# ALOSQB: Design of an Ant Lion Optimizer for enhancing Security of QoS aware Blockchain deployments

***Manisha bhatnagar***
***Assignment professor, ISBA institute of professional studies***
***manishaprasanna@gmail.com***

**Abstract:**

Because of their dependability, increased security, and high levels of confidence, blockchain-controlled businesses are becoming increasingly prevalent in cutting-edge and medicinal Internet of Things (IoT) applications. Due to the distributed nature of their infrastructure, which enhances the protections that are already in place, these blockchains are ideally suitable for data applications that require a rapid response time. When dealing with these blockchains, however, a significant amount of processing capacity as well as memory is required. The majority of this CPU time is taken up by tedious and infrequent encryption computations, which are necessary but time-consuming. Because the information that is stored in the chain by one substance is only occasionally watched by other substances, a significant portion of the RAM that is used to keep these networks running is also wasted. An Ant Lion Optimization (ALO)-based side chaining model is proposed in this article with the goal of enhancing the functionality of blockchain technology. In this approach, the principal blockchain is partitioned into a great number of subsidiary blockchains that operate on their own. Sandboxing makes it possible for these side-chains to have the optimal memory consumption and processing requirements, which in turn makes it possible to carry out more complicated operations. It is predicted that the suggested computation will have a delay efficiency that is 4.5% lower while having an energy efficiency that is 19.5% higher than alternative blockchain techniques.

**Keywords:** Ant, Lion, Optimization, Blockchain, Sidechain, Delay, Energy, Scenarios
**DOINumber:10.48047/nq.2022.20.22.NQ10232** **NeuroQuantology2022;20(22):2426-2435**



## 1. Introduction

In recent years, blockchains have become a de facto standard for obtaining any kind of structure. [C]onsider the Ethereum blockchain, for example. Encoding information in these networks can be made more fascinating by utilizing a cycle in which data and its timestamp are connected to a nonce number. After determining the hash value of the combination, the value is compared to a number of different benchmarks. If the hash value is validated as authentic and compliant with the specifications, the hash of the parallelogram that came before it is prepended to the output. The new state of this cube is determined by how many times it is rearranged and then uploaded to the blockchain. The chain must be maintained in such a way that each square includes the hash value of the square that came before it. Only then can the blockchain be guaranteed to exist eternally. The entire transaction has to be carried out once more after the addition of a new rectangle. Figure 1 represents the entirety of the movie demonstrating how to add circles to the Bitcoin network that was presented in the previous section. In order to add a new block to the chain, there are two fundamental cycles that must be completed. These cycles consist of registering hash values with various variations of the secure hashing algorithm (SHA), encrypting blocks, validating the hash values against the supplied set of blockchain rules, and retrieving the hash values in the event that the rules become ambiguous. These two endeavours are not only

extraordinarily challenging but also demand a significant amount of computational capability in order to be successful. The longer a database has been around, the more difficult this transaction is going to be to complete for different use cases.

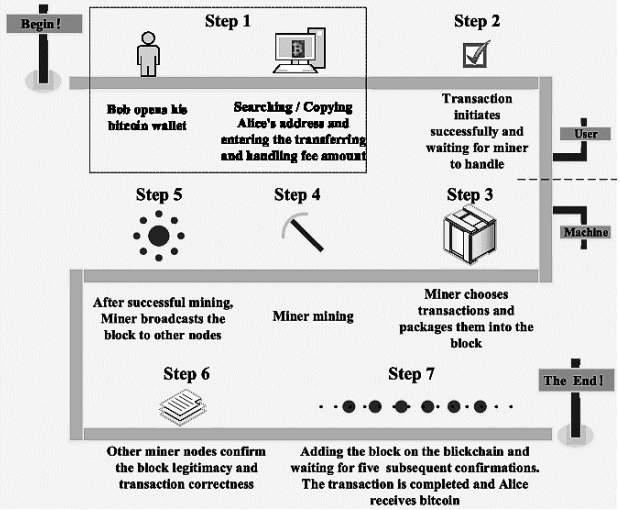


Figure 1. Process of block addition in blockchains

Because of the unchangeable nature of the blockchain network, there is an assurance that there will be an unlimited number of squares in any application. Because of this, determining the hash age is a challenging and difficult challenge. There have been several different algorithms developed that have the potential to be utilized in the complete square age procedure. Following the previous section, which offers a high-level overview of these computations as they relate to IoT businesses, the following section discusses the ALO-based side binding architecture that is recommended. The concluding portion of this article provides some intriguing perspectives on the work that is scheduled as well as some recommendations for its continued development in the future. In this concluding portion, we will evaluate the results and make any necessary correlations between the recommended computation and the actual implementation of the calculations.

