Blockchain Meets Secured Microservice Architecture: A Trustworthy Consensus Algorithm

Mohiuddin Ahmed[1][a], A. F. M. Suaib Akhter[2][b], A. N. M. Bazlur Rashid[1][c], Mahdi Fahmideh[3][d], Al-Sakib Khan Pathan[4][e] and Adnan Anwar[5][f]

[1]*School of Science, Edith Cowan University, Perth, Australia*

[2]*Computer Engineering Department, Sakarya University of Applied Science, Sakarya, Turkey*

[3]*School of Business, University of Southern Queensland, Queensland, Australia*

[4]*Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh*

[5]*School of IT, Deakin University, Geelong, Australia*

Keywords: Blockchain, Microservices, Consensus Algorithm, False Data Injection Attacks, Internet of Everything.

Abstract: Microservices are becoming an integral component in the architecture design and development of Internet-based distributed systems, such as the Internet of Things. A critical ongoing challenge in microservice architecture design is to ensure the integrity and availability of data. Blockchain technology offers the solution to these challenges in the distributed microservice architecture. Blockchains use consensus algorithms for validating their transactions and also providing extra security. Taming the advantages of consensus algorithms in blockchain-based architecture models, this paper proposes a trustworthy consensus algorithm to tackle data integrity challenges in microservice architectures. The results of the evaluation highlight the efficacy of the proposed algorithm in real-world scenarios of microservice architecture endeavour. Lessons learned in applying the algorithms, and future research directions are also discussed.

1 INTRODUCTION

IoT deployments are not flexible, reliable, efficient, and easy to build despite these solutions (Lu et al., 2017). To overcome the limitations for IoT deployment, many solutions have been proposed in the literature. One of the interesting solutions is based on *service-oriented* approach. In this approach, any IoT node can be considered a smart object that provides a number of services over the network. Therefore, the developers can focus on the level of services and data instead of the devices and communication network. Accordingly, the *microservice*-based approach proposed in the literature to tackle the IoT system deployment challenges (Lu et al., 2017). A microservice-based deployment allows the IoT systems to construct the fine-grained and self-contained independently developed microservices. Microservice architecture is composed of microservices connected and deployed via composition techniques. The microservice architecture allows the decomposition of larger services into several small, loosely-coupled, self-contained, and focused services. Because microservices can be distributed over the network, there can be the problem of data sharing between nodes in a trustable way. Blockchain technology is fundamentally a distributed database of records, which can be executed and shared between the associated nodes (Khan et al., 2020). There are five basic principles of blockchain. These include a distributed database, irreversibility of records, transparency with pseudonymity, computational logic, and peer-to-peer transmission. These principles ensure access to the new information when available over the network. These also ensure not to update or erase the data (Khan and Byun, 2020). Blockchain technology can solve microservices' data sharing problem by providing a stable and distributed base. A distributed service that can be trusted by all

[a] https://orcid.org/0000-0002-4559-4768
[b] https://orcid.org/0000-0002-2675-1684
[c] https://orcid.org/0000-0002-8672-5023
[d] https://orcid.org/0000-0001-7196-7217
[e] https://orcid.org/0000-0001-6572-3451
[f] https://orcid.org/0000-0003-3916-1381

Ahmed, M., Akhter, A., Rashid, A., Fahmideh, M., Pathan, A. and Anwar, A.
Blockchain Meets Secured Microservice Architecture: A Trustworthy Consensus Algorithm.
DOI: 10.5220/0011290400003286
In *Proceedings of the 19th International Conference on Wireless Networks and Mobile Systems (WINSYS 2022)*, pages 53-60
ISBN: 978-989-758-592-0; ISSN: 2184-948X

its participating nodes and can guaranty the data immutability may provide trustworthiness in microservice architecture data integrity. Blockchain uses a consensus algorithm to validate all of its transactions and ensure the data have not been tampered with since the first definition (Reyna et al., 2018; Zhang et al., 2021; Nartey et al., 2021). Therefore, with the combination of microservice and blockchain technology, the independently developed and deployed microservices can be created as a secured and robust system (Sousa et al., 2020).

