Leveraging Blockchain technology on bitcoin from Cyber-Security Issues

[1] B Sri Harsha Vardhini, [2] Priyanka kumari Bhansali
[1]M.Tech Scholar, Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.
[2]Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India

Abstract: With the enhanced iteration of technological innovation, blockchain has rapidly become one of the hottest Internet technologies in recent years. As a decentralized and distributed data management solution, blockchain has restored the definition of trust by the embedded cryptography and consensus mechanism, thus providing security, anonymity and data integrity without the need of any third party. But there still exists some technical challenges and limitations in blockchain. Bitcoin is a popular cryptocurrency that records all transactions in a distributed append-only public ledger called blockchain. In this paper, we present a systematic survey that covers the security and privacy aspects of Bitcoin. We start by presenting an overview of the Bitcoin protocol and its major components along with their functionality and interactions within the system. We review the existing vulnerabilities in Bitcoin and its underlying major technologies such as blockchain. This paper has conducted a systematic research on current blockchain application in cybersecurity. In order to solve the security issues, the paper analyzes the advantages that blockchain has brought to cybersecurity and summarizes current research and application of blockchain in cybersecurity related areas. Through in-depth analysis and summary of the existing work, the paper summarizes four major security issues of blockchain and performs a more granular analysis of each problem. Finally, we summarize the critical open challenges and suggest directions for future research towards provisioning stringent security and privacy techniques for Bitcoin.

Index Terms **– Block chain, Cybersecurity, Privacy-Protection, Bitcoins, Cryptocurrency ECC, SHA.**

I. INTRODUCTION

Bitcoin is a cryptocurrency that has recently emerged as a popular medium of exchange, with a rich and extensive ecosystem. Bitcoin is a consensus network that enables a new payment system as completely digital money. Bitcoin uses peer-to-peer (p2p) technology, and it operates without any trusted third party authority that may appear as a bank, a chartered accountant (ca), a notary, or any other centralized service [1]. In particular, an owner has full control over its bitcoins, and she could spend them anytime and anywhere without involving any centralized authority. Bitcoin design is open-source and nobody owns or controls it.

The concepts of Bitcoin were conceived in the month of January, 2009 by a researcher going by the name 'Satoshi Nakamoto' pseudonymously. The open source project known as Bitcoin was created on the proof-of-work principle that transactions can be securely processed on a decentralized peer to peer network without the need for a central clearinghouse[2]. Bitcoins are controlled by the user of the currency around the world. Bitcoin operates as a p2p file sharing protocol and it is based on SHA-256 algorithm [5]. Bitcoin coin (BTC) is essentially a hashed chain of digital signatures based upon asymmetric or public key cryptography. Each participating Bitcoin address in the P2P network is associated with a matching public key and private key wherein a message signed by private key can be verified by others using the matching public key. The public transaction history also allows network analysis to cluster some groups of public Bitcoin pseudonyms into individual users. Real time analysis of the Bitcoin peer-to-peer network then provides enough data to identify a portion of users with specific IP addresses. Existing security solutions for Bitcoin lacks the required measures that could ensure an adequate level of security for its users. We believe that security solutions should

cover all the major protocols running critical functions in Bitcoin, such as blockchain, consensus, key management, and networking protocols. Blockchain was initially put forward as an underlying technical framework of Bitcoin [3]. Although due to the excessive value fluctuation and supervisory management reasons, Bitcoin was once forbidden or restricted to a variable extent in China, Russia, Europe and some other countries [2-4]. The confidentiality, security and reliability of blockchain technology are realized by the public. Blockchain is considered a bran-new data storage, transmission and management mechanism because it realizes reliable transfer of data and value in a decentralized way, without the need of any trusted third-party organization. Bitcoin derives its reliability from a public record of valid past transactions. Users check against this history to verify new transactions. Once it has been verified, it is then added to the block chain [6]. Because this history is just a record of past events, disagreements over transactions are possible. In this paper, we will have a quick study about what is blockchain then we'll discuss different application in blockchain and what service do they offer at the end, we shall talk about the security issues and those challenges we need to overcome.

