Tanzania Journal of Engineering and Technology 2023, **42(2)**: 44-54
OPEN ACCESS articles distributed under Creative Commons Attribution Licence [CC BY-ND]
Websites: https://ajol.org/tjet; https://tjet.udsm.ac.tz

ISSN 1821-536X (**print**); ISSN 2619-8789 (**electronic**)
https://doi.org/10.52339/tjet.v42i2.876

Regular Research Manuscript

Path of Trust: An Off-Chain Performance Enhancement Algorithm for Public Blockchains

Anthony Kigombola[†], **Mercy Mbise and Prosper Mafole**

Department of Computer Science and Engineering, University of Dar es Salaam, Dar es Salaam, TANZANIA

[†]Corresponding author: kigombola@gmail.com;

ORCID: https://orcid.org/0000-0003-1838-5861

ABSTRACT

Blockchain technology is one among the latest innovations in computing industry. Blockchains have gathered widespread interest in the industry due to their potential as secure data storage. Despite the potential benefits of blockchains, there are several limitations which hinders mass deployment, one of these limitations being low throughput. Low throughput has limited blockchain adoption in large scale applications such as banking or mobile payments. This study addresses this limitation through development of a performance enhancement algorithm called Path of Trust (PoT). PoT uses off-chain stratergy in which transactions meeting certain criteria bypass the main chain and sent direct to the recipient. The PoT algorithm was incorporated into a blockchain wallet that was developed as a mobile app. Experiments were run to verify the performance of the developed solution. Based on the experiments performed, the performance of the blockchain based on the developed solution was improved when compared to the original blockchain. With PoT algorithm running, the average transaction processing time was 12.81 secs per transaction compared to 18.52 secs when PoT was not running.

.

ARTICLE INFO

First submitted: Jan. 15, 2023

Revised: Mar. 14, 2023

Accepted: Apr. 20, 2023

Published: June 20, 2023

Keywords: *Blockchain, Off-Chain Transactions, Performance, Path of Trust*

INTRODUCTION

A blockchain is a data structure that stores digital objects and their ownership history (Crosby, 2016). Blockchain was made famous through Bitcoin, a decentralized peer-to-peer electronic cash system (Nakamoto, 2008). Two features that distinguish blockchains from other data structures are first, immutability and second decentralized trust (Yli-Huumo et al., 2016). Immutability is the difficult to change data once recorded in a system. Blockchain uses cryptographic hash to link data stored between blocks. This makes a cascaded chain of blocks that are linked with one another making transactions modification rather difficult. Decentralized trust feature implies that in blockchains there is no central authority with control over the network of participating nodes (Crosby, 2016). Since the system is decentralized, it does not require a third-party organization in the middle, this feature makes the system more transparent and reliable than it is in centralized systems (Yli-Huumo et al., 2016). Blockchain technology has a big potential to address the many challenges facing electronic financial services delivery (Crosby, 2016) which is faced by several security challenges

including fraud and theft (Fernandes, 2013). A study performed by IBM in 2022 showed that between 2015 to 2020, finance and insurance were the most targeted industries by cyber criminals globally (IBM Security, 2022). The study also shows that 70% of the attacks on these firms targeted banks, 16% targeted insurance companies, and 14% targeted other financial institutions in 2021 (IBM Security, 2022). However, blockchains have relatively low throughput for processing transactions (Golan Gueta et al., 2019; L. Yang et al., 2020; Li et al., 2020; Nguyen et al., 2019; Nurfatih et al., 2020; Tao et al., 2020). Having low throughput has limited the adoption of blockchains in mainstream financial services such as banking and mobile payments which process a huge volume of transactions at a time (Dashkevich et al., 2020).

There are several initiatives carried out by researchers in the area of blockchain performance. Most of these initiatives falls under three main categories: First, providing alternative to the Proof of Work consensus ((Wang, 2019), (Kwon & Yu, 2019), (Nurfatih et al., 2020), (Cao et al., 2019) and (Dai et al., 2019)). Second, sharding which is partitioning of the blockchain network into smaller broadcast domains ((Nguyen et al., 2019), (Tao et al., 2020), (Yu et al., 2020), (Dang et al., 2019) and (Chen & Wang, 2019)) and third, use of off-chain channels which bypass the main blockchain to send transactions directly between sender and receiver ((Poon & Dryja, 2016), (Yang et al., 2020), (Sakakibara et al., 2018), (Lind et al., 2018) and (Li et al., 2020)). While these studies were aimed at improving the throughput of blockchains, literature showed that these studies were focused on general performance improvement with less emphasis on specific needs for a particular sector for example mainstream financial services. This study was aimed at improving the performance of blockchains while considering the specific and sensitive requirements of the mainstream financial services such as security, performance, and usability.

