9th IEEE International Conference on Communication Systems and Network Technologies

Security Issues & Seclusion in Bitcoin System

Depender Kumar Soni[1], Harbhajan Sharma[1], Bharat Bhushan[1], Nikhil Sharma[1], Ila Kaushik[2]
[1] Department of Computer Science and Engineering
[2]Department of Information Technology
[1]H.M.R Institute of Technology & Management, Delhi, India
[2]Krishna Institute of Engineering & Technology, Ghaziabad, U.P.
{dependerkumarsoni, harbhajansharma04, nikhilsharma1694, ila.kaushik.8.10}@gmail.com
bharat_bhushan1989@yahoo.com

Abstract – In the dawn of crypto-currencies the most talked currency is Bitcoin. Bitcoin is widely flourished digital currency and an exchange trading commodity implementing peer-to-peer payment network. No central athourity exists in Bitcoin. The users in network or pool of bitcoin need not to use real names, rather they use pseudo names for managing and verifying transactions. Due to the use of pseudo names bitcoin is apprehended to provide anonymity. However, the most transparent payment network is what bitcoin is. Here all the transactions are publicly open. To furnish wholeness and put a stop to double-spending, Blockchain is used, which actually works as a ledger for management of Bitcoins. Blockchain can be misused to monitor flow of bitcoins among multiple transactions. When data from external sources is amalgamated with insinuation acquired from the Blockchain, it may result to reveal user's identity and profile. In this way the activity of user may be traced to an extent to fraud that user. Along with the popularity of Bitcoins the number of adversarial attacks has also gain pace. All these activities are meant to exploit anonymity and privacy in Bitcoin. These acivities result in loss of bitcoins and unlawful profit to attackers. Here in this paper we tried to present analysis of major attacks such as malicious attack, greater than 52% attacks and block withholding attack. Also this paper aims to present analysis and improvements in Bitcoin's anonymity and privacy.

Keywords – Anonymity and Privacy, Blockchain, Bitcoin, crypto-currency, trading, assets, exchange, market, digital currency.

I. INTRODUCTION

Blockchain and Bitcoin have given a new vision and revolution in the field of Information Technology. It used to be a theoretical concept to exploit decentralized money as much as possible until it came in consideration of Satoshi Nakamoto. Satoshi Nakamoto in 2008 proposed the concept of Bitcoins and Blockchain technology. This is a currency which is in digital format. This currency was supposed to be involved in many illegal transactions. Also, some researchers marked it as a currency supporting unlawful acts. There is very less information available about the so-called founder of this digital currency, Satoshi Nakamoto. He has been covered under many controversial articles but the fact is that no solid evidence is available to proof their statements. Satoshi himself has claimed that he is no longer related to Bitcoins.[1]

The model of digital currency is not new, but it never came in existence so successfully as Bitcoins made their place in market. Chaum [2] proposed the idea where anyone could be the contributor. This idea included untraceable mails, return addresses and pseudo names (the technology implementing pseudo names is termed as pseudonym).

In 1993, the concept of proof of work was proposed by Moni Naor and Cynthia Dwork. This was considered as one of the best ideas to perform exchange of Digital Assets.

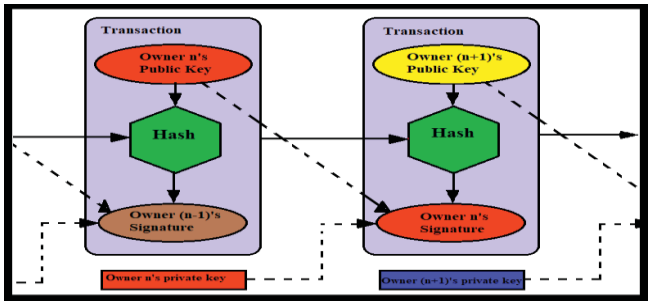

Fig 1: Blockchain Simplified

In this paper, Section I explains the fundamental information about Bitcoin Technology and Blockchain. This section is followed by section II which describes the work taken place in respective fields. This section also explains about the functionality of Blockchain Technology. Also, this section is designed in a way so that everyone can understand what Blockchain technology means and how this could be implemented in real life situations. Section III has been written, taking in consideration to explain the current security issues and future security scopes. In the same order, the next section, Section IV covers the risk issues in any Blockchain Technology which is later followed by the information of cyberattacks mentioned in section V. The next two sections, Section VI and Section VII includes the conclusion and future scope respectively.

