# PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism

H. Baniata and A. Kertesz
*University of Szeged, H-6720 Szeged, Dugonics ter 13, Hungary*

Keywords: Privacy, Fog Computing, Blockchain, IoT, Validation, Trust.

Abstract: Blockchain technology has been successfully implemented in cryptocurrency industries, yet it is in the research phase for other applications. Enhanced security, decentralization and reliability are some of the advantages of blockchain technology that represent beneficial integration possibilities for computing and storage infrastructures. Fog computing is one of the recently emerged paradigms that needs to be improved to serve Internet of Things (IoT) environments of the future. In this paper we propose PF-BVM, a Privacy-aware Fog-enhanced Blockchain Validation Mechanism, that aims to support the integration of IoT, Fog Computing, and the blockchain technology. In this model the more trusted a fog node is, the higher the authority granted to validate a block on behalf of the blockchain nodes. To guarantee the privacy-awareness in PF-BVM, we use a blockchain-based PKI architecture that is able to provide higher anonymity levels, while maintaining the decentralization property of a blockchain system. We also propose a concept for measuring reliability levels of blockchain systems. We validated our proposed approach in terms of execution time and energy consumption in a simulated environment. We compared PF-BVM to the currently used validation mechanism in the Proof-of-Work (PoW) consensus algorithm, and found that PF-BVM can effectively reduce the total validation time and total energy consumption of an IoT-Fog-Blockchain system.

## 1 INTRODUCTION

Fog Computing (FC) as defined in (Yi et al., 2015) is a geographically distributed computing architecture, in which various heterogeneous devices at the edge of network are ubiquitously connected to collaboratively provide elastic computation, communication and storage services. While according to another definition in (Markakis et al., 2017), FC is a horizontal, physical or virtual resource paradigm that resides between smart end-devices and traditional cloud datacenters. FC, also known as Fog Networking and Fogging, was introduced by Cisco in 2013, as the future of the current Cloud Computing systems, and mostly an extension of the continuous chain of development of the Radio Access Networks (RAN). Such integration is usually referred to as Fog RAN (F-RAN) (Yousefpour et al., 2019).

Blockchain is a distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism (Beck et al., 2017), where participants that do not fully trust each other agree on the ledger's content by running the consensus algorithm (Faria, 2018). In the beginning, the main aim of a blockchain (Nakamoto et al., 2008) was to:

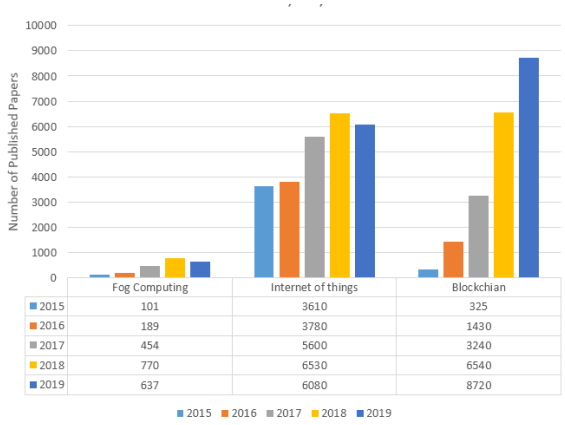
1. Transfer money without the Trusted Third Party (TTP), usually required in a traditional system,
2. Reduce the fees required for performing a transaction,
3. Reduce the time needed to perform the transaction.

As the topics of Blockchain, IoT, and FC are becoming more of hot research topics each year, we needed to investigate the current research trends in these fields. To do so, we searched for published articles having the key words 'Fog Computing', 'Internet of Things', and 'Blockchain', in their titles[1]. As presented in Figure 1, we have found that, in the years 2018 and 2019, the number of published papers having 'Blockchain' keyword in their title exceeds the number of published papers having 'Internet of Things' keyword in their title. As Figure 2 suggests, we have found that most of the integration proposals

[1]Numbers presented in the figures are gained by searching in Google Scholar: Accessed on 09-November-2019

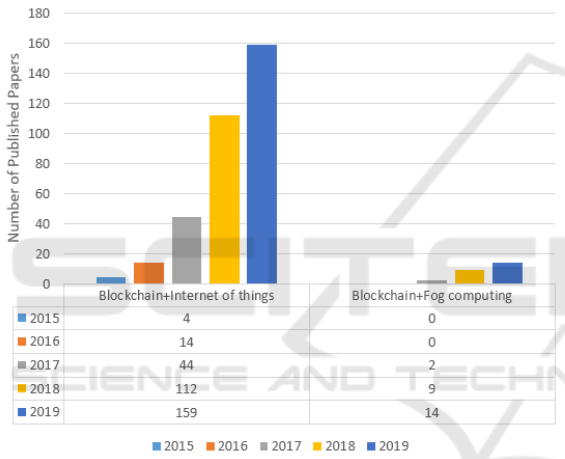


Baniata, H. and Kertesz, A.
PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism.
DOI: 10.5220/0009487904300439
In *Proceedings of the 10th International Conference on Cloud Computing and Services Science (CLOSER 2020)*, pages 430-439
ISBN: 978-989-758-424-4




| | Fog Computing | Internet of things | Blockchian |
|---|---|---|---|
| 2015 | 101 | 3610 | 325 |
| 2016 | 189 | 3780 | 1430 |
| 2017 | 454 | 5600 | 3240 |
| 2018 | 770 | 6530 | 6540 |
| 2019 | 637 | 6080 | 8720 |

Figure 1: Research trends in the fields of Fog Computing, Internet of Things, and Blockchain, in the the period 2015-2019.




| | Blockchain+Internet of things | Blockchain+Fog computing |
|---|---|---|
| 2015 | 4 | 0 |
| 2016 | 14 | 0 |
| 2017 | 44 | 2 |
| 2018 | 112 | 9 |
| 2019 | 159 | 14 |

Figure 2: Research trends concerning the integration of Blockchain with Fog Computing and the Internet of Things in the the period 2015-2019.

of Blockchain were performed with an IoT system, and only a small number of approaches tried to integrate the Fog computing paradigm with Blockchain.

