European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 08, 2020

Countering Selfish Mining For Minimum 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—We examine the impact of propagation delay on the evolution of the Bitcoin blockchain in the sense of the selfish-mining strategy suggested by Eyal and Sirer. First, we use a simplified Markov model to control the contrasting belief that a small group of miners and the 'rest of the population' are blocking the growth rates of production through orphew block-hiding strategies such as selfish mining. Then we use a space process model of Poisson to investigate the values of the β-parameter by Eyal and Sirer. It indicates the proportion of the honest community mine in a hidden block which was released by the pool in reaction to a block's mining by the honest community. In the last analysis of the actions of a network of miners from Bitcoin, a proportion of whom are interested in using the strategy of egoism, we use discreet event simulation on the assumption that knowledge between miners has a propagation delay.

1. INTRODUCTION

Bitcoin is an electronic peer to peer payment system in which transactions are carried out without needing to be approved by a central clearing agency. Bitcoin users perform transactions by emailing who will be debited, who will be credited and where the change should be deposited (where applicable). The use of Public Key Encryption is Bitcoin transfers. The payors and payrollers have their Bitcoin Wallet Identification Public Keys established. Any Bitcoin exchange is encoded and sent over the Internet. Accept that you're getting a Mary exchange. On the off chance that you can unscramble Mary's message with her public key, you presumed that Mary's private key was encoded and consequently Mary's message came undeniably. Yet, how would you check? Mary has enough bitcoins for you to pay? By checking the exchanges in an encoded structure in an information structure called a blockchain that is kept up by a taking an interest bunch called excavators, the Bitcoin framework settles this issue. Various diggers can have distinctive blockchain variants, which is due to propagation delays, see Decker and Wattenhofer [1]. In order for Bitcoin to work, it is necessary to address these contradictions within a short period of time. We want to know how the anomalies occur and can be overcome.

A. Blockchain

The computing process called mining is at the heart of the Bitcoin system and includes solution to a difficult computational cryptography problem. Copies of all transactions as produced will be obtained by Bitcoin miners. They investigate the blockchain to research the past of the bitcoins involved. If ample Bitcoin credit is available for the proposed transaction, it is acknowledged as part of the block the miner is currently in operation.

A double hash of SHA-256 identifies each transaction. Mining companies collect transactions and use their Hash as inputs for the cryptographic problem.

This is how the mechanism works. A miner M calculates a block hash h over a special order of hazards for each transaction to be added to his next block B. The block solution si−1 is also taken as an input at the head of its existing blockchain version. The cryptographic problem that M needs to solve is: compute a hash of SHA-256 for the denoting concatenation by symbol +

if = hash(n + h + if−1); (1)

If the new blocks have been mined, the peer network members are told and the new blockchain for each peer has been added, subject to the fine detailed rules that are to be defined in the next section. To that end, for each collection of new blocks in 2016 the value of x, which represents the computational complexity of (1) is changed. The dilemma is made more complex if the previous blocs were created in 2016 at an average of six blocks per hour. If they are created at a slower average pace, then this is less daunting. The consequence of the issue is that the overall computing power used by the mining community varies.

A triumph/disappointment test whose outcomes rely upon past analyses checks whether the particular hash has the essential number of key zeros. Consequently, in light of the amazingly low likelihood of accomplishment of any individual examination, the time taken to do an analysis, an opportunity to make progress is very much formed by a remarkable arbitrary variable. The results are consequently extremely restricted. The demonstrating of squares of moment arrangement as a Poisson cycle at a steady pace of six every hour is accordingly normal.

The challenge of a block sequence is to calculate how hard the sequence is to produce the calculation effort. The numbers of leading zeroes necessary for creating the blocks in the series can be evaluated. Once we started Bitcoin, miners used PCs to solve the encryption puzzle and to gain bitcoins. The puzzle has been increased in order to reduce the rates of bitcoin production. To solve the cryptographic puzzlement, miners started to use the parallel processing capabilities of GPUs. The puzzle has been made more complex. Miners began using General Programmable Arrays of Field (GPFAs). The issue was further increased. Miners interact through a peer-to-peer network via the transmission of newly discovered blocks. Each miner maintains its own blockchain version based on the information and findings it receives. The protocol is designed to localise blockchains such that the variations can soon be settled and the block chains will be similar to each miner, if they differ. The way this method works is explained in the following paragraph.

B. Regulations for blockchain

This material is derived from [3]. A branch with the highest overall complexity is the main branch of the blockchain.

Blocks. Three block categories are available

1) Main branch blocks: transactions are thought tentatively to be confirmed in these blocks.
2) Side branch blocks off the main branch: the blocks have lost the race in the main branch, tentatively.
3) The blocks not related to the main branch due to missing predecessor or predecessor at the third level.

