Volume: 5, Issue: 3
Page: 71-82
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions

Ibrahim Shamal Abdulkhaleq & Shavan Askar

Abstract:

Blockchain technology has lately become widely regarded, partially because of the surge in cryptocurrencies such as Bitcoin and their ability to be a force for economic and financial shift. While tokenomics also helped push blockchain in mainstream, this technology's strengths are far more than crypt-monetary. Often known as distributed leader technologies, it is hypothesized that blockchain would serve like a catalyst for global disruptions and that blockchain-based applications in many industries such as the supply chain; the medical and legal fields are now being developed and implemented. By simultaneous research, we prove that the six confirms convention is vulnerable to peer-to-peer latency in the network and show just how readily PoW mining is broken. The divergences between these latest blocks open the transactions in question to the possibility that the blockchain fork will not be used. We concentrate on evaluating block detection accuracy and the breach of the six confirmed blockchain agreement.

IJSB
Literature review
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4497512

Keywords: *Blockchain, network latency, PoW, cryptocurrency, IoT.*

About Author (s)

Ibrahim Shamal Abdulkhaleq, Information System Engineering, Erbil Polytechnic University, Erbil, Iraq.
Shavan Askar (Corresponding Author), Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

1. Introduction

There are special properties in Blockchain. When data is used in a committed blockchain contract, it is in practice unchanged. The unchangeable sequence of past transactions authenticated by cryptography does not replicate stored data. Cryptographic tools also promote data privacy, offers open public access to blockchain data and fair protection empower each participant to access and exploit a blockchain in the same way. The communications between nodes in the network gain trust in the blockchain. Blockchain network users depend instead on the blockchain network itself to render transfers easy for trustworthy third parties who have the capacity to monitor and exploit the mechanism and are a single point of failure. Blockchain opposed both data protection and scalability. There are no privileged users, and each member may access the details on the Blockchain through the network. The secrecy is limited. Through increasing network latency, the block convergence of blockchain can quickly be broken down. Ideally, nodes can listen as easily as possible to freshly mined blocks. Faster delivery to a new block's network encourages other nodes to verify it faster, encouraging the blockchains to update for the new block that is validated. The blockchain would thus stabilize in shorter timeframes to a globally converged state. However, as network latency decreases, the blockchain is far more likely to form forks because various nodes remove several new blocks. The diversity of new blocks will lead to honest nodes becoming confused about which fork is the longest chain, destabilizing global consensus.

The disparity between these new blocks opens the subsequent transactions to the possibility of a not adopted blockchain fork. Nodes with lower latency can gain disproportionate control over greedy mining when situations with variable network latency are present in various nodes. Modern technologies designed for high-latency communications in the network context, blockchain protection might become vulnerable by delaying communication between blockchain maintainers (Choubey et al., 2019). The important thing is that Blockchain consensus algorithm only guarantees probabilistic accuracy. Solid continuity may bring three essential benefits to cryptocurrencies. Second, any mining company immediately agree on the validity of blocks without wasting computer resources to fix discrepancies (forks). Secondly, consumers do not wait until lengthy times are confident a requested transaction will be committed; the transaction can be deemed as validated as soon as it occurs inside the blockchain. Third, good durability offers protection for the future: when a block is added to the blockchain, it remains for always. While the consistency of cryptocurrencies has been proposed, current proposals abandon blockchain de-centralization and/or implement fresh and non-intuitive security assumptions or refuse to show efficiency and scalability experimentally (Zheng et al., 2020; Sulaiman & Askar, 2015; Fares & Askar, 2016)

2. Literature Review

According to Vukolić (2015), across the thousands of nodes, the utility of the globe has been particularly demonstrated by the Bitcoin cryptocurrency. It is also necessary for various other processes and perspectives. Due to such kinds of various terms, digital transactions are changing the world forever. In the initiating time of the Bitcoin, its performance was probably lower, and later on, it has become faster. The consequences fabric was introduced particularly for the probabilistic proof of work. This particular term and process are known as the blockchain which was not considered as the major issue. The study of Vukolić, (2015) is particularly contrasted the PoW based blockchain with the BFT state replication machine (Vukolić, 2015). As indicated in the study of Kuzlu (Kuzlu 2019), This study is particularly focusing on the most important and famous source of the blockchain frameworks, which is particularly known as the Hyper ledger fabrics. The particular study examines the effect of the workload of the network for the performance platform of the blockchain. In this study, the platform of the Hyperledger Fabric is evaluated particularly in specific terms of the throughput. It includes latency, scalability, and successful transactions. The specifications of the blockchain, also include the time responses per transactions. It also includes the scale scalability of the participants in specific manners (Kuzlu, 2019).