In this paper, we propose a new *Validation* mechanism that maintains an equivalent consensus feature, where trusted fog nodes are able to validate transactions on behalf of blockchain nodes authenticated with it. Meanwhile, all nodes are deployed for the block confirmation and mining. The proposed mechanism is an approach for reducing the heavy load on the network, represented by extended validation time, and high energy consumption. On the other hand, the privacy-awareness property is preserved in our proposed mechanism by limiting the number of network nodes verifying a transaction generator.

The remainder of this paper is organized as follows. Section 2 presents the state of the art regarding integration approaches of blockchain, IoT, and fog computing. Secrion 3 explains the currently used validation mechanism in the Proof-of-Work (PoW) algorithm. Section 4 presents the motivations of our work, the proposed Un-Reliability concept, and the proposed framework of the PF-BVM. The experiment model and its results are presented in section 5, while Section 6 concludes our current and future work.

## 2 RELATED WORK

As FC was found a suitable paradigm to overcome IoT limitations, authors of (Puliafito et al., 2019) highlighted six IoT application domains that may benefit from the use of FC paradigm such as health care applications, vehicle applications, and smart cities.

Cisco started its own virtual Fog Data Services platform early in 2019 (Cisco, 2019), with at least 1.00 GHz computing power, 4-GB vRAM, and 23 GB storage. Authors of (Marin-Tordera et al., 2016) defined fog nodes as mini-clouds and categorized them according to the devices they are connected to; 'dump' and 'smart'. Authors of (Capra et al., 2019) surveyed the main techniques to design hardware platforms able to cope with IoT requirements. They discussed power consumption and management, IO architecture, security, memory, processing, and multicore enhancement.

Despite the fact that most previous works considered miners to be computationally-strong devices relatively to other nodes, some researchers proposed ideas where miners can be moderately strong mobile devices too (Suankaewmanee et al., 2018).

L.Axon (Axon, 2015) and colleagues (Axon and Goldsmith, 2016) discussed the public key infrastructure (PKI) concepts, and proposed a privacy-aware Blockchain-based PKI architecture. The trust in Blockchain is typically gained by the majority consensus of a piece of information validity, and a user verify-ability (Steem, 2017). However, the proposed architecture in (Axon, 2015) limits the necessity of verification by all nodes of the network. That is, public keys and private keys -online and offline versions- are only registered and verified by few previously-verified and trusted neighbours. Those keys are timestamped and have an expiration so that they should be regularly replaced. Also, a user-controlled identity disclosure mechanism is built, where each user chooses *whether* and *when* to disclose their identities or past public keys. Consequently, a PKI in which users have *total anonymity* and *neighbour group anonymity* is used.

A privacy-preserving carpooling system that uses

a private blockchain in a vehicular fog computing context, where the evaluation criteria were computational costs and communication overhead (Li et al., 2018). The second paper proposed an approach for using Blockchain to ensure the privacy of patient medical data in Fog environment by limiting authorized users accessing the patient's medical information (Silva et al., 2019).

Authors of (Debe et al., 2019) proposed a reputation system for fog nodes that are delivering services to the IoT devices, using Blockchain Ethereum smart contracts. The system suggests that IoT devices rate fog nodes according to specific modifiable criteria. Accordingly, fog nodes obtain trustworthiness value that would indicate how reliable they are. IoT devices' credibility is also computed, according to specific contributions, for the more credible the IoT device, the more effective its evaluation is on the final score of evaluated fog nodes.

# 3 VALIDATION IN A PoW-BASED BLOCKCHAIN SYSTEM

The probability that different nodes solving the puzzle at the same time is quite low yet existing. Such event is solved by *Forking*. Once a fork appears, two different versions of the blockchain will be considered valid to two different groups of nodes. After a while, the distribution of the two versions through the network will result in the consensus algorithm accrediting the longer chain, and withdrawing the shorter. However, each consensus algorithm has different forking protocol. Proof-of-Work (PoW) algorithm, specifically, is used in Bitcoin, Litecoin, and Ethereum platforms (Andrew Tar, 2018). Other examples of used consensus algorithms include versions of Proof-of-Stack (PoS), Distributed Proof-of-Stack (DPoS), and Practical Byzantine Fault Tolerance (PBFT) (Zee Ali, 2019).

