A Precarious Study of network propagation delay in Blockchain Technology

Summiya A Pathan[1],Dr. Yogesh Kumar Sharma[2]

[1]Research Scholar Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan
[2]Associate Professor & Research coordinator; Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan

Abstract: This paper analyses the Bitcoinblockchain selfish-mine strategy. A colluding group of miners could use this tactic to earn more than their fair share of mining profits and thereby forcefully join other honest men in decreasing the variance of their revenues and making their revenues more stable for months. It is a very dangerous dynamic that could enable the disbelieving mining body, accumulating news adherents' forces and manipulating the entire network, to enter the majority. Given that information spread between two miners in the network is not negligible and is accompanied by a normally distributed midway distribution proportional to the physical gap between the two miners, and by a permanent variance, regardless of other people's delays, we show that the success or failure of the attack on the selfish mines can not be assured due to uncertainty.

Keywords: IoT, Brine water, Energy consumption, Water treatment, pH vale

1. INTRODUCTION

The lack of scalability is regarded as the key barrier to mass use of blockchain technology. All current blockchain ventures are searching for solutions that can boost their network efficiency.

Many new ventures claim they have a magic bullet to fix the problem. Such statements are not always true, however. Sadly, the core and origin of an issue is not understood by many analysts and investors.It is difficult to define secret bottlenecks and trade offs without a detailed analysis and considerable technical context. In this article, we will address a popular bottleneck that prevents Bitcoin from scaling [1].

Shortly after the invention, researchers became interested in the limits of Bitcoin's scaling, the decentralised peer-to-peer network Bitcoin. The core question was soon established and presented in terms of the delay of block propagation or block propagation.For the new block to enter most of the nodes in the network, it is an average time. Whenever the new block is produced, it is broadcasted under the Gossip protocol on a broadly decentralised network like Bitcoin. If there is a new node, the node tells you of the new nodes connected to it.The node then passes the block to those nodes that it has requested. It passes through seven intermediate nodes before the block arrives at each complete node in the network. Any honest node should check the block before it is transmitted to other people [2].

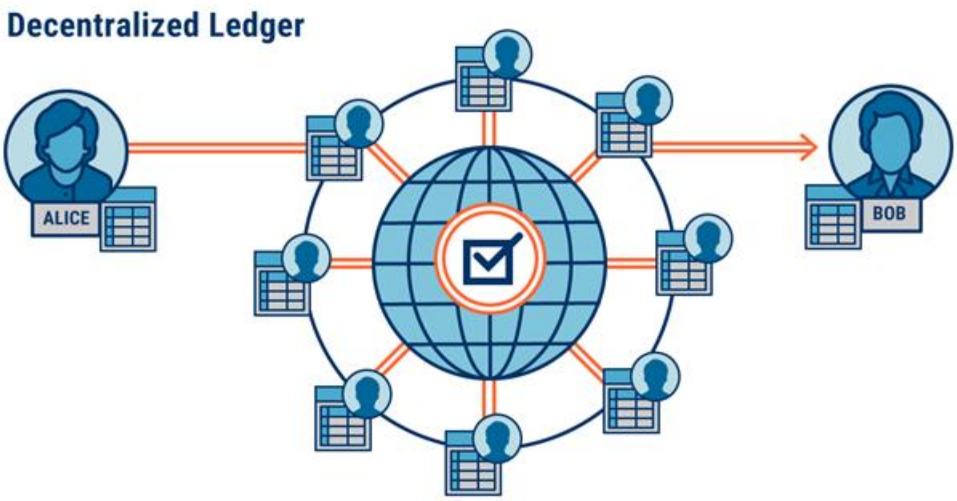

Figure 1 Decentralized Ledger

Of course, it takes a while for the whole thing. Each new block shakes the network and makes nodes and ethernet connections work entirely between them.One might argue that many changes have been made to the Gossip protocol since the launch of the network. For instance, the Bitcoin BIP 0152 proposal for a change proposed the option of only transferring a short transaction ID in a block body instead of the entire transaction list.If this node is not included in its Mempool, however, it must ask its peers in a separate message to move it on. If a large number of these transactions occur in the block, BIP 0152 progress will be lost [3].

