Software Defined Networking and Network Function Virtualization for improved data privacy using the emergent blockchain in banking systems

Anfal ALRUWAILI[1†] and Saloua Hendaoui [2††]

Department of computer Science, College of Computer and Information Sciences, Jouf University,
Jouf, Skaka, Saudi Arabia

Summary
Banking systems are sensitive to data privacy since users' data, if not well protected, may be used to perform fake transactions. Blockchains, public and private, are frequently used in such systems thanks to their efficiency and high security. Public blockchains fail to fully protect users' data, despite their power in the accuracy of the transactions. The private blockchain is better used to protect the privacy of the sensitive data. They are not open and they apply authorization to login into the blockchain. However, they have a lower security compared to public blockchain. We propose in this paper a hybrid public-private architecture that profits from network virtualization. The main novelty of this proposal is the use of network virtualization that helps to reduce the complexity and efficiency of the computations. Simulations have been conducted to evaluate the performance of the proposed solution. Findings prove the efficiency of the scheme in reducing complexity and enhancing data privacy by guarantee high security. The contribution conducted by this proposal is that the results are verified by the centralized controller that ensures a correct validation of the resulted blockchains. In addition, computation complexity is to be reduced by profiting from the cooperation performed by the virtual agents.

Key words:
cybersecurity, data privacy, network virtualization, complexity, computation, public, private blockchain

1. Introduction

The transition and continuous transformation to the digital world and the development of digital infrastructure remained among the main priorities and principles to follow advancement with the accelerating global change in digital services.

This transition includes facilitating and protecting the flow of information and ensuring the integrity of all systems. It also calls for preserving and assisting cybersecurity to protect all strategic interests, basic assets, national security, government services and practices, and high-priority sectors of all the nations.

The main purpose of these objectives or controls is to set minimum cybersecurity standards for organizational information and technology characteristics. These standards focus on leading industry practices that help companies in reducing cybersecurity risks resulting from threats, whether internal or external.

With the transformation into the digital world that we are witnessing, data security, and mainly privacy, become one of the main pillars for the success of this transformation, along with the need to spread information awareness among the society. Moreover, the technologies used in information security internationally require continuous development and research due to the development of risks, their exponential growth, and their rich diversity.

In various modern areas, digital information is flowing through unreliable communication channels. The big issue here is confidentiality and privacy. Blockchain technology is currently one of the most in-demand areas of science in various applications and data privacy particularly. Buying real estate is quite complicated and takes a long and expensive process. Inspectors, banks, local governments, and real estate agents have to verify our transactions, as shown in fig.1.

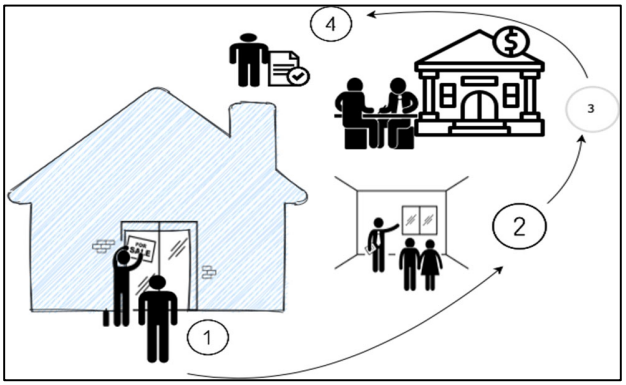

Fig. 1 Blockchain usage in buying and selling

The advancement of blockchain technology has made buying and selling realistic, easy, and accurate. Laws and rules differ depending on the country, city, the state in

Manuscript received August 5, 2021
Manuscript revised August 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.15

which we perform transactions. Real estate and how to buy all these dilemmas and regulations require multiple intermediaries to obtain them with high costs in terms of money. Here comes the role and power of the blockchain.

If we want to legalize the national and local housing rules in the blockchain, we can use the regulations for smart contracts to simplify the process. The seller sends to the site the requested price with some information related to the contract. Then withdraws them from the database for selling real estate. The property on the seller's site generates a smart contract for it and tax actions record any action required to sell the property. The potential buyer can meet with the seller to agree on the prices. Then if an agreement is reached, their signatures are sent. Their digital data to verify the purchase updating documents is done in the background. The presence of identities on both sides of the transaction permits to prove the parties. When adding a new transaction to the blockchain, each block must possess a unique identifier. Whenever a block links to others, no third entity will be able to make any change because of the stability of the blockchain.