Transaction validation is the process of checking whether the generator of the transaction (i.e. sender) has sufficient amount of money to spend, or determining whether the new transaction conforms to the network or consensus algorithm rules. This is usually performed in the nodes' level by checking the companion signature of a transaction; if the signature is valid, the transaction is accepted. The checking process includes comparing the amount of money the sender is willing to spend, to the amount of money registered in the sender's wallet in the blockchain, which is held locally within the nodes' memory (Chen et al., 2018). Once the transaction is *validated* by a miner, it is held in the miner's mempool until it is processed and added to a new block, hence *confirmed* (chytrik, 2017). When a whole block is confirmed, the miner broadcasts it to all nodes in the network. All recipient nodes then *validate all* transactions within the new block again (Nakamoto, 2008), and check if the solution of the puzzle was correct. If the block is valid in terms of transactions and puzzle solution, it is *confirmed* and added as the head of the locally saved blockchain, otherwise the block is ignored and the block generator is reported as malicious (Macdonald et al., 2017). However, as clarified in (Nguyen and Kim, 2018), the puzzle condition applies in most proof-based consensus algorithms such as the Proof of Work (PoW), Proof of Schedule (PoSch) (Wilczyński and Kołodziej, 2019), and Proof of Stack (PoS) algorithms(Wahab and Mehmood, 2018). In case of private blockchain systems, voting-based consensus algorithms are preferred, such as the Practical Byzantine Fault Tolerance (PBFT) algorithm used by IBM (Gerrit, 2018).

We also use the term '*Verification*' in this paper, which is also used in some papers to indicate what we call here *validation* as in (Pungila and Negru, 2019) and (Huang et al., 2019), while others might use the term *Approval* to indicate what we call here *Verification* as in (Wilczyński and Kołodziej, 2019). Nevertheless, we use the 'Verification' term in this paper to indicate the recognition of a transaction generator by other network entities through the linkage with his/her public/private keys.

# 4 PF-BVM: OUR PROPOSED VALIDATION MECHANISM

## 4.1 Motivations

1. **Privacy Awareness:** as declared in the global Blockchain survey (Deloitte, 2019), 62% of Chinese surveyed business owners believed that the biggest concern for them adopting Blockchain-based technologies is *privacy*. The percentage is close in Malaysia and USA with 51%. On the other hand, 50% of surveyed companies in twelve different countries think it would be better if they only could use Blockchain technologies privately/internally. Hence, we believe that the term Data-Protection-By-Design that was recently introduced for enhancing privacy (Varadi et al., 2020), needs to be adopted in Blockchain systems.
2. **Data Validation:** Blockchain is currently used in cryptocurrenies, but it is expected that within

few years blockchain will be used in most of the applications that require high security and reliability. For example, Blockchain-enabled e-voting (BEV) systems implementation is lately highly investigated and researched (Hanifatunnisa and Rahardjo, 2017)(Kshetri and Voas, 2018)(Ayed, 2017)(Hjalmarsson and Hjlmtsson, 2018). 43% of surveyed IT managers and CEOs think that they would recommend blockchain solutions for data validation, while 37% would recommend it for payment issues.

3. **Latency Enhancement:** Fog computing is mainly targeting delay-sensitive applications and services. On the other hand, the less validation time a Blockchain node consumes, the more time it spends on accepting new transactions (Pungila and Negru, 2019). This absolutely means higher operational efficiency of the system. However, not all fog nodes are resource rich; some of them have limited computation power, memory and storage (Yi et al., 2015). Authors of (Xu et al., 2018) categorized blockchain nodes into three types, namely: super, regular, and light nodes. Similarly, we consider two types of fog nodes; resource rich nodes, and resource poor nodes.
4. **Energy Efficiency:** Maintaining Blockchain security, reliability, and trust, depends on very high total power consumption rates (Miller et al., 2016). A single bitcoin transaction confirmation, for instance, consumes more power than an average U.S. household in 21 days (digiconomist, 2019). We are motivated by this fact to come up with a solution that maintains the decentralization and reliability of blockchain, yet be more energy efficient.

## 4.2 Trust in Blockchain

According to (Babar et al., 2010), Security, Privacy, and Trust are different but related concepts. Trust as viewed by (Kochovski et al., 2019), can mainly be described using probability, and, in a Fog Computing environment, should rely on binary decisions: Trusted or not Trusted. The privacy awareness, on the other hand, should consider identity, data, usage patterns, and location information. However, privacy in blockchain is preserved by different means. In blockchain, ledgers and blocks are transmitted to all connected nodes, blocks can be easily detected but can hardly be related to specific identity. This anonymity is caused by keeping public keys available for all nodes, yet anonymous. Blockchain relies on the exponential reduction of attack probability as the chain is growing, leading to the state where it is computationally impractical to attack the chain and change transactions. However, multi transaction generations with the same public key indicates the ownership of all these transactions by the same entity, which was proven to be a privacy threat in Bitcoin (Androulaki et al., 2013). Also, authors of (Chen et al., 2018) have shown the ability to infer identity information from smart contracts' source codes.

Trust, specifically, in a blockchain system majorly increases by the reliability the system provides (Lemieux, 2017). As will be shown later in this paper, the more transactions held in a block, the higher the time consumption for a block validation. Relatively, it should also be agreed on that the higher the number of transactions per block, the lower the trust in the system should be.