However, because of the Internet-connected devices in the IoT system, the deployed microservice-based architecture can have cyber security issues. Cyber security is an absolute necessity in today's Internet connected world, a.k.a. Internet of Everything (IoE). Cyber criminals have the capability to launch sophisticated attacks which can have deadly consequences, e.g., shutting down the power gird for a complete blackout. It is also found that the hackers have the power to tamper with the election results(Ahmed and Pathan, 2020a). In recent times, due to cyber attacks in a hospital facility in Germany, a patient died(Goodin, 2020). Although embracing Internet has impacted the security and privacy aspects in our daily life, at the same time, it has become impossible to deny the advantages it has introduced, such as microservices(Eismann et al., 2020). Blockchains use consensus algorithms to validate their transactions and add extra security, integrity, trustability, etc. To attack a blockchain, the attacker has to overcome the security services provided by the consensus. Following the popular consensus algorithms and their weaknesses, a trustworthy consensus algorithm (TCA) has been proposed in this paper. The proposed TCA can ensure the data integrity and different cyber attacks in blockchain, such as 51% attack, selfish attack, miner bribe, and N confirmation. The efficiency of TCA has been evaluated based on different false data injection attacks. Hence, TCA is a more robust and trusted system for the microservice architecture using blockchain technology.

Rest of the paper is organized as follows. Section 2 presents the microservice architecture. Section 3 discusses the false data injection attacks in the context of blockchain. Section 4 contains the critical analysis of the consensus algorithms, which are the key reasons for false data injection attacks in blockchain-supported microservice architecture. Section 5 presents the proposed TCA (Trustworthy Consensus Algorithm) and Section 6 includes the performance analysis. The paper is concluded in Section 7.

2 MICROSERVICE ARCHITECTURE

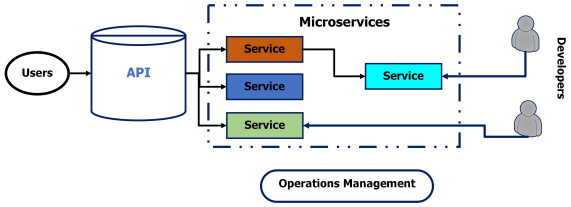

Figure 1: A simple microservices architecture, adapted from Microsoft.

Microservice architecture is generally used for large software projects as an architectural style. The fundamental objective of microservices is providing short-release cycles and flexible on-demand scalability to the target venue. This microservice architecture decomposes an application into several independent components, which are called microservices. Each microservice runs on its individual process (Koschel et al., 2017). Microservices are used by the developers who find it convenient as function-specific solution. The corporations such as Amazon, Netflix are taking full advantage of the microservice architecture. Microservice architecture benefits the complete independence and developers can revise an existing service without rebuilding and redeploying the entire application. The microservice architecture has key advantages, including independent development and deployment, decentralized data management and governance, small and focused teams (Jamil et al., 2020). Because microservices can be independently scaled, they can also efficiently allocate computing resources and enable flexible horizontal scaling in the cloud (Khan et al., 2020). Such architecture contains a collection of small, autonomous services and these services are self-contained (as shown in Figure 1 - in the figure, API stands for Application Programming Interface). However, the main challenge with microservices is to coordinate various small parts. This is deemed as the loophole or vulnerability of the microservice architecture. Hence, microservices are not as effective as it seems to be in terms of cyber safety and its trustworthiness.

3 FALSE DATA INJECTION ATTACKS on BLOCKCHAIN

The strength and uniqueness of blockchain is its consensus algorithms. Trusted security and integrity are ensured by blockchains by applying consensus algorithms. However, recent studied have proved that

popular consensus algorithms, such as PoW (Proof-of-Work), PoS (Proof-of-Stake), DPoS (Delegated Proof-of-Stake) are vulnerable to several types of attacks like DDoS (Distributed Denial-of-Service), Sybil, and 51% attacks. An overview of the possible attacks in the blockchain are discussed in this section as problem statement and potential motivation for this work.