## 2. Literature review

Simplifying the processing and resource needs of Internet of Things devices is a necessary condition for achieving high-quality service delivery from those devices. (QoS). However, these numbers go up as a result of the additional computational component that the system needs to have in order to incorporate the additional security features. This component is required so that the system can function properly. The writers of [1] suggest using random key management in combination with an analytical hierarchy process (AHP) for managing the application of these keys in order to keep an acceptable level of service and security in a blockchain-powered Industrial Internet of Things (IIoT) system. This would allow the system to maintain an acceptable level of both service and security. Because of this, we are able to maintain the highest possible levels of both quality and safety in our operations. The system makes adjustments to the blockchain's parameters, such as the duration of the key, the security algorithm, the agreement algorithm, and the interoperability parameters, in order to increase performance, latency, and the ratio of packets lost. These adjustments guarantee that the best performance is achieved. Finding a solution that satisfies both of these conflicting objectives is absolutely necessary in order to manage the system in a way that ensures its interoperability, convergence, and trustworthiness. According to the findings of current research, a blockchain-based system needs only a middling amount of consistency and interoperability in order to achieve a high degree of trustworthiness. [Citation needed] [Citation needed] [Citation needed] To reference [citation required] Many different types of businesses and organizations are able to take advantage of the use cases provided by the Industrial Internet of Things. To mention just a few, these businesses fall into the categories of agriculture, construction, education, energy, public transportation networks, finance, and insurance. If you look at [2], which offers a comprehensive account of the application of blockchain technology to various fields in industry 4.0, you will find a study that examines the use of blockchain technology in all of these areas. This study demonstrates that blockchain technology can improve the privacy and security of IoT networks; however, dependable methods are still necessary to evaluate the potential benefits of implementing this technology. The writers of [3] introduce a privacy evaluation model for blockchain-based systems that is constructed on a customizable scoring strategy. This model can evaluate the privacy of blockchain-based systems. The previous research done by the writers served as the foundation for this approach. The assessment of

the system takes into account both the advantages and the disadvantages of utilizing a system that is based on blockchain technology. This figure is the perfect representation of the flexibility of choice provided by the underlying blockchain software, as it shows how many different ways there are to do something. The following criteria are utilized by researchers in order to assess the degree of confidentiality provided by various blockchain-based security systems: For instance, 0.375 for key management, 0.4 for multiple signatures, 0.425 for ephemeral pseudonyms, 0.47 for route concealment, 0.47 for off-chain/on-chain/sidechain/partner matching, 0.5 for secret sharing, 0.5 for data concealment, 0.525 for subnetwork/ring signature, and 0.62 for zero-knowledge, for a total of 0.62. Zero-knowledge has a weighting of 0.62.

Not only does the use of side-chaining and other related techniques make the system more secure, but it also helps users maintain their anonymity. Because of this, there is a greater resilience to duplicity, which, in turn, makes these systems impervious to a broad variety of security concerns. [4] provides a concise introduction to both of these problems as well as the blockchain-based solutions that have been developed to combat them. They investigate attacks such as node tampering, RF interference, node jamming, malicious node injection, physical damage, insecure initialization, sleep scheduling, social engineering, sybil, masquerading, spoofing, and malicious code injection, and they discuss ways that blockchain technology can be used to mitigate the effects of these threats. We investigate the many different ways that blockchains can be used, as well as the protections that are in place to prevent them from being compromised by malicious actors. This encompasses implementations at the full-stack, hybrid, and distributed levels, as well as implementations at the analytics and storage, gateway, cloud, and site/device levels. Blockchains, despite the high level of security they offer, are not yet capable of fending off attacks such as cryptoanalysis, reputation level attacks, service-based attacks, hybrid attacks, dynamic and adaptable attacks, firmware-level attacks, and trustworthy update attacks. These types of attacks are still too new for blockchains to defend themselves against. All of these problems can be addressed by either implementing distinct side-chaining for each type of assault, as described in [5], or by complementing existing techniques with ones that are based on machine learning and artificial intelligence. Both of these solutions are possible. The Internet of Things is made more secure by the application of these strategies, which make use of chain management techniques and adjustable cryptography. To achieve greater overall system effectiveness, a number of intermediaries consisting of QoS administrators, security suppliers, resource managers, and so on are utilized.