To clarify, we propose a concept for measuring the reliability of a Blockchain system called Un-Reliability (denoted by $R$), which depends on the probability of withdrawing a confirmed transaction, after a while of adding it to the chain, because of a malicious behaviour of the miner who generated the block, or simply because of the forking "Longest-Chain-Remains" protocol. If the probability of forking is $p$, then the probability a block being withdrawn is $p/2$ since one block will be withdrawn and the other will remain. For example, if $p$ equals to 0.001%, and the number of transactions $tx$ per a block $B$ equals to '5', then the probability that these transactions will be withdrawn, equals to $5 * p/2$ relative to total number of generated transactions on that day $T$. To generate the concept of percentage Un-Reliability $R$, we propose equation 1.

$$R = \frac{t * (p/2)}{T} \tag{1}$$

In the case of Bitcoin, the average number of transactions per block is 2,700 transactions as announced on Mar. 29. 2019 (Mitchell Moos, 2019). While the probability of forking evaluates to approximately $(5.54 * 10^{-6})$. This is about 0.000554% i.e. we'd expect two blocks to occur within two seconds once every 180k blocks (Murch, 2019). The total average transactions per day announced on Nov. 03. 2019 is about 290 thousand transactions (BlockChain.com, 2019). Here we can calculate $R$ /day as: $2700 * (0.000554/2)/290000\% = 2.6 * 10^{-6}$. Consequently, the following result can be observed:

***"The higher the probability of forking, or the higher the number of transactions per block, the higher the Un-Reliability indicator of the system, hence, the lower the level of Trust in the system should be."***

Out of the box, the concept of Un-reliability can be extended using other factors to indicate how reliable and trust-worthy the evaluated system is. Factors may include the probability of attacks, such as 51% attack (Dai et al., 2019) or selfish mining attack (Eyal and Sirer, 2018), encryption deployment, or the privacy-awareness in the system all in all (Androulaki et al., 2013). For instance, some famous blockchain systems, like Bitcoin and Ethereum, do not encrypt network messages (Faria, 2018), which shall negatively affect the level of trust in the system due to the lack of privacy, which is a foundation principal in some applications (Tuli et al., 2019). Private keys in those systems, however, are specifically encrypted using the Elliptic Curve Digital Signature (ECDS) which requires $((2^2)^5)^6$ trials in order to successfully fraud a signature. This is computationally impossible (Nguyen and Kim, 2018), which shall positively affect the level of trust in the system.

### 4.3 Framework and Principals of the Proposed PF-BVM

The trust management in PF-BVM is, in general terms, similar to the reputation system proposed by (Debe et al., 2019). The difference in our mechanism is that a fog node shall maintain 100% match score, as clarified in this subsection. In contrast, PF-BVM deploys some trust management concepts proposed in (Debe et al., 2019), yet it is not the same. Also, PF-BVM aims to provide privacy awareness, and enhanced BC validation using fog nodes. In order to achieve this goal, we need a trust management scheme. PF-BVM is a combination of different services provided by the fog, who must prove that it is trustful in order to be allowed to validate blocks instead of network nodes.

Generally, the system proposed by (Debe et al., 2019) is flexible and modifiable, so its deployment in PF-BVM is possible if some of the conditions were edited (Thresholds). Nevertheless, this system is only aiming to rank fog nodes according to their behaviour, yet it is not concerned with the validation and privacy as PF-BVM. The following principles present our proposed PF-BVM:

- *Trusted* fog nodes are authorized to validate new transactions on behalf of the nodes authenticated with it. A fog node is considered *trusted* as long as its acceptance/rejection decisions regarding new transactions match the decisions made by nodes authenticated with it in a percentage of 100% .
- A default status of a fog node is *not Trusted*. The level of trust increases through time by comparing decisions made by the fog node to decisions made by the blockchain nodes regarding new transactions. If the match percentage stays 100% for named number of transactions, the fog node status is switched to *Trusted*.
- A *Trusted* fog node is randomly, yet regularly, tested by nodes authenticated with it. In contrast, a new trusted fog node should be tested more frequently than a trusted fog node that had maintained the status of *Trusted* for longer time.
- The longer the fog node is *Trusted*, the fewer times it is tested for maintaining the 100% match. Yet the frequency of testing should never reach ZERO times per named number of transactions.
- The privacy awareness of the system is preserved by applying the PB-PKI architecture proposed in (Axon and Goldsmith, 2016). Using this architecture, the real identities of nodes shall be only known to the least number of users in the network. That is, a node reveals its user's identity only to neighbours that share the same fog-node domain, while the public keys are kept in the fog node's local memory. When a new transaction is generated, the node's public key is replaced with the fog-node's public key. Hence, the transaction can only be related to all nodes authenticated with that fog node. Consequently, the probability of disclosing the generator's real identity shall be totally minimized. This idea is shown in Figure 3. In scenario 'a', all nodes are connected and all nodes should *validate* a transaction, hence all network nodes shall *verify* the generator. In scenario 'b', only the fog node and the blockchain nodes connected to it are able to validate the transaction, yet the transaction is generated to the network as valid and referred to by the public key of the fog node domain.

## 5 EVALUATION

The evaluation experiments in our work considered two main factors, time consumption, and energy consumption. For doing so, we implemented a Python simulation[2] to exactly test what we needed to measure. Simulators like BlockSim (Alharby and van Moorsel, 2019), iFogsim (Gupta et al., 2017), and PeerSim (Montresor and Jelasity, 2009) simulates the validation time with a delay without actually performing the validation as it is in reality, hence all transactions in these simulators are considered valid.