In this study, the approach used to address blockchain performance limitation was based on developing an off-chain performance enhancement algorithm called Path of Trust (PoT) Algorithm. The PoT algorithm is a routing algorithm which routes transaction either off-chain (directly to the recipient wallet) or on-chain (broadcasting it to the blockchain network). The routing is based on the trusting relationship between the sender and receiver. When sender A sends a coin to recipient B, the PoT algorithm will check if A and B are trusting partners (TP). If yes it will send the coin direct to B through the off-chain channel. If A and B are not trusting partners, it will forward the request to the blockchain for normal transaction processing. Figure 1 shows a high-level architecture of the PoT algorithm**.**

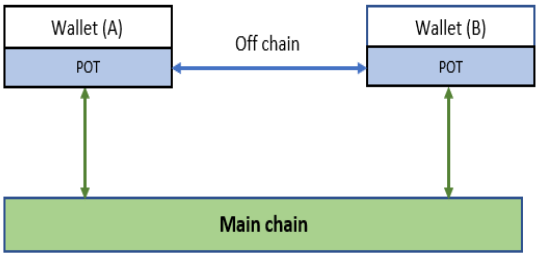

Figure 1: Off-chain payments.

Now, the questions to ask and guide this research study are

(i) What are the design limitations causing blockchains to have low throughput?
(ii) What are the performance requirements for systems in electronic financial services?
(iii) What blockchain system will meet throughput requirements suitable for mainstream electronic financial services?
(iv) How does the performance of the developed blockchain system meet the requirements for mainstream electronic financial services?

METHODS AND MATERIALS

The solution to address the performance problem was developed as a blockchain wallet which incorporates the PoT algorithm. The development activities were broken down

into four stages, definition of requirements, design, development, and testing. The first stage, requirements definition was conducted through documents review and analysis. The documents reviewed includes proposals, specifications, and white papers on electronic payments systems. The second stage, design was done to translate the system requirements to a format that can be easily implemented into code. The design of the solution was performed using UML software design tools. In the third stage, the proposed solution was developed as a blockchain wallet with PoT algorithm embedded in it. The wallet was developed as a mobile app using React Native and Dart programming language. VS Code IDE was used as the development environment for the app. In the last stage the developed solution was tested to verify its performance against the set objectives. The testing was done by users running the wallet app in their smart phones and sending transactions to each other over Ethereum blockchain platform.

Design and development work

The Path of Trust (PoT) algorithm was designed to provide an alternative path for sending transactions between users without passing through the main blockchain. These transactions that are sent direct between users are called off-chain transactions. Off-chain transactions are sent directly from sender wallet to recipient wallet, any delay in the blockchain processing will not delay the delivery of the transaction to the recipient and hence not affect the user experience. As off-chain transaction bypass the main blockchain to enhance the speed, they also bypass the security stronghold provided by blockchains. To mitigate the security bypass, two more components were added to the PoT algorithm to ensure transaction integrity. Firstly, the sender and receiver have to create a trust partnership (TP) before they can send off-chain transactions. Secondly, the system constantly updates wallets with actual values from the blockchain, this makes sure that users balance between wallets and the blockchain are consistent. The PoT algorithm has 4 main workflows: trust partnership (TP) establishment, transactions routing, trust partnership eligibility rating and balance update.

Trust partnership establishment

Before users can participate in off-chain transactions, a trust partnership (TP) pair with each other must be established. The TP is established as a request sent from user A and accepted by target recipient B. The procedure for two users A and B to establish a trust partnership is described in the workflow as summarized by the activity diagram shown in Figure 2.