The infrastructure makes use of a variety of different tools, including distributed acyclic graphs (DAGs), neural networks, and a few others, in order to identify and prevent assaults of this nature. While these assaults do strengthen the security of the blockchain, they can also be adjusted to enhance the anonymity of the blockchain. The following are some examples of privacy concerns that are addressed in [6]: identification privacy, data transmission privacy, data storing privacy, third party data processing privacy, and other concerns along these lines. The addition of a private component to the blockchain technology that is currently in use is the solution to all of these problems. There are many different industry 4.0 applications case studies that have the potential to gain advantages from the enhanced data preservation that is made possible by blockchain technology. Examples of data related to healthcare are addressed in [7] and [8], and blockchain technology is recommended for managing these examples.



An application case study is presented in [9], which demonstrates the improved identification afforded by blockchain technology, incredibly private access management, and improved confidentiality. The architecture is dependent on a proof system that is mutually strengthening, and this system is used to maintain tabs on two distinct smart contracts. The first contract covers information pertaining to the device itself, while the second covers information pertaining to the individuals who make use of the device. The combination of the two contracts constitutes the concluding step in the identification procedure. Because of the authentication process that is based on blockchain technology, this system is immune to the myriad of identifying assaults that

could be launched against it. On the other hand, this approach is susceptible to assaults launched from within the organization. The research presented in [10] suggested utilizing a trustworthiness management system that was powered by blockchain technology as a means of warding off an assault of this nature. This approach makes use of confidence management that is founded on Bayesian reasoning in order to ensure the security of mobile health networks. (MSN). The MSN design, which is linked to a primary computer, synchronizes data on statistics and restrictions using mobile phone communication at the network level.

Before reaching the device itself, each and every communication that takes place between MSN devices is first added to a blockchain directory. This documentation on the blockchain level guarantees the dependability and transparency of every messaging communication, which encourages a great deal of confidence in the network as a whole. This network can be expanded to facilitate contact monitoring by making use of fundamental characteristics of blockchain technology, as demonstrated in [11], where radio frequency identification (RFID) is used to track smartphones belonging to individuals exhibiting indications of communicable illnesses like CoVID. Because it is so effective in monitoring links using blockchains, this technique is being implemented by governments all over the world. Cases very comparable to these are addressed in [12], which offers comprehensive treatment of patient identification and surveillance in addition to isolation, virtual healthcare, and the beginnings of medical data. This program makes use of a device design for the internet of medical things (IoMT) that is compatible with blockchain technology in order to provide uninterrupted service delivery and to enhance communication between patients and healthcare providers.

See also [13], which discusses a broad variety of topics, such as the surveillance of patients, the administration of documents, the sharing of X-rays and images, and additional blockchain-based healthcare applications. Because of blockchain technology, the transfer of data between all of these different systems can be made secure, in addition to being extremely adaptable and secret.

The primary issue with these single-chain systems is that they are unable to scale, due to the fact that the difficulty of adding new blocks, searching for blocks, and authenticating transactions increases at an exponential rate with chain length. In recent research [14], a potential solution to this problem is referred to as "side-chaining," which involves the division of single chains into a large number of smaller side chains. These secondary networks are each tasked with the responsibility of keeping an eye on a particular component in the primary chain. In the same vein as [14], we use connections that only go in one direction to symbolize each civilization, and the number of networks that are produced as a result grows in direct proportion to the total number of human communities. Every side chain of the sociopolitical hierarchy has its own sub-chains that are in charge of the administration of a particular geographical location. It has been demonstrated that the use of a side-chaining protocol, which is what distinguishes a two-way peg protocol, reduces the amount of time required for the processing by 33 percent.

In reference number 15, we find the definition of a new side-chaining architecture. This architecture ensures that only sanctioned communications can take place between 5G-enabled Internet of Things devices. All of the prerequisites for cross-domain identification confirmed Internet of Things device authentication are dispensed according to the side-chain approach that has been suggested. As a consequence of this, IBC is utilized rather than PKI in order to cut down on communication latency by more than 18 percent while simultaneously improving overall system effectiveness. The innovation splits the infrastructure of a singular blockchain into two separate categories: friend blockchains and domain blockchains. where numerous blockchains for different domains are connected to one another via an alliance blockchain in order to make the system run more quickly.