[2]https://github.com/HamzaBaniata/BlockChainValidation/blob/master/First%20Code

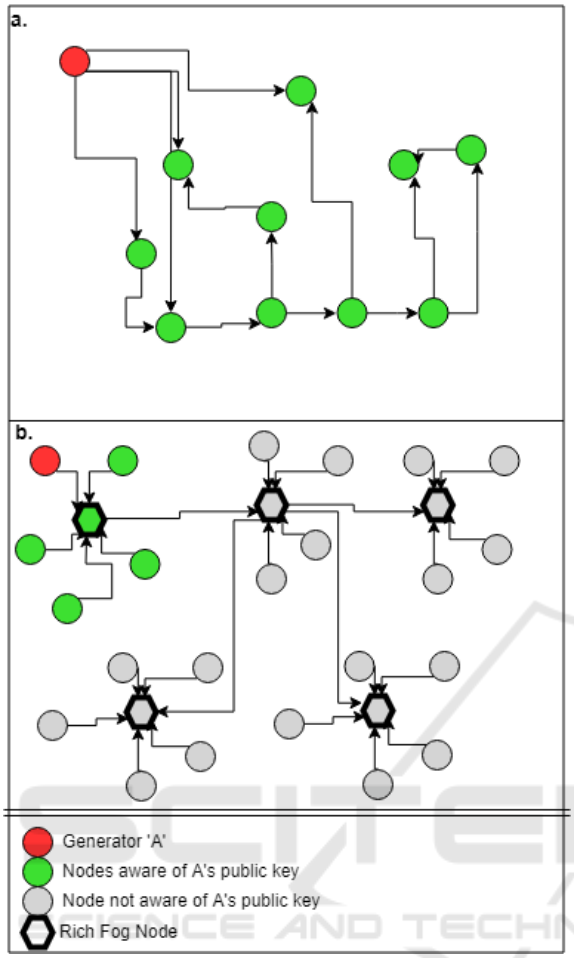



Figure 3: a PF-BVM conceptual network compared to the currently used network. a. all blockchain nodes are connected and responsible for a transaction validation. b. all blockchain nodes are connected yet few are responsible for a transaction validation.

In our implementation, we simulated a simple blockchain, where randomly generated numbers represented the transactions. Once a transaction is generated, it gets checked whether it is in a list of the valid transactions. If the data already exists in the list, an error message is printed on the screen, and the program moves to the next randomly generated transaction. If the data is not in the list, the program adds it to the list. Once the number of Tx/B -or gas limit- is reached the block is mined. The workflow of our simulation is presented in Figure 4.

## 5.1 Time Consumption

We performed the first experiment using an Intel i5-8265U CPU, backed up by 12 GB of DDR4 SDRAM and 45 GB vRAM. Figure 5 shows the re-

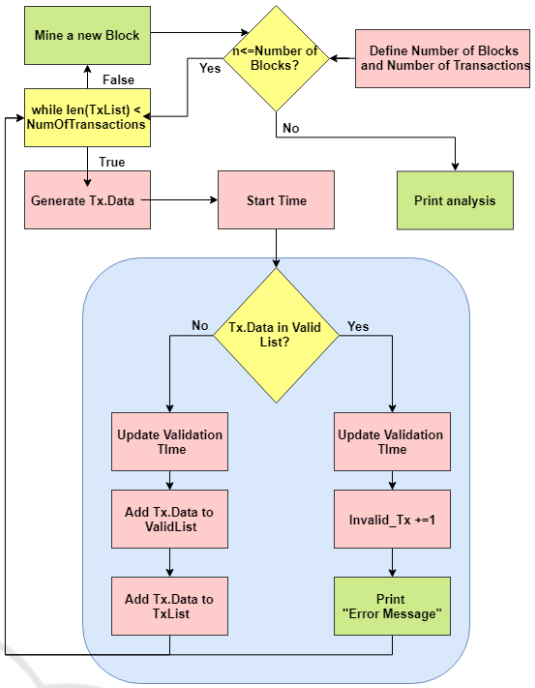



Figure 4: Workflow of our validation simulator.

sults of this experiment in which we tested four scenarios. The first scenario had a block configuration of 100 Transaction(Tx)/Block(B). Followed by the second scenario with a block configuration of 1000 Tx/B, Third scenario with 10000 Tx/B, and Fourth with 100000 Tx/B. We performed the four scenarios on eight groups of randomly generated transactions; 10,20,50,100,200,400,1000, and 3000 blocks. And finally we computed the average block validation time for each group by adding two variables to the code. The first variable before the start of transaction validation holding the value of current time, while the second is after the result of the validation holding the value of current time minus the first variable's value. A variable holding the summation of elapsed times is used at the end of the code to compute the average by dividing its value by the number of processed blocks.

It can be seen in the figure that the average time consumption for validating blocks holding 1000 transactions or less evaluates to almost zero. However, the validation time increased exponentially when multiplying the Tx/B ratio by '10'.

According to this experiment, more transactions saved in the ValidList, or more Tx/B rate, lead to exponential increase in time consumption of the validation process in general. such conclusion indicates that proposing a system where transactions and blocks be validated outside blockchain nodes, would save much processing time for them. Consequently, we compare, as suggested in (Svorobej et al., 2019), the average

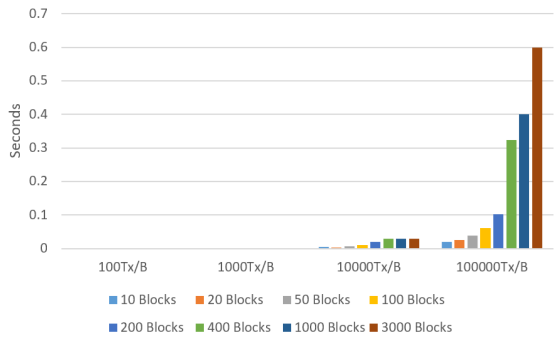



Figure 5: Average time consumption for block validation in a Blockchain node.

validation time consumed by two scenarios similar to those shown in Figure 3.