II. OVERVIEW OF BITCOIN

Bitcoin is a decentralized electronic payment system introduced by Nakamoto [11]. It is based on peer-to-peer (P2P) network and a probabilistic distributed consensus protocol. In Bitcoin, electronic payments are done by generating transactions that transfer bitcoins among users. The destination address (also called Bitcoin address) is generated by performing a series of irreversible cryptographic hashing operations on the user's public key. In Bitcoin, a user can have multiple addresses by generating multiple public keys and these addresses could be associated with one or more of her wallets [21]. The private key of the user is required to spend the owned bitcoins in the form of digitally signed transactions. Using the hash of the public key as a receiving address provides the users a certain degree of anonymity, and it is recommended the practice to use different Bitcoin address for each receiving transaction. The blockchain keeps the records of the transactions in units of blocks. Each block includes a unique ID, and the ID of the preceding block. Any miner may add a valid block to the chain by simply publishing it over the network to all other miners that are connected by p2p network. Bitcoin uses the Hashcash proof of work. Bitcoin's use of a Proof of Work system is one of the defining and unique characteristics it has as a cryptocurrency. Bitcoin uses SHA-256 hash function [3]. The network perform hashing on the block sent by the miner and checks if it still fits the pattern for the next block, by doing this the network can easily prove that the new block found by the miner is legitimate. The difficulty for the calculation of the Proof of Work can be adjusted by the network so that a new block is found at approximately every 10 minutes so it is unpredictable that which worker node in the network will generate the next block.

III. OVERVIEW OF BLOCKCHAIN

Blockchain technology was originally developed to facilitate the digital currency Bitcoin. But these are two separate technologies. While bitcoin is an encrypted currency, blockchain is the platform for peer-to-peer payment, supply chain tracking, and lots more. Consider this as an operating system for applications such as bitcoins and ethereum to function. In the simplest words, blockchain technology is a shared and open ledger that keeps a record of the transactions and cannot be modified. And as the name implies, blockchain includes an ever-increasing blocks of data with each block containing transaction information. The blockchain technology is based on decentralization which means the data is accessible to everyone while the data is managed by a cluster of computers and not owned by a single person. Blockchain technologies is not just only single one technique, but contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem, it's an integrated multifold infrastructure construction [5, 6, 15]. The blockchain technologies composed of six key elements.

Decentralized: The basic feature of blockchain means that blockchain doesn't have to rely on centralized node anymore, the data can be record, store and update distributed.

Transparent: The data's record by blockchain system is transparent to each node, it also transparent on update the data, that is why blockchain can be trusted.

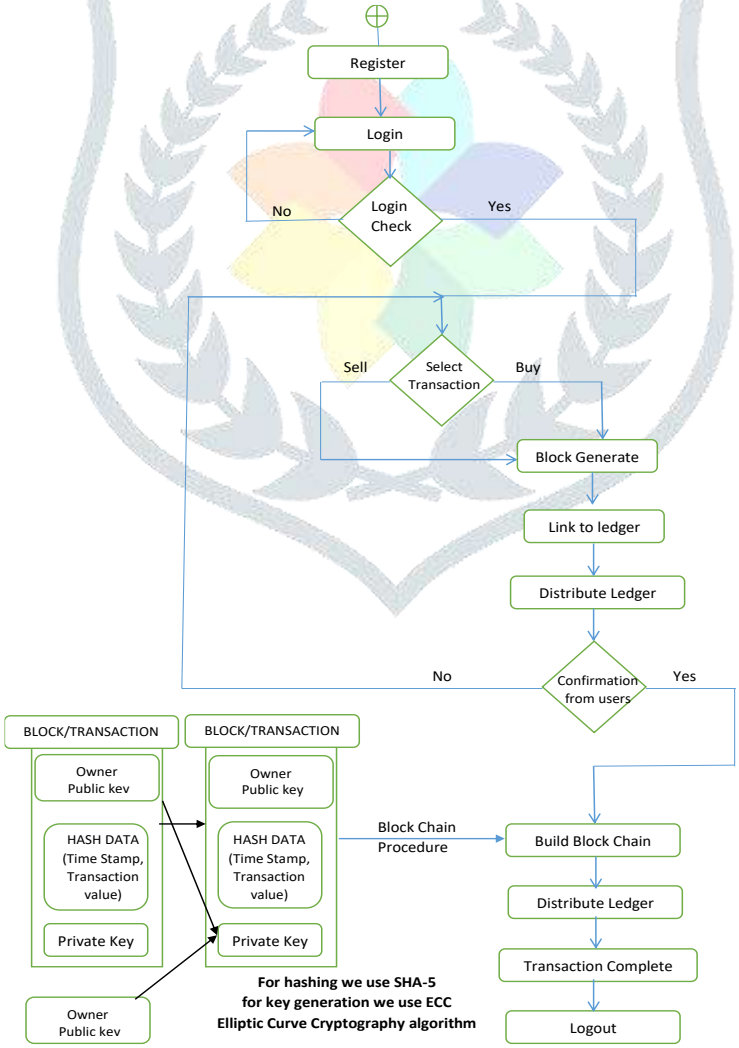
Open Source: Most blockchain system is open to everyone, record can be check publicly and people can also use blockchain technologies to create any application they want.