II. LITERATURE REVIEW

In our work, we tried to provide detailed information related to privacy and anonymity issues in bitcoin technology which are studied thoroughly. We begin with the studies related to many books and articles published in 2007. The objective of our paper is to give a comprehensive readymade idea about the working of Blockchain technology which can

978-1-7281-4976-9/20/$31.00 ©2020 IEEE
DOI: 10.1109/CSNT.2020.42

be used by customers or whoever interested in getting familiar. We studied the survey by Schaffner,[3] which includes the brief overview on the issues which comes into existence. Also, the studies and the information is very less. A research compiled by Shen- Tu and Yu [4] on the Bitcoin's deanonymization and anonymization methods. They use methods of deanonymization for example – They linked the addresses of the bitcoin from the same user by doing network and blockchain analysis. They gave several studies having various methods. Yet, sufficient information is not available about this technology, which we tried to provide in this paper. Herrera – Joancomarti [5] classified the bitcoin anonymity into three categories; (i) traffic issues, (ii) analysis of Blockchain (iii) various techniques for privacy and anonymity. But still these studies are not sufficient and present properties for the analysis of the technology. Bonneau et al. [6] gave detailed studies about the cryptocurrency and bitcoin technologies. A book published by Narayanan et al. [7] providing various information about cryptocurrency and bitcoin technologies that have the concept of anonymity in Bitcoin. The depth overview of these studies was given by the technical survey done by Tschorsch and Scheuermann. [8] But still anonymity and privacy are not focused in this survey as well. Issues related to network and privacy are well discussed in this paper and the complete information on Proof-of-X schemes are given. Also, privacy and anonymity issues, analysis of Blockchain technology and deanonymization are given in detail. In this paper we gave key topics, trends and emerging fields for analysis. We also use the points identify to the given literature, particularly restricts the Blockchain technology in present scenario and how these spawn across various industries and fields in our country. On the basis of these observations, we analyze the future scope and various research fields which are most important for value both for researchers and practitioners.

A. Anonymity and Privacy

Anonymity can be considered as an e-mail address which is visible to everybody but the emails associated with that email could not be accessed by others without a particular password. This is the same way how Bitcoin implements anonymity.[9] Transactions are a feature of Blockchain Technology's mainstream feature - Cryptocurrencies. Cryptocurrencies rely on Blockchain, "a chain of blocks which contains records". Here records are the information of each and every transaction which takes place! The transaction's information gets stored on Blockchain ledgers. [10,11] Every transaction is done using a unique value called its hash value which give a set of numbers used to identify the transactions and a specific set of input data and output data. An output data set can be used only once in the entire process of the transaction. The aim of same citation of the output data set more than once gives rise to the double-spending difficulty and is prohibited in the network.[12] For example, if you like to send Bitcoins from one user to another, a transaction request is first initialized and then, by checking various parameters a transaction is said to be completed and added up as a new block.[13]

However, anonymity is advantageous for criminals, because what does a criminal do become public but the real identity of criminal remains concealed due to anonymity. [14]

B. Change Addresses

Bitcoin's change output is merely the extra amount of Satoshis (i.e., bitcoins) that spender doesn't wish to spend and thus are returned to the spender.[15] And the address on which this Change Output (i.e., extra Satoshis) is returned back to the spender is called the Bitcoin change address. This needs to be done because if you want to pay someone with a certain number of bitcoins, then the total amount of bitcoins on that particular address needs to be spent in its entirety.[16] And most of the times the value of bitcoin available on a Bitcoin address is higher than what the sender wishes to pay.[17]

In this case Bitcoin client (Bitcoin wallet) generates new Bitcoin change addresses in the wallet itself to send the difference back to this address.[18] This is also known as change or change output. Let us take an example of spending a $30 bill for bag to pay a cost of $10.[19] Now you would give the $10 to shopkeeper, also shopkeepers gave you $20. The customer should use a different output address so that take the left amount of $20.[20]

C. Mining and Incentives

The Way through which process of transactions in Blockchain are confirmed and open to a public platform and also the way by which new coins (Assume Bitcoins for BTC Blockchain) are used.[21] Every customer having internet and needful hardware get involved in the process of mining. It is also the process of adding a block.[22] The network of nodes in bitcoin initiates with recent data of transactions being send to all blocks or nodes. Each new block in the chain collects data of transactions in the block and have task of searching or finding proof-of-work [23], so that it is transmitted to all the blocks in the chain. In a Network node, valid blocks are those which have the correct data transaction and do not spend any part of it already. The recent transaction in a block is known as coin-based transaction.[24]