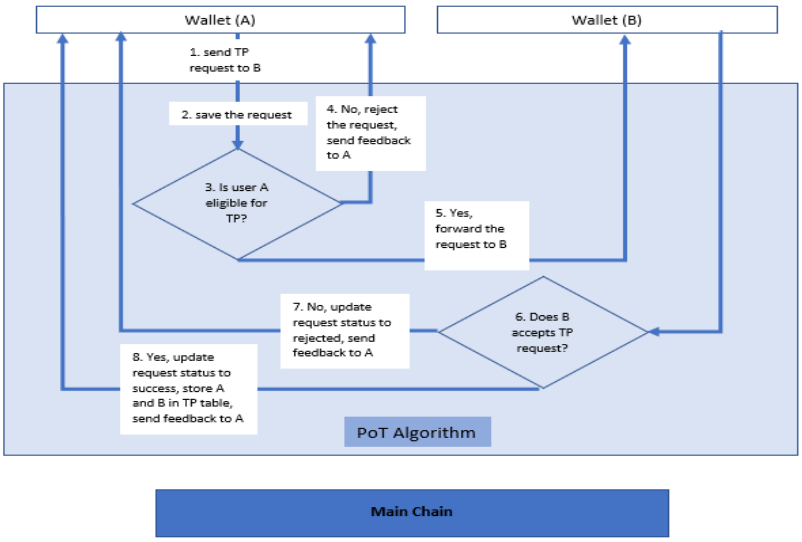

Figure 2: TP establishment.

Transactions routing

When a user sends a coin the system routes it either on-chain or off-chain based on the PT relations between the users. The procedure for user A to send a transaction to user B is described in the workflow below:

Step 1: A sends x coins to B

Step 2: PoT stores the transaction with status "new"

Step 3: PoT checks if A and B are trusting partners (TP)

If No, then PoT forwards the transaction to the main chain AND PoT updates the transaction status to "fwd not tp'

If Yes, PoT checks if A has enough balance to send x coins?

- If No enough balance, PoT forwards the transaction to the main chain AND PoT updates the transaction status to "fail no balance''.
- If Yes, PoT debits x coins from A wallet AND PoT credits x coins to B wallet THEN PoT updates the transaction status as "completed".

Step 4: PoT forwards the transaction to the main chain and checks if the transaction processed successfully by the main chain

If Yes, PoT updates transaction status to "confirmed"

If No, THEN PoT updates balance with the current balance from main chain AND PoT sends a signal to other wallets to update their balances with values from the main chain

OTHERWISE PoT updates the transaction status to rejected.

Eligibility rating

Periodically the system evaluates and rates the eligibility of a user to establish a TP pair based on their past activities in the system. This rating is used by the PoT layer to either accept or reject TP establishment request from a user. The eligibility criterion is calculated based on the following parameters: current rating, past request success rate and past transactions success rate. The eligibility rating is either 1 (eligible) or 0 (not eligible). The proposed mathematical equation for computing the eligibility rating (er) is

$$er = round(0.3cr + 0.3tp_{succ}\% + 0.4tn_{succ}\%) \quad (1)$$

where: *cr* (Current user rating). It has two values, 1 the user is eligible, 0 the user is not eligible for TP establishment, tp_{succ} (TP requests success rate) is the percentage of successful trusting partnership requests made by the user. The tn_{succ} (Transactions success rate). Percentage of successful transactions made by the user. The TP eligibility update workflow is summarized in the flowchart in Figure 3.

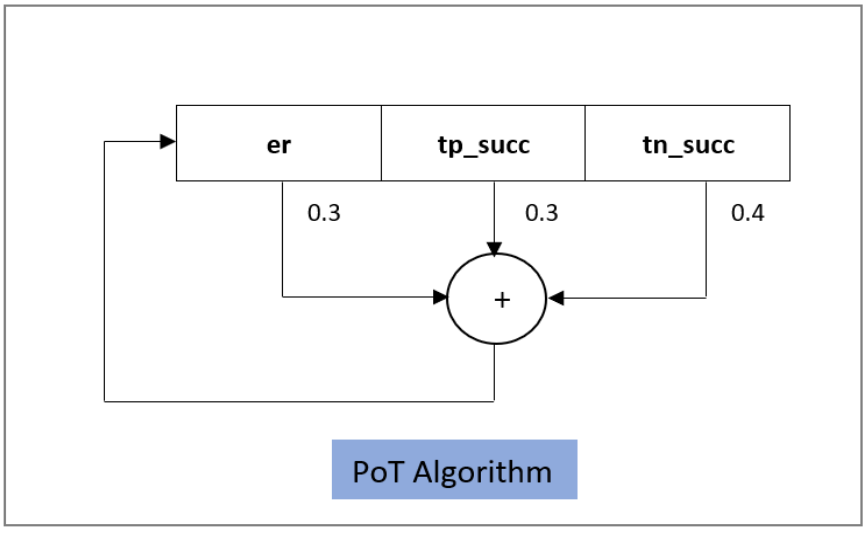

Figure 3: TP eligibility rating.