Several proposals have executed blockchain in data privacy, especially in banking systems. A Multi-Blockchain bank digital currency model for the Central Bank Digital Currency's (MBDC-CBDC) [1] based on authorization blockchain has efficiently expanded the scalability and the process of transactions by employing multi-blockchain technology and chain identifiers. The outcome is consistent with the blockchain traffic which was considerably reduced by using the bank reserves protocol to create accounts and to test the transaction execution time. However, the allocation method for transactions is still a crucial issue to be addressed.

In [2], researchers introduced a novel data privacy policy based on blockchain divided into three parts: a data privacy classification method, a modern collaborative-filtering-based model, and a data disclosure validation scheme. Experiments confirm that the proposed method is accurate in accomplishing banking data privacy. However, the proposal still needs to be approved by experiments.

Within modern standard cryptocurrency and the model of the CBDC policies, authors in [3] analyzed the performance and security requirements of CBDC. They proposed a three-layer blockchain-based for CBDC: supervisory layer, network layer, and user layer. They handled the cross-border payment to explain the CBDC transaction mechanism and implement theoretical guidelines for CBDC design.

CBDC supervised anonymous issuance (SAI) scheme based on the blockchain is proposed in [4]. A transaction of around 2 KB needs less than six milliseconds to be checked in the SAI scheme. The proposed system resolves the financial information leakage challenge in the indirect CBDC model. Following some cryptographic hypotheses, this system was accurate by performing similarly to Zcash in terms of data privacy performance.

Data privacy is crucial for secured systems in delicate domains. As presented above, blockchain is usually used in those systems due to its high privacy. Blockchain may be either public or private. In a public blockchain, any member can observe and perform transactions in addition to validity insurance. It has a decentralized database of transactions on public networks that allows high confidentiality and integrity due to its large number of nodes and decentralization. Private blockchains are often the opposite of the public blockchain as it manages to maintain the write permissions, for one institution, with restricted permissions. This type has greater flexibility in administration where each transaction has to be transmitted through the node that issued it. Compared to the public blockchain, private blockchain has lower complexity, deployment cost, and lower data security due to the centralization of its database.

Public blockchains have a concern regarding privacy which is the ability to discover addresses of nodes in the blockchain. Thus, a private blockchain is preferred since it guarantees better privacy because the blockchain is not open.

Our contributions in this paper revolve around three main goals:

- Improve the privacy of banking transactions.
- Decrease the complexity and the cost of computations.
- Guarantee an enhanced security level.

To achieve these goals, we propose an architecture that mixes both private and public blockchains.

The rest of this paper is organized as follows:

In section 2, we give the main problems targeted in this research paper. Section 3 presents our proposed solution. Section 4 presents the performance analysis of our proposed scheme. Section 5 concludes the paper and opens perspectives.

2. Problems statements

Blockchain is a sequence of blocks distributed in a public ledger [5]. Each block has a digital signature in the form of

a hash code [6]. Blockchain works by dividing bank clients into corporate and individual clients. Then, they collect data from customers while doing financial business and then use it for product recommendations, marketing, and anti-fraud control. The financial statements, known as financial customer data, include customer profile information and capital transactions. It is crucial to prioritize the privacy of financial data such as the identity of basic information (such as addresses, name, and identity number), network data (such as IP address, location, and cookie data), biometric data (such as an iris or fingerprint) and ethnic data. The data privacy department also needs to work on expanding the data subject's access rights.

Each banking system being the middleman between the exchanged transactions is vulnerable to threats like frauds, crashes, and cyber-attacks [5]. Therefore, managing data privacy in the financial blockchain has three main aspects:

- Use "Privacy by Design" to enforce data privacy management first and foremost. Banks should ensure that the minimum required financial business data and employees' data are processed and accessed. Classification management for different dimensions of customer information should be implemented and given to customers with fast monitoring via the data retention function of the blockchain.
- Quickly create customer data disclosure schemes among broad groups of customers and reduce artificial contract signatures by applying successful techniques and algorithms.
- Understand the complex data behavior that will be positioned with the in-chain and off-chain blockchain, allowing frequent changes, additions, and removal of customer information.