To compare the average time, we study a case where three rich fog nodes are connected to each other. Each fog node is connected to 10 blockchain nodes (both miners and non-miners), with total of 30 blockchain nodes. Once a transaction is generated by a node, it is distributed through the network to all nodes. Then, locally, all nodes perform the validation. If the time needed to validate this transaction equals x, then the total processing time consumed to validate this transaction equals 30x. In the case of PF-BVM, the total processing time consumed to validate this transaction equals 3x. That is, only the three fog nodes will spend time on validation, while the rest of network nodes are free to perform what ever else tasks they need to do. Equations 2 and 3 generalize the computation.

$$Time(Current) = nx \quad (2)$$

$$Time(PF-BVM) = kx \quad (3)$$

where;

- Time(Current): the total processing time needed to validate a transaction
- n: The total number of network nodes,
- x: Time needed to locally validate a transaction on one node,
- Time(PF-BVM): the total processing time needed to validate a transaction when using PF-BVM
- k: The number of authorized nodes to validate transaction.

Regarding the range of the time consumption in this experiment, it can be noticed that the maximum time consumed for validating a block is 0.6 sec. This is because we saved the blocks and the lists of our code in the RAM, which is faster than, and closer to, the CPU. To check if the pattern of the time consumption remains, we have implemented our code using Apache HTTP Server 2.4.41, with the valid transactions being saved in a MySQL database on the hard disk[3]. We got similar results of exponential increasing in time consumption, yet the range was higher. For example, using SSD disk, the scenarios of 100 Tx/B, 1000 Tx/B, and 10000 Tx/B applied on 10 Blocks resulted an average block validation time of 0.112, 4.9, and 419.9 seconds respectively.

## 5.2 Energy Consumption

When there are too many nodes, the communication performed to exchange agreements between them would be very complicated (Nguyen and Kim, 2018) and energy consuming (Kreku et al., 2017). To highlight energy consumption values of Blockchain systems, we recall the results shown in paper (Kreku et al., 2017), and summarize them in Figure 6. Kreu et al. showed the energy consumption for mining 400 blocks by two blockchain execution platforms: 'Raspberry Pi 2' and 'Nvidia Jetson TK1'. These results suggested that the more the miner nodes relative to the total number of nodes in the network, the less energy consuming the block confirmation is. Further, least energy consumption was gained when using only one miner node in a network that contains only one node in total.

Following these investigations, we can state that there is one explanation for such results, which is the wasted amount of energy. To clarify this, lets suppose that a network has two miner nodes out of total five network nodes. When a transaction is put in the mempool, the two miner nodes will start their Brute-Force process for finding the next block's nonce. One of these two miner nodes will find the solution before the other. This leads the winning miner to distribute the new block, while loser miner accepts the new block and stops working on it. The amount of energy spent by the loser miner had been wasted for no use at all, hence the lower the number of miner nodes working on a next block at the same time, the lower the energy consumed -by the system- to generate the block.

Similarly, the lower the number of nodes validating a transaction, the lower the energy consumed as a whole in the system. To clarify, lets suppose that the same five nodes of the previous example received a block from some other network entity. The five nodes will each consume equal amount of energy '$x$' to validate this block, depending on the Tx/B ratio and the number of blocks in the locally saved chain

[3]https://github.com/HamzaBaniata/BlockChainValidation/blob/master/Second%20Code

(Suankaewmanee et al., 2018). The total amount of energy consumed to validate this block equals to $5x$. If a validation protocol -such as ours- in which only one of the five nodes is trusted and authorized to validate the block on behalf of the other four nodes, then the total amount of consumed energy evaluates to $1/5$ relative to the energy consumed by the first system. To generate the computation method of the consumed energy in PF-BVM, we used equation 4.

$$E = \frac{k}{n}\% \tag{4}$$

Where;

- $E$: Consumed energy percentage by PF-BVM compared to current protocol,
- $k$: The number of authorized nodes to validate transactions,
- $n$: The total number of network nodes

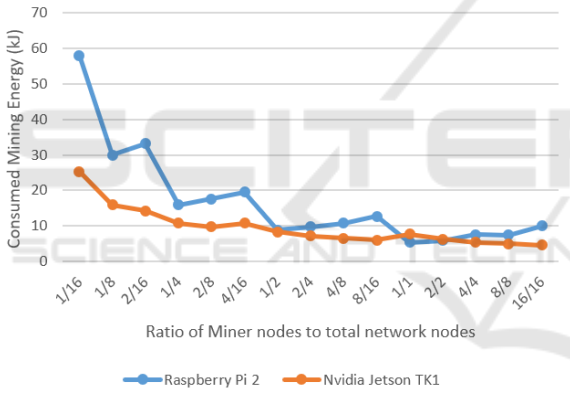



Figure 6: Energy consumption when mining 400 blocks by two different blockchain execution platforms.

To present the effect of our proposed PF-BVM, we simulated the energy consumption, using equation 4, in our provided validation simulation code. The results of our simulation are presented in Figure 7. In our simulation experiment, the value of $k$ changes, while the value of $n$ equals 50 nodes.