According to Yazdinejad (2020), The technology is considered as a dispersed record without any concentrated administration that is particular utilized to store entire exchanges of transactions which prompts a lot of information that increments after some time. The gadgets of IoT are generally obliged in energy, stockpiling, and calculation. These are probably not utilized for going to have the option that is required to store all information of blockchain. An Enormous Amount of information sums will be more articulated along with the expanding IoT gadgets and blockchain use cases including IoT. It also includes the current implementation that is required for blockchain and it also utilized for friendly IoT (Yazdinejad, 2020). According to King (2012), to From Satoshi Nakamoto's Bitcoin A shared cryptographic money configuration has been got derived. In order to give the majority of the organization security, the evidence of-stake replaces confirmation of-work is required. By considering such kinds of the particular design of the verification of-work chiefly, it gives largely nonessential as well as initial minting in long run. The level of security of the organization isn't subject to utilization energy in the drawn-out along with these lines in order giving an energy effective as well as peer to peer cryptocurrency that is more competitive than others. On the coinage confirmation, of-stake depends as well as it is created by every hub through a hashing plan bearing comparability to Bitcoin's yet over restricted hunt space (King, 2012). According to (Crosby, 2016), The Shared advanced cash is decentralized by Bitcoin that is considered the most well-known model utilizes for the innovation of blockchain. The advanced and mostly innovative cash bitcoin itself is considered as the exceptionally disputable that is referred to as the fundamental of the technology of blockchain. It has worked faultlessly and discovered wide scope of utilization in both worlds monetary and non-monetary. It is considered as the primary theory is that the blockchain is utilized to builds up an arrangement of making a conveyed agreement in the computerized online world. This is required permits taking an interest substance to know for sure that a computerized occasion occurred by making an undeniable record in a public record. It is specifically utilized for opening the entry that is required for building up popularity which is based on the adaptable computerized economy from a various concentrated one (Crosby, 2016).

Alrubei (2020), has explained For some applications, the Internet of Things (IoT) and its products are progressively being used by the individual and organization both. In various kinds of smart devices, this usage implies increments that are associated with the Internet of Things. It will altogether utilize to build the difficulties that are identified with these specific devices. It includes interconnectivity and the executives, information and client protection, and organization, information, along with the security of devices. Simultaneously, the approaches blockchain gives a decentralized, permanent, and technology of peer to peer ledger that could be the correct response for all of these various challenges. In any case, Huge difficulties go with the mix of blockchain into the Internet of Things. Since the smart devices of IoT may experience the bad effects of asset and force requirements. Blockchain is related to adaptability and postpones issues (Alrubei, 2020; Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015). Astarita (2020), has indicated in this study that The particular literature is presented in the study of the Astarita, (2020) that is related to the use of blockchain which is based upon the frameworks in transportation. The major principle point that was required to recognize, by considering the usage of a multi-step technique. It includes momentum research patterns, fundamental holes in the writing, and conceivable future difficulties. Initially, a bibliometric examination was done to acquire an expansive diagram of the subject of interest. In this way, the most persuasive commitments were analyzed particularly for a top to bottom. It is also concerning the following two regions: street traffic the board and keen urban areas store network and coordination's. According to Gervais (2015), in the particular study of Gervais, (2015) the current scalability of the measure has been presented. It is adopted by Bitcoin that is come with various security systems. The systems of the bitcoin can not be explained easily. Specifically, this paper is conducted to present an adversary exploit that is required to effectively measure propagation that has been delayed. It also includes the transaction which are required blocks the specific nodes. It is also required for siderbale amount of time by considering its causes network partitioning in its particular systems. It includes the information which is specifically received by the nodes of Bitcoins. It utilized to modifies their various views of ledger states. Bonneau (2015), has explained in his study As the cryptographic currency most popular in history, Bitcoin has appeared. Within two years of Bitcoin's quiet 2009 debut, amid just a cursory study of the system's architecture, it expanded to contain billions of dollars. Since then, increasing literature, the system's secret but essential virtues have been established, attacks uncovered, promising solutions suggested and threats for the future identified. In the meantime, a broad and diverse open-source group has introduced and adopted several amendments and extensions. We give the first Bitcoin structural exposure and the underlying cryptocurrency or 'altcoins.' We define the three key elements of Bitcoin's architecture which can be isolated from a broad range of information. Thus, Bitcoin's properties and potential viability are analysed more thoroughly. The room for several suggestions is mapped, comparative analyses of alternative consensus structures, currency allotment mechanisms; machine puzzles and key management instruments are presented. In order to evaluate a number of data security proposals, we review anonymity problems in Bitcoin and have an appraisal structure. Finally, we offer new ideas on what we call disintermediation protocols, which absolve the need for trustworthy intermediaries in a fascinating range of applications. We define three general disintermediation methods and offer a thorough comparison (Bonneau, 2015).