Applications such as high-speed Internet of Things networks [17, 18] and intelligent vehicle ad hoc networks [16, 17] are two examples of where similar architectures can be used. Blockchain technology offers cutting-edge security techniques that can be implemented at the physical, application, and data-link levels of any security system. These techniques serve to strengthen the aforementioned networks. We learn about one such blockchain-based system in [19], which is so secure that it can be used to store and

communicate historical medical documents in addition to the most recent ones. [19] is available online. In addition to this, the system makes use of smart contracts and suggests connecting to ancillary networks in order to achieve maximum productivity. According to the findings of the research presented in [20], which discusses a variety of blockchain designs including ChainMaster, BitCoin, Ethereum, NeonCoin, and others, additional blockchain architectures can be used to enhance the overall system's level of security. According to what they have said, ChainMaster offers improved safety and stability, greater flexibility, increased speed and adaptability, expanded capacity, and a lower overall cost for the application. Distributed service level agreements (SLAs) are another method that can be used to enhance the effectiveness of blockchains. Blockchains already offer a variety of advantages. Within the blockchain networks, this makes it easier to enter reliable data and administer the network.

In the research article [21], the authors suggest a distributed service level agreement management architecture that, in order to enhance system control, can be combined with blockchain technology. Auxiliary networks form the foundation of the architecture, which was designed to ensure the greatest possible efficiency in the process of data dissemination across all blockchain implementations. If this system is expanded to offer it, as described in [22], which describes smart contracts with the aforementioned service level agreements (SLAs), then any and all service level agreements (SLAs) can be revised to encompass access to digital assets and the administration of those assets. This SLA-based technique reduces the amount of time required to access the network generally while simultaneously improving network security against malicious assaults by a factor of 25%. It is possible to further enhance these systems by incorporating machine learning-based designs into the construction of adaptable service level agreements (SLAs) and administration methods. In addition, as described in [23], distributed trust and reputation management in blockchain systems can increase the efficiency of this process. This is accomplished by delegating to each node the responsibility of accumulating and maintaining the confidence level of all other nodes as well as their individual reputation ratings. These numbers are recalculated after taking into account a wide range of additional information, such as the rate at which packets are lost, the number of times that incorrect access requests are made, the sequence in which packets are lost, and so on. Access to the network is provided to nodes on a discretionary basis according to these assessments. The application of this method is expanded upon in [24] to incorporate confidence management in order to provide superior data control. It gives nodes the ability to delegate responsibility for their data to other nodes in the network that they have more confidence in.

Blockchains offer Internet of Things (IoT) networks another opportunity to enhance the performance of their recommendation algorithms. For instance, the research presented in [25] recommends making use of cognitive frameworks in order to put assurance-based recommendations into action. The system builds a reliable network and then uses this to generate helpful recommendations by drawing on earlier concepts that are described in [23] and [24]. [23] and [24] respectively. Because of the recommendations regarding route node selection, packet delays, slumber scheduling, and other factors, it is feasible to achieve an enhancement in end-to-end QoS effectiveness of more than 15 percent. The security of cryptocurrency networks can also be improved with the help of these confidence numbers. An illustration of a blockchain-based, highly dependable healthcare security system is provided for us in [26]. In this system, random characteristics are utilized in order to establish a trustworthy connection between various blockchain servers. Chance variables can be replaced with alternative models, such as those described in [27], which can be used instead. These models make use of a variety of agreement algorithms, encryption protocols, encoding methods, and the like with the intention of enhancing the reliability and security of blockchains. It has been established that the proof of stake (PoS), secure hashing algorithm (SHA), and elliptic curve encryption (ECC) versions are the most effective techniques for enhancing the functionality of a blockchain. The Blockchain-based Distributed IoT Data Transaction architecture (BDDT), which was suggested in [24], is an example of a system that makes use of these approaches to

protect the data transfers that take place on blockchains. Some of the eight interconnected components that make up this design are local Internet of Things devices, proxy nodes, user (client) nodes, store nodes, flier nodes, transaction credentials, and virtual networks. Additionally, this design includes virtual networks.