Balance update

The PoT algorithm will regularly update account balances on wallets with values from the main chain to ensure that the off-chain values are in sync with the actual values on the main chain. The procedure for updating account balance is described in the workflow below:

1. Has the timer reached the update time, T?

1.1. Yes, Is there a transaction failure message from BC

1.1.1 No, Do nothing

1.1.2 Yes, Update all users with current balance from BC

1.2 No, Do nothing

The wallet was developed as an Android mobile app using Flutter, an open-source software development kit which enables cross-platform mobile app development. Based on the modular approach used during design stage, the wallet was segmented into several modules which are grouped as frontend and backend components. Frontend components consisted of user access management, payments management, accounts management and trust partnership establishment. Backend components consisted of data storage, public key cryptography, routing, peer to peer middleware and interface for connecting to the blockchain. The wallet app can be downloaded from Google Play Store under the name Dinari.

A blockchain platform was set up for conducting experiments to showcase the functionality of the prototype and verify its performance. The developed wallet connected to this blockchain platform for performing operations such as checking balance, sending, and receiving transactions. The platform consisted of six nodes interconnected with one another via an IP network. The blockchain platform was based on Geth, an open-source implementation of Ethereum. Figure 4 shows the network diagram of the blockchain platform set up for experimentation. The experimentation platform can be accessed online at https://dinari.co.tz and the wallet can be downloaded as a mobile app from Google Play Store.

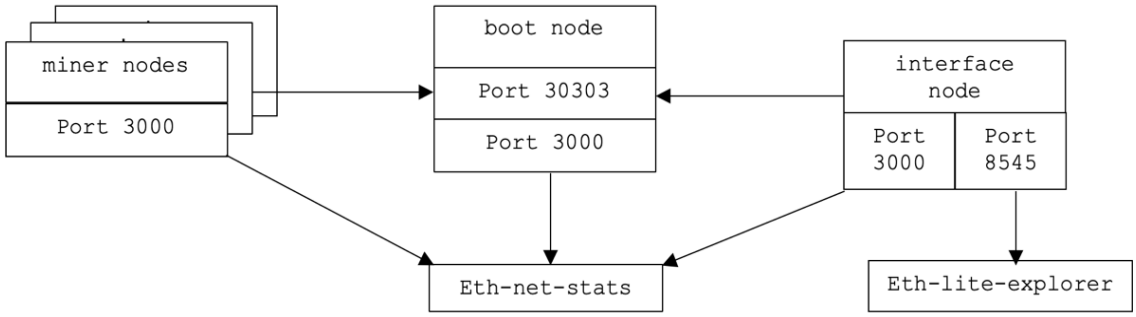

Figure 4: Experimentation platform layout.

Experiments and data collection

The question to be answered by these experiments was whether the introduction of the PoT algorithm has resulted to an increase in blockchain performance. In the experiment setting, the independent variable was the PoT functionality on the wallet app. The independent variable had two manipulation levels 'Off' and 'On' where the value of 'Off' reflects an original blockchain system without the performance enhancement functionality and 'On' was the blockchain system with the performance enhancement functionality in place. The dependent variable was the transaction processing time whose values were monitored and recorded as the independent variable was altered.

The collected metric was the time taken to process a transaction from when it was sent by user A to when it is received by user B. This

metric was important as it was used to verify the performance of the developed algorithm. To get control and test data, the experiments were divided into three sets, first running the experiments using CLI tool, second running experiments using the developed wallet but with PoT feature switched off and lastly with PoT feature switched on. The first experiment was a control experiments which provided control data that was used as a benchmark to verify the data collected using the developed wallet. Table 1 shows the transaction times recorded from running the experiment. The results show that the transaction processing time had a minimum value of 1 s per transaction, maximum value of 42.37 s, a median value of 5.02 s and average value of 15.28 s.