D. Proof of Work

The main objective of Proof of work is deterring cyber and hacker attacks which has the task of destroying the securities of computer system by using several fake requests. The concept of proof of work introduced even before digital currency, existed even before Bitcoin, but in another way, Satoshi Nakamoto implement this skill.[25] Bitcoin made a significant change in the previously used traditional transactions process. The concept of Proof of work was firstly given by Dwork and Noar in the year 1993, But the term proof of work came into existence in 1999, given in a document by Jakobsson and Juels. But Proof of work is the one of the revolutionary concepts of Nakamoto's digital currency paper that was published in 2008.[24]The hashing technique of PoW is same as Hashcash and on the other hand it totally depends on hash function. [25] By increasing the nonce in a block we can increase the Pow till the count of zeros bits need to produce the start of the block in nonce in the block hash.

After completing once it cannot be undo without doing the same computation process.[26] In case of any criminal activity done by hacker than all the hash block becomes invalid. Majority consensus is the longest group or chain of blocks in any network is important rule, if the attacker wants to modify a node then he needs to compete all the honest block of a majority chain.[27]

E. P2P Network

P2P network is network of computer which works run on protocol and have a duplicate copy of the data of transactions of ledger, this transmission of data is important for the blocks to do their jobs.[28] In a Blockchain every node in the transmission network share the information about the nodes and task, that is to modify nodes and confirm its data information as per its rules and cryptographic process which ensures that this data and information unchangeable and indubitable.[29] Disseminate P2P networks can have dissimilar patterns of nodes connection between two consecutives and the rate of the data transmission on the chain of network. The transmission of data could modify the work of nodes, their separate plan of action, also the group execution of the P2P network. The nodes which are connected on P2P networks share files and data stored in permanent storage i.e. hard drives.[30] The downloading data and information or sharing files among nodes in a network can be done software implementation. After downloading the needful data, it can act as a source. In a unique method, data can be download from other nodes by making one of the nodes as client.[31] But if node used as server, it can download files from other networks. In technical way both task downloading and uploading run on same time. So, each node propagates and send data and receive data from other nodes. One more advantage is that also P2P networks can be made very secure against these cyberattacks by arrangement of nodes by using distributed architecture Unlike conventional systems networks don't have any error or failure.[32] To understand much deeper structure of Bitcoin and its associated information can be found at Bitcoin Developer Guide.

F. Double Spending

Double spending is a mode of paying the same money more than once. As we know, any transaction can be processed only in two ways. One is offline, and another is online. Let us take an example:

Imagine you go to Hotel and order a room worth $50. The service man at Hotel immediately confirmed that the amount of currency you have paid, and you get your room in exchange for the money. Now is it possible to spend the same $50 somewhere else to make another purchase? The answer is NO. But what if the answer is YES? It means the same person can use the same cash more than one times. This type of problem is known as Double Spending Problem. Double spending issues never arise in physical currency.[33] But it is not true in case of digital currency, customers face double spending issues in bitcoins. So, the problem is bitcoins transactions can be made duplicate and rebroadcasted. It increases the way that the same currency could be used many times by its owner. Digital currency can also handle the double-spending problem by using verification procedure in bitcoin and handles a unique technique called Blockchain. Now imagine you have 15BTC and want to use it multiple times. You made a transaction of 15BTC to Harry. Now you want made a same transaction of 15BTC to Jack. These two payments go into the pool of unconfirmed transactions where many unconfirmed transactions are stored already. The unconfirmed transactions are transactions which do not pick by anyone. Now, whichever transaction first got accepted and was verified by miners, will be valid. Another transaction which could not get enough confirmations will be pulled out from the network. In this example, transaction T1 is valid and Harry will receive the bitcoin.