- **51% Attack:** Blockchain technologies are attracting users from different areas for their strong security services but still the top blockchain based cryptocurrencies lost huge amount of money because of 51% attacks. Whenever a single entity or a group of entities acquires more that 51% of the hashing power, it is possible to include block or chain of blocks by winning the consensus everytime (Ahmed and Pathan, 2020b). In that case, the miner can perform double spending attack anytime which is the biggest threat for the cryptocurrencies (Zhang and Lee, 2019). However, it is also possible to perform similar kind of attack while the the hashing power is less than 51%, but with less probability to get a success.
- **Selfish Mining:** When two or more miners are trying to add their mined blocks into the blockchain, the chain that consists of maximum number of blocks will be accepted for the main chain. This is called the longest chain rule (Nakamoto, 2019). Thus to win the race, miners mine blocks secretly and submit long chain to win the race. Miners with relatively higher hash power can dominate the race and by mining longer chain, win the race, whereas the miners with comparatively lower hash power remain behind and face losses as their contributions become wasted because of this rule. This process is called selfish mining. It is easy to perform selfish mining if someone has more than 25% of the network's hashing power. It will allow the selfish miners to mine too many blocks within a short amount of time to win the chain and earn more profit. In contrast, others would continuously lose the race as they are not able to generate that many blocks within the short time.
- **Miner Bribe:** Because of consensus, it requires some time to complete a transaction. Attackers try to generate a second transaction just after the first one and offer high transaction fees for the second one to attract miners to perform mining for the second transaction quickly. Target of this bribing process is to use the same coin to perform the transactions. If it is possible to complete the second transaction before the first one is confirmed, the success rate of double spending is 100% (Sun et al., 2020).
- **Zero Confirmation:** The Zero confirmation is another attacking technique to perform double spending. Attackers show a fake output of a real transaction and convince them (the victims) to provide the service before the transaction is been confirmed. If the merchant agrees to provide the service before the transaction is confirmed, attacker withdraws the transaction and replaces it by another one (Nicolas et al., 2019).
- **One Confirmation:** Similar to the zero confirmation, one confirmation is an attack where the attacker's transaction is confirmed in the block and shows the output to the merchant so that the merchant can provide the product or service. However, when the attacker's block is sent for remining by losing the race to another miner because of the longest chain rule, the attacker gets the opportunity to remove the transaction and gets refunded (Judmayer et al., 2017).

Table 1: Vulnerabilities of the popular consensus algorithms.

Attacks	Consensus algorithms		
	PoW	**PoS**	**DPoS**
51% Attack	✓	×	✓
Selfish mining	✓	✓	✓
Miner bribe	✓	×	×
Zero confirmation	✓	×	×
One confirmation	✓	×	×

4 CRITICAL ANALYSIS OF THE CONSENSUS ALGORITHMS

Consensus algorithms are used by blockchains to validate their transactions and to add extra level of security, integrity, trustability, etc. To attack a blockchain, the attacker has to overcome the security services provided by the consensus. In this section, weaknesses of the popular consensus algorithms are described in brief. In Table 1, vulnerabilities of the popular consensus algorithms are summarized.

- **Proof-of-Work (PoW):** PoW is a consensus algorithm initiated by bitcoin where miners are responsible to generate transactions requested by nodes. To generate blocks from one or multiple transactions, it requires to solve complex equation to generate hash for the next block. Nodes of the blockchain verify the blocks before it gets accepted to be added into the blockchain. PoW

is vulnerable if any of the miners gets more than 50% of the hashing power because in that case, it will be easy for the miner to perform most of the attacks, such as double-spending, 51% attack, and P+Epsilon attack (Wang, 2017). By generating large number of fake nodes, it is possible to perform Sybil attack.