Table 1: Control Experiment

S/N	Time (sec)
1	5.24
2	3.18
3	5.33
4	3.51
5	17.22
6	2.15
7	42.37
8	31.28
9	14.21
10	31.25
11	12.37

The recorded values were compared and found to be matching with values from other public Ethereum blockchains such as Mainnet, Ropsten and Kovan. Table 7.1 shows the summary of transaction times recorded from different Ethereum public networks using Etherscan tool (etherscan.io). From the summary it is seen that the other public networks have transaction processing times between 1 sec to 41 s and an average of 14 s. The second run of experiments were performed by users exchanging transactions through the wallet app while switching off the PoT functionality. Table 3 shows the transaction times recorded from running the experiment.

Table 2: Transaction times from public networks

	Min Value	Max Value	Average	Median
Mainnet	01	41	12.76	09
Ropsten	01	33	9.92	09
Kovan	16	39	18.88	19
Dinari	01	42	15.28	12

Table 3: Processing time with PoT switched Off

Time (Sec)			
1 Transaction	**2 Transactions**	**4 Transactions**	**8 Transactions**
24.89	13.76	30.23	19.31
25.54	23.82	17.35	18.52
9.16	16.20	13.64	
17.58	11.3		
20.34	13.45		
16.58	22.22		
23.35			
24.42			
21.39			

Based on the collected data, the transaction processing time had a minimum value of 7.08 s maximum value of 30.23 seconds and an average value of 18.71 s. When compared to the control data presented earlier, the collected values are within the acceptable range of accuracy. This verify that the developed wallet did not introduce unnecessary delays or lags inherent with introduction of a software program layer to an existing system.

The third set of experiments were performed by user sending transactions through the wallet app while switching on the PoT functionality. Table 4 shows the transaction times recorded from running the experiment.

Table 4: Transaction times with PoT switched On

Time (Sec)			
1 Transaction	**2 Transactions**	**4 Transactions**	**8 Transactions**
1.24	1.54	2.16	3.01
1.20	2.54	2.11	2.27
1.31	2.31	3.17	
1.16	1.58		
1.49	2.35		
1.27	2.27		
1.15			
1.34			
1.47			
1.23			
1.52			

From Table 4 it is seen that the transaction processing times had a minimum value of 1.15 s, maximum value of 3.17 s and an average value of 2.13 s. The results show lower transaction processing times when compared to the results with PoT switched off (average of 18.81 s). The reduction in transaction processing time suggests that the introduction of the PoT algorithm improved the performance of the blockchain system. The 2 s average which is a little bit higher compared to traditional services such as mobile payments with an average processing time of 1 second was due to delays introduced by the P2P protocol implemented in the wallet for transferring off-chain transaction.

RESULTS AND DISCUSSION

Experiment results show that the introduction of PoT algorithm has decreased the average transaction processing time from about 18 secs to 2 secs. This decrease in transaction processing time was contributed by the fact that transactions that goes off-chain were delivered almost immediately. Experiments also shows that, the performance improvement increased as the number of concurrent transactions issued in in the network increases. Figure 6 shows comparison of transaction processing times with increase in the number of parallel transactions for the case when PoT is off and when it is on

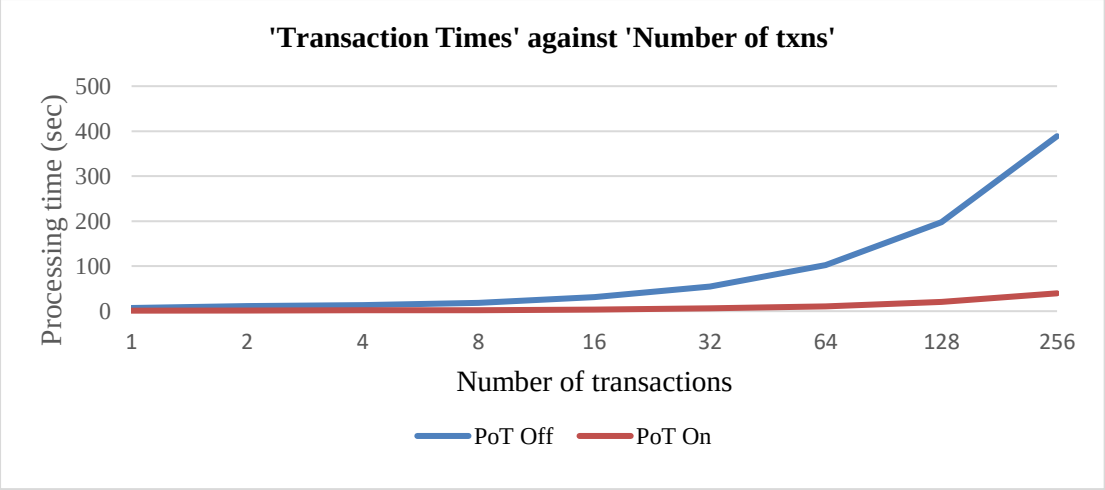

Figure 6: Performance vs number of parallel transactions.