According to Putri, (2018) the highest market share of all digital currencies lies with Bitcoin. Transaction protection in Bitcoin is protected using the hash-based work proof (PoW) mechanism of blocks. Bitcoin PoW takes an average of 10 minutes to complete, and for a single device transaction, six consecutive blocks are recommended. PoW is a functional protocol validating all incoming data for spam and DDoS attacks (Distributed Denial of Service). The ego miner is an infringement on Bitcoin's dignity. It is successful because fair miners have to spend part of their machine cycle on the blocks not to be in the public chain. The greedy miner is successful. In order to achieve better scalability, the network latency must be minimal, which decreases the amount of time taken to validate the transaction. The author will calculate the effect of block latency in Bitcoin time with a selfish attack using NS3 in this analysis. In this study the author The test results indicate that the latency variance is applied, and the lower the MBRT value, the more produced blocks. The average MBRT of each parameter indicates the reception time required by the number of blocks between about 15 and 16 minutes. This extends the time limit for the resistance of PoW while transacting. The egotism of miners and latency is accountable. As indicated in the study of Choubey et al., (2019), There is a need for a highly safe and privacy-protected transaction environment in a decentralised V2V energy trading between electric vehicles (EVs). Most blockchain apps have a similar cryptocurrency infrastructure for safe processing as digital currencies such as

Bitcoin come into play. In this piece, we suggest a blockchain-based approved electrical trading mechanism to improve the protection and privacy of the details of the EV customer. We are launching a new "ETcoin" crypto-currency for electricity trading. All of this matched offers are held in blockchain with a traded power unit and exchanged ETcoins. Using large-scale Big Data Analytics, the transaction graph generated by the energy trading can be analysed. Current works have not dealt with blockchain technology to process massive energy trading transaction graphs. Analytics was considered for any blockchain transactions submitted over a pre-defined duration. For Blockchain analysis of broad-scale transaction graphs we suggest an Energy Exchange Rank (ETR) algorithm. ETR algorithm uses the Weighted Ranking method to measure the ETR score for each VR over a traded time, which takes into account both the edge and vertex properties of the graph. Transaction graph analytics on trade in energy serve to prove its activity and to enable the EVs to engage in the most environmentally friendly way. We used IBMs hyperladen cloth, composer with reduced transaction delay and in-time device templates for each participant in the system. We applied the blockchain based Proof of Concept (POC). For real-time, dataflow processing distributions, transaction graph analytics are deployed using Apache Spark's open-source GraphX library. Transactions are modelled as edge triplets on many computers, and ETR score is determined to converge with a set of tolerances for any vertex at the same time. The simulation results show that, as parallel machines grow, the algorithm converges faster and scaled better. We also evaluated that the total reward benefit for EVs with optimum, real and dedicated participation improves so the scheme is active (Choubey et al., 2019; Askar et al., 2011; Al Majeed et al., 2014). According to Conti, E, Lal, & Ruj (2018), Bitcoin is a common cryptocurrency that contains the details in a distributed appended-only public ledger called blockchain. Bitcoin's protection primarily depends on the distributed consensus protocol based on the reward compliant proof-of-work (PoW) mechanism operated by the miners' Networks. The miners are required to preserve the blockchain sincerely in substitution for the opportunity. Bitcoineéconomie has risen at a tremendous pace since its introduction in 2009 and now stands at some 150 trillion dollars. This rapid increase of bitcoin market valuation motivates adversaries to take advantage of loopholes and scientists to identify new device flaws, propose countermeasures and foresee the coming developments. In this article, the security and privacy dimensions of Bitcoin have been surveyed extensively. We begin by presenting a summary of the Bitcoin framework and its key components and their operating characteristics and interactions (Conti, E, Lal, & Ruj, 2018).