According to the design, high-risk occurrences can be saved in a replicated chain and then used later for effective evidence. This functionality is suggested. When this chain's verification is complete, the data will be transferred to the principal blockchain, which will result in an increase in the general security of the system. Examples of multi-chain systems can be found in [25, 26, and 27]. These references detail a variety of applications, including supply chain management, access control categorization, and data traceability, among others. Every one of these research publications demonstrates that multi-chain architectures and side-chains provide a substantial improvement to the overall effectiveness of blockchain systems. The use of machine learning in conjunction with these networks is required if the Quality-of-Service performance of the implemented blockchain is to be improved. The suggested side-chaining architecture for enhanced security and QoS performance of IIoT and HIoT systems will have its effectiveness evaluated as soon as its description is complete for different scenarios.

## 3. Proposed Design of an Ant Lion Optimizer for enhancing Security of QoS aware Blockchain deployments

It has been suggested to tamper-proof new as well as established IIoT and HIoT systems by keeping blockchain data in smart contracts using a technique called machine learning-based side chaining. Each block is responsible for storing information in a format that is specific to that format, and the blocks are organized hierarchically. Table 1 presents the entire configuration for your perusal, including the hash values, the data values, and the nonce values and samples.

| | | |
|---|---|---|
| Hash of Previous Block | Data from different IoT device sets | Time stamp of the blocks |
| IP of Sender | IP of Receiver | Information about the Miners |
| Node information for current set of miners | Value of stochastic Nonce | Hash of the Current Block |

Table 1. Structure to store blocks

In the architecture that has been suggested, the hash of the block in the chain that occurred before it is what is referred to as the preceding hash. In the realm of medicine, sensor data can originate from a broad variety of sources. These sources can include temperature, humidity, oxygen levels, and other medical instruments. In addition, sensor data can originate from any kind of industrial equipment. The length of time that data was stored is indicated by the time stamp on the block that is presently operational. In a correspondence, the transmitting organization can be identified by the Sender IP and the receiving organization can be identified by the Receiver IP. The primary method of navigation is in charge of controlling the route data that documents the journey's particulars. The "current hash" refers to the hash of the most recent batch of blocks, and the number that it represents. When referring to the process of data transmission, the "present node" is the computer that is currently storing the data. Hash values that are both one-of-a-kind and compliant with the rules are produced with the assistance of an arbitrary integer known as a nonce. Any data that is produced by devices connected to an IIoT or HIoT network can be safely recorded on a blockchain once these specifications have been established. When there are more communications, the database will remain functional for an extended period of time. The following are some of the factors that can have an impact on the amount of time it takes to add a new block to the network: the amount of time it takes to generate a random nonce number that will result in a unique hash (D(Mining)), the amount of time it takes to verify the newly added block before adding it to the network; Delaying both the block hashing and encryption processes (abbreviated D(HE)). Adding to the chain should be put on hold while additional miners work on the block (D(diss)).

The D_HE number is generated from these delays and is determined by the specified encryption and encoding techniques. These encryption and encoding techniques cannot be diminished without jeopardizing the security of the system. (which is by using weak encryption and hashing algorithms).

However, D(Mining) and D(diss) can be improved by using side-chains, as described in [14]. [Citation needed] [Citation needed] The disadvantage of the construction of [14] is that it separates the blockchain into multiple sidechains based on the anticipated length of each sidechain's existence. which may result in a gradual decrease in the value of D(Mining), but may result in an increase in the value of D(diss) due to the proliferation of side-chains. Each blockchain depository needs to implement the Ant Learner Optimization (ALO) methodology described in the following sentence in order to cut down on this latency and increase the production of side-chains.

- A set of $NA$ Ants are generated by selecting $RL$ number of sidechains.
- A stochastic sidechain is selected from these set of chains.
- Dummy blocks are added to this chain, and mining delay$D(Mining)$along with$D(diss)$ delay is observed for adding these blocks.
- Fitness of the addition process is estimated via equation 1,

$$f_{interm} = \frac{\left(\frac{D(Mining)}{D(Max)} + \frac{D(diss)}{D(Max)}\right)}{2} * \frac{E(Mining)}{E(Max)} \dots (1)$$

Where, $D_{max}$represents maximum level of dela needed for adding blocks.

- As per this selection for all $NA$ Ants, a fitness threshold is calculated via equation 2,

$$f_{th} = \sum_{i=1}^{NA} \frac{f_{interm_i}}{NA} * LA \dots (2)$$

Where, $LA$ represents learning rate for Ant particles.

