. This was developed in order to store digital assets of a person. But since then, it has evolved into something greater. The technology, which was invented in 2008 to power Bitcoin. From then, a year later, is being used for everything from storing digital currency to copyright protection. The blockchain is a distributed global storage. Instead of being maintained by a central authority, blockchain is globally maintained by nodes of the network. Each node of the network has its own copy of blockchain. To achieve consistency, nodes communicate with each other. Most recent and longest chain among all the copies is assumed to be valid. This blockchain is then used by all the nodes within the network for verification of new blocks. Bitcoin and ethereum blockchains have seen significant adoption in the past few years. Bitcoin is a decentralized P2P digital currency in which coins are generated by a distributed set of miners and transactions are broadcasted via a peer-to-peer network [1]. In bitcoin network, blockchain solves the purpose of holding coin blocks. These blocks are a container for bitcoin transactions.

Hash: 000000000043a8c0fd1d6f726790caa2a406010d19efd2780db27bdbbd93baf6
Previous block: 00000000001937917bd2caba204bb1aa530ec1de9d0f6736e5d85d96da9c8bba
Next block: 000000000000036312a44ab7711afa46f475913fbd9727cf508ed4af3bc933d16
Time: 2010-09-16 05:03:47
Difficulty: 712.884864
Transactions: 2
Merkle root: 8fb300e3fdb6f30a4c67233b997f99fdd518b968b9a3fd65857bfe78b2600719
Nonce: 1462756097

Input/Previous Output	Source & Amount	Recipient & Amount
N/A	Generation: 50 + 0 total fees	Generation: 50 + 0 total fees
f5d8ee39a430....:0	1JBSCVF6VM6QjFZyTnbpLjoCJ....: 50	16ro3Jptwo4asSevZnsRX6vf...: 50

Fig. 1. Storing a bitcoin block on blockchain [2]

Above figure depicts how bitcoin block is stored on the blockchain. It consists of two parts. First part is header and second is the transaction. The header consists of has of the block, hash of the previous block, timestamp, current mining difficulty, number of transactions in the block etc. Transaction portion consists of input transactions, output transactions, and their indexes. Input transactions show the ownership of coins being spent in the current transaction. Apart from use in cryptocurrencies, blockchain has evolved for other purposes. Now we discuss some recent uses of the blockchain. The blockchain is used in identity infrastructure. In ethereum blockchain, we dont have to build an identity. We just use ethereum open blockchain to store identity details. For verification of identity, we just have to query blockchain. Another use is tamper-free storage. The blockchain is a chain of blocks model. Every block contains the hash of its previous block. Changing any block will change its hash and hence, break the chain. This model enhances tamper-free storage. The blockchain is also used for digital assets. ICO(initial coin offering) is a new way to raise investment. ICO's offer tokens in return for some investment. These tokens are called digital assets. Blockchains also supports various other services like the smart contract, digital voting etc. All these reasons help in making blockchain a great field for research.Due to these uses and opportunities, blockchains qualify as a good research field. There are some notable issues with blockchain. First is the security breach. Blockchain depends on mining power of miners. If any miner or mining pool gains more than total 51 percent hash power

than a theoretical attack is possible. Another problem with blockchains is too much network delay. Blockchain needs confirmation from multiple sources to maintain consistency. This happens due to decentralization. This leads to slow down of the network. Many other problems do exist in the network such as selfish mining, transaction cost etc. Till now, we discussed blockchain and related concepts. Now we discuss the purpose of blockchains. Then challenges, limitations of blockchain come into play. Afterward, solutions to these problems would be discussed. Some comparison is also drawn related to the problems and their solutions. Finally, we depict graphically up to what extent these problems persisted in the network. We also show the amount of damage caused by problems.

II. Review of literature

The cited sources are relevant to the study of the blockchain. Reviews from papers highlight about various purposes of the blockchain, persisting problems in the network. Papers also talk about some solutions to above problems. Drawing analysis of these solutions. All the references belong to recent conferences.

III. Purposes of blockchain

Blockchain has seen adoptions in many fields. The main reason for this adoption is security, distributed, global, public and many more. Due to all these reasons, people trust blockchain. Also, security is maintained at multiple points using cryptography, mining process etc. Some uses of blockchain are decentralized versions of domain name servers, public key cryptography etc. Let's discuss some of them in detail.