- **Proof-of-Stake (PoS):** PoS is a consensus algorithm where the transactions are mined and validated by the nodes selected by a voting system. Nodes with higher stake will get priority to be selected as miner and rather than calculating complex hash value, a single miner can perform the mining to minimize the computation cost. As it is nearly impossible to achieve more than 51% stake value, PoS is considered as secured compared to 51% attack. However, it is vulnerable to P+Epsilon (Wang, 2017), long-range attack (Sharma, 2018) and it is possible to minimize the performance by using DDoS and Sybil attack.
- **Delegated Proof-of-Stake (DPoS):** To make the mining process faster and to reduce the wastage of energy, DPoS proposed where witnesses are selected to perform mining. A voting process is used to select the witness where higher stake holders have the opportunity to cast more than one vote. A penalization model is used where the miners, i.e., the witnesses win coins for successful block generation while receive penalties for failure. Although, DPoS performs better than PoW in terms of energy consumption and mining speed. However, the system is not fully decentralized. In addition, if a single or a group of stakeholders gains more than 51% of voting power, the system will become vulnerable to 51% attack. Furthermore, likewise other consensus methods, DPoS also suffers from balance attack, long-range attack, P+Epsilon attack, Sybil attack and DDoS attack.

4.1 Existing Works and Their Limitations

A time penalty based system proposed by Horizen (Garoffolo et al., 2018) where the gap between transaction received and block creating was calculated. When the delay crosses a threshold time, the miner received a punishment. During the punishment time, the miner is not be able to perform any sort of action in the blockchain. With the amount of delay and frequency of similar action, the punishment period increases. The proposed method can mitigate the attack up to a certain level. However, a miner with high hashing capacity does not face any punishment because it does not require much time for that miner to generate large number of blocks. To minimize the double-spending attacks, a consensus technique called delayed proof of work (dPoW) proposed (ChainZilla, 2019). Firstly, dPoW removes the longest chain rule from the PoW to minimize the selfish mining and 51% attack. Additionally, it elects a number of nodes to create a checkpoint to monitor all the transactions of bitcoin targeted to stop double spending attacks. dPoW provides comparatively stronger security but checking every transaction increases the time consumption. Because of monitoring nodes, the system is not fully decentralized and by attacking the supervisor nodes, it is possible to perform those attacks. Another centralized algorithm called PirlGuard proposed by Rado Minchev to mitigate the 51% attack (Minchev, 2018). In this proposal, masternode operates notary contracts on multiple blockchains and monitoring system. If the notary nodes find someone who has mined blocks privately to win the longest chain race, they would assign penalty that means the miner will be suspended from mining to a certain number of blocks. The penalty increases with the number of secret mining nodes. Similar to (Garoffolo et al., 2018), Pirlguard is able to mitigate the 51% attack up to a certain level and a miner with high computational power can (still) avoid punishment easily. However, presence of masternode brings the drawbacks of centralization.

A consensus algorithm, ChainLocks, proposed in 2018 to mitigate the 51% attack (Block, 2018). In the proposed method, it requires positive response from 60% nodes to get acceptance as a block. After the block generation, P2P messages are generated to inform all the nodes about the block generation. Additionally, the method does not support reverse transaction after the transaction is signed. A master node is there to manage the algorithm which brings the limitations of centralized system. However, by gaining much hashing power, it is still possible to perform attacks.

From the literature review of related works on consensus algorithms for blockchain technology, it can be observed that the proposed algorithms suffer from a number of drawbacks, including 51% attack, selfish mining, miner bribe, and zero or one confirmation attacks. Therefore, there is a need to study a new or trustworthy consensus algorithm that can be used by blockchain technology to offer a secured microservice architecture. The proposed trustworthy consensus algorithm has been discussed in the next section.