As the data transmission is the time-consuming part of the block relay, scientists have wanted to decide how much time is required to hit 50%, 90% or 95% of the nodes in the network.The block propagation delay was found to be almost equal to the block size of blocks larger than 20 kB. In 2013, every additional kB of the block data induced an additional 80ms of delay in block propagation according to research released.Several academic papers and surveys have since been published annually on this topic. They update the above data and address different ideas for change [4].

The platform also tracks the current status and block time of the Bitcoin network. It also offers historical background on the subject in maps.Many well knownblockchain networks have the same architecture as Bitcoin. This means that in these networks the block propagation time follows the same rules.The block propagation time unfortunately has a huge effect on blockchain protection. The more the network spreads, the more likely the miners mine on old blocks.The main chain is then forked more frequently, and the number of orphan blocks is increased. The long delay in propagation leads to the Problem verifiers [5-10].

Some nodes could find that it would be a profitable strategy to resolve the block verification phase. They are at risk of mining on the wrong block in this situation.However, this strategy could be profitable if the block verification time is significant. Researchers concluded that the long delay in propagation decreases node resistance to 51 percent attacks and selfish mining.Blockchain developing companies are also trying to keep the block propagation time below 1 percent in the average block time in order to resolve the above issue [11].

That is true of Bitcoin, Ethereum and other big PoW consensus-based blockchain networks. This makes it always less than 6 seconds to distribute the block to 50% of the nodes in the Bitcoin network.While fast block relays, such as BIP 0152, reduce the average block propagation time, it can take longer than a simple protocol in the worst-case scenario.It is critical that the propagation delay be fair even in the worst-case scenario so that miners keep their node most of the time synchronised and always check proposed blocks.Whenever people speak about the blockchain's scalability, they discuss the system's transaction performance. However, people forgot that transaction efficiency changes do not jeopardise network safety or build conditions for data storage for nodes that wish to participate in the network [12-15].

These modifications may reduce the number and decentralisation of independent transaction validators in the network.Bitcoin transaction efficiency could easily be estimated using the formula:

$$\text{Throughput} = \frac{B_{size}}{T_{size} \cdot B_{time}},$$

where

B_{size} is the block size in bytes,

T_{size} is the average size of transaction record in the block,

B_{time} is the average time between consecutive blocks in the blockchain.

Transaction output can obviously be improved by increasing the block size, reducing the transaction record size or reducing the block interval. The scale of the transaction documents is very difficult to minimise.

Two other choices could be pursued instead. However, the percentage of time spent on block propagation is increased. This will undermine the network's stability and decentralisation [16].

It should be noted that network resources are used inefficiently in the mentioned Bitcoin protocol. Every node transmits and processes only a small fraction of the vital data for a new block. It's very essential network bandwidth, but it is used for just a few seconds at a time in full [17].

This node transmits transactions and supporting data only the rest of the time. This discovery has motivated researchers to pursue more efficient protocol designs to enhance transaction processes significantly without compromising network security and decentralisation [18].

1. Information Propagation

A network of homogeneous nodes is the Bitcoin network. No coordinating positions are available and each node contains a complete replica of all information necessary to verify that transactions are true. Each node checks information that it receives separately from other nodes and the trust between the nodes is limited [19].

A. Topology Network

By creating a random graph, the nodes in the network. When paired, the node can learn more about other nodes, demanding known addresses from its neighbours and listening randomly to new addresses' advertisements. The network cannot be directly left. The node addresses that the network left lying a few hours before the other nodes purge it from its established addresses. Around 16000 unique addresses, some 3500 of which were available at one time, were announced at the time of writing.

Partitions are not actively observed in the link graph and if the partitions occur, they will continue to function independently. While from an amusing viewpoint this is definitely ideal, the condition tracked in the divisions would vary over time, producing two parallel and probably conflicting transaction stories. The identification of network partitions is therefore of utmost importance. This could be carried out by monitoring the observed network aggregate capacity. A fast decrease in the detection rate of the block may indicate a partition [20-26].

B. Method of spreading

Only transaction (tx) and block (block) messages are important for updating and syncing the replicas. These messages are much more frequent and can expand to significant proportions than any other message sent on the network. They will not be sent directly to nodes received from other nodes, so as to prevent sending transactions and block message. Instead, the neighbours will be notified of their availability by sending an inv message to them after full verification of the transaction or block. The inv message has a collection of transaction hashings and block hashings that are now accessible and received by the sender.