A. Namecoin

It is recently developed on the blockchain [3]. Till date, DNS(domain name servers) are centralized services. This service converts a humanly readable website into IP address. For example, converting www.google.com to 172.217.26.132. Currently, traditional domain name servers are being used. There exist some problems with the traditional approach. DNS poisoning is one of the prominent problems. If any DNS is open to attack, then entries can be easily changed. In namecoin network, a new approach has been adopted, to decentralize this service. Users register with namecoin network. They establish a name-value pair for the website. The user is allotted a set of his keys [3]. Only the person having private keys can update name-value pair on the network. Benefits of this approach are it is difficult to tamper the blockchain [4]. Cost of tampering blockchain is much higher compared to a single database [3]. Drawbacks of this approach include network anomalies, security problems etc.

B. Smart contracts

These are another popular use of blockchain. Smart contracts are a set of digital rules to enforce negotiation of a contract. Smart contracts allow execution of credible transactions to successful [5]. Consider a situation where A needs to purchase a car from B. B needs bitcoins from A. So, both of them sign a smart contract. A submits specified bitcoins in the contract and a time locked transaction is created. When B provides digital keys to home to A, A allows the payment kept held in the transaction. In case of cheating, if B does not provide keys to A, the transaction is not released. After specified lock time, bitcoin amount is released back to A. If A receives the key from B and then refuses to pay, other nodes on network come into play and enforces transaction to be successful. Hence, B receives the amount. Benefits of this approach are an unbiased agent in contract signing, deal signing is automated, the absence of hand-filled forms leads to high precision [5]. Drawbacks of this approach are that it is technically difficult to make changes once the deal is signed if network breach takes place then the contract details might be leaked or modified.

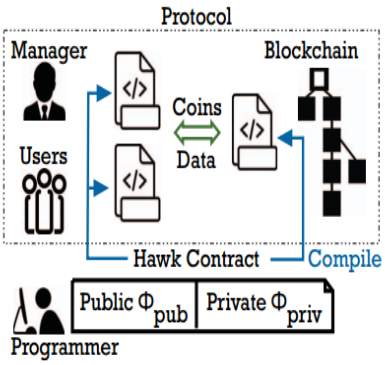

Fig. 2. Smart contract layout from [5]. Here 2 parties namely manager and user's digitally sign a contract. This keeps coin and data on blockchain.

C. Trusted distributed ledger

The blockchain is also used as trusted distributed ledger. It is used to store blocks of bitcoins [6]. To store transaction on the chain, nodes need to perform mining. After successful mining, blocks are added to the global ledger. Before adding on the blockchain, it needs a global confirmation from other nodes in the network. This is why blockchain is called distributed. It does not depend on centralized authority. The benefit of this approach is data gets stored on a much secure platform [7]. That's why blockchain is said to be tamper free [3]. It can be breached, but this would result in a huge loss. And attackers won't be benefitted. Drawback of this approach is that all the data is stored publically. It can be extracted and read by any person within the network.

D. Digital Identity

Blockchains can be used for storing and verifying digital identities [8]. In the current scenario, companies hire a database or cloud service. Any new user registers there. After the registration process, the user receives his identity. For verification, the company needs to check credentials from the database or cloud. All this procedure incurs a cost at

various steps. For example using a database or cloud service, memory at these storages, querying them etc. This can be easily accomplished using blockchains. User registers there publically. Some nodes store the data. The company just needs to query the system. The benefit is that the company need not pay for storage. Blockchain nodes do that for their own purpose. The company can just publically query the system. The drawback is that the user identity is stored publically. Anyone can see that data and misuse it. All the purposes discussed above make blockchain stand apart from traditional approaches.

IV. Challenges of blockchain

A. 51 percent attack

This attack on blockchain aims at disrupting trust in the blockchain [9]. Mining process selects a node with maximum mining power to mine a node. If multiple nodes combine to gain more than half of mining power, they can interfere with recording new blocks on the chain. This pool can prevent other miners from competing for adding blocks. They dictate adding blocks to the blockchain. Now, this mining pool can run a parallel blockchain. This parallel blockchain is trustless. It is under the control of a biased group.