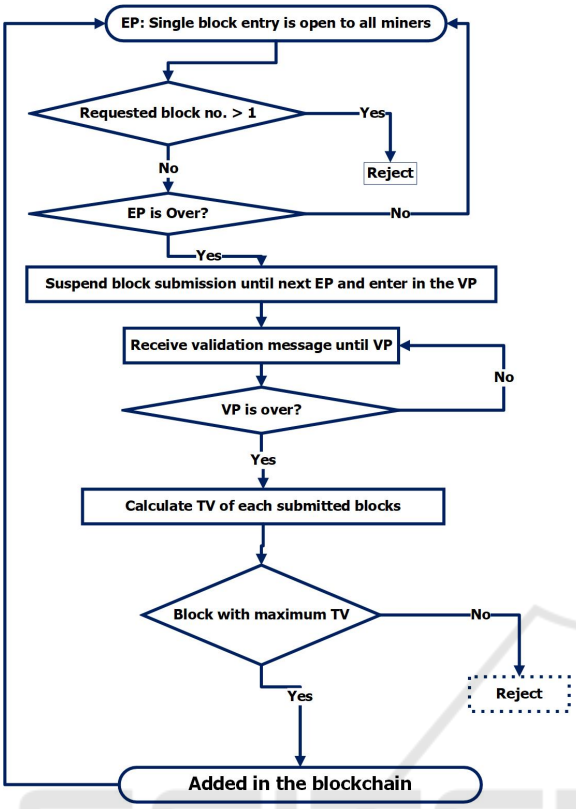

Figure 2: TCA: Trustworthy Consensus Algorithm.

5 PROPOSED TRUSTWORTHY CONSENSUS ALGORITHM

To enhance the efficiency of the consensus techniques used by blockchains, a novel consensus algorithm (Algorithm 1) is proposed in this paper, named **TCA** (Trustworthy Consensus Algorithm). The aim of the proposed consensus algorithm is to protect the microservice architecture from the above mentioned attacks. The flow chart in Figure 2 illustrates the proposed technique and it can be summarized as follows.

After every successful mining, there is a mining Entry Period (EP) where miners competes to get chance and perform the verification/validation process. Miner continues mining and tries to get chance in the next time slot. Only one block is allowed per miner to enter into the Validation Period (VP). This removes the longest chain rule problem to mitigate 51% attack. During the validation period, no miners are allowed to submit blocks. Instead, they wait for the next slot. Multiple blocks can enter into the VP and after collecting the votes from the nodes, Trust Value (TV) of each of the miner is calculated and the block with the highest TV is selected for the chain to be added. The rate of positive responses from the participating nodes is multiplied by the block size i.e., size of the transactions added in the block to get the TV (Eq. 1). Block Size (BS) is added so that blocks with more number of transactions gets advantage. In Eq. 1, PR is Positive Responses and TR is Total Response.

Algorithm 1: Trustworthy Consensus Algorithm (TCA).

Begin
Step 1: Entry Period (EP) open to all miners;
Step 2: Check the requested block numbers;
if *requested block number* > 1 **then**
  Reject;
end
if *EP is avialable* **then**
  Go to Step 1;
  else
    Suspend block submission until next EP;
  end
end
Step 3: Enter into Validation Period (VP);
Step 4: Receive validation message;
Step 5: Check VP status;
if *VP is not available* **then**
  Await validation message;
  else
    Calculate TV (Eq. 1);
  end
end
Step 6: Add the block with maximum TV;
Step 7: Go to Step 1.
End

$$TV = \frac{PR}{TR} * BS \tag{1}$$

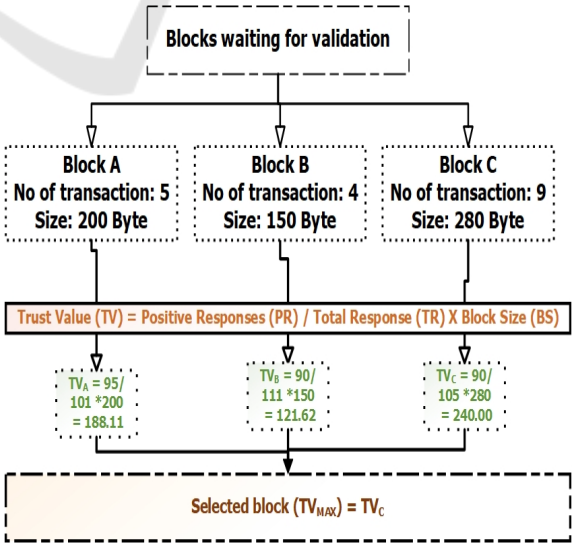

Figure 3: Blocks in the validation period (VP) and their trust value (TV) calculation.