2. Problem Formulation

It demonstrates the flow of protocols in the broadcast with a single hop. Node A receives a block, checks and informs its neighbours. Node B will receive the inv message and will issue a getdata message because the block is unknown. Node A will deliver the Node B block when the getdata message is sent.

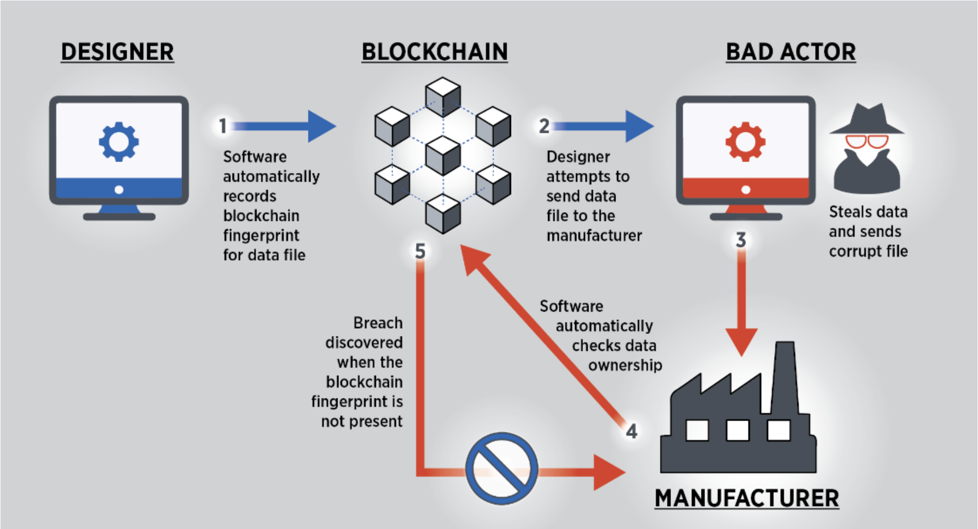
DESIGNER
BLOCKCHAIN
BAD ACTOR
1
Software automatically records blockchain fingerprint for data file
2
Designer attempts to send data file to the manufacturer
3
Steals data and sends corrupt file
4
Software automatically checks data ownership
5
Breach discovered when the blockchain fingerprint is not present
MANUFACTURER

Figure 2 Blockchain working

The network will be inserted into one of its nodes at each block or transaction, its root, and then distributed over the entire network using the above-mentioned diffusion mechanism. The message involves a propagation delay at each hop in the transmission. The delay is the combination of the time of transmission and the local block or transaction authentication. The delivery time involves a notification in the form of a call, the receiving party's request and a delivery. Though inv and data messages are small (in most cases the block or transaction is only reported in immediate broadcasting), the block message may be very big - up to 500 kB at the time of writing. It is checked until the block is notified to the node's neighbours. The checking of a block involves checking each block transaction. The verification of transactions in turn includes random access to disc data.

The regular histogram of tb,j displays the calculated interval for all blocks b. The long threshold of the distribution means that 5% of nodes that have not obtained the block are still present even after 40 seconds.

Matters of Scale

The size of a message and the delay in propagation in the network correlates strongly. The delay is described as the delay of any kilobyte causing a transaction or block to be disseminated. Note that both verification and transmission times are a mix of costs.

The cost can be assumed to be constant for sizes greater than 20kB, while a substantial overhead is given for small sizes. The expense of the 50 percentiles, 75 and 90 is to wait. The plot concentrates on the smaller y-range to illustrate the continuous enforcement after 20kB. This is due to the delay of the round trip, i.e. because even small messages are exchanged via a call message and then received via a getdata message. For transactions, the round trip delay is dominant as 96% of all transactions are smaller than lkB. Per kilobyte is a further 80ms delay for blocks of larger sizes than 20kB, until the majority understands the block. Therefore, it would be prudent to forward transactions directly and thereby avoid the extra round trip overhead. This cannot however be said for blocks in which the overhead is not as significant as disseminating the time [27-35].

3. Selfish Mining in Blockchains

In the paper, we research an important safety question: Does selfish mining become more profitable if there are many egotistical miners, and how many rounds can an egotistical miner wait for profit? The former request seeks to decide if any selfish miner needs a smaller Hashrate threshold to earn more money honestly than mining. The latter focuses on the temporary actions in the egotistical mining process, which takes mining changes into account.