Autonomy: Because of the base of consensus, every node on the blockchain system can transfer or update data safely, the idea is to trust form single person to the whole system, and no one can intervene it.

Immutable: Any records will be reserved forever, and can't be changed unless someone can take control more than 51% node in the same time.

Anonymity: Blockchain technologies solved the trust problem between node to node, so data transfer or even transaction can be anonymous, only need to know the person's blockchain address.

ARCHITECTURE

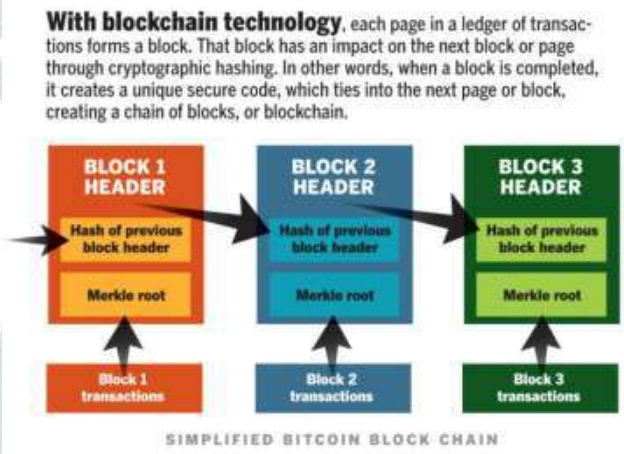


IV. WHY IS IT CALLED BLOCKCHAIN?

A block is record of new transactions. When a block is completed, it's added to the chain. Bitcoin owners have the private password (a complex key) to an address on the chain, which is where their ownership is recorded. Crypto-currency proponents like the distributed storage without a middle man — you don't need a bank to verify the transfer of money or take a cut of the transaction.

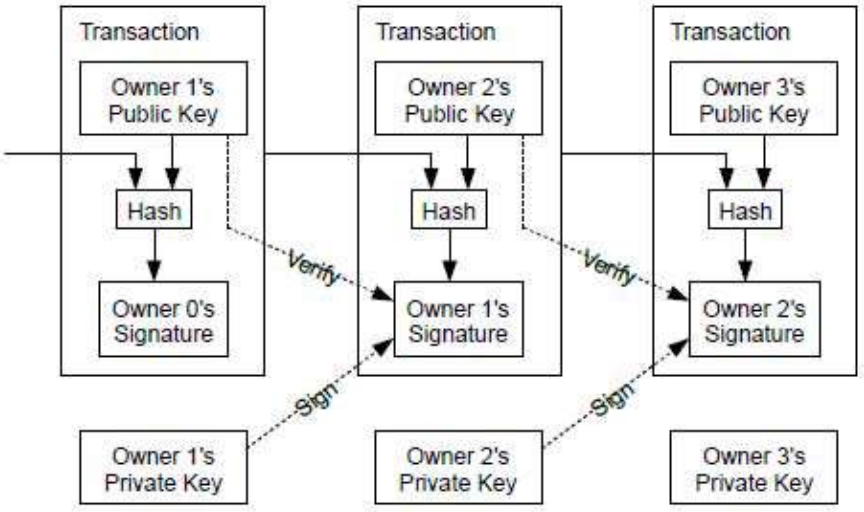
V. HOW DOES BLOCKCHAIN WORK?