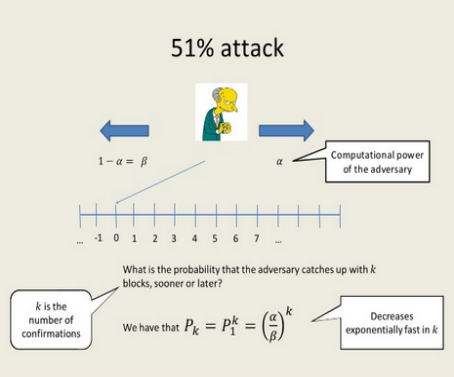

Fig. 3. 51 percent Attack from [10].

In this figure, it is shown that the probability of the miner to mine the block increases if he owns more than 51 percent of hash power.

B. Double spend attack

his attack results in spending of same coins to multiple parties. [2] Any transaction on blockchain refers to some set of input coins. This proves ownership of the coins. To spend these coins, the user creates a transaction. If a user wants same coins to be paid to multiple people, this is double spend [2]. This takes place if the user is part of a 51 percent group. So, the user can publish block to its group. Due to their monopoly, they would get to mine this block. This results in cheating the network.

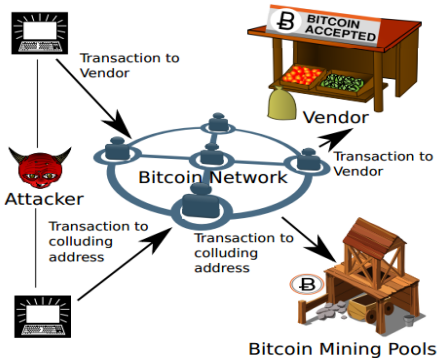

Fig. 4. Double spend attack mechanism from [2].

In this figure, the attacker A generate two transactions that use the same bitcoins from the network. Attacker A pays them to multiple nodes. If both of these transactions are successfully mined, then the attack would be assumed to be successful. The probability of this is very low.

C. Selfish mining

This is another type of challenge in public ledger [3]. This attack is performed against a specific target. This is where miner, mining pool does not publish a valid solution to the network. Selfish miner continues to mine other blocks. After some time, other miners catch up with the misbehaving miner. At this time, misbehaving miner releases other mined blocks. This way miners perform selfish mining and still keep the lead.

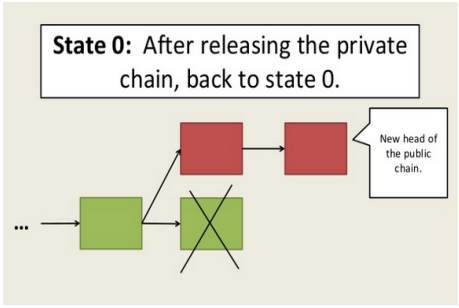

Fig. 5. Selfish mining attack mechanism part 1 from [10].

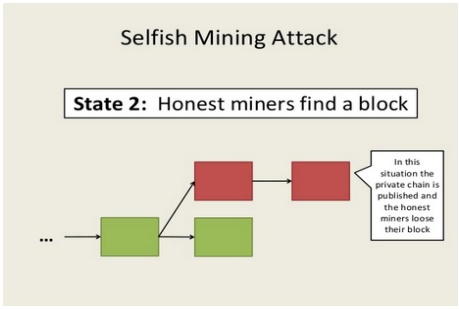

Fig. 6. Selfish mining attack mechanism part 2 from [10].

In these figures, true miners keep mining on green chain. A selfish miner mines red chain and doesn't publish it. Then

after some time, selfish miner publishes it. Due to this, true miners are fooled and they have to mine again on the longest red blockchain.

D. Lack of privacy

This is a basic issue in any network. All the data is published globally. All the nodes in the network are able to check this data. This public display of information leads to disclosure of privacy of the user's. Without public display of data, decentralization is not possible. So, there is a tradeoff between decentralization and privacy.

E. Network delay

This is also a persisting problem in the network [8]. A single node cant add a block to the chain. Node mines the block. Then publishes it to other nodes. Other nodes verify whether mined blocked is correct.