We review the current vulnerabilities in Bitcoin and the main underlying technology like blockchain and a consensus protocol centred on PoW. These vulnerabilities lead to numerous security threats against Bitcoin's standard function. We then evaluate whether state-of-the-art safety solutions can be practical and durable. In addition, the latest anonymity issues of Bitcoin and the safety risks to consumers of Bitcoin are addressed as well as analyses of established secrecy solutions. In conclusion, we outline the crucial open problems and offer recommendations for future investigation to provide Bitcoin with rigorous protection and privacy solutions (Conti, E, Lal, & Ruj, 2018). As indicated in study of Ersoy et al. (2018) Current blockchain technologies depend on structures of peer-to-peer spread where nodes are receiving their neighbours during a network transaction. Unfortunately, such transaction propagation would not give explicit rewards. Therefore, in a completely autonomous blockchain with rational nodes, current dissemination processes would not stay viable. In this work, the problem with incentivizing transaction propagation nodes is described formally. We are suggesting an incentive system in which the transaction fee is shared to each node participating in the spread of a transaction. We also explain that Sybil is our proposal. We also integrate the reward mechanism with intelligent routing to simultaneously reduce connectivity and storage costs. The suggested routing function reduces the redundance of the transaction from network size to an average shortest distance factor. A particular form of consensus is formed for this routing process, in which the round leader who constructs the transaction block is decided in advance. Please notice that our routing system is standardised and can be used independently of the reward mechanism (Ersoy et al., 2018).

According to Decker & Wattenhofert (2013), Bitcoin is a decentralised currency that does not count on a single authority, in contrast to traditional currencies. Instead, Bitcoin depends on a voluntary network that mutually implements and verifies the transactions. In this paper we discuss how Bitcoin uses multi hop transmission to distribute transactions and network blocks to upgrade replicas of the LED. We then use the information obtained to validate that the network spread delay is the key cause of blockchain forks.. Blockchain forks should be avoided because they are symptomatic of incoherence of the network replicas. We further demonstrate what can be done with unilateral improvements in the actions of the customer by bringing the new protocol to the limit (Decker & Wattenhofert, 2013). According to Dirgantoro, Lee, & Kim (2020), This essay proposes to acknowledge the face of the safety infrastructure focused on artificial intelligence and small data set edge computing. Generative opposing networks (GANs) are used to exploit the data set to solve the problem of the exact constraint of the data set. The average precision of GANs reaches 92.79% of the minimal results. Edge computer is used with the Jetson Nano board to resolve the cloud delay, which creates an average of 8.8 frames per second. In addition, the sensed face pays for the blockchain network with low static difficulties in opening the door or door lock by means of an intelligent contract. In contrast, the demonstration of consent algorithm in transaction times of around 33-39 milliseconds is exceeding a low static complexity (Dirgantoro, Lee, & Kim, 2020). According to Dorri, Steger, Kanhere, & Jurdak (2017), Linked smart vehicles provide a range of advanced car owners, traffic agencies, automakers and other service providers with a wide range of services. This could open intelligent vehicles to a variety of risks to safety and privacy, such as location detection or remote hijacking. In this post, we suggest that the groundbreaking platform blockchain (BC), which discovers multiple technologies from cryptocurrency to smart contracts, may fix the problems. We deliver a BC architecture that safeguards users' privacy and improves vehicle ecosystem protection. The effectiveness of the proposed security architecture can be demonstrated by wireless remote app upgrades and other new utilities, such as car complex insurance costs. We also promote the architectural resistance to common security threats in a qualitative way (Dorri, Steger, Kanhere, & Jurdak, 2017). According to Nakamoto (2018), a variant of electronic cash solely peer-to-peer will allow the transfer of online paying money from one party to the next without a financial institution. Digital signatures offer part of the solution, but key advantages would be missed if a trustworthy third party remains essential to avoid replication. We suggest a solution to the issue of double spending using a network of pairs to pairs. The network time stamps transactions by hashing them through a dangerous proof of operating chain, making a record that cannot be altered without the proof of work being replenished. Not only does the longest chain act as evidence of the sequence of events, but it demonstrates that it originated from the greatest pool of CPU capacity. As long as most CPU power is managed by nodes which do not cooperate to attack the network, the longest chain and out-pace attackers are created. The network itself has to be organised minimally. Messages are sent on the best effort, and nodes will leave and re-enthusiastically rejoin the network and embrace the longest evidence chain to show their mistake (Nakamoto, 2018).