III. FACELESSNESS & PRIVACY IN BITCOIN

As per conventional banking frameworks, details of parties and their transactions are securely kept capsulated from others by trusted third parties. These trusted third parties are actually the banks. However, these third parties, banks, have all the detailed information about their customers. But when talking about Bitcoins, all the transactions are kept unambiguous and clear.[34] The transactions are transparent to public only the public keys are maintained anonymous. While making transactions in bitcoins, everyone can keep track of flow of money but the names of users are hidden from each-other. Only pseudo names are used. This working methodology resembles the stock exchange operations. As pseudo names are used, it has become a general mentality that there is anonymity in bitcoins but Bitcoins itself has explicitly remarked that it is not anonymous. Here all the transactions are maintained public such that payers and payees are marked by their pseudo names, which depicts that the address of all the Bitcoin transaction can be monitored. All the transactions are, related to a particular address is considered to check for its balance because Blockchain cannot keep the balances. It only stores the transactions.[35]

Having said that, along with accessing services and goods from merchants and/or payment processors, one also need to reveal or link its identification during trading Bitcoins on interchange, reason of, exchanges may be a subject to conceal illegally earned currency and/or scams. In such case it is mandatory for a user to show to be true to respective exchange.

Also, it has been noticed that the comportment, or say, the habit of using bitcoins by a user is used to determine the level of privacy provided to that user. Bitcoins have suggested some countermeasures such as generating and using a new key pair during every transaction. This new key pair is never related to previous key pair, hence making it impossible to predict the number or value of bitcoins a person holds. Also, one can use different wallets for different transactions. While using different transactions, it is not possible to link those transactions resulting in an isolated transaction. Also, one must take care to not to unveil their address in order to make secure transactions. The addresses of users are known to the service hosts as the data related to transactions and wallets are uploaded on server of respective hosted wallet services.

As the idea of Blockchain, it aimed to be public yet it can be used for a variety of causes in multiple tracts of industry. Here we will mention some prime Blockchain privacy studies.

IV. Issues in the Bitcoin System

Although bitcoin has faced innumerable critics for its misuse in illegal transactions, its extreme electricity consumption, price volatility, and its frauds from exchanges, some of the economists marked it as a speculative bubble. But that doesn't mean that it has no other issues. As explained by Mauro Conti in bitcoin has its own issues which are much important to be discussed in order to understand the bitcoin payment system in a much better way.

A. Social Risks

Bitcoins can be termed as a young technology as it came roughly about 12 years ago and it yet need to be developed in a much solid form of currency. It is somewhat difficult to trust a boom and bust market created by Bitcoins. Also, there is some ideologies that propose that Bitcoins may vanish in some decades. These things affect the interest of users in investing into bitcoins.

B. Legal Risks

As bitcoin transactions are taking place globally still there are some political parties and some public communities which have marked bitcoins as an illegal currency due to its pseudonym.

C. Economic Risks

Bitcoin resemble somewhat like a Ponzi Scheme, where people trading with high investments are profited on the loss of others. As number of buyers of bitcoins increases, a bubble economy is generated. And on the moment when this bubble ruptures, the low-level investors may try to sell their investments but they are unable to do so. Hence in that case, there is no surety of return of their investment, or say, the money will go vain. This may ultimately result in a painful loss. In such scenario there is a chance that investors may shift to other currencies where better services are being provided.

D. Technological Risks

Bitcoin is a digitally mined technology which is exchanged via wallets and is being monitored by various systems. It is completely reliant on technology such as the associated hardware equipment and network protocol strength. Without this, it is nothing.

E. Security Risks

This technology is prone to cyberattacks. Hacking is a consequential issue because there remains no method to recuperate the bygone or theft bitcoins. Also, if one has a wallet and he/she misplace its key than it is impossible to retrieve his/her bitcoins. Thus, key management is a major issue of bitcoins.

V. Bitcoin System & Cyber Attacks

This section briefs about network side and also with client side (user side) unauthorized access in Bitcoin system along with their elimination methods.

A. Attacks on wallet software

This kind of attacks are meant to steal or tamper the key. In this way the money is lost and the user has no way to track his/her money. Such type of attacks can be prevented by using more secure user wallets. One should not make accounts with trustless hosted wallet services. Also, it is advised that one should not keep huge amount of e-cash such as bitcoins in these digital wallets.

B. Greater than 50% attack

If an attacker is having a mining power of more than 50% hash-rate of mining a network, then that attacker may command over the whole mining pool or other miners. DoS attack may also be performed once the attacker dominates the network. This attack may bring small loss or dread to the users and miners. This attack can be prevented by a scheme like Two Phase Proof-of-work.