Squares in the initial two classifications structure a tree established in the primary square, known as the beginning square, associated with the past square hash, on which each square was built. The tree is practically straight and has a couple of branches past the principle branch.

• Blockchain cautions. Look at how as a hub finds out about another square. Either this block can be mined locally or after mining at another node communicated. The steps taken by the node are:

1) Reject the new square when there is one of the three square gatherings over that have a copy of the square.
2) Search whether in the primary branch or a side branch is the archetype block (in other words, the square comparing to the earlier hash). If not, inquiry the pair sending the new square for the sending of the archetype block.
3) Add another square to the blockchain if an archetype block has been put in the principle branch or a side branch. Three cases happen.

a) The principle part of the new square is stretched out: to interface with the primary branch the new square. In the event that the new square is privately mined, send the square to the companions of the hub.
b) the new square grows the parallel branch, yet doesn't add enough difficulty for it to be the new principle branch.
c) the current square applies to the side branch that will turn into the new principle branch.

i. find the principle branch fork block from this side branch,
ii. the principle branch ought to be re-imagined to cover just this fork block,
iii. to interface with the principle branch any square from the lower part of a fork to a leaf,
iv. detach from the child of the fork square to the leaf any square from the old fundamental branch,
v. relay to the hub's friends the new square.

4) Run the steps for each block in which the new block is its preceding block (including this one), recursively.

2. PREVIOUS WORK: THE SELFISH-MINE STRATEGY AND ITS OUTCOME

The Bitcoin mining network is reasonable, for example it tries to advance its benefits and can go amiss from the convention to do as such. A mining gathering may shape a pool with an incorporated facilitator as an individual specialist. In this situation, the mining pool is the measure of its individuals' mining force, and its income is allotted by their overall mining power among their individuals (see Ref. [3]). The foreseen relative pay, or basically a pool's pay is the assessed division of squares mined by this pool out of the complete number of squares in the longest chain. Each individual from a pool cooperates to mine every obstruct and share his pay when a square is found. In Bitcoin it is perceived that it is outlandish that a solitary homegrown excavator utilizing an ASIC for quite a long time could mine a block[4]. At that point singular excavators readily enter the enormous pools to expand their incomes. While entering a pool doesn't change the normal pay of an excavator, it lessens the change and expands the normal pay of a month.

In Ref [1], the mining methodology is named narrow minded mining procedure if a mining excavator or pool diggers basically discover an alliance and cover it up furtively without consequently distributing it in the convention that purposely forks the chain, as it is expressed in the convention. It causes a pool of enough size to accomplish a pay higher than its mining energy proportion, as seen in Ref.[1] and later in Section 4. On the off chance that all excavators embrace the Bitcoin Protocol, the portion of payouts in a pool or a solitary digger is equivalent to the PC power it manages (out of the computational assets of the whole organization). At that point clearly, an egoismic mining procedure permits pool excavators or a solitary digger to acquire than their mining limit. Higher incomes can lead new diggers to enter a prideful mining pool that permits the free mining pool to develop into a larger part (regarding hash power).

The fundamental knowledge into the covetous mining system is to force legit diggers to complete inefficient counts in the stalky public area. Specifically, prideful mining makes fair diggers contribute their cycles on squares not intended to turn out to be essential for the blockchain. Selfish diggers achieve this point by uncovering their mining squares to specifically refute their fair mining work. The avaricious mining pool keeps up its mined squares generally secretly, furtively forks the blockchain and sets up a secretly held branch. The legitimate excavators are currently beginning to mine the more limited public area. Since self-sufficient diggers control a moderately little part of the general mining limit, their private area won't remain always in front of the public area. The egotish diggers at that point open to general society carefully obstructs from the private area so some legit excavators venture into newfound boundaries, leaving the more limited part of the public area. This waste their past endeavors on the more limited public area and encourages the insatiable pool to support higher incomes by adding more squares into the blockchain.

This summary gives you a complete description of the selfish mining strategy presented in ref.[1], Algorithm 1. Mining events by the egoistic pool or the other push the strategy. Its decisions only depend on the relative duration of the private pool against the public sector. The operation of the autonomous mining strategy is best demonstrated by using sample scenarios of various lengths of the private and public sector.