- Modify all Ants with $f_{interm} > f_{th}$, and pass other Ants to the next set of iterations.
- Repeat this process for $NI$ iterations.

When constructing a new block, the fitness of the ant with the lowest score is used to determine which sidechain configuration should be utilized. When the duration of a blockchain is greater than the average length of all ancillary networks, this procedure is replicated. This guarantees that the amount of time necessary for a sidechain to be extracted and deteriorate will be as short as is practically possible. When a new side chain is established, its original hash value is sent to a centralized database. This allows the status of all of the chains to be viewed and managed from a singular location. Because of this, the greatest possible degree of security is maintained, and it is not feasible to alter any component. If the hash values of a compromised server do not match those of the main blockchain or the authorized side-chain, the server will be removed from the network and its associated data will be lost. This straightforward method renders the system private enough for confidential applications, such as those found in the Internet of Things (IoT) industries of manufacturing and healthcare. In the following section, we will compare the outcomes obtained by the system to those obtained using a strategy that is centralized and uses a blockchain that is based on Ethereum for different scenarios.



## 4. Results and statistical comparison

Solidity is used in the construction of the primary infrastructure, and the efficiency of the system is evaluated according to how rapidly new blocks can be added, messages can be sent, and data can be moved around the network. First, in order for solidity to be able to process numerous files, we had to transform them to a format called CSV, which stands for comma-separated values. An additional section is appended by the algorithm for each record that is contained in a CSV file. At a variety of transaction amounts, the functionality of the original Ethereum network was analyzed and compared to measurements from [15] and [18]. Figure 2 illustrates the typical amount of time that elapses between the completion of a new transaction and its addition to a set of blockchains.

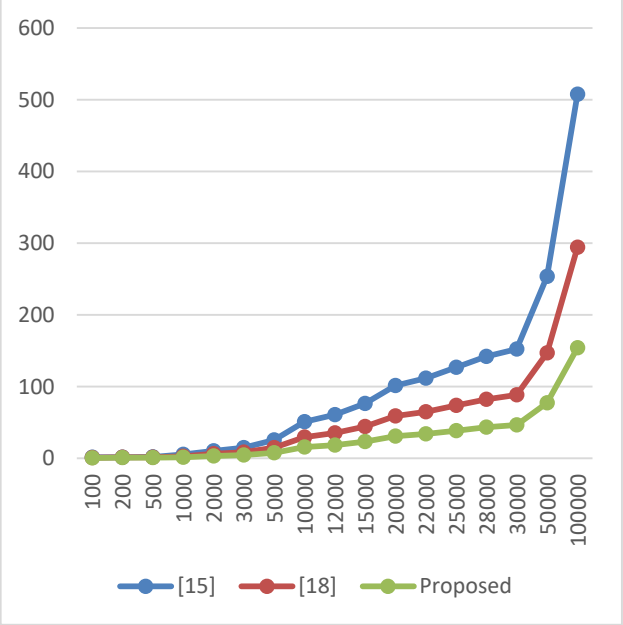

Figure 2. Block addition delay for different number of blocks

As a result of this comparison, it can be seen that the proposed model is able to enhance the rate at which blocks are added by 19.4% when compared with [15], and by 24.5% when compared with [18]. This is because the proposed model makes use of ALO to create various sidechains. In a similar vein, one can witness the communication latency that occurred during these procedures by looking at figure 3, which is presented as follows,

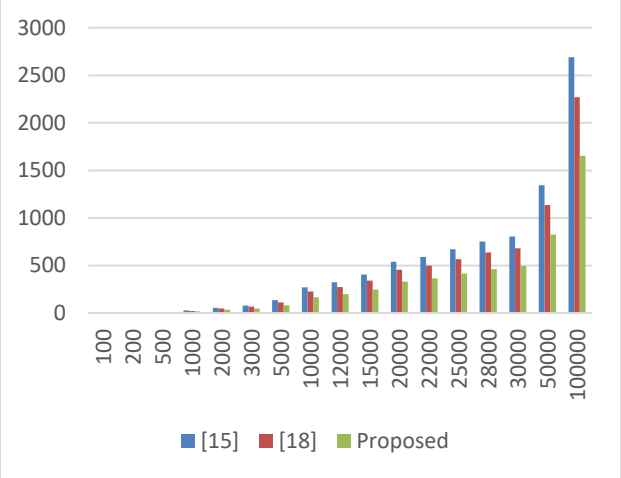


Figure 3. Block communication delay for different number of blocks

As a result of this comparison, it can be seen that the suggested model is able to increase communication speed by 14.5% when compared with [15] and by 19.4% when compared with [18]. This is because ALO is used to create different sidechains, which contributes to the improvement. In a similar vein, the communication throughput during these activities can be seen as follows in figure 4 for different number of blocks.