C. Selfish Mining

In block withholding attack or selfish mining attack the attacker attempts to withhold a successfully validated block from being publicized to other miners in mining pool. After an attacker withholds a successfully mined block, mining is being continued to the next block by him/her. In other way the attacker holds the private branch and hold his solution until the length of the private branch becomes more than the public branch. This results in demonstration of more proof-of-work than other miners in the pool. Because every member of pool contributes into pool to solve the proof-of-work and to earn incentive, this attack benefits attacker by earning him inappropriate incentives. Also, the CPU power of honest miners is wasted.

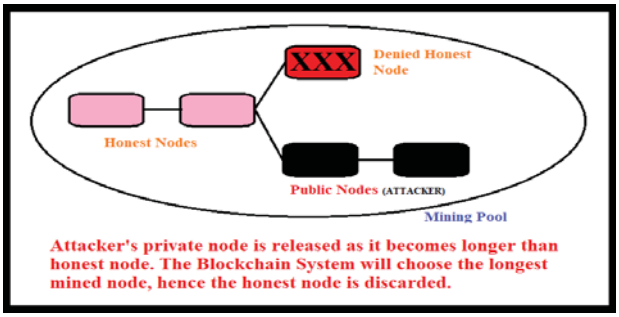

Fig 2: Depiction of Selfish Mining Attack

Several selfish mining stoppage methods are Zero-block, Fruit-chain techniques, and oblivious share.

D. Eclipse attack

In order to perform Eclipse attack, the attacker needs to organizes a 50% malicious attack having 41% mining strength. Here the node is managed by attacker in such a way

that all its connection goes to the attacker's Id in place of P2P network.

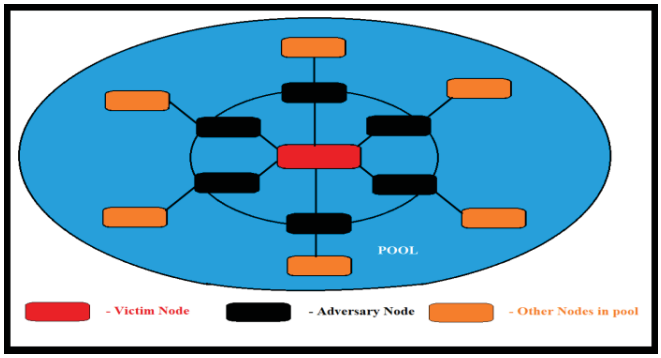

Fig 3: Eclipse Attack: How honest node's traffic is controlled by attacker

To prevent this attack, generally, the miners maintain a Black/White list of other pool members which are marked honest and/or attacker nodes. Otherwise, overlay network is also considered as a much better solution for such sort of attacks.

E. DDoS Attack

DDoS (Distributed Denial of Service) attack aims to corrupt the mining pools which trigger downturn of operations of the pool. This discourages the honest and distributed miners and they may finally make a decision to remove the pool.

Various proposed solutions for this attack include Traffic Monitoring and botnet detection.

F. Sybil Threat

As given in [36], In Sybil threat, the criminal makes various Sybil pirated identities. The criminal may then deny to receive or transmit blocks resulting in out-voting of the honest nodes available on the network or pool.

If the attacker becomes able to control major part of networks computing power or the hash-rate, which is generally observed in large scale Sybil attacks, then he/she can accomplish a 51% attack which may ultimately harm the whole network. And it will become impossible to trace him/her. The attacker may alter the arrangement of transactions. Even he/she may keep transactions from being confirmed. Also, they may reverse their earlier transactions in order to perform double spending.[37]

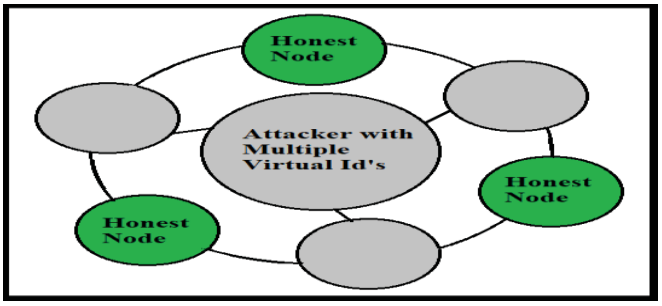

Fig 4: Multiple fake ID's present as different entity node

This attack can be protected if the ability to create new blocks is made proportional to the total processing power of proof-of-work mechanism. That implies that the attacker needs to own the computer power required to generate a new node. Which is actually very expensive for an attacker. Hence, the attacker may make much incentive by mining honestly in place of generating new block.