The characteristics of public blockchain allow several benefits in structuring, such as verification of the transaction, integrity, and transparency of the process, and thus its durability. The privacy requirements in the blockchain are:

- The links between transactions must be invisible and non-discoverable.
- The content of the transactions is only known to the participants and only activated by setting policies on it.

The privacy requirements of the blockchain are subject to two main factors:

- Identity privacy: it means the intractability of the treatment texts and the true identity of their posts.
- Transaction privacy: no entity can access the content of transactions except by specific and known users of the blockchain network.

Each transaction, in the blockchain, contains the identifier of its previous transaction, a commercial value, the addresses of the participants in the whole blockchain, the signature of the sender, and the timestamp. However, due to the general nature of blockchain networks, it is possible to track the flow of transactions to extract identities for users or any information.

Several techniques can be used by the attackers that work to conceal the identity of the legitimate user. As the blockchain depends on the Peer-to-Peer (P2P) network, a node may leak its IP address when transmitting transactions. In addition, there are features in a blockchain transaction that are applied to linking addresses and that are controlled by the same user. Another well-known attacker in P2P networks is the Sybil attack where the attacker sabotages the reputation of the P2P network by creating large numbers of identities with pseudonyms and fake names and using them to obtain a negative impact. Moreover, by exposing the pattern of the transactions, the data can be used in the public network, which can reveal new organizations or some of them in applications by analyzing the transaction graph. This type focuses on revealing some features of the transaction.

The above-mentioned dilemmas arise the advantages of the private blockchains where data privacy is better ensured since all transactions and blocks are saved in the global ledger and are completely non-modifiable. In addition, the global ledger will be fully synchronized between all nodes in the blockchain after the compatibility mechanisms. Thus providing large degrees of trust to users that ensure the data in the blockchain is not modified in a very high and short time. In addition, the blockchain relies on a consensus process, whereby consensus is reached by implementing some of the rules from the blockchain without central permission. These rules ensure that any procedure is executed and applied appropriately and at the right time and assure the correctness of transactions without human intervention. However, intentionally or unintentionally, it is still possible to wrongly modify some transactions by the central entity. The centralized database may maintain a wrong transaction without the consensus of the other nodes of the blockchain. We highlight in table 1 a comparison between private and public blockchain.

Table 1: Comparison between private and public blockchains

	Private blockchain	***Public blockchain***
Similarities	Records can be added but cannot be changed or deleted	
	Each node in the network has a complete duplicate of the ledger	
	The validity of the record is validated with a high level of consistency	
Differences	Whoever can join the network, read, write and participate	Access is restricted

	Transaction verification by any node	Transaction verification by authorized entities
	Decentralized database	Centralized database
	Lower scalability	Higher scalability
	More secured	Less secured

3. Proposed scheme

As mentioned above, our contribution aims to improve the privacy of the banking transactions and decrease the complexity and the cost of computations thus we will adapt private blockchain. At the same time, we aim to guarantee an enhanced security level, so we will adjust the public blockchain. Subsequently, the proposal will be a heterogeneous approach.

3.1. Heterogeneous architecture

As presented in fig. 2, the proposed architecture is composed of both private and public blockchains.