Therefore, when its private branch falls behind, the greedy mining pool adopts simply the main branch. As many others discover and publish new blocks, the latest headquarters updates and mines. The greedy miners hold this block to the pool in private rather than naively publishing it and informing the rest of the miners of the newly discovered block. Two potential results are at this stage. This results in a leap where either branch can gain. This results. Egotistical miners are embracing and expanding their previously private branch unanimously, and honest miners, based on news, can choose between branches. In the event that the self-absorbed pool figures out how to remove the accompanying square from the legitimate excavators who have not taken on the square as of late found in the pool, it in a flash distributes to profit by the income of both the first and the second squares of its industry. At the point when the self-seeker pool figures out how to locate a subsequent square, it builds up an agreeable two-block lead which offers it some cover to keep the legit excavators from finding it. At the point when the pool shows up, it holds mine at the highest point of its private branch. For each square the others will discover, it distributes a square from its private branch. Since the egotistical pool is a minority, its existence is presumably reduced to one block at long last. The pool is publishing its private branch at this stage.

They are not conscious of the hidden extension blocks and keep mining and publishing their mining blocks and solutions in line with the standard protocol. The danger to the pools is that if they have formed exactly one lead by mining the block that they have kept secret, by keeping their blocks clandestinated, and then they are telling themselves that the group has mined a block (honest block), then they do not get the loan for the block. The selfish approach allows the pool to publish the block sooner it hears about, so that this risk can be minimised. The potential discovery of the block in this branch gives the pool a reward. Following the standard implementation of the Bitcoin protocol, the honest miners are on my branch.

In particular, the egotistical methodology without assessing the postponement in engendering of organization information is profitable (as in it gets too much) where the hash limit α satisfies the condition (1). The singular thing that can be seen is: if contact delays are invalid, that is, if the correspondence time period between any two diggers is endeavored to be unimportant (tallying charming tanks), as they expect by the Eyal and Sirer terms in Ref. [1] (see Formula 1), the base PC power prerequisite (the limit) is among (if) and beneficial

childish mining (if). They likewise recommend a basic in reverse viable steady improvement to the Bitcoin convention to build the 0 to 0 edge (Section 6 of [1]). Note that the paper[1] dealt only with the income obtained by an attacker in accordance with the egotistical mine strategy, suggesting an alternative protocol to increase the level of the computational danger required for profitable self-mining. The likelihood of success or failure of the selfish attacks is not given by other authors[1] as quantitative value. The emphasis was on the income generated by the selfish mining pool and the impact of the data spreading delay in the network was not taken into account.

Their findings are relevant and notify Bitcoin users of the security predictions of the Bitcoin Network in Ref. [5]: the α hash power must be at a minimum of the overall network hash power. Their results are highly significant. The threshold of an effective attack on the network demonstrated by Nakamoto is β. The honest culture is starting to spread in the greedy technique before dishonest miners have heard it and then there is a further pause in propagating it before other honest staff arrive. In the event of propagation delays, the natural intuition is that α is likely to be very tiny.

3. MINIMIZING NETWORK PROPAGATION DELAY

We assumes that we have an egoistic miner who is able to remove in race conditions two or more blocks. The selfish miner's target is to measure and maintain valid blocks in a private chain in order to create a barrier against honest miners. The assailant thus wants the network's lengthened private chain to transform and discard the honest miner's block. If this is the case, the attacker would like to see his private chain being at least a block longer than the main blockchain, which will persuade the network to prove its function longer and persuade them to move.

A. Assault Baseline

A greedy miner creating two blocks, BS1 and BS2, and forking the main blockchain to invalidate honest miner's block BH is the simple attack technique. The attacker rents Bitcoin from NiceHash for 10 minutes for 50 percent hash power. There are two rounds of the attack series. The attacker calculates the first block, BS1, using its own hash power in the first round. As a result, the network changes into the greedy miner's forked private chain and refuses the honest miner's block.

4. COMMUNICATIONS.

We use the notion of "truth state" to address this attack for blocks on the fork so that automatic mining behaviours are known. In the transaction data structure, we attach a parameter of "expected confirmation height." The tallness of the square in blockchains is the record number that shows its area in the chain. Another square will add a factor of 1 to the chain tallness. The assessed tallness of the affirmation is the number list of things to come block for which the exchange is probably going to be mined, contingent upon the size of the exchange, the mining charge and the memory pool size. The exchange is focused on by the mining charge and the exchange size. The priority factor indicates that a miner is driven to choose his block transaction. If mining costs are high and the size of the transaction is low, they are more likely to make this transaction their priority. The Memory Pool is a repository for unconfirmed transactions in blockchains. When the memory pool is high, a transaction backlog is generated, and outstanding transactions must wait for mining.

The exchange is probably going to be mined under typical mining with 90% unwavering quality in the objective square. Along these lines, all exchanges in the objective square will have a normal affirmed tallness equivalent to the genuine square stature. It is utilized to give

a "truth status" to the square and to trap selfish diggers who digress from conventional mines. We will explain our style in the following.