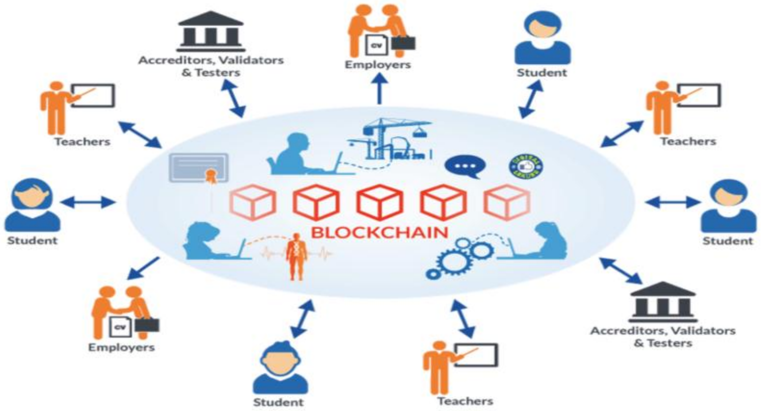

Figure 3.Blockchain applications

In a transient study, the selfish mining of computing resources is found to be useless and thus certainly unworthy without the modification of puzzles subsequently. The key contributions and comments are summarised hereinafter.

- We set a number of chain models for Markov to describe the state transition of public and private mining chains and to quantify the stable distribution of the government.
- Hashrate's minimum threshold is symmetrical at approximately 21.48 per cent if two egoistic miners gain both. When a selfish miner raises his hashrate and causes more fury, the successful selfish mining becomes more difficult.
- After 51 difficulty-adjustment rounds (714 days in Bitcoin), selfish mining is profitable, if both Hashrates of selfish miners are 22% (slightly higher than the profitably threshold). This delay falls to the five rounds (i.e. 70 days in Bitcoin) as its Hashrateis still very long and hits 33%.

2. SYSTEM MODEL

In this section we define the Blockchain mining basic model in the presence of two opponent pools.

A. Definition of the framework

Consider the two Alice and Bob mining ponds and an honest mining pond, Henry1. Consider the blockchain mining method. They are competing for the resolution of cryptographic puzzles in order to create a correct block for the acquisition of Bitcoin rewards. The consensus on proof-of-work (PoW) is decided and block mining is stateless: the likelihood of a miner's finding a block is proportional to the current Hashrate but inversely proportional to the real blockchain aggregate Hashrate. The cryptographic puzzles can be dynamically modified by the blockchain framework to construct new blocks at a set average rates (e.g. one block per 10 minutes on average in Bitcoin). A "round" is defined as the time to continue with an attack. By adoption and mining the longest chains, miners maintain a globally negotiated orderly sequence of transactions. The income of a mining operator is the estimated fraction of the blocks he mines from the largest chain of blocks

We make the following assumptions for simplicity which are consistent with the literature[2].

- Complete blockchain system hashrate is standardized as a unit. The hash rate of a mining pool is then a percentage of the entire population.
- When its Hashrate is high, the discovery time of the block through a mining pool is stretched exponentially.
- The payout is standardized as a cryptographic coin of each valid block.

B. Mode of egotism

The function of each other is ignorant to Alice and Bob. All miners, we believe, are operating on the same public chain at the beginning, where multiple honest miners begin, for their linear additives of Hashrates, to be reduced to one miner. Alice and Bob retain the length of the private chain as private knowledge, and both of them follow the length of the public chain. Our analysis methodology can be extended to a number of other approaches, we consider the selfish manipulation process as suggested by [2]. There are two occasions in the mining process.

The discharge process is tougher than the mining process. As soon as it is identified, Henry will broadcast his mined block and, according to the length of the public chain, Alice and Bob will determine if their mine blocks are released.

- (Forfeit case) Alice (resp. Bob) leaves her (or her) private chain to comply with public chain mining when latter is longer. If Alice or Bob publish a longer chain, Henry also gives up his public chain.
- (Risk-avoiding release cases) In view of the fear of loss of the new block being mined and leading advantages of its privacy chain are no more than two blocks, Alice (or her) releases her (or her) privately mined block.

The chain-response case is the mixture of forfeit and risk-avoiding situations, while the presence of a chain-response makes it impossible for the public chain to evolve. Assume Alice publishes its own private blocks to make the existing public chain redundant.

C. Release and breakdown of logic

The public chain consensus allows it to be the longest. A key issue is the growth of the public chain when it is as long as Alice or Bob.