As indicated in the study Fabiano (2017), The IoT is revolutionary and important, but should take into consideration the legal problems relating to the data security legislation, as well as applications for different services. Legal problems relating to data security and privacy legislation should, however, be taken into consideration. It is welcome to have technical solutions, but the threats that we cannot overlook need to be addressed before designing applications. Personal knowledge is worthwhile. The assessment and prevention, taking the privacy in each project by design approach, is important in this sense. In this context. With respect to privacy and protection threats, certain concerns with possible data security and liability implications are present. We can move data on the Internet, including personal information, via the IoT device. The latest European General Data Protection Regulation (GDPR), which will apply on 25 May 2018 and has been in effect since 24 May 2016, is relevant to remember in this sense. In the light of infringements of the Law, the GDPR is implementing data security evaluation (DPIA), data breach information and very serious administrative penalties. A thorough legal review encourages risk management to be undertaken to avoid the abuse of sensitive knowledge (Fabiano, 2017).

The IoT environment evolves rapidly with numerous implementations in the diverse fields. Big Data and the blockchain are the key subjects for the last time. Because of its future specific use for utilities and software, the more recent is provided priority and improved safety steps are taken to ensure a stable device. But analyzing the legal questions leading to them is equally relevant. Everyone has the freedom to defend his or her personal records. Here we cannot refuse the promise that any programme is appropriate to secure sensitive data. We cannot reject the appeal. The contribution discusses the key legal issues relating to the security of privacy and records, notably with regard to the blockchain, focussing on the GDPR approach to privacy by design. I sincerely assume, however, that it would be possible for companies to create a global privacy standard system for data security. According to HAFID, HAFID, & SAMIH (2016), It was a lot recognized and widely extended in recent years by Blockchain (e.g. Bitcoin and Ethereum). But the scalability of blockchain continues to be an obstacle. This paper outlines the current solutions to the scalability of blockchains and can be divided into two categories: first layer, and second layer solutions: first layer, secondary layer solutions, first layer solutions, and block chaining frameworks. We focus in particular on sharding the scalability problem as a promising first layer solution; the core concept behind sharding consists of breaking up the blockchain network into numerous commissions, each handling a different collection of transactions. In specific, (a) we are proposing a taxomy focused on intracommittee consensus and committee membership; and (b) we are contrasting the key current blockchain protocols based on sharing. Furthermore, we present the advantages and drawbacks of current scalability technologies in a performant comparative study (i.e., efficiency and latency) (HAFID, HAFID, & SAMIH, 2016). Hari, Kodialam, & Lakshman (2018) has explained that The Bitcoin blockchain is a decentralized, distributed directory that facilitates trustworthy transactions between non-reliable businesses. However, certain implementations need much quicker transaction recognition than the existing Bitcoin blockchain. In this article, we are proposing an extremely successfully developed, low-latency definite method called ACCEL to accelerate the block validation mechanism of Bitcoin. The accelerated labelling of the singular components of the blockchain is our main concept for quicker proof. Since it may not be definitively established if a block belongs to a blockchain while the netbound delays are infinite, a special block identification shows that the bottom-to-bottom latency of Bitcoin miners is considerably below and can be supposed to be upper restricted. ACCEL is particularly appropriate for low-latency blockchains where block spacing can be tailored for the limited latencies of the network to increase the output dramatically. With comprehensive simulations and actual execution, we test ACCEL's performance, designed with minimal adjustments and completely compliant with the Bitcoins blockchain. We demonstrate that transaction validation latencies can be reduced with ACCEL to milliseconds and thus satisfy performance requirements of a large variety of applications with adequate constraints on end-to-end latency (Hari, Kodialam, & Lakshman, 2018). According to Khan, Jung, Hashmani, & Waqas (2020), In recent years, academics and business experts have paid considerable attention to state-of-the-art Blockchain technologies. Blockchain is essentially a global, immutable, user-focused blockchain network that uses transactions exclusively through multiple nodes through a shared awareness of all the related network nodes. Blockchain is known for the cryptocurrency of Bitcoin. Blockchain has had multiple applications with a global valuation of 150B disrupted since 2017. The consensus models are responsible for committing to a new block between all blockchain nodes. The consensus paradigm plays an important role in preserving productivity in Blockchain. Using the proper consensus model, the efficiency of the blockchain can be greatly improved. There are two types of consensus structures. The first type is the evidence-based consensus model, which offers enough evidence for a node in the Blockchain against other nodes to allow the next block to be put in the chain. The second type is the voting model in which nodes must share their votes before they validate a new block transaction. In this document we examine the features and critical feedback on the performances of some of the most current consensus models. These factors are analysed primarily for transaction throughput, latency, bandwidth of the network and storage (Khan, Jung, Hashmani, & Waqas, 2020).