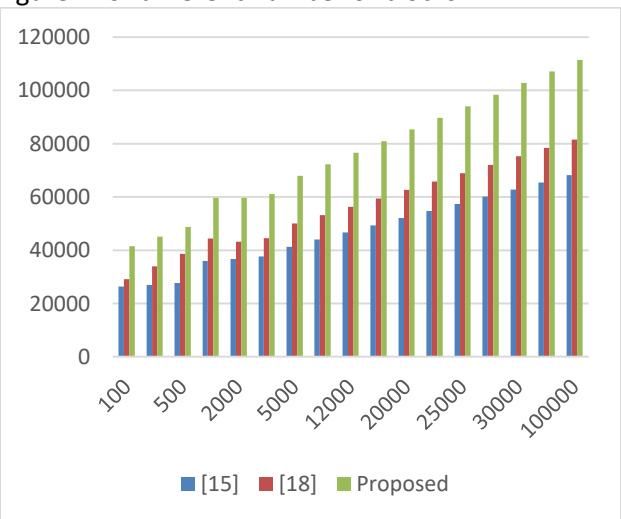


Figure 4. Block communication throughput for different number of blocks

In light of these findings, it is abundantly obvious that the suggested model, which makes use of ALO to generate numerous sidechains, has the potential to increase transmission capacity by 23.5 percentage points in comparison to [15] and 18.5 percentage points in comparison to [18]. Because of the aforementioned improvements, it is now feasible to implement the suggested technique to a variety of different cryptocurrency environments.

## 5. Conclusion & Future work

According to the findings of these evaluations, the machine learning driven side-chaining protocol that was suggested decreases overall latency by 18.3% in comparison to the static side chaining protocols and by 19.5% in comparison to the standard Ethereum protocols. The fundamental protocol is 23.5% quicker than the Ethereum blockchain software, and it is 18.5% quicker than the conventional approaches to side-chaining operations. These figures are based on comparisons with other techniques. Researchers should use machine learning models to minimize encryption and hashing latency using application-specific adaptive encryption and hashing techniques in order to achieve a further improvement in this performance's overall quality levels.



## 6. References

[1] S. Ma, S. Wang and W. -T. Tsai, "Delay Analysis of Consensus Communication for Blockchain-Based Applications Using Network Calculus," in IEEE Wireless Communications Letters, vol. 11, no. 9, pp. 1825-1829, Sept. 2022, doi: 10.1109/LWC.2022.3183197.

[2] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3562-3574, Dec. 2022, doi: 10.1109/JSAC.2022.3213326.

[3] P. Zheng et al., "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.

[4] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof

Bidirectional Blockchain Paradigm for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4371-4384, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103275.

[5] H. Xiong et al., "On the Design of Blockchain-Based ECDSA With Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1977-1986, May 2022, doi: 10.1109/JBHI.2021.3112693.

[6] W. Liang, D. Zhang, X. Lei, M. Tang, K. -C. Li and A. Y. Zomaya, "Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1410-1420, 1 July-Sept. 2021, doi: 10.1109/TETC.2020.2993032.

[7] A. Welligton dos Santos Abreu, E. F. Coutinho and C. Ilane Moreira Bezerra, "Performance Evaluation of Data Transactions in Blockchain," in IEEE Latin America Transactions, vol. 20, no. 3, pp. 409-416, March 2022, doi: 10.1109/TLA.2022.9667139.

[8] F. Wilhelmi, S. Barrachina-Muñoz and P. Dini, "End-to-End Latency Analysis and Optimal Block Size of Proof-of-Work Blockchain Applications," in IEEE Communications Letters, vol. 26, no. 10, pp. 2332-2335, Oct. 2022, doi: 10.1109/LCOMM.2022.3194561.

[9] T. Meng, Y. Zhao, K. Wolter and C. -Z. Xu, "On Consortium Blockchain Consistency: A Queueing Network Model Approach," in IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 6, pp. 1369-1382, 1 June 2021, doi: 10.1109/TPDS.2021.3049915.