When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a Blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.



VI. OVERVIEW OF BLOCKCHAIN SECURITY ADVANTAGES

Essentially, blockchain is an underlying technical framework which enables the users to collectively maintain a reliable database in a decentralized manner. As depicted in a typical blockchain system, data is generated and stored in units of blocks. Consecutive blocks are connected in chronological order to form a chained data structure. All user nodes participate in the validation, storage and maintenance of data. Usually the creation of a new block should be approved by more than half of the users, and broadcasted to all user nodes to perform a network-wide synchronization. Once synchronized, the modify or delete operation is not allowed optionally.



Blockchain technical framework

VII. THE STRUCTURE OF BLOCKCHAIN

Generally in the block, it contains main data, hash of previous block, hash of current block, timestamp and other information. shows the structure of block [10].

Main data

It depends on what service, this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record.

Hash

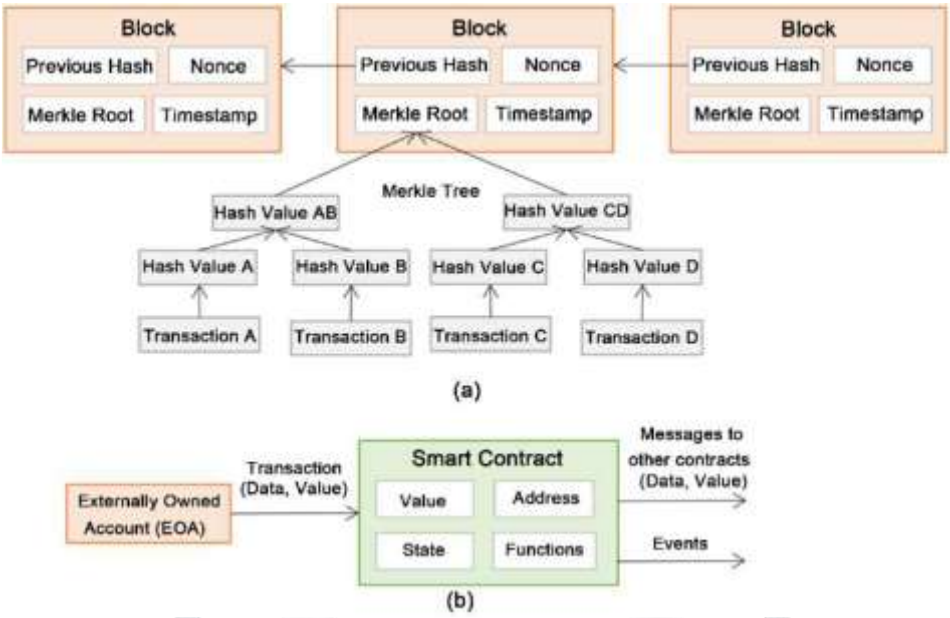
When a transaction is executed, it had been a hash to a code and then broadcasted to each node. Because it could contain thousands of transaction records in each node's block, blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be recorded in block header (hash of current block), by using Merkle tree function, thus reducing data transmission and computing resources drastically.

Timestamp

Time of block generated.

Other Information

It means like signature of the block, Nonce value, or other data that user define.



Structure of Block

VII SECURITY ISSUES AND CHALLENGES

So far, blockchain has got many attention in different areas, however, there exists some problems and challenges that needs to be faced [1, 2, 10].