As depicted in the study of Kosba, Miller, Shi, Wen, & Papamanthou, (2016) Key element contract structures over decentralised cryptocurrencies allow mutually distrustful parties without trustworthy third parties to transact safely. The transparent blockchain guarantees that honest parties are paid for mutual breaks or abortions. Yet there is no transactional anonymity on current networks. Both transfers, including cash flow between pseudonyms and transactions in the number, will appear on the blockchain. We introduce Hawk, a decentralised intelligent contract scheme that does not clear up financial transactions in the blockchain and hence maintains public transactional anonymity (Kosba, Miller, Shi, Wen, & Papamanthou, 2016). According to Poon & Dryja (2016), The bitcoin Protocol will now include the global volume of financial transactions in all e-payment networks without any single third-party custodial supported or enabling participants to use a broadband link on a device. A decentralised mechanism is proposed under which micropayment networks (i.e. payment channels or transaction channels) are sent via a network of transactions of off-blockchain exchanging value. If Bitcoin transactions can be signed with a new form of sighash that resolve mixability, such transfers can take place between untrusted parties along the transfer path, under agreements that can be implemented, in the case of unco-operative or aggressive party, by a sequence of decremental time blocks, through a Bitcoin blockchain broadcast (Poon & Dryja, 2016).

TABLE 1: AUTHOR BASED COMPARATIVE ASSESSMENT

Auhtors and years	Objective	Algorithms	Tool and Technique	Significant Results
(Vukolić, 2015)	To analyze the PoW-based blockchains to those based on BFT state machine replication	POW and BFT	Byzantine fault-tolerant (BFT Crypto currency	The study is contrasted the PoW based blockchain with the BFT state replication machine.
(Kuzlu, 2019, July)	To examine the performance analysis of the two versions of Hyperledger Fabric, v0.6 and v1.0.	Hyperledger Fabric, v0.6 and v1.0.	It results evaluates throughput, metrics, scalability, execution time and latency	platform of the Hyperledger Fabric is evaluated particularly in specific terms of the throughput