Case of risk avoidance

Figure 1 shows that the private chain of Alice is published without risk. After Henry has mined a new block for the public chain, Alice is just one block ahead. Since Alice fears losing their contest, she is publishing her own private blocks, obsequious to Henry's public chain, so that Alice as well as Henry will then join the new largest chain.

Breakthrough resolutions. Henry might catch up with her if the private chain of Alice only is one block ahead of Henry's. When this happens, Alice immediately publishes her private squads for Henry. In Figure 2, there are therefore two public chains of the same length. Since only one public chain prevails, it is important to take into account a breaking law. The first is that Alice and Henry's public chains are equal in length and the private chain of Bob is either 0 or very long. So only the relationship between Alice and Henry needs to be solved. After block A1, all miners can be mine, while Henry and Bob can mine after block H1. The longest public chain is five possibilities and the shortest chain would be redundant. We skip the breakdown between Bob and Henry, since this can also be examined.

To the point that everyone Alice and Bob are hiding a private block, immediately after Henry discovers a new block, they will publish their private companies. There are three competing public chains, as shown in Figure 3. Henry doesn't know which chain is maliciously forked so he can mine on each public chain. Alice mines after A1 and he definitely mine after B1. Five potential scenarios are also available. The reduction of risk and two breakthrough solutions constitute all of the dynamics between public and private companies.

Release of chain reaction. We would then implement the chain reaction release, which makes the production of private and public chains more complicated. Note that a series of risk-avoiding releases and tie-breaking resolution consists of the chain reaction release. The private chain of Alice comprises four blocks at stage 1 while the private chain of Bob is lengthy.

3. CONCLUSION

To make it simpler for the reader, we begin by remembering how the Bitcoin network has achieved an effective dual-costing process. The assailant is:

- Send a transaction to the network that pays the attacked merchant to the network.Secretly I am creating a branch at that time, which involves a contradictory transaction paying the attacker, on the most recent block (before the transaction became a block).
- Wait until the deal is confirmed to the merchant and the dealer, secure in his payment, will submit the product.

The well-known results of a massive double-spent attack in the bitcoin network, shown in reference [5] and explained in reference [9]: as long as the attacker has less than 50 percent of the network's total calculating power and as long than the anticipated block time, all sincere miners are able to communicate quickly, there is a decrease in the likelihood of a two-string attack being successful. This likelihood is therefore always 1, when the machine hash power is more than 50 percent and for all confirmatory numbers (Fig. 4 of [9]).

At the time of this writing, the double-spending success of an intruder without 50 percent of the total computing threat potential is very difficult in view of scientific articles. In this section we will demonstrate that selfish mining can be an alternative strategy, without great machine hash power, to effective duplication of spending.

How can that be? How can the autonomous attack substitute for the double attack?

The SM pool operates as follows: when the SM miner finds the last public hash block he secretly hides it, before awaiting the network details and establishing a privately owned subsidiary. Meanwhile on the first hash they hear the honest miners continue to mining. The SM-pool expands its hidden branch and is looking forward to the longest chain. This becomes the global public sector as a result. The SM-pool therefore proceeds to secretly mine its block and will disperse it as soon as information is transmitted. The situation is that "an assailant can finish mining his secret block and disseminate it after a public block" and is described as making a good fork. And in this paper we have looked at the possibility that their private branch will become public, depending on the hazhnut power of the assailant α denoted by ðα dir, in consideration of the effects of a network data propagation delay. This study clearly shows that an alternative strategy for achieving dual expenditure can be the egoism strategy. Since the ðα-to values are usually not zero, our result is similar to the result [10]. That is, the double-dedicated attack is not guaranteed. The authors examined the problem of dual expenditure in the reference[10] and concluded that no promise can be made if it is possible to select the time when the attacker prefers transmitting this transaction.

We firmly believe that it is a reasonable starting point to look in more depth at the effect of a propagation delay in an assault with ego-mines that results in the likelihood of a dual-cost delay. For future study, authors of this paper propose to explore this issue: it is very important to look at the likelihood of double spending on different hazardous power levels below 50 per cent with the delayed assumptions we consider in the report, taking into consideration the Rosenfield model of reference [3].