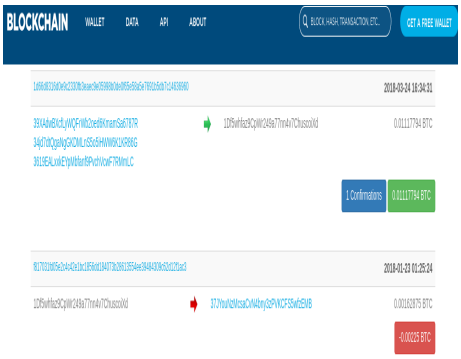

Fig. 7. Transaction showing 1 received confirmation [11].

After verification, the node needs confirmation from 6 other nodes. This process of receiving 6 confirmations leads to delay in the network. Due to this network delay, one block is mined every 10 minutes.

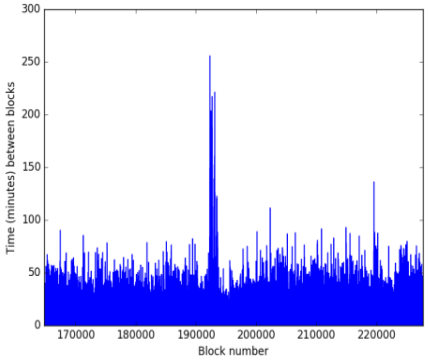

Fig. 8. Graph showing network latency with increasing blocks [3].

F. Transaction cost

This is an all-time challenge for the blockchain. Due to decentralization, no central authority manages the blockchain. The work has to be done by miners. Miners are rewarded for maintaining blockchain. This reward depends upon two factors namely coinbase and transaction fee [12]. When transactions exceed a certain size limit, they qualify for a transaction fee. In coinbase, miners get rewarded a number of certain bitcoins on mining a new block [13]. Currently, this reward is 12.5 bitcoins. It halves every 4 years. The main challenge of blockchain is the transaction fee. The transaction fee is to be paid by the sender. This fee is a certain percentage of the amount being paid. There can be possibilities if the sender does not pay this transaction fee. In that case, miners wont mine the blocks which do not include a fee because mining this block would be of no benefit to the miner. Hence, mining of such blocks takes too much time. Although, after some time, the priority of the block increases due to scarcity effect. This time delay also leads to network delay problem. This problem was discussed previously.

V. Solutions to Challenges

A. 51 percent attack solution

To defend against 51 percent attack, the blockchain protocol can be updated. A minimum number of required confirmations can be increased. This is adopted by Reddcoin protocol. In this protocol, a number of confirmations require a number of compromised nodes. This results in a boycott of the cheating node if the attack is identified. Once a mining pool named Ghash reached 51 percent of total hash power in 2014. Protocol changes were adopted at that time. Any pool extending 39 percent of total hash power is divided. This reduces the probability of any pool to reach 51 percent.

B. Double spend attack solution

A method has been proposed regarding double spend attack. It helps to detect double spend attack. It does not protect from double spend attack.
Some vendors are set up in different parts of the network [2]. These vendors act as full nodes. Full nodes store complete blockchain. Whenever a new block is to be added to the blockchain, it is propagated to these full nodes. Full nodes act as servers in the chain. To achieve consistency, full nodes communicate and decide upon the final valid chain. At this point in the network, full nodes can check for double spend.

C. Selfish mining attack solution

As per [12], there has been no evidence of a selfish mining attack occurring and it remains unknown what equilibria exist given the available strategy of temporary block withholding. Yet authors detected selfish mining by following methods. The network would see a delay in the mining of some blocks followed by blocks in succession. There would be a lot of rejected blocks. All these blocks are announced from some specific target. These methods help in detecting selfish mining attacks. After detection, cheating nodes can be blocked from the network. This attack reduces network bandwidth. Since many blocks are present in the network which are not mined. Blocking such nodes will also help in improving network latency.

D. Solution to attain privacy in the network

Privacy is another concern in the blockchain technology. To maintain privacy, a new security model is introduced in [14]. Any transaction on the chain refers to some previous transaction. A transaction doomed to fail if it refers to some unsuccessful transaction. A solution proposed is time locked transactions. This paper introduces a new transaction named Fuse [14]. This keeps checking on referred transactions. If the previous transaction fails to get on the chain within a specified time, the lock expires. The recent transaction is also taken back from nodes. Otherwise, both get on the chain successfully. This way privacy of failed transactions remains hidden from the network.