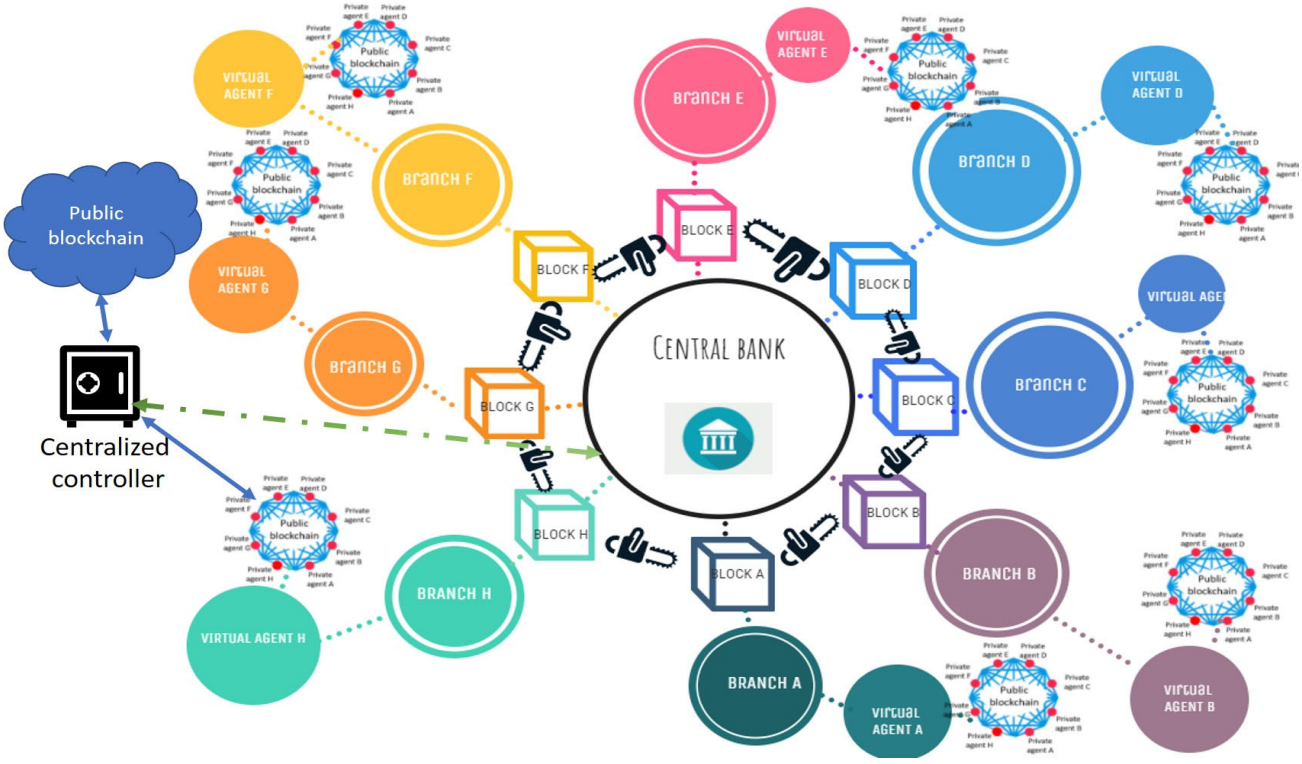

Fig. 2 Heterogeneous architecture

In the system, we have two main categories of equipment: physical and virtual.

- Physical equipment: we have many banks branches. Each branch is attached to a particular block. All the blocks are grouped in the central bank in the form of a private blockchain. A branch may add or modify transactions within the blockchain after authorization of the central bank.
- Virtual equipment: Whenever a novel transaction is created, the branch adds it to its block in the private blockchain and simultaneously transfers it to the virtual agent that will, in turn, adds it to the virtual public blockchain.

We propose the following scenario: branch X creates a new transaction. This transaction has to be transferred to the central bank and appended to the private blockchain. Branch X forwards the transaction to its attached virtual agent X that has to share it within a peer-to-peer virtual network. As fig.2 presents, agents A, B, C, D, E, F, G, and H are virtual entities that communicate regularly within the peer-to-peer network. The purpose of virtual agents is to receive transactions, append them to the public blockchain, and validate the resulted blockchain.

Here comes the purpose of the centralized controller that has to match public and private blockchains. It approves the blockchains, their accuracy as well as their integrity.

If physical-private and virtual-public blockchains are equivalent, the centralized controller holds a copy in the cloud. In the case of a mismatch, the controller can recover

the fault block and discard the transaction. Of course, the central bank has to be informed.

3.2. Network virtualization

Virtualization in computing is the creation of virtual entities such as hardware, software, policies or an operating system or storage, or a network device [7]. Our proposal adapts network virtualization thanks to its numerous advantages, ease in deployment, and computations. Software-Defined Networking (SDN) is a network architecture that includes softwarization and programmability in the network by separating network control and data functions. Network Function Virtualization (NFV) utilizes the virtualization of network components. While NFV virtualizes the network infrastructure, the SDN centralizes network management. SDN and NFV build a network designed, controlled, and managed entirely by software.