Soft Fork

Soft Fork means when system comes to a new version or new agreement, and it wasn't compatible with previous version, the new nodes couldn't agree with the mining of old nodes. Because the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approved by the new nodes, but new nodes and old nodes will still continue to work on the same chain. When Soft Fork happens, nodes in the network don't have to upgrade the new agreement at the same time, it allows upgrading gradually. Not like Hard Fork, Soft Fork will only have one chain, it won't affect the stability and effectiveness of system when nodes upgrade. However, Soft Fork makes the old nodes unaware that the consensus rule is changed, contrary to the principle of every nodes can verify correctly to some extent.

The Majority Attack (51% Attacks)

With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). Because of this mechanism, people will want to join together in order to mining more blocks, and will become ―mining pools", a place which holds most computing power. Once it holds 51% computing power, it can take control of this blockchain. Apparently, it cause security issues [3, 4, 10]. If someone has more than 51% computing power, then he/she can find Nonce value quicker than others, means he/she has the authority to decide which block is permissible.

What it can do is:

1. Modify the transaction data, it may cause double spending attack [5, 6, 10].
2. To stop the block verifying transaction.
3. To stop miner mining any available block.

A majority attack was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hash rate was much lower and prone to reorganization with the advent of new mining technologies [7, 10].

Fork Problems

Another issue is fork problem. Fork problem is related to decentralized node version agreement when the software upgrades. It is a very important issue because it involves a wide range in blockchain.

Types of Forks

When the new version of blockchain software gets published, the new agreement in consensus rule also changed to the nodes. Therefore, the nodes in blockchain network can be divided into two types, the New Nodes and the Old Nodes. There can be four situations:

- The new nodes agree with the transaction of block which is sent by the old nodes.

- The new nodes don't agree with the transaction of block which is sent by the old nodes.
- The old nodes agree with the transaction of block which is sent by the new nodes.
- The old nodes don't agree with the transaction of block which is sent by the new nodes.

Because of these four different cases in getting consensus, fork problem happens, and according to these four cases, fork problems can be divided into two types, the Hard Fork and the Soft Fork..

Hard Fork

Hard Fork means when system comes to a new version or new agreement, and it wasn't compatible with the previous version, the old nodes couldn't agree with the mining of new nodes, so one chain became two chains. Although new nodes' computing power were stronger than old nodes, old nodes will still continue to maintain the chain which it thought was right. Figure 6 shows the hard fork problem. When Hard Fork happens, we have to request all nodes in the network to upgrade the agreement, the nodes which haven't been upgraded will not continue to work as usual. If there were more old nodes which weren't upgraded, then they will continue to work on the other completely different chain, which means the ordinary chain will fork into two chains.

Soft Fork

Soft Fork means when system comes to a new version or new agreement, and it wasn't compatible with previous version, the new nodes couldn't agree with the mining of old nodes. Because the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approved by the new nodes, but new nodes and old nodes will still continue to work on the same chain. Figure 7 shows the soft fork problem. When Soft Fork happens, nodes in the network don't have to upgrade the new agreement at the same time, it allows to upgrade gradually. Not like Hard Fork, Soft Fork will only have one chain, it won't affect the stability and effectiveness of system when nodes pgrade. However, Soft Fork makes the old nodes unaware that the consensus rule is changed, contrary to the principle of every nodes can verify correctly to some extent.

Scale of Blockchain

As blockchain is growing, data becomes bigger and bigger, the loading of store and computing will also be getting harder and harder and it takes plenty of time to synchronize data. At the same time, data still continually increase, and bring a big problem to client when running the system [8, 10]. Simplified Payment Verification (SPV) is a payment verification technology, without maintaining full blockchain information, it only Uses block header message. This technology can greatly reduce user's storage in blockchain payment verification, and lower the user's Pressure when transaction will drastically increase in the future.

Time Confirmation of Blockchain Data

Compared to traditional online credit card transaction, which usually takes 2 or 3 days to confirm the transaction, bitcoin transaction takes about 1 hour to verify. It's much better than the usual, but it's still not good enough to the extent to what we want it to be. Lightning Network is a solution to solve this problem [9, 10]. Lightning Network is a proposed implementation of Hashed Timelock Contracts (HTLCs) with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels. This allows the formation of a network where any peer on the network can pay any other peer even if they don't directly have a channel open between each other.