The simple strategy of selfish mining, as examined in Ref.[1], results in the prize won by the colluding party. The results are given, regardless of the existence of the Bitcoin network propagation delay. It seems that the delay variability is a gain for the attacker during the attack by egoism. Then a comparative analysis of the income of dishonest miners would be required to solve these problems and constitutes a real move forward for the cryptocurrency community. Our analytical and simulation models are idealized.

4. REFERENCES

[1]. V. Martinez, M. Zhao, C. Blujdea, X. Han, A. Neely, and P. Albores, “Blockchain-driven customer order management,” Int. J. Oper. Prod. Manag., vol. 39, no. 6, pp. 993–1022, 2019, doi: 10.1108/IJOPM-01-2019-0100.

[2]. R. van Hoek, “Exploring blockchain implementation in the supply chain: Learning from pioneers and RFID research,” Int. J. Oper. Prod. Manag., vol. 39, no. 6, pp. 829–859, 2019, doi: 10.1108/IJOPM-01-2019-0022.

[3]. S. Höhne and V. Tiberius, “Powered by blockchain: forecasting blockchain use in the electricity market,” Int. J. Energy Sect. Manag., vol. 14, no. 6, pp. 1221–1238, 2020, doi: 10.1108/IJESM-10-2019-0002.

[4]. M. Kizildag et al., “Blockchain: a paradigm shift in business practices,” Int. J. Contemp. Hosp. Manag., vol. 32, no. 3, pp. 953–975, 2019, doi: 10.1108/IJCHM-12-2018-0958.

[5]. A. C. Issac and R. Baral, “A trustworthy network or a technologically disguised scam: A biblio-morphological analysis of bitcoin and blockchain literature,” Glob. Knowledge, Mem. Commun., vol. 69, no. 6–7, pp. 443–460, 2020, doi: 10.1108/GKMC-06-2019-0072.

[6]. W. L. Harris and J. Wonglimpiyarat, “Blockchain platform and future bank competition,” Foresight, vol. 21, no. 6, pp. 625–639, 2019, doi: 10.1108/FS-12-2018-0113.

[7]. S. Burmaoglu, O. Saritas, and H. Sesen, “IdeaChain: a conceptual proposal for blockchain-based STI policy development,” Foresight, vol. 22, no. 2, pp. 189–204, 2020, doi: 10.1108/FS-07-2019-0067.

[8]. J. Veuger, “Trust in a viable real estate economy with disruption and blockchain,” Facilities, vol. 36, no. 1–2, pp. 103–120, 2018, doi: 10.1108/F-11-2017-0106.

[9]. J. W. Lian, C. T. Chen, L. F. Shen, and H. M. Chen, “Understanding user acceptance of blockchain-based smart locker,” Electron. Libr., vol. 38, no. 2, pp. 353–366, 2020, doi: 10.1108/EL-06-2019-0150.

[10]. J. H. Jo, S. Rathore, V. Loia, and J. H. Park, “A blockchain-based trusted security zone architecture,” Electron. Libr., vol. 37, no. 5, pp. 796–810, 2019, doi: 10.1108/EL-02-2019-0053.

[11]. X. (Alice) Qian and E. Papadonikolaki, “Shifting trust in construction supply chains through blockchain technology,” Eng. Constr. Archit. Manag., 2020, doi: 10.1108/ECAM-12-2019-0676.

[12]. H. Singh, G. Jain, A. Munjal, and S. Rakesh, “Blockchain technology in corporate governance: disrupting chain reaction or not?,” Corp. Gov., vol. 20, no. 1, pp. 67–86, 2019, doi: 10.1108/CG-07-2018-0261.

[13]. S. B. Rane and Y. A. M. Narvel, “Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0,” Benchmarking, 2019, doi: 10.1108/BIJ-12-2018-0445.

[14]. A. Shojaei, J. Wang, and A. Fenner, “Exploring the feasibility of blockchain technology as an infrastructure for improving built asset sustainability,” Built Environ. Proj. Asset Manag., vol. 10, no. 2, pp. 184–199, 2019, doi: 10.1108/BEPAM-11-2018-0142.

[15]. G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” Smart Learn. Environ., vol. 5, no. 1, pp. 1–10, 2018, doi: 10.1186/s40561-017-0050-x.

[16]. H. Yi, “Securing e-voting based on blockchain in P2P network,” Eurasip J. Wirel. Commun. Netw., vol. 2019, no. 1, pp. 1–9, 2019, doi: 10.1186/s13638-019-1473-6.