[10] J. Zhou, G. Feng and Y. Wang, "Optimal Deployment Mechanism of Blockchain in Resource-Constrained IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8168-8177, 1 June1, 2022, doi: 10.1109/JIOT.2021.3106355.

[11] M. O. Okoye and H. -M. Kim, "Optimized User-Friendly Transaction Time Management in the Blockchain Distributed Energy Market," in IEEE Access, vol. 10, pp. 34731-34742, 2022, doi: 10.1109/ACCESS.2022.3162214.

[12] F. E. Alzhrani, K. A. Saeedi and L. Zhao, "A Taxonomy for Characterizing Blockchain Systems," in IEEE Access, vol. 10, pp. 110568-110589, 2022, doi: 10.1109/ACCESS.2022.3214837.

[13] Y. E. Oktian, S. Heo and H. Kim, "SIGNORA: A Blockchain-Based Framework for Dataflow Integrity Provisioning in an Untrusted Data Pipeline," in IEEE Access, vol. 10, pp. 89714-89731, 2022, doi: 10.1109/ACCESS.2022.3199878.

[14] M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

[15] S. Yao et al., "Blockchain-Empowered Collaborative Task Offloading for Cloud-Edge-Device Computing," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3485-3500, Dec. 2022, doi: 10.1109/JSAC.2022.3213358.

[16] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao and Y. Xiang, "A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2964-2973, April 2021, doi: 10.1109/TII.2020.3007817.

[17] R. Chen et al., "BIdM: A Blockchain-Enabled Cross-Domain Identity Management System," in Journal of Communications and Information Networks, vol. 6, no. 1, pp. 44-58, March 2021, doi: 10.23919/JCIN.2021.9387704.

[18] P. Alemany, R. Vilalta, R. Munoz, R. Casellas and R. Martinez, "Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection," in Journal of Optical Communications and Networking, vol. 14, no. 4, pp. 211-221, April 2022, doi: 10.1364/JOCN.447833.

[19] K. O. -B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," in IEEE Systems Journal, vol. 16, no. 1, pp. 1685-1696, March 2022, doi: 10.1109/JSYST.2021.3076759.

[20] Y. Jiao and C. Wang, "A Blockchain-Based Trusted Upload Scheme for the Internet of Things Nodes," in International Journal of Crowd Science, vol. 6, no. 2, pp. 92-97, June 2022, doi: 10.26599/IJCS.2022.9100010.

[21]L. Kleinknecht, "Can Blockchain Capabilities Contribute to Sustainable Supply-Chain Governance?," in IEEE Engineering Management Review, vol. 49, no. 4, pp. 150-154, 1 Fourthquarter,Dec. 2021, doi: 10.1109/EMR.2021.3123205.

[22]J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," in Tsinghua Science and Technology, vol. 27, no. 4, pp. 760-776, Aug. 2022, doi: 10.26599/TST.2021.9010046.

[23]H. M. Kim, H. Turesson, M. Laskowski and A. F. Bahreini, "Permissionless and Permissioned, Technology-Focused and Business Needs-Driven: Understanding the Hybrid Opportunity in Blockchain Through a Case Study of Insolar," in IEEE Transactions on Engineering Management, vol. 69, no. 3, pp. 776-791, June 2022, doi: 10.1109/TEM.2020.3003565.

[24]M. Touloupou, M. Themistocleous, E. Iosif and K. Christodoulou, "A Systematic Literature Review Toward a Blockchain Benchmarking Framework," in IEEE Access, vol. 10, pp. 70630-70644, 2022, doi: 10.1109/ACCESS.2022.3188123.

[25]J. Yang, C. Ma, D. Li and J. Liu, "Mapping the Knowledge on Blockchain Technology in the Field of Business and Management: A Bibliometric Analysis," in IEEE Access, vol. 10, pp. 60585-60596, 2022, doi: 10.1109/ACCESS.2022.3179714.

[26]Nisha Balani, Pallavi Chavan, and MangeshGhonghe. 2022. Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks. Multimedia Tools Appl. 81, 25 (Oct 2022), 36699–36713. https://doi.org/10.1007/s11042-021-11604-6

[27]Chavan, P. V., & Balani, N. (2022). Design of heuristic model to improve block-chain-based sidechain configuration. In International Journal of Computational Science and Engineering (Vol. 1, Issue 1, p. 1). Inderscience Publishers. https://doi.org/10.1504/ijcse.2022.10050704