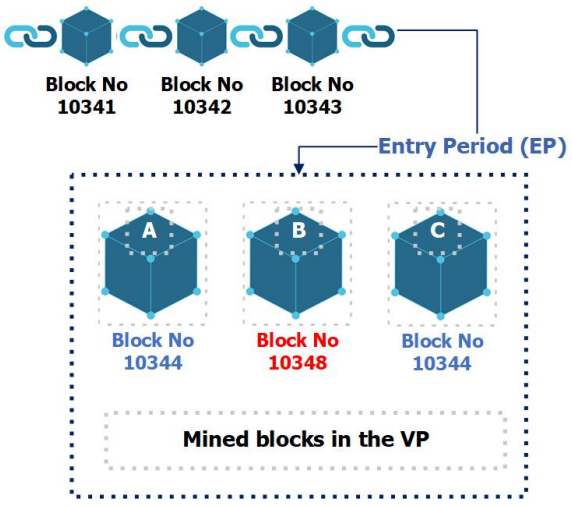

Figure 4: Mitigation technique from the 51% attack.

For example, in Figure 3, blocks are illustrated who get chance in the VP and after validation and TV calculation, block C is selected to be the next block. Delay calculation and punishment, negative reputation value assignment etc. are not required to perform likewise the previously proposed methods, which can minimize the additional computational costs performed by the server. Miner with more than 51% computational power would not be able to get benefits by wining the longest chain rule as only one block is allowed from each miner.

6 PERFORMANCE EVALUATION OF TCA

Table 2 presents the efficiency of TCA under several false data injection attacks. It is evident that the state-of-the-art consensus mechanisms are not suitable to address the false data injection attacks, which are serious threats to the microservice architecture. It is important to provide trustworthiness to any technology; however, due to the vulnerabilities in the consensus algorithms, the blockchain ecosystem is still in jeopardy. The proposed **TCA** is a more robust and trusted system for microservice architecture within blockchain framework.

A miner with more than 51% hashing power can generate a long chain to perform 51% attack. However, in the proposed consensus algorithm (TCA), only one block is selected to enter in the evaluation period. Thus, it is not possible to add more than one block in the blockchain. When any miner comes with multiple blocks and applies to get a chance in the EP with a block height, which is more than the expected height would get rejected before the validation period. For instance, a miner comes with a block height 10347, where the EP is expecting a block to be selected for a block of height 10344, the mined block by the miner will be rejected. In Figure 4, the scenario has been explained graphically. During VP, a block from miner B is rejected because it is applied for block number 10348, while the system is processed to add block number 10344.

PoW is vulnerable to zero and one confirmation attacks and other similar type of attack including miner bribe attacks. All these attacks take the advantage of the transaction confirmation delay of the bitcoin as it requires 6 blocks confirmation to validate a single transaction. That means, a transaction mined in block number 1024 can be confirmed after block number 1030. When it is required around 10 minutes to generate one block, the waiting time for confirmation is almost one hour. Within this delay period, the attackers could find opportunities to perform any of the above mentioned attacks. To mitigate this kind of problem, in the proposed method, each block is being confirmed immediately after the block verification. Thus, the waiting times for the transactions are very little. Because each and every block is validated separately, it is not possible to perform the above mentioned attacks, i.e., zero confirmation, one confirmation, miner bribe, and other attacks.

Referring to the discussion in Section 3, the selfish mining is the process where a miner or a group of miners with higher computational strength can perform fast mining to generate longer chain of blocks to get chance in the main blockchain. Because of faster mining capacity, they can add more blocks than other miners, which make the miner with normal computation power unable to receive award of mining. It has been found that a group that consists of 6 miners are able to generate more than 67% of the total blocks generated by bitcoin in a single day and as a set of selfish miners, they are able to perform conjugative block generation (Sayeed and Marco-Gisbert, 2019). To remove this alarming attack, the proposed method (TCA) accepts only one block per miner in the EP. Thus, a miner with high mining capacity cannot get entry there with multiple blocks. Instead, they have to wait for the next slot. Additionally, mining power is not able to affect the proposed algorithm because the system does not accept multiple blocks from a miner.