(Yazdinejad, 2020, May)	To explores the various aspects of Secure and Low latency Proof of Work (SLPoW) protoco	Field-programmable gate array (FPGA), Proof of Work (PoW)	In order to improve the processing speeds of computation Field the programmable gate array (FPGA) has been used	The gadgets of IoT are generally obliged in energy, stockpiling, and calculation.
(King, 2012) (Crosby, 2016)	To explores the process if the block chain history and transaction settlement	PPCoin	hybrid design proof-of-work	It gives largely nonessential as well as initial minting in long run
(Alrubei, 2020)	To explores the topic of the current research challenges along with block chain future direction	Systematic literature review	To explain the technology of the Bit coin by considering Bitcoin	It has worked faultlessly and discovered wide scope of utilization in both worlds monetary and non-monetary
(Astarita, 2020)	To demonstrates a blockchain practical incorporation that is required the Internet of Things	Ethereum Proof of Authority (PoA).	Performance analyses,	The smart devices of IoT may experience the bad effects of asset and force requirements.
(Gervais, 2015)	Major aim to explores the trends of the research along with the implementation of the multistep methodology	bibliometric analysis	multi-step methodology	Initially, a bibliometric examination was done to acquire an expansive diagram of the subject of interest.
(Bonneau, 2015)	To examine current scalability measures that is adopted by Bit coin	Nit identified	Systematic review	It has been presented an adversary exploit that is required to effectively measure propagation that has been delayed.
(Putri, 2018)	To explain and explores first systematic exposition Bit coin and its relevant crypto currencies	'altcoins.'	Drawing from a scattered body of knowledge,	we offer new ideas on what we call disintermediation protocols, which absolve the need for trustworthy intermediaries in a fascinating range of applications
(Choubey, Mahidhar, Misra, Behera, & Patel, 2019)	In this study the author examine test results indicate that the latency variance is applied, and the lower the MBRT value, the more produced blocks.	NS3, MBRT	PoW) mechanism	. In order to achieve better scalability, the network latency must be minimal, which decreases the amount of time taken to validate the transaction.

3. Discussion

In the 21sy century it has become very important that the information related to transaction is transparent. When the information related to transactions is going to be transparent than the issues such as fraud or manipulation of information will not occur. Block chain technology is like a ledger which is distributed to each individual who is the part of a network. It means that block chain increases the transparency of the information. This research will try to evaluate how much transparency does the block chain technology provides and how it reduces the risk related to frauds. As discuss earlier the aim of the research is to provide deep insights regarding the risks & benefit of the Block chain technology.

The research will evaluate the benefits of this technology from different aspects such as security, accuracy, efficiency, cost reduction and traceability. It is very important for any organization to perform its finance related activities efficiently otherwise various issues can arise which not only decrease the performance of the organization but also profitability of the organization decreases as a result. There is a need of such technology which improves the security and efficiency of the activities so that organization can manage its financial activities more accurately. Block chain technology has proved beneficial for finance related activities or transactions because not only the speed of the process increases but also the security of the process also increase as a result of this technology. However it is not known how much block chain can support organization and whether its benefits are more than the risks or not. Furthermore, the cost and challenges, at present, associated with a blockchain technology use for recordkeeping of the public of Vermont outweigh the identifiable benefits. The authors of this research emphasized that providing the blockchain technology's legal recognition may create the advantage as a "first mover" with the potential to bring the activity of economy surrounding the blockchain technology's development to Vermont. However, according to the authors, this potential is challenging to capture and difficult to quantify because of the nature of technology.

It has bee discusses in this study that Bitcoin cryptocurrency, blockchain technology is characterized as the decentralized, distributed, open source database for storing information of transaction. Rather than trusting the centralized intermediaries such as banks or other financial institutions, two parties are allowed by this technology to transact directly using linked and duplicate ledgers known as blockchains. Accordong to the authors, blockchain technology makes transaction more transparent than the other centralized systems. Transactions, as a result, are executed without relying on the third party. Moreover, the authors have credited the blockchain in bringing transparency of supply chain to the new level, but, according the authors, currently managerial and academic blockchain technology adoption is limited.

4. Conclusion

It is concluded that cryptographic tools also promote data privacy, offers open public access to blockchain data and fair protection empower each participant to access and exploit a blockchain in the same way. The diversity of new blocks will lead to honest nodes becoming confused about which fork is the longest chain, destabilizing global consensus. The important thing is that blockchain consensus algorithm only guarantees probabilistic accuracy. Solid continuity may bring three essential benefits to cryptocurrencies. While the consistency of cryptocurrencies has been proposed, current proposals abandon Blockchain de-centralization and/or implement fresh and non-intuitive security assumptions or refuse. This article applies to a collective group of miners who have a stable consensus protocol on the global state. Round robin (RR) is typically used in Blockchain permitted. The method offers the ability to publish your latest block to the next node in the queue. We assess and thus revoke transactions the effect of various network latency settings on blockchain security. Relationship between winner number and blockchain length. The length of the blockchain can be seen to be purely equal to the number of winners at each network latency.