As it can be seen in Figure 7, the less the number of nodes validating a transaction, the less the total energy consumed to validate a transaction, hence, the more efficient the system is. We also need to mention here that the same approach of calculations can be applied for evaluating the storage efficiency proposed by PF-BVM. For example, $n*$ 150 and 46 GB storage, used to locally save Bitcoin and Ethereum chains respectively (Reyna et al., 2018), can be reduced to $k/n$ % needed storage capacity for the whole system.

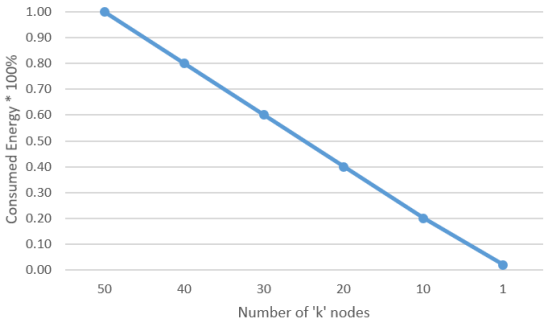



Figure 7: Energy consumption when validating a transaction using PF-BVM.

## 6 CONCLUSION

In this paper we proposed a Privacy-aware Fog-enhanced Blockchain Validation Mechanism (PF-BVM), which contributes to the integration of fog computing, the internet of things and blockchain techniques. We used the concept of Un-Reliability to indicate, how reliable a blockchain system is. As a conceptual criterion, PF-BVM allows trusted rich fog nodes to perform transaction validation on behalf of other network nodes. The trust is gained by randomly running matching tests by network nodes. Our work showed that the higher the number of transactions per block, and the higher the probability of forking, the higher the Un-Reliability metric of the blockchain system. To evaluate our proposed mechanism, we implemented a specially designed simulation code and the experimental results showed that PF-BVM can significantly enhance a blockchain system validation in terms of time consumption, energy efficiency, and storage capacity. Our future work will be directed towards investigating available BC-FC integration approaches. According to our investigations, we will build a simulation environment for BC-FC solution, relying on the PF-BVM source code. We will also be developing PF-BVM in order to measure the dynamics of trust evolution over time for BC nodes.

## ACKNOWLEDGEMENTS

The research leading to these results was supported by the Hungarian Government and the European Regional Development Fund under the grant number GINOP-2.3.2-15-2016-00037 (”Internet of Living Things”), by the Hungarian Scientific Research Fund under the grant number OTKA FK 131793, and by the grant TUDFO/47138-1/2019-ITM of the Ministry for Innovation and Technology, Hungary.

# REFERENCES


Alharby, M. and van Moorsel, A. (2019). Blocksim: A simulation framework for blockchain systems. *ACM SIGMETRICS Performance Evaluation Review*, 46(3):135–138.

Andrew Tar (2018). Proof-of-work. https://cointelegraph.com/explained/proof-of-work-explained. [Online; accessed 29-October-2019].

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., and Capkun, S. (2013). Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 34–51. Springer.

Axon, L. (2015). Privacy-awareness in blockchain-based pki. *Cdt technical paper series*.

Axon, L. and Goldsmith, M. (2016). Pb-pki: A privacy-aware blockchain-based pki.

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09.

Babar, S., Mahalle, P., Stango, A., Prasad, N., and Prasad, R. (2010). Proposed security model and threat taxonomy for the internet of things (iot). In *International Conference on Network Security and Applications*, pages 420–429. Springer.

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. (2017). Blockchain technology in business and information systems research.

BlockChain.com (2019). Blockchain charts. https://www.blockchain.com/en/charts. [Online; accessed 03-November-2019].

Capra, M., Peloso, R., Masera, G., Ruo Roch, M., and Martina, M. (2019). Edge computing: A survey on the hardware requirements in the internet of things world. *Future Internet*, 11(4):100.

Chen, T., Zhu, Y., Li, Z., Chen, J., Li, X., Luo, X., Lin, X., and Zhange, X. (2018). Understanding ethereum via graph analysis. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 1484–1492. IEEE.

chytrik (2017). How blockchain transaction verification takes place? https://bitcoin.stackexchange.com/questions/64455/how-blockchain-transaction-verification-takes-place. [Online; accessed 03-November-2019].

Cisco (2019). Cisco fog data services. https://www.cisco.com/c/en/us/products/cloud-systems-management/fog-data-services/index.html?dtid=osscdc000283. [Online; accessed 09-November-2019].

Dai, H.-N., Zheng, Z., and Zhang, Y. (2019). Blockchain for internet of things: A survey. *arXiv preprint arXiv:1906.00245*.

Debe, M., Salah, K., Rehman, M. H. U., and Svetinovic, D. (2019). Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain. *IEEE Access*, 7:178082–178093.

Deloitte (2019). Deloitte's 2019 global blockchain survey.

digiconomist (2019). Bitcoin energy consumption index. https://digiconomist.net/bitcoin-energy-consumption. [Online; accessed 14-November-2019].

Eyal, I. and Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102.

Faria, C. (2018). Blocksim: Blockchain simulator.

Gerrit (2018). Hyperledger fabric. https://github.com/hyperledger/fabric. [Online; accessed 09-November-2019].

Gupta, H., Vahid Dastjerdi, A., Ghosh, S. K., and Buyya, R. (2017). ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. *Software: Practice and Experience*, 47(9):1275–1296.

Hanifatunnisa, R. and Rahardjo, B. (2017). Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pages 1–6. IEEE.

Hjalmarsson, Fririk, H. G. K. H. M. and Hjlmtsson, G. (2018). Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986. IEEE.