Network virtualization is deployed due to its numerous benefits. It allows network operators to save money, decrease time-to-market for new or updated products, and adapt the resources available to applications and services. Better resource efficiency can be reachable with a lower cost. A single server can control various VNFs simultaneously so fewer servers are required to achieve the same amount of work.

Flexibility is also a significant feature of network virtualization since it enables businesses to efficiently respond to the evolving customer needs and emerging market opportunities.

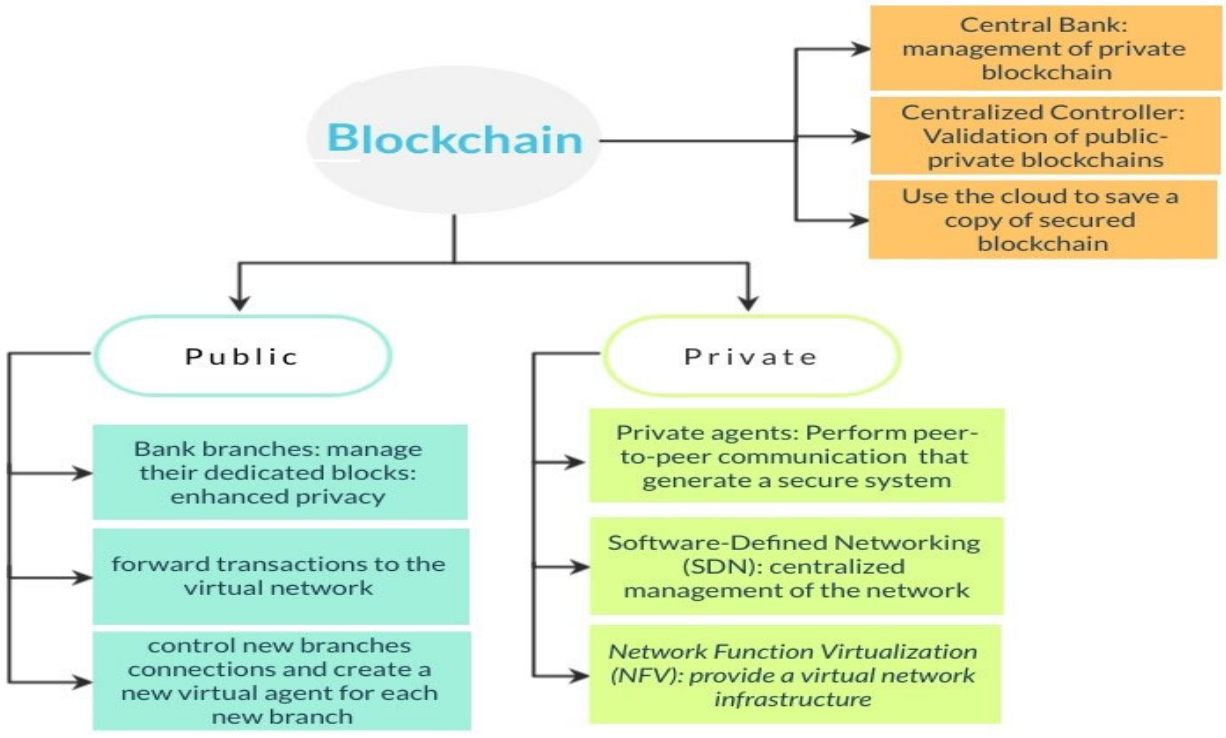

Fig. 3 Functions of networks' entities

SDN allows efficiently managing the network. Since the interfaces are "Open," they allow automation and programmability that provide a network virtualization enabler Virtual network (overlay) over a physical system. In fig.3, we summarize the functions of the different entities in our proposed heterogeneous architecture.

4. Performance evaluation

This section presents the outcomes of the proposed policy. To approve our scheme, we create a blockchain applying python programming languages, library sha256 from hashlib for keys encryptions, and pandas for data set interpretation. We downloaded a bank data set with five columns and 1000000 rows. Transactions that are added to the blockchain are based on data from this data set.

To study the security of the proposed scheme, we will discuss two scenarios: In the first scenario, both private and public blockchains will add 100 legal transactions. Then, the centralized controller performs a validation check of the generated blockchains. As fig.4 presents, in this case, the blockchains are successfully validated so the centralized controller has to save data in the cloud for later use.