To generate longer chain, transactions had to face delay because miners need a large number of transactions to generate a high number of blocks for winning the longest chain race in the PoW consensus algorithm. However, in the proposed TCA, there is no benefit in creating longer chain (because a miner can

Table 2: Efficiency of TCA.

Attacks	Comparison with State-of-the-art					
	PoW	**(Garoffolo et al., 2018)**	**(ChainZilla, 2019)**	**(Minchev, 2018)**	**(Block, 2018)**	**TCA**
51% Attack	×	×	×	×	✓	✓
Selfish mining	×	×	×	×	×	✓
Miner bribe	×	×	×	×	✓	✓
Zero confirmation	×	×	×	×	✓	✓
One confirmation	×	×	×	×	✓	✓

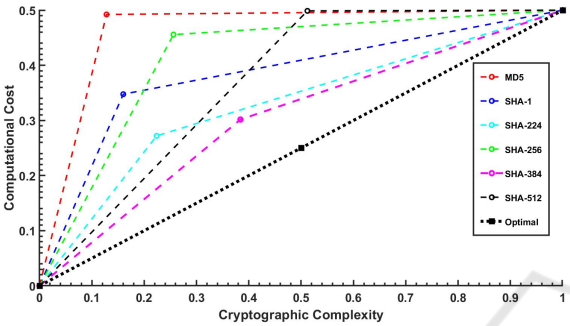

Figure 5: Computational cost vs Cryptographic Complexity.

submit only one block in the EP). Thus, miners can mine single block rather than keeping transactions waiting. Then, they can try to get chance in the EP. For bitcoin, average block generation time is 10 minutes. It requires generating 6 blocks to get confirmation for a transaction, which is a good amount of time. In the proposed algorithm, this waiting time can be removed because all transactions will get confirmation just after the block verification and selection process.

6.1 Hashing

Hashing is one of the integral parts of blockchain technology. There are different types of hashing algorithms available and each algorithm has different outputs. It is important to keep in confederation, which hashing technique is optimal for the proposed consensus algorithm in this paper. It is also important to note that, the proof of work requires to solve a predefined mathematical puzzle, which is both computationally and energy intensive task regardless of hashing process. Therefore, the combination of **SHA-224** with TCA will be an optimal solution for ensuring data integrity and availability. However, there is a trade-off between the cryptographic complexity or the length of hash values and the computational cost or time required. In Figure 5, it can be shown that the optimal solution is the diagonal line and only SHA-384 seemed to be very close to that. Meaning, the SHA-384 hashing is more balanced and can be useful for integrating with the proposed consensus algorithm (TCA) in this paper.

7 CONCLUSIONS

Internet of Things (IoT) offers distributed connectivity of networked items, and microservice architecture is becoming an essential part of IoT in designing the system. Furthermore, blockchain can ensure the data integrity for the microservices architecture by using a consensus algorithm. However, to tackle the cyber security issues, a trustworthy consensus algorithm can help to mitigate the security issues. In this paper, a robust and trustworthy consensus mechanism, called TCA has been proposed for use in a blockchain-based microservice architecture. The key objective of this algorithm is to address the data integrity and availability attacks in blockchain, i.e., 51% attack, selfish mining, miner bribe and N confirmation. Although data availability is well studied, data integrity attacks, e.g., false data injection attacks (similar to the man-in-the-middle), are less explored, which can benefit from the proposed framework. It is crucial to identify the need to address availability and integrity attacks in the blockchain ecosystem used for secure and dependable microservice architecture. Hence, it is necessary to devise critical components of the blockchain, i.e., the consensus mechanism, in a trustworthy way to enhance the reliability and immutability of the blockchain-based microservices. The TCA will be studied using a real-case scenario as a future study.