Current Regulations Problems

If we use Bitcoin for example, the characteristics of decentralized system, will weaken the central bank's ability to control the economic policy and the amount of money, which makes government be cautious of blockchain technologies. Authorities have to research on this new issue, accelerate formulation of new policy, otherwise it will have risk on the market.

Integrated Cost Problem

Of course it will have a lot of cost including time and money to change an existing system, especially when it's an infrastructure. We have to make sure this innovative technology not only create economic benefits, meet the requirements of supervision, but also bridge with traditional organization, and it should always encounter difficulties from internal organization which is existing now.

CONCLUSION

Bitcoin is becoming widely used and widely trusted as a valid currency. Many users employ Bitcoin for the sake of anonymity for a variety of reasons. Some just want more privacy in their lives, while others need anonymity in order to accomplish their goals due to legal reasons. There's no doubt that blockchain is a hot issue in recent years, although it has some topics we need to notice, some problems has already been improved

along with new technique's developing on application side, getting more and more mature and stable. The government have to make corresponding laws for this technology, and enterprise should ready for embrace blockchain technologies, preventing it brings too much impact to current system. When we enjoy in the advantage of blockchain technologies bring to us, in the same time, we still have to stay cautious on its inuence and security issues that it could be have.

.

References

[1] I. Bentov, A. Gabizon, and A. Mizrahi, \Cryptocurrencies without proof of work," CoRR, vol. abs/1406.5694, 2014.

[2] 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 IEEE Symposium on Security and Privacy, pp. 104{121, May 2015.

[3] N. T. Courtois and L. Bahack, \On subversive miner strategies and block withholding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.

[4] I. Eyal and E. G. Sirer, \Majority is not enough: Bitcoin mining is vulnerable," CoRR, vol. abs/1311.0243, 2013.

[5] J. Garay, A. Kiayias, and N. Leonardos, The Bit-coin Backbone Protocol: Analysis and Applications,pp. 281{310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[6] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, \Is bitcoin a decentralized currency?," IEEE Security Privacy, vol. 12, pp. 54{60, May 2014.

[7] A. Gervais, G. O. Karame, K. W • ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, \On the security and performance of proof of work blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3{16, New York, NY, USA, 2016.

[8] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, \Tampering with the delivery of blocks and transactions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Com- munications Security (CCS'15), pp. 692{705, New York, NY, USA, 2015.

[9] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, \Eclipse attacks on bitcoin's peer-to-peer network," in 24th USENIX Security Symposium, pp. 129{144, Washington, D.C., 2015.

[10] G. Karame, \On the security and scalability of bitcoin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 1861{1862, New York, NY, USA, 2016.

[11] G. O. Karame, \Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," in Proceedings of Conference on Computer and Communication Security, pp. 1{17, 2012.

[12] S. King and S. Nadal, Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, 2012. (https://archive.org/stream/PPCoinPaper/ ppcoin-paper_djvu.txt)

[13] 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'16), pp. 839{858, May 2016.

[14] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S.Gilbert, and P. Saxena, \A secure sharding protocol for open blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communica- tions Security (CCS'16), pp. 17{30, New York, NY,
USA, 2016.

[15] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/ bitcoin.pdf)

[16] E. U. Opara, O. A. Soluade, \Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 10{18, 2015.

[17] M. Rosenfeld, \Analysis of hashrate-based double spending," CoRR, vol. abs/1402.2009, 2014.

[18] J. Singh, \Cyber-attacks in cloud computing: A case study," International Journal of Electronics and In- formation Engineering, vol. 1, no. 2, pp. 78{87, 2014.

[19] Y. Sompolinsky and A. Zohar, Secure High-Rate Transaction Processing in Bitcoin, pp. 507{527, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[20] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, \A system view of nancial blockchains," in IEEE Symposium on Service-Oriented System Engineering (SOSE'16), pp. 450{457, Mar. 2016.

[21] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, \Blockchain contract: Securing a blockchain applied to smart contracts," in IEEE International Conference on Consumer Electronics (ICCE'16),
pp. 467{468, Jan. 2016.