References

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Alrubei, S. M. (2020). Latency and Performance Analyses of Real-World Wireless IoT-Blockchain Application. IEEE Sensors Journal,, 20(13), 7372-7383.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 1*6th European Conference on Networks and Optical Communications*, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Astarita, V. G. (2020). A review of blockchain-based systems in transportation. Information,, 11(1), 21.

Bonneau, J. M. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE symposium on security and privacy (pp. 104-121). IEEE.

Choubey, A., Mahidhar, K., Misra, R., Behera, S., & Patel, Y. S. (2019). EnergyTradingRank Algorithm for Truthful Auctions among EVs via Blockchain Analytics of Large Scale Transaction Graphs. 2019 11th International Conference on Communication Systems & Networks (COMSNETS).

Conti, M., E, S. K., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin . IEEE Communications Surveys & Tutorials, 1553-877X .

Crosby, M. P. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, , 2(6-10), 71.

Decker, C., & Wattenhofert, R. (2013). Information Propagation in the Bitcoin Network . 13-th IEEE International Conference on Peer-to-Peer Computing .

Dirgantoro, K. P., Lee, J. M., & Kim, D.-S. (2020). Generative Adversarial Networks Based on Edge Computing With Blockchain Architecture for Security System. Authorized licensed use limited to: Auckland University of Technology, 039-042.

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. AutomotIve networkIng And ApplIcAtIons, 119-125.

Ersoy, O., Ren, Z., Erkin, Z., & Lagendijk, R. L. (2018). Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms. 2018 Crypto Valley Conference on Blockchain Technology, 20-30.

Fabiano, N. (2017). Internet of Things and Blockchain: legal issues and privacy. The challenge for a privacy standard. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Gervais, A. R. (2015). Tampering with the delivery of blocks and transactions in bitcoin. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, (pp. 692-705).

HAFID, A., HAFID, A. S., & SAMIH, M. (2016). Scaling Blockchains: A Comprehensive Survey. IEEE Access.

Hari, A., Kodialam, M., & Lakshman, T. (2018). ACCEL: Accelerating the Bitcoin Blockchain for High-throughput, Low-latency Applications. Blockchain.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *6th International Conference on Intelligent Systems, Modelling and Simulation*, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Khan, D., Jung, L. T., Hashmani, M. A., & Waqas, A. (2020). A Critical Review of Blockchain Consensus Model . 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2-6.

King, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August,, 19, 1.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 2016 IEEE Symposium on Security and Privacy, 839-858.

Kuzlu, M. P. (2019). Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability. In 2019 IEEE international conference on blockchain , (Blockchain) (pp. 536-540).

Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. 2018 Annual National Seminar.

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Blockchain Problems and solutions.

Putri, B. D. (2018). The Effect of Latency on Selfish-Miner Attack on Block Receive Time Bitcoin Network Using NS3. In 2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA) (pp. 1-5).

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In. International workshop on open problems in network security (pp. 112-125). Springer, Cham.

Yazdinejad, A. S. (2020, May). SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. . In 2020 IEEE 91st Vehicular Technology Conference (VT.

Zheng, X., Li, M., Chen, Y., Guo, J., & Alam, M. (2020). Blockchain-Based Secure Computation Offloading in Vehicular Networks . IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.

Zhong, Q. T., & Cole, Z. (2018). Analyzing the Effects of Network Latency on Blockchain Performance and Security Using the Whiteblock Testing Platform. Blockchain Performance and Security.

Cite this article:

Ibrahim Shamal Abdulkhaleq & Shavan Askar (2021). Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions. *International Journal of Science and Business, 5*(3), 71-82. doi: https://doi.org/10.5281/zenodo.4497512

Retrieved from http://ijsab.com/wp-content/uploads/687.pdf

Published by

IJSAB International