Algorithm 1: Detecting Selfish Mining
State: Fork on blockchain FS
Inputs: BSi , BH; 1 Sstate = XSn − (Pp j=1 E(T xj)) p ; // Truth state for selfish miner
2 F state = XS1 − (Pp j=1 E(T xj)) p ; // Future state for selfish miner
3 Hstate = YH − (Pq k=1 E(T yk)) q ; // Truth state for honest miner
4 if (Hstate < Sstate or F state < 0) then
5 Reject BSi ; // Reject selfish miner
6 else
7 (Hstate > Sstate) ; // Circumvention
8 Asize = 0
9 foreach p ∈ BSi do
10 Asize = Asize + p ; // Compare number of transactions
11 if (q > Asize n or Asize = 0) then
12 Reject BSi ; // Reject if transactions size is small
13 else
14 ccept BSi ; State: Normal State NS

5. RESULTS

For example, in Bitcoin, an online services known as "earn" employs simulation techniques in Monte-Carlo to predict the anticipated confirmation height of a 90% trust transaction [4]. Their criteria for simulation take the transaction backlog, the miners fee priority over the last three hours and the incoming transaction rate as input. Based on these criteria, Earn forecasts the expected confirmation amount and the expected transaction delay.

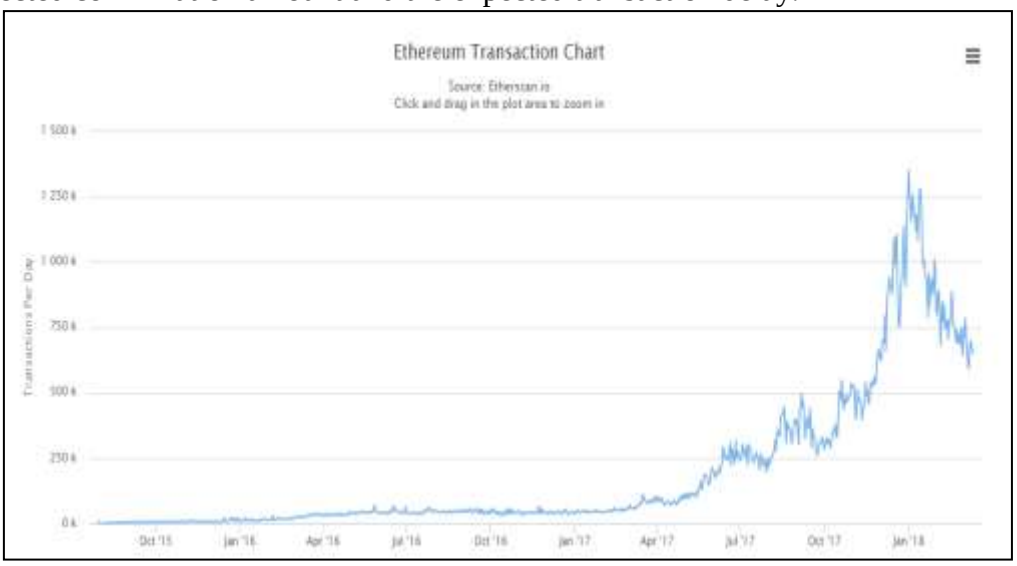

Figure 1: Ethereum Transaction Chart

This algorithm can also be applied to the users' software clients in order to allow their software client to measure the expected block confirms and apply it to the operation until it is broadcast on the network when the user produces a transaction.