From Figure 6 it is seen that when the number of parallel transactions increases, the system becomes congested and longer times are required to process the transactions. For the case of Ethereum with a block size of around 70 transactions per block, some of the transactions have to be kept in a queue waiting to be included in the next block. Using PoT algorithm relieved the system by sending transactions directly between wallets hence by-passing the blockchain system. This reduces the number of transactions waiting in the queue and also reduce transaction waiting time.

RQ 1: What are the design limitations causing blockchains to have low throughput?
Answer: The low throughput in blockchains is caused by the design of its architecture especially in the consensus algorithm. Most of the early blockchain platforms such as Bitcoin and Ethereum used Proof of Work (PoW) as a consensus algorithm. PoW mining process uses complex probability computations to verify transactions. These computations consume a lot of resources including computing resources and time. This makes PoW-based consensus to be the major cause of performance bottleneck in most blockchains. Other factors which contribute to blockchain performance limitations includes small size of transaction blocks, latency in the underlying network which can cause delays in blocks transmission, and lack of parallelism in blockchains as transactions and block processing are done in series one after the other.

RQ 2: What are the performance requirements for systems in electronic financial services?
Answer: Based on the data collected from several financial services applications including M-Pesa, Airtel Money, NBC Kiganjani, GePG and TIPS the performance requirements for mainstream financial services were established to T values between 1 to 30 seconds and for TPS values from 100 and above.

RQ 3: What blockchain system will meet throughput requirements suitable for mainstream electronic financial services?
Answer: This study developed a blockchain wallet that runs a performance enhancement algorithm, called PoT algorithm, which routes transactions directly between users based on Trusting Partnership (TP) relations between the users. Direct exchange of transactions bypasses the blockchain hence reducing transaction processing times. Experiments results showed that the PoT algorithm improved the transaction processing time from an average of 18 s per transaction to 2 s per transaction.

RQ 4: How does the performance of the developed blockchain system meet the requirements for mainstream electronic financial services?

Answer: The developed platform provided an average transaction processing time of 2 secs for a transaction to reach the intended recipient with the PoT feature switched on. This is within the threshold of 30 secs that was set as a requirement for mainstream financial services. Based on the experiments results, PoT algorithm provides a 9-factor performance gain when compared to a traditional blockchain system. Considering the case of Ethereum with an average throughput of 15 TPS, the use of PoT based wallet will improve its throughput to 135 TPS.

Limitation to the Study

The performance of the ToP functionality depends on the number of established Trust Partnerships (TP) between users performing transactions. In an ideal scenario, as in the experiments described above, all senders had established TP relations with receivers which made 100% of transactions to be routed off-chain. In a real scenario this might be different as the number of TP relations between users will be less than 100%. For users with no TP relations, their transactions will be sent on-chain via the blockchain network thus minimizing the benefits of the PoT functionality. A mathematical model that relates time taken to process transactions in a scenario where there is a mix of transactions sent both on-chain and off-chain is constructed using weighted average formula as:

$$T_w = wT_{pot-on} + (1 - w)T_{pot-off} \quad (2)$$

where *Tw* is the average transaction time with *w* transactions going off-chain, *w* is the percentage of transactions going off-chain, $T_{pot\text{-}on}$ is the time taken by off-chain transactions, $T_{pot\text{-}off}$ is the time taken by on-chain transactions.

CONCLUSION

The objective of this study was to enhance the performance of blockchains for successful adoption in the mainstream financial services. The study has achieved this objective through the development of a performance enhancement algorithm called Path of Trust (PoT). Based on the performed experiments, transactions with PoT switched on had lower transactions processing time that when the PoT functionality was switched off. The developed solution once scaled up for production use is expected to boost the adoption of blockchains in mainstream financial services such as banking and mobile payments. The adoption of blockchain in mainstream financial services is expected to strengthen the security of these services.