REFERENCES

Ahmed, M. and Pathan, A. (2020a). False data injection attack (fdia): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, 8:1–14.

Ahmed, M. and Pathan, A.-S. K. (2020b). Blockchain: Can it be trusted? *Computer*, 53(4):31–35.

Block, A. (2018). Mitigating 51% attacks with llmq-based chainlocks. https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9. Accessed: 2021-04-08.

ChainZilla (2019). Blockchain security and how to mitigate. https://medium.com/chainzilla/solutions-to-51-attacks-and-double-spending-71526be4bb86. Accessed: 2021-04-08.

Eismann, S., Bezemer, C.-P., Shang, W., Okanović, D., and van Hoorn, A. (2020). Microservices: A performance tester's dream or nightmare? In *Proceedings of the ACM/SPEC International Conference on Performance Engineering*, ICPE '20, page 138–149, New York, NY, USA. Association for Computing Machinery.

Garoffolo, A., Stabilini, P., Viglione, R., and Stav, U. (2018). A penalty system for delayed block submission. https://www.horizen.global/assets/files/A-Penalty-System-for-Delayed-Block-Submission-by-Horizen.pdf. Accessed: 2021-04-08.

Goodin, D. (2020). A patient dies after a ransomware attack hits a hospital. https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/. Accessed: 2021-02-22.

Jamil, F., Ahmad, S., Iqbal, N., and Kim, D.-H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, 20(8).

Judmayer, A., Stifter, N., Krombholz, K., and Weippl, E. (2017). Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms. *Synthesis Lectures on Information Security, Privacy, & Trust*, 9(1):1–123.

Khan, P. W. and Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial internet of things. *Entropy*, 22(2).

Khan, P. W., Byun, Y.-C., and Park, N. (2020). A data verification system for cctv surveillance cameras using blockchain technology in smart cities. *Electronics*, 9(3).

Koschel, A., Astrova, I., and Dötterl, J. (2017). Making the move to microservice architecture. In *2017 International Conference on Information Society (i-Society)*, pages 74–79.

Lu, D., Huang, D., Walenstein, A., and Medhi, D. (2017). A secure microservice framework for IoT. In *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 9–18.

Minchev, R. (2018). Pirlguard — innovative solution against 51% attacks. https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-87dd45aa1109. Accessed: 2021-04-08.

Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.

Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., and Diawuo, K. (2021). On blockchain and IoT integration platforms: Current implementation challenges and future perspectives. *Wireless Communications and Mobile Computing*, 2021.

Nicolas, K., Wang, Y., and Giakos, G. C. (2019). Comprehensive overview of selfish mining and double spending attack countermeasures. In *2019 IEEE 40th Sarnoff Symposium*, pages 1–6. IEEE.

Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with IoT. challenges and opportunities. *Future Generation Computer Systems*, 88:173–190.

Sayeed, S. and Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51*Applied Sciences*, 9(9).

Sharma, A. (2018). Understanding proof of stake through it's flaws. part 3— 'long range attacks. https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-part-3-long-range-attacks-672a3d413501. Accessed: 2021-04-08.

Sousa, P. S. d., Nogueira, N. P., Santos, R. C. d., Maia, P. H. M., and Souza, J. T. d. (2020). Building a prototype based on microservices and blockchain technologies for notary's office: An academic experience report. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 122–129.

Sun, H., Ruan, N., and Su, C. (2020). How to model the bribery attack: A practical quantification method in blockchain. In *European Symposium on Research in Computer Security*, pages 569–589. Springer.

Wang, K. (2017). Cryptoeconomics: Paving the future of blockchain technology. https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971. Accessed: 2021-04-08.

Zhang, J., Lu, C., Cheng, G., Guo, T., Kang, J., Zhang, X., Yuan, X., and Yan, X. (2021). A blockchain-based trusted edge platform in edge computing environment. *Sensors (Basel, Switzerland)*, 21(6):2126.

Zhang, S. and Lee, J.-H. (2019). Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE transactions on Industrial Informatics*, 15(10):5715–5722.