[17]. M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, “Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology,” BMC Med. Inform. Decis. Mak., vol. 20, no. 1, pp. 1–10, 2020, doi: 10.1186/s12911-020-01275-y.

[18]. Chahar, P., Dalal, S.: Deadlock resolution techniques: an overview. Int. J. Sci. Res. Publ. 3(7), 1–5 (2013).

[19]. X. Burri, E. Casey, T. Bollé, and D. O. Jaquet-Chiffelle, “Chronological independently verifiable electronic chain of custody ledger using blockchain technology,” Forensic Sci. Int. Digit. Investig., vol. 33, 2020, doi: 10.1016/j.fsidi.2020.300976.

[20]. Dr. Yogesh Kumar Sharma and P. C. Harish (2018), “Critical Study of Software Models Used Cloud Application Development”, International Journal of Engineering & Technology, E-ISSN: 2227-524X, Vol. 7, Issue 3.29, Pp. 514-518.

[21]. B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” Internet of Things, vol. 11, p. 100227, 2020, doi: 10.1016/j.iot.2020.100227.

[22]. AD Vyas, DYK Sharma, “Significance Study of User Web Access Records Mining For Business Intelligence” Indian Journal of Applied Research (IJAR) 9 (7), 10-13.

[23]. A. Sydow, S. A. Sunny, and C. D. Coffman, “Leveraging blockchain’s potential – The paradox of centrally legitimate, decentralized solutions to institutional challenges in Kenya,” J. Bus. Ventur. Insights, vol. 14, no. March, p. e00170, 2020, doi: 10.1016/j.jbvi.2020.e00170.

[24]. P. Velmurugadass, S. Dhanasekaran, S. ShasiAnand, and V. Vasudevan, “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm,” Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.08.519.

[25]. MadhavPanthee, Dr. Yogesh Kumar Sharma, “Review of E-Government Implementation,” International Journal of Recent Research Aspects, vol. 6, Issue 1, 2019, pp. 26-30.

[26]. G. Kumar et al., “Decentralized accessibility of e-commerce products through blockchain technology,” Sustain. Cities Soc., vol. 62, no. March, p. 102361, 2020, doi: 10.1016/j.scs.2020.102361.

[27]. F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, “Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development,” Sustain. Cities Soc., vol. 55, no. December 2019, p. 102018, 2020, doi: 10.1016/j.scs.2020.102018.

[28]. Yogesh Kumar Sharma, " Designing enhanced Security Architecture for 5G Networks", International Journal of Management, IT & Engineering, vol. 8, no. 1, pp. 73-83, 2018.

[29]. B. Guidi, “When Blockchain meets Online Social Networks,” Pervasive Mob. Comput., vol. 62, p. 101131, 2020, doi: 10.1016/j.pmcj.2020.101131.

[30]. S. Saini, Y. Sharma, “Li-Fi the Most Recent Innovation in Wireless Communication”, International Journal of Advanced Research in Computer Science and Software Engineering 6(2), February - 2016, pp. 347-351.

[31]. M. T. de Oliveira, L. H. A. Reis, D. S. V. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. F. Mattos, “Blockchain reputation-based consensus: A scalable and resilient

mechanism for distributed mistrusting applications," Comput. Networks, vol. 179, no. May, p. 107367, 2020, doi: 10.1016/j.comnet.2020.107367.

[32]. J. Wang, G. Sun, Y. Gu, and K. Liu, "ConGradetect: Blockchain-based detection of code and identity privacy vulnerabilities in crowdsourcing," J. Syst. Archit., no. October, 2020, doi: 10.1016/j.sysarc.2020.101910.

[33]. V. K. Samyal and Y. K. Sharma, "Performance evaluation of Delay Tolerant Network routing protocol under varying time to Live", International Journal of Advanced Research in Computer Science, 2017, pp. 299-302.

[34]. T. M. Choi, S. Guo, and S. Luo, "When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management?," Transp. Res. Part E Logist. Transp. Rev., vol. 135, no. December 2019, p. 101860, 2020, doi: 10.1016/j.tre.2020.101860.

[35]. W. Serrano, "The Blockchain Random Neural Network for cybersecureIoT and 5G infrastructure in Smart Cities," J. Netw. Comput. Appl., vol. 175, p. 102909, 2021, doi: 10.1016/j.jnca.2020.102909.