REFERENCES

Cao, K., Lin, F., Qian, C., & Li, K. (2019). A High Efficiency Network Using DAG and Consensus in Blockchain. *2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 279–285. https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00049

Chen, H., & Wang, Y. (2019). SSChain: A full sharding protocol for public blockchain without data migration overhead. *Pervasive and Mobile Computing*, **59**: 101055. https://doi.org/10.1016/j.pmcj.2019.101055

Crosby, M. (2016). *BlockChain Technology: Beyond Bitcoin*. *2*, 16.

Dai, W., Xiao, D., Jin, H., & Xie, X. (2019). A Concurrent Optimization Consensus System Based on Blockchain. *2019 26th International Conference on Telecommunications (ICT)*, 244–248. https://doi.org/10.1109/ICT.2019.8798836

Dang, H., Dinh, T. T. A., Loghin, D., Chang, E.-C., Lin, Q., & Ooi, B. C. (2019). Towards Scaling Blockchain Systems via Sharding. *Proceedings of the 2019 International Conference on Management of Data*, 123–140. https://doi.org/10.1145/3299869.3319889

Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain Application for Central Banks: A Systematic Mapping Study. *IEEE Access*, **8**: 139918–139952. https://doi.org/10.1109/ACCESS.2020.3012295

Fernandes, L. (2013). Fraud in Electronic Payment Transactions: Threats and Countermeasures. *Management Review*, **10**.

IBM Security. (2022). *X-Force Threat Intelligence Index 2022*. https:/www.ibm.com/downloads/cas/ADLMYLAZ

Kwon, M., & Yu, H. (2019). Performance Improvement of Ordering and Endorsement Phase in Hyperledger Fabric. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 428–432. https://doi.org/10.1109/IOTSMS48152.2019.8939202

Li, P., Miyazaki, T., & Zhou, W. (2020). Secure Balance Planning of Off-blockchain Payment Channel Networks. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 1728–1737. https://doi.org/10.1109/INFOCOM41043.2020.9155375

Lind, J., Naor, O., Eyal, I., Kelbert, F., Pietzuch, P., & Sirer, E. G. (2018). Teechain: Reducing Storage Costs on the Blockchain With Offline Payment Channels. *Proceedings of the 11th ACM International Systems and Storage Conference*, **125**. https://doi.org/10.1145/3211890.3211904

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Nguyen, L. N., Nguyen, T. D. T., Dinh, T. N., & Thai, M. T. (2019). OptChain: Optimal Transactions Placement for Scalable Blockchain Sharding. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 525–535. https://doi.org/10.1109/ICDCS.2019.00059

Nurfatih, M. S., Idris, M. Y. bin, Stiawan, D., & Winanto, E. A. (2020). Enhancing Trust Model of Information Vehicular Ad-Hoc Networks Through Blockchain Consensus Algorithm. *2020 3rd International Conference on Information and Communications Technology (ICOIACT)*, 487–492. https://doi.org/10.1109/ICOIACT50329.2020.9332128

Poon, J., & Dryja, T. (2016). *The Bitcoin Lightning Network:* **59**.

Sakakibara, Y., Tokusashi, Y., Morishima, S., & Matsutani, H. (2018). Accelerating Blockchain Transfer System Using FPGA-Based NIC. *2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, 171–178. https://doi.org/10.1109/BDCloud.2018.00037

Tao, Y., Li, B., Jiang, J., Ng, H. C., Wang, C., & Li, B. (2020). On Sharding Open Blockchains with Smart Contracts. *2020 IEEE 36th International Conference on Data Engineering (ICDE)*, 1357–1368. https://doi.org/10.1109/ICDE48307.2020.00121

Wang, Q. (2019). Improving the Scalability of Blockchain through DAG. *Proceedings of the 20th International Middleware Conference Doctoral Symposium*, 34–35. https://doi.org/10.1145/3366624.3368165

Yang, L., Dong, X., Tong, W., Ma, S., Qiao, H., & Xing, S. (2020). Secure Off-chain Payment in Consortium Blockchain System. *2020 International Conference on Networking and Network Applications* (*NaNA*), 259–264.

https://doi.org/10.1109/NaNA51271.2020.00051

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE*, **11**(10): e0163477. https://doi.org/10.1371/journal.pone.0163477

Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., & Liu, R. (2020). Survey: Sharding in Blockchains. *IEEE Access*, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2020.2965147