E. Reducing network delay

Network latency issue is discussed in [3]. Authors investigated the issue and analyzed the root cause. The cause was the software issues in the network. Some node sent transaction with large data fields to the network. This lead to crashing of the daemons. Block was not added to the chain in a timely manner. Hence, stable nodes were introduced in the network [3]. Crashing of daemons of stable nodes was comparatively low. Hence, overall network becomes stable. This also solves the network latency problem.

F. Lowering down the transaction fees

Here exist multiple solutions to transaction fees problem [15]. First is not paying the fee. In this case, the block is not mined during appropriate time durations. It becomes a victim of selfish mining. It also leads to network delay. This doesnt mean, that block wont be mined. A priority level is set for each block. As soon as time passes after the broadcast of the block to the network, the priority of block keeps on increasing. After some time, the block gets mined.
Another solution is the lightning network as per [8]. In this solution, another network layer is built on top of the bitcoin network. The Lightning Network would essentially allow users to send multiple transactions to and from outside of the blockchain. Due to this multiple transactions club up to form a block before broadcast to the network. Hence, the user needs to pay to just once for multiple transactions.

VI. Feasibility of attacks

A. 51 percent attack feasibility

According to theory, 51 percent attack seems to be practically possible. In 2014, a mining pool Ghash almost crossed 51 percent of hash power.
It was then decided that no pool should share over 39 percent of total hash power.

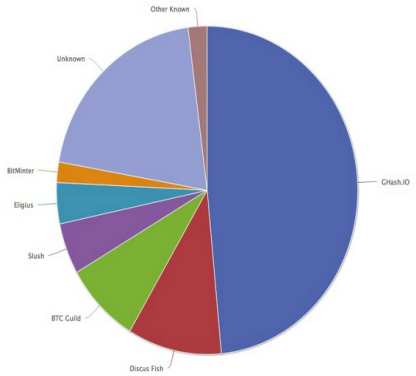

Fig. 9. Pie chart showing mining power of various pools [16].

B. Double spend attack feasibility

In an experiment over 6 * 10000 bitcoin nodes, double spend attack was performed. The possibility of success of the attack was noted as follows.

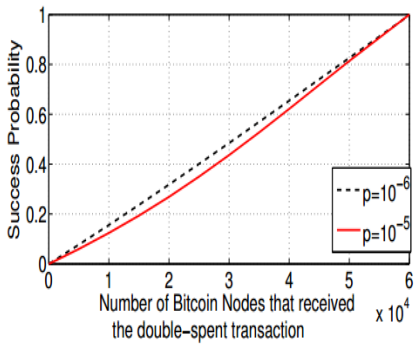

Fig. 10. Feasibility of double spend from [2]. As per the graph, success of double spend attack per total blocs is shown.

C. Network delay

Block addition in the network depends upon a target difficulty. As we can see in the graph, this difficulty is increasing with time. Hence, we need stable nodes in the network to reduce this delay [3].

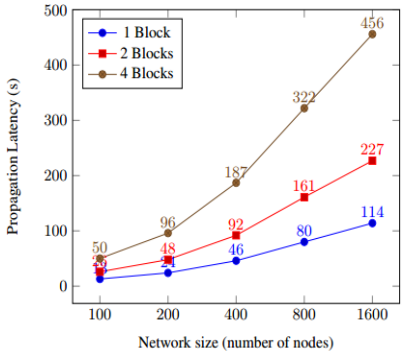

Fig. 11. Mining delay in bitcoin network from [8]. This shows the latency of the bitcoin network with different number of microblocks.

These graphs represent feasibility of various attacks on the blockchains.

VII. Conclusion

This review paper discusses blockchain. It began with the concept of the blockchain, how it started, why is it gaining popularity, why it qualifies to be a great research field. Then discussed purposes of blockchains, their benefits, and drawbacks. For example namecoin, smart contracts to exchange products digitally without paperwork, a distributed ledger to store bitcoin network data etc. After this, some challenges were presented to the blockchains, solutions to overcome these challenges.
Below listed is a mere summary of challenges and solutions.