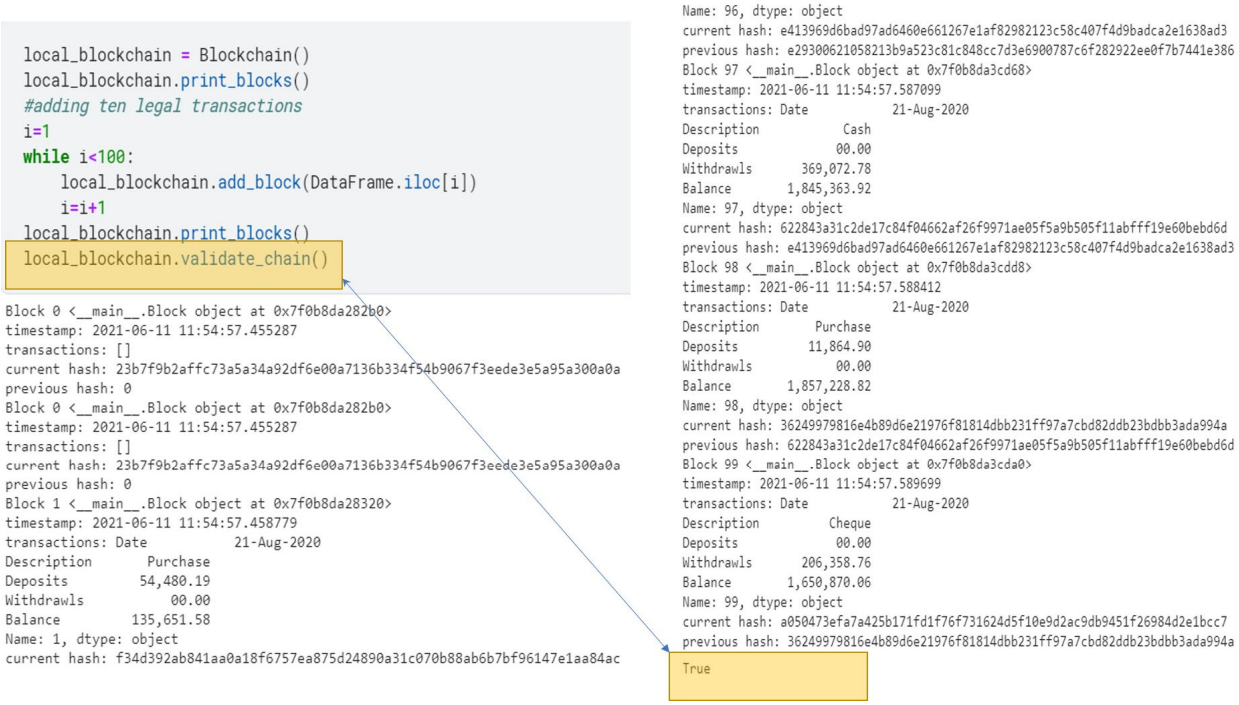

Figure 4. Adding legal transactions

In the second scenario, transaction number 100 in the private blockchain is modified. In this case, as reported in fig. 5, the validation has failed. The centralized controller will notify a mismatch between the private and the public blockchains to the central bank. In this case, a recovery of the correct blockchain has to be restored from the cloud. As mentioned in the objectives of our proposal, we aim to reduce the complexity of computations and processing time.

To do so, we draw in fig. 6 the processing time of adding up to 90000 transactions. We can see that the processing time increases with the number of transactions.

Let's assume that we have 1000000 branches in our banking system and each branch generates a transaction each 1 minute. In the public blockchain (virtual), each agent will perform computations to generate this public blockchain. The processing time will be very high, even may be impossible to perform the required computations in a real-time concept.