VI. Conclusion

We have Bitcoin, Dash, Ethereum, Litecoin, Ripple, Zcash, Altcoin and hundreds of other crypto-currencies used globally in exchange trading and as Stock commodity. But the most liked is Bitcoin, that is why, it is considered as the first choice for attackers to dabble. A comprehensive survey for improvement in Anonymity and Privacy of Bitcoin users is presented in this paper. Also, in this paper, we reviewed different methods to prevent cyberattacks on Bitcoin. But yet there is a great extent of solutions to be discovered or invented. Yet there are some attacks such as double spending for which solutions do exist but is yet to be overworked to prevent attacks in future. We examined a variety of security protocols and look forward for researchers to enhance security in Bitcoin Technology.

VII. Future Scopes

Blockchain technology is the most innovative and booming technology of twenty-first century. A Blockchain is a digital ledger which is firstly used to generate the database (record) of financial and non-financial mode of payments. All the data stored permanently in hard drives. All the records are completely accessible to all the nodes in the chain.

Blockchain Technology has a powerful future worldwide. An unimaginable scope of Blockchain technology has been seen in the financial field. The Industrial Sectors were destroyed financially as they are unable to balance the heavy workload after demonetization and need a specialist for their financial sectors. This is because RBI gave instructions to use digital currency in banking system. After implementing the Blockchain technology in banking, a large amount time and money could be saved which are used for processing and verification of transactions and keep it safe from malicious attacks.

Instead of Banking sector, Blockchain can also support in flow of money back and helps in cleaning of money as every

information of data or transaction is stored in the databases in the chain of nodes of a network. Also, government is perceiving the Blockchain which helps the government to have a control on the country's economy.

In modern world, a number of issues are also facing by the digital advertising because of malicious attacks, domain fraud and unusual traffic. But no need to worry about it Blockchain has given a way to deals with this problem as it fetches belief in an untrusted society. This technology permits trusted business companies to success, by decrementing the figure of doubtful players in the network.

Being a public ledger, the information and data sets is checked and encrypted by using the technique of cryptography. Through this way, the data files and information can be prevented by cyber and malicious activities. Also, world trade system can be controlled by using Blockchain, in present scenario shipment or object tracking is done by using consignment numbers in a supply network is old fashioned. To improve this system, it is easy to detect fake, duplicate products like fake electronic gadgets, medicines, books, clothes etc. by illegal ways or pirated serviceman who are providing these pirated items within a nation or city without obeying country's laws. With this technology, we can also keep the record of everlasting payments or transactions done by the user more efficiently and transparently. In this we also reduce the mistakes and lag in time.

This technology also helps us in IoT and Network system in creating sharable network for the devices used in IoT. By this we can remove the middle positioned to maintain the network among them; this will work as public ledger for more devices. These devices are in internal communication to fix the error and update the software. So, these are some real-life cases where we can make the use of this technology for solving real life problems more efficiently by fulfilling present needs of the system.

REFERENCES

[1] Bitcoin Block Explorer. [Online]. Available: https://blockexplorer.com/blocks-date/[year-month-day]. Accessed: 13- Jun-2017

[2] D. Chaum, "Blind signatures for Untraceable payments," Advances in Cryptology: Proceedings of Crypto 82, Springer US, pp. 199–203, 1983

[3] T. Schaffner, "Bitcoin Anonymity and Security," 2014. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2014/tschaffner.pdf. Accessed: 9-Jan-2017.

[4] Q. ShenTu, and J. Yu, "Research on Anonymization and Deanonymization in the Bitcoin system," arXiv:1510.07782, Oct. 2015.

[5] J. Herrera-Joancomartí, "Research and challenges on Bitcoin anonymity," in Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, Springer Science + Business Media, pp. 3–16, 2015

[6] 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, pp. 104–121, 2015.

[7] A. Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.

[8] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016.

[9] D. Chaum et al., "cMix: Anonymization by High-Performance Scalable Mixing," IACR Cryptology ePrint Archive, 2016:008, 2016.

[10] A. Back, "Hashcash - A Denial of Service Counter-Measure," Aug. 2002. [Online]. Available: http://www.hashcash.org/hashcash.pdf. Accessed: 06-Jul-2016.