TABLE I
Problems of blockchain network and their solutions

Challenges of blockchain	Solutions
51 percent attack	Increase minimum number of required confirmations.
Double spend attack	Decision depends on how full nodes communicate.
Selfish mining attack	Finding pending transactions in network and then blocking the nodes.
Lack of privacy of users	Secure multiparty communication.
Network delay	Introducing stable nodes in the network.
Transaction cost	Lightning network layer over distributed ledger.

Discussed problems and solutions are an important part of the discussion. Since we discussed uses and importance of blockchain, also we claimed that it is a good research area, to accept these we need to learn about issues with the concept. Listing all the issues won't be sufficient, so we also discussed their solutions as proposed by different papers. It would be right to say these problems might impact blockchain network, though the impacts are short lived. Developers have already come up with solutions to lower down impacts and restore the network.

VIII. Overall Assessment

The blockchain is one of the most important areas of research. We need efficient methods for implementation of the blockchain. Some of these are secure multiparty algorithms, the lightning network [8], introducing more stable nodes [3], checking for misleading nodes etc. We also need to think more efficient uses of blockchains. Researchers have analyzed many problems in the network. They have come up with appropriate solutions. Still, no system is perfectly unhackable. The blockchain is a public network. People need to test it for benefit of all. After any success, they also need to come up with solutions. This indeed keeps the blockchain intact. This prevents blockchain from any misuse. Various researchers also proposed other techniques like tor , mixing. But these techniques could not be adopted due to some drawbacks. Some approaches like secure multiparty communication, secure sharding protocol are still being used in the network. After reviewing several research papers on this topic, I can conclude that there are many challenges for blockchains. New challenges arrive with time. The choice of the most appropriate security protocol depends upon the usability of that protocol the level of security needed.
Also, new challenges might depend on some previous challenges. For example, the double spend attack depends upon 51 percent attack to be successful. If a miner doesn't have 51 percent of total hash power, the possibility of successful mining of a doubly spent block is low. Hence, miner needs to gain control of 51 percent of total mining power to successfully mine doubly spent block. Hence, some new attacks fail because of their dependence on some previous attack, which has been taken care of by the developer team. So, we can trust blockchains till the time they prove to fail drastically.

Acknowledgment

I would like to thank Dr. Anubha Gupta for guiding me and providing an opportunity to write a review paper.

References

[1] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *2015 IEEE Symposium on, Security and Privacy (SP)*. IEEE, 2015, pp. 122–134.

[2] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 906–917.

[3] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains." in *USENIX Annual Technical Conference*, 2016, pp. 181–194.

[4] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 279–296.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on,Security and Privacy (SP)*. IEEE, 2016, pp. 839–858.

[6] E. Anceaume, T. Lajoie-Mazenc, R. Ludinard, and B. Sericola, "Safety analysis of bitcoin improvement proposals," in *2016 IEEE 15th International Symposium on, Network Computing and Applications (NCA)*. IEEE, 2016, pp. 318–325.

[7] E. Ben-Sasson, A. Chiesa, M. Green, E. Tromer, and M. Virza, "Secure sampling of public parameters for succinct zero knowledge proofs," in *2015 IEEE Symposium on, Security and Privacy (SP)*. IEEE, 2015, pp. 287–304.

[8] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 17–30.

[9] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on, Security and Privacy (SP)*. IEEE, 2014, pp. 459–474.

[10] P. Camacho, "Analyzing attacks," 2017. [Online]. Available: https://www.slideshare.net/philippecamacho/analyzing-bitcoin-security

[11] B. Info, "Confirmation to transactions," 2017. [Online]. Available: https://blockchain.info/address/1Df5whfaz9CpWr249a77nn4v7ChuscoiXd

[12] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on, Security and Privacy (SP)*. IEEE, 2015, pp. 104–121.

[13] I. Eyal, "The miner's dilemma," in *2015 IEEE Symposium on, Security and Privacy (SP)*. IEEE, 2015, pp. 89–103.

[14] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *2014 IEEE Symposium on,Security and Privacy (SP)*. IEEE, 2014, pp. 443–458.

[15] A. Ben-David, N. Nisan, and B. Pinkas, "Fairplaymp: a system for secure multi-party computation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 257–266.

[16] BitFury, "The threat of 51 percent attack," 2017. [Online]. Available: https://www.coindesk.com/bitfury-pulls-power-ghash-community-uproar/