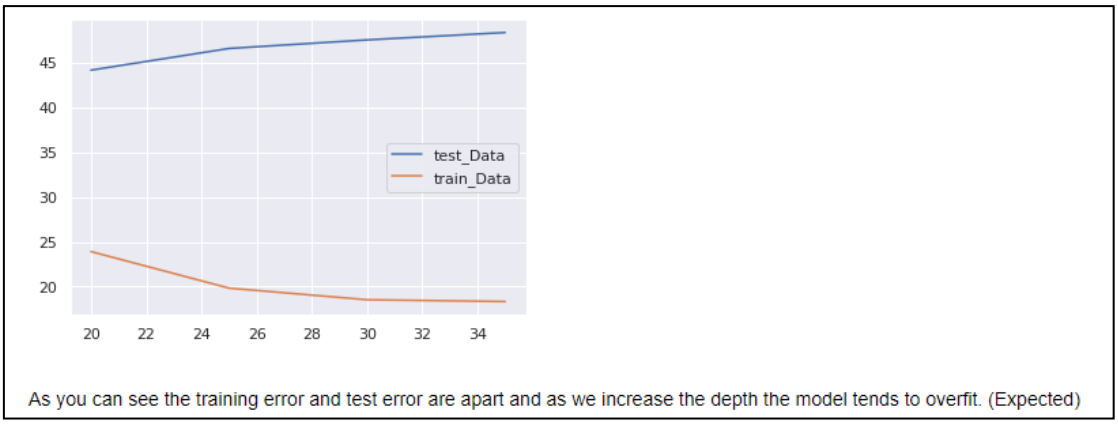

Figure 2: Random Forest Graph

Model 2: Recurrent Neural Networks with LSTM and GRU

Bitcoin2015Daily => Contains all the prices aggregated by day.

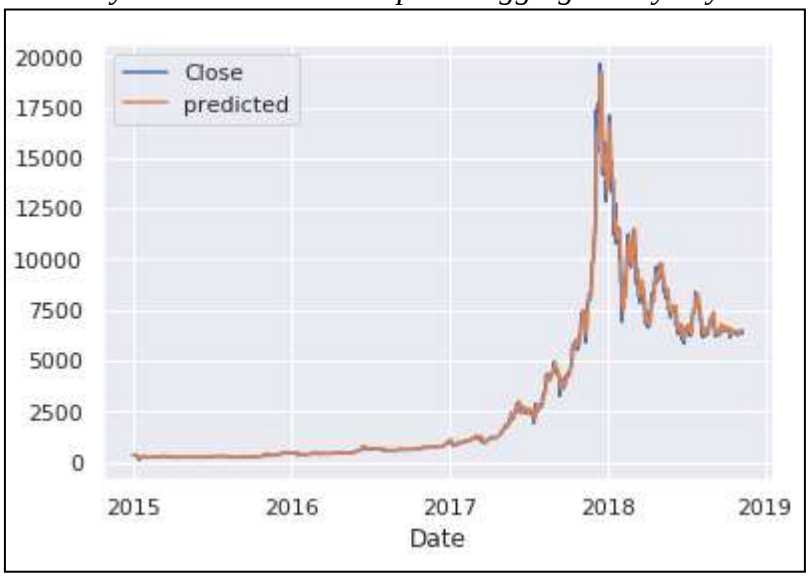

Figure 3: Comparison of prices predicted and actual price.

6. CONCLUSION AND FUTURE WORK

We describe the essence of the attack and show its benefit marge. We review the previous study and address its methodology and limitations. We use genuine mining practises to counter this strike to formulate a "truth status" notion for blocks during egotistical mining. Each transaction is assigned the expected confirmation height to detect egoistic network mining behaviour. Our algorithm proposed effectively deters selfish mining and supports equitable mining practises. In addition to the overhead phase for the implementation of our algorithm to the consumer, we will be able to estimate the overhead charge for including the expected confirmation height in each transaction.

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]. D. O. Jaquet-Chiffelle, E. Casey, and J. Bourquenoud, "Tamperproof timestamped provenance ledger using blockchain technology," Forensic Sci. Int. Digit. Investig., vol. 33, p. 300977, 2020, doi: 10.1016/j.fsidi.2020.300977.
[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]. R. Martino and A. Cilardo, "Designing a SHA-256 processor for blockchain-based IoT applications," Internet of Things, vol. 11, p. 100254, 2020, doi: 10.1016/j.iot.2020.100254.
[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]. S. A. Surdi, "Space Situational Awareness through Blockchain technology," J. Sp. Saf. Eng., vol. 7, no. 3, pp. 295–301, 2020, doi: 10.1016/j.jsse.2020.08.004.
[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. Shasi Anand, 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]. S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," J. Inf. Secur. Appl., vol. 54, 2020, doi: 10.1016/j.jisa.2020.102554.
[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]. G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi, and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," Sustain. Comput. Informatics Syst., vol. 28, no. October, p. 100464, 2020, doi: 10.1016/j.suscom.2020.100464.
[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]. J. L. Ferrer-Gomila and M. F. Hinarejos, "A 2020 perspective on 'A fair contract signing protocol with blockchain support,'" Electron. Commer. Res. Appl., vol. 42, no. May, p. 100981, 2020, doi: 10.1016/j.elerap.2020.100981.
[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]. P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for Internet of Vehicles," J. Syst. Archit., no. September, p. 101877, 2020, doi: 10.1016/j.sysarc.2020.101877.
[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 cybersecure IoT and 5G infrastructure in Smart Cities," J. Netw. Comput. Appl., vol. 175, p. 102909, 2021, doi: 10.1016/j.jnca.2020.102909.