[11] Saini, H., Bhushan, B., Arora, A., & Kaur, A. (2019). Security vulnerabilities in Information communication technology: Blockchain to the rescue (A survey on Blockchain Technology). 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). doi: 10.1109/icicict46008.2019.8993229

[12] Protect your privacy, Bitcoin. [Online]. Available: https://bitcoin.org/en/protect-your-privacy. Accessed: 13-Jun-2016.

[13] L. Xu et al., "Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 15-21, 2017.

[14] Adam Back (2002). "Hashcash - A Denial of Service Counter-Measure". Modern Economy, Vol.6 No.7, July 2015.

[15] Joseph Bonneau, "Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus", International Conference on Financial Cryptography and Data Security, 2016.

[16] Siamak Solat, Maria Potop-Butucar, "ZeroBlock: Preventing Selfish Mining in Bitcoin", arXiv preprint arXiv:1605.02435, 2016.

[17] Sharma, T., Satija, S., & Bhushan, B. (2019). Unifying Blockchian and IoT:Security Requirements, Challenges, Applications and Future Trends. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974552

[18] Morgen e. peck. "The Bitcoin Arms Race Is On! Powerful mining machines are changing the nature of the popular cryptocurrency". Internet: https://spectrum.ieee.org/computing/networks/the-bitcoin-armsrace-is-on. [Dec. 24, 2017]

[19] Jindal, M., Gupta, J., & Bhushan, B. (2019). Machine learning methods for IoT and their Future Applications. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974551

[20] Arora, D., Gautham, S., Gupta, H., & Bhushan, B. (2019). Blockchain-based Security Solutions to Preserve Data Privacy and Integrity. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974503

[21] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on, pp. 187–190, IEEE, 2015.

[22] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 458–467, IEEE Press, 2017.

[23] M. Kyriakidis, R. Happee, and J. C. de Winter, "Public opinion on automated driving: Results of an international questionnaire among 5000 respondents," Transportation research part F: traffic psychology and behaviour, vol. 32, pp. 127–140, 2015.

[24] G. Hileman and M. Rauchs, (2017), "Global cryptocurrency benchmarking study," Cambridge Centre for Alternative Finance.

[25] Jang, H., & Lee, J. (2018). An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. IEEE Access, 6, 5427–5437.

[26] Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Authentication & Encryption Based Security Services in Blockchain Technology. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974500

[27] Khamparia, A., Gupta, D., Albuquerque, V. H. C. D., Sangaiah, A. K., & Jhaveri, R. H. (2020). Internet of health things-driven deep learning system for detection and classification of cervical cells using transfer learning. The Journal of Supercomputing. doi: 10.1007/s11227-020-03159-4.

[28] D. D. F. Maesa, A. Marino, L. Ricci, "Uncovering the bitcoin blockchain: An analysis of the full users graph", *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, pp. 537-546, 2016.

[29] Q. Kong, W. Mao, G. Chen, D. Zeng, "Exploring trends and patterns of popularity stage evolution in social media", *IEEE Trans. Syst. Man Cybern. Syst.*.

[30] Y. Yuan, F.-Y. Wang, "Blockchain and cryptocurrencies: Model techniques and applications", *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 48, no. 9, pp. 1421-1428, Sep. 2018.

[31] N. Z. Aitzhan, D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures blockchain and anonymous messaging streams", *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 5, pp. 840-852, Sep./Oct. 2018.

[32] E. Casagrande, E. Arnautovic, W. L. Woon, H. H. Zeineldin, D. Svetinovic, "Semiautomatic system domain data analysis: A smart grid feasibility case study", *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 47, no. 12, pp. 3117-3127, Dec. 2017.

[33] Soni, S., & Bhushan, B. (2019). A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). doi: 10.1109/icicict46008.2019.8993210

[34] M. Saad and A. Mohaisen, “Towards characterizing blockchain-based cryptocurrencies for highly-accurate predictions,” IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, 2018, pp. 704–709. (2018).

[35] T. Phaladisailoed and T. Numnonda, “Machine Learning Models Comparison for Bitcoin Price Prediction,” 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), Kuta, 2018, pp. 506–511. (2018).

[36] S. Velankar, S. Valecha and S. Maji, “Bitcoin price “Top 10 cryptocurrency (2017), — best cryptocurrency to invest”.

[37] Sinha, P., Rai, A. K., & Bhushan, B. (2019). Information Security threats and attacks with conceivable counteraction. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). doi: 10.1109/icicict46008.2019.8993384