In our scheme, we avoid this problem as follow:

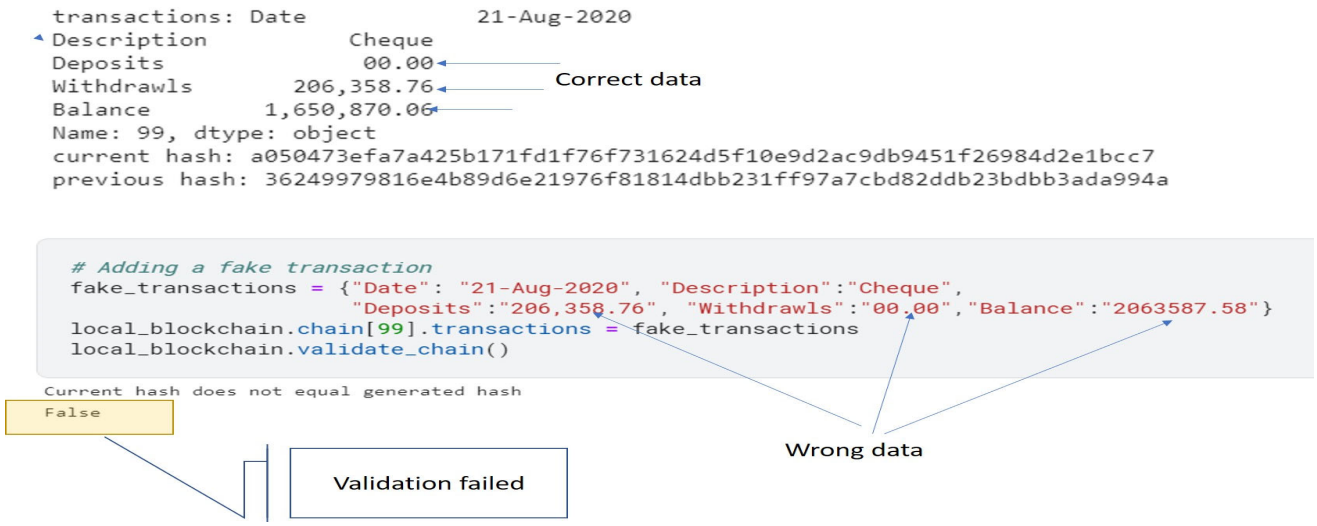

Fig 5. Adding fake transactions

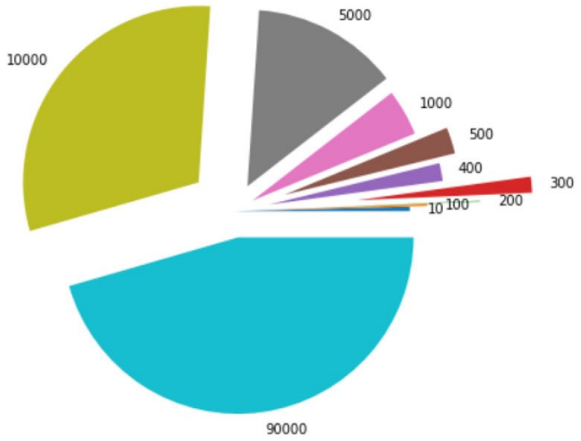

Fig 6. Processing time of adding up to 90000 transactions

The centralized controller has to synchronize the work among the private agents. Each of them has to save the received transactions, from its attached bank branch and at the same time forward them to the centralized controller that gathers data from the different private agents and saves it in the cloud. The computations are distributed among these agents to guarantee faster and easier deployment and the centralized controller synchronizes the resulted blockchain. Periodically, the centralized controller has to assign the computation of the public blockchain for some of the private agents. Then, the public blockchain, generated by the centralized controller, is compared with that calculated by these agents. Of course, after comparison with the private blockchain, and in case of problem detection, the peer-to-peer blockchain has to be recalculated using the classic methods (each agent has to perform the whole computation since it has already saved received transactions).

It will guarantee easier and faster computation since the private blockchain generated by the physical branches serves as proof for the centralized controller that will benefit from the cooperation between the virtual agents.

We draw in fig.7 the processing time of adding up to 90000 transactions with and without the cooperation of virtual agents in computation. As seen, this cooperation allows decreasing the processing time. The public blockchain is not computed independently by each agent. However, agents are grouped, in this case in a group of five agents, to allow faster computation. This allows to decreases the efficiency of the whole system. We can see that in the case of adding 10000 transactions, the execution time is the same in both cases (with and without cooperation). This is expressed by the fact that the centralized controller discovered a mismatch between the public and private blockchains. In this case, cooperation is canceled and the public blockchain is recalculated.