Huang, H., Li, K.-C., and Chen, X. (2019). Blockchain-based fair three-party contract signing protocol for fog computing. *Concurrency and Computation: Practice and Experience*, 31(22):e4469.

Kochovski, P., Gec, S., Stankovski, V., Bajec, M., and Drobintsev, P. D. (2019). Trust management in a blockchain based fog computing platform with trustless smart oracles. *Future Generation Computer Systems*, 101:747–759.

Kreku, J., Vallivaara, V. A., Halunen, K., Suomalainen, J., Ramachandran, M., Muñoz, V., Kantere, V., Wills, G., and Walters, R. (2017). Evaluating the efficiency of blockchains in iot with simulations. In *IoTBDS*, pages 216–223.

Kshetri, N. and Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, 35(4):95–99.

Lemieux, V. L. (2017). Blockchain and distributed ledgers as trusted recordkeeping systems. In *Future Technologies Conference (FTC)*, volume 2017.

Li, M., Zhu, L., and Lin, X. (2018). Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet of Things Journal*.

Macdonald, M., Liu-Thorrold, L., and Julien, R. (2017). The blockchain: a comparison of platforms and their uses beyond bitcoin. *COMS4507-Adv. Computer and Network Security*.

Marin-Tordera, E., Masip, X., Garcia Almiñana, J., Jukan, A., Ren, G.-J., Zhu, J., and Farre, J. (2016). What is a fog node a tutorial on current concepts towards a common definition.

Markakis, E. K., Karras, K., Zotos, N., Sideris, A., Moysiadis, T., Corsaro, A., Alexiou, G., Skianis, C., Mastorakis, G., Mavromoustakis, C. X., et al. (2017). Exegesis: Extreme edge resource harvesting for a virtualized fog environment. *IEEE Communications Magazine*, 55(7):173–179.

Miller, A., Xia, Y., Croman, K., Shi, E., and Song, D. (2016). The honey badger of bft protocols. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 31–42. ACM.

Mitchell Moos (2019). Bitcoin transactions per block at all-time highs. https://cryptoslate.com/bitcoin-transactions-per-block-at-all-time-highs/. [Online; accessed 03-November-2019].

Montresor, A. and Jelasity, M. (2009). Peersim: A scalable p2p simulator. In *2009 IEEE Ninth International Conference on Peer-to-Peer Computing*, pages 99–100. IEEE.

Murch (2019). What is the probability of forking in blockchain? https://bitcoin.stackexchange.com/questions/42649/what-is-the-probability-of-forking-in-blockchain. [Online; accessed 03-November-2019].

Nakamoto, S. (2008). Bitcoin whitepaper.

Nakamoto, S. et al. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nguyen, G.-T. and Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, 14(1).

Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., and Rana, O. (2019). Fog computing for the internet of things: A survey. *ACM Trans. Internet Technol.*, 19(2):18:1–18:41.

Pungila, C. and Negru, V. (2019). Improving blockchain security validation and transaction processing through heterogeneous computing. In *International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)*, pages 132–140. Springer.

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.

Silva, C. A. d., de Aquino Júnior, G. S., and Melo, S. R. M. (2019). A blockchain-based approach for privacy control of patient's medical records in the fog layer. In *Proceedings of the 25th Brazillian Symposium on Multimedia and the Web*, WebMedia '19, pages 133–136, New York, NY, USA. ACM.

Steem (2017). Steem an incentivized, blockchain-based, public content platform. https://steem.io/SteemWhitePaper.pdf. [Online; accessed 21-November-2019].

Suankaewmanee, K., Hoang, D. T., Niyato, D., Sawadsitang, S., Wang, P., and Han, Z. (2018). Performance analysis and application of mobile blockchain. In *2018 international conference on computing, networking and communications (ICNC)*, pages 642–646. IEEE.

Svorobej, S., Takako Endo, P., Bendechache, M., Filelis-Papadopoulos, C., Giannoutakis, K. M., Gravvanis, G. A., Tzovaras, D., Byrne, J., and Lynn, T. (2019). Simulating fog and edge computing scenarios: An overview and research challenges. *Future Internet*, 11(3):55.

Tuli, S., Mahmud, R., Tuli, S., and Buyya, R. (2019). Fogbus: A blockchain-based lightweight framework for edge and fog computing. *Journal of Systems and Software*.

Varadi, S., Varkonyi, G. G., and Kertész, A. (2020). Legal issues of social iot services: The effects of using clouds, fogs and ai. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, pages 123–138. Springer.

Wahab, A. and Mehmood, W. (2018). Survey of consensus protocols. *arXiv preprint arXiv:1810.03357*.

Wilczyński, A. and Kołodziej, J. (2019). Modelling and simulation of security-aware task scheduling in cloud computing based on blockchain technology. *Simulation Modelling Practice and Theory*, page 102038.

Xu, Q., Aung, K. M. M., Zhu, Y., and Yong, K. L. (2018). A blockchain-based storage system for data analytics in the internet of things. In *New Advances in the Internet of Things*, pages 119–138. Springer.

Yi, S., Hao, Z., Qin, Z., and Li, Q. (2015). Fog computing: Platform and applications. In *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, pages 73–78. IEEE.

Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., Kong, J., and Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*.

Zee Ali (2019). A simple introduction to blockchain algorithms. https://blog.goodaudience.com/a-simple-introduction-to-blockchain-algorithms-ca05b9bcc32f. [Online; accessed 26-October-2019].