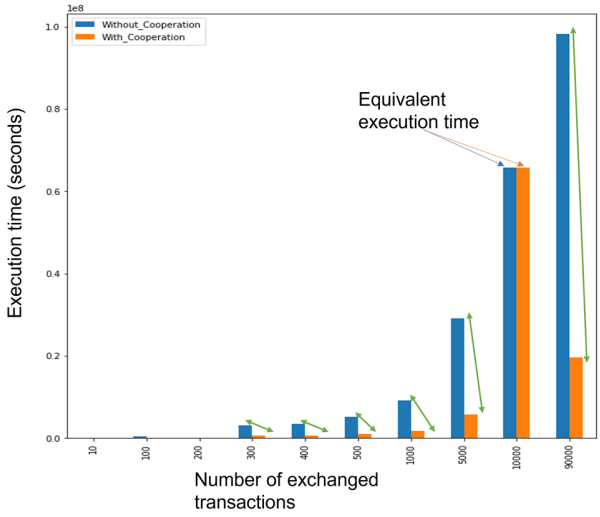

Fig 7. Comparison of processing time of adding up to 90000 transactions without (blue) and with (orange) cooperation of virtual agents.

5. Conclusion and future work

Private blockchains are easy in deployments, fast in computations, and guaranteeing high privacy with a low-security level. Public blockchains have low privacy, high security, and costly computations.

In this proposal, we give a heterogeneous architecture that profits from the high level of security, provided by the public blockchain, enhance the protection of blocks addresses, by physically using private blockchain that is not open, and reducing the complexity of computations, by introducing the cooperation between the virtual agents. Network virtualization plays a major role in this contribution as it provides a virtual system infrastructure that is easy to deploy and that has powerful capabilities.

Findings prove that the proposed solution may enhance the level of system security and data privacy and reduce the complexity of computations.

We are working to dynamically determine the number of agents in each cooperation group to guarantee the best system performance in terms of accuracy and complexity.

Acknowledgments

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

[1] H. Sun, H. Mao, X. Bai, Z. Chen, K. Hu and W. Yu, "Multi-Blockchain Model for Central Bank Digital Currency," 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2017, pp. 360-367, doi: 10.1109/PDCAT.2017.00066.

[2] Hao Wang, Shenglan Ma, Hong-Ning Dai, Muhammad Imran, Tongsen Wang, Blockchain-based data privacy management with Nudge theory in open banking, Future Generation Computer Systems, Volume 110, 2020, Pages 812-823, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.09.010.

[3] X. Han, Y. Yuan and F. Wang, "A Blockchain-based Framework for Central Bank Digital Currency," 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2019, pp. 263-268, doi: 10.1109/SOLI48380.2019.8955032.

[4] Dai W., Gu X., Teng Y. (2020) A Supervised Anonymous Issuance Scheme of Central Bank Digital Currency Based on Blockchain. In: Qiu M. (eds) Algorithms and Architectures for Parallel Processing. ICA3PP 2020. Lecture Notes in Computer Science, vol 12454. Springer, Cham. https://doi.org/10.1007/978-3-030-60248-2_32

[5] N. R. Bagrecha, I. Mustafa Polishwala, P. A. Mehrotra, R. Sharma and B. S. Thakare, "Decentralised Blockchain Technology: Application in Banking Sector," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-5, doi: 10.1109/INCET49848.2020.9154115.

[6] I. Ahmed, Shilpi, and M. Amjad, "Blockchain Technology A Literature Survey," Oct 2018 Volume: 05 Issue: 10 International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056.

[7] Michael Kretzschmar, S Hanigk, "Security management interoperability challenges for collaborative clouds", Systems and Virtualization Management (SVM), 2010, Proceedings of the 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and the Cloud, pp. 43-49, October 25-29, 2010. ISBN:978-1-4244-9181-0,DOI: 10.1109/SVM.2010.5674744

Anfal Rwily: Master student in jouf university received the B.E.. degrees, from jouf Univ

Saloua Hendaoui received the B.E. and M.E. degrees, from tunis Univ. in 2011 and 2009, respectively. She received the Dr.. degree from Cartage Univ. in 2017. Working as a assistant professor (from 2018) in the Dept. of computer Science Jouf University