BLOCKCHAIN-BASED DECENTRALIZED USER AUTHENTICATION SCHEME FOR LETTER OF GUARANTEE IN FINANCIAL CONTRACT MANAGEMENT

Sasikumar A. [1] ***, Karthikeyan B*** [2]***, Arunkumar S.***[3]***, Saravanan P.***[4]***, Subramaniyaswamy V***[5]***, Logesh Ravi***[6*]

[1]Department of Electronics and Communication Engineering, K Ramakrishnan College of Technology, Tiruchirapalli, Tamilnadu, India

[2,3,4,5]School of Computing, SASTRA Deemed University, Thanjavur, Tamilnadu, India

[6]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India

Email: SasikumarAPhD@gmail.com[1], bkarthikeyan@it.sastra.edu[2], vgsarun@gmail.com[3], sharan.doit@gmail.com[4], vsubramaniyaswamy@gmail.com[5], LogeshPhD@gmail.com[6*] (corresponding author)

DOI: https://doi.org/10.22452/mjcs.sp2022no1.5

ABSTRACT

The use of blockchain technology in the financial contract management system leads many challenges for user authentication and key distribution. In traditional financial system, the core endeavor with strong letter of guarantee play an irreplaceable role in the supply chain management. In this context, fraud in financial contract management is severe problem for economical growth. To overcome the problems of the conventional transaction process, in this paper, we develop a user access control and key management scheme that uses blockchain decentralized network to manage the letter of guarantee. This decentralized network platform can helps the problem of no trust among the users, improves the efficiency of data transmission, reduces costs, and provides better financial services to the relevant parties in the supply chain. The proposed user authentication is developed based on the deterministic encryption algorithm to achieve decentralized security for trusted data transmission. Finally, the experimental results shows that the computation cost of the proposed authentication increases due to the rising of number of customer added to the blockchain network. Overall the proposed authentication scheme most suitable for banking system to issue the LoG contract in right time.

Keywords: Financial System, Letter of Guarantee, Blockchain Technology, Security, User Authentication

1.0 INTRODUCTION

Blockchain is a growing technology for financial systems and network transactions [1]. The rapid development of blockchain technology, a large number of user documents are needs to integrate with bank system, and the amount of network traffic to be tremendously high. On the other hand, with the rising of network traffic load on centralized systems required huge resources for the conventional network organization and data storage. Even without the consideration of the system cost and manpower, the centralized network server could be the restricted access of the complete system. Once the central network server fails, it will affect the whole network. It could be challenging task for different service providers to guarantee system interoperability and security among network nodes belonging to various service providers.

The blockchain technology is integrated with financial system; it can bring countless promise to the various system applications [2]. When millions of smart grids need to transact with each other, the conventional centralized network model may pace the huge traffic and increase the computation cost. Therefore, the next generation of banking system required decentralization network with distributed system organization and data storage. However, the system implemented through the decentralized network must have high security requirements.

Blockchain security model seems to be a powerful mechanism to provide trusted transaction for a decentralized system. This is a technology comes from the digital cryptocurrency to represents Bitcoin interaction approach, which was introduced in 2008 [3]. The merit of blockchain technology is decentralization, and it can perform user-to-user interactions, management and association without any centralized support. It can adopt multiple security mechanisms such as encryption, third party authentication, multi-agent, and financial incentives. The Blockchain model can able to solve the real time security problem in digital world such as high costs, manpower, inefficiency, and centralized data storage. With the advance development and rapid growth of decentralized security in recent

times, blockchain mechanism research has been provoked to develop rapidly, which is viewed as the fifth disruptive modernization of the computing standard for user transactions [4].

Blockchains have been successfully implemented to following applications:

- Smart contracts [5]: the blockchain has been implemented for trusted computing and software sharing in smart contracts. The security of distributed computing in smart contacts relies on blockchain.
- Public Key Infrastructure (PKI) [6]: A distributed PKI model implemented for the Certcoin. In this infrastructure provide the bitcoin assurance and ensures individuality preservation.
- Cloud storage: A peer-to-peer storage system integrated with the MetaDisk [7] network. This cloud storage uses a decentralized blockchain network for secure communication.
- Anti-counterfeiting technology [8]: In this model a Blockverify mechanism is supported to provided secure network for the pharmaceutical, luxury goods and electronics industries.
- Domain Name Server [9]: The advance of decentralized backchain provided secure and privacy based domain server avoids the censorship in the system.
- Decentralized IoT [10]: A blockchain based IoT offers a decentralized security and used to maintain the public ledger.

Blockchain infrastructure is the emergent block of future generation crypto computing, and it is expected to entirely restyle human common actions, and reach the revolution of banking systems. Generally, blockchain technologies have been applied for various applications, for example, using hash encryption model to verify and store data. Then, the stored data are updated using consensus algorithm. Finally, the algorithm generates the script code for each node in the decentralized network. Blockchain presents a new decentralized and secure model for computing paradigm.

Since, the banking system needs to improve system quality in terms data storage, network management, intelligence, accuracy and security. This is possible through the integration of Blockchain and the bank infrastructure. Particularly for financial, because the network communication between node to node or server to node is unbalanced or may not be secure. Therefore, it is necessary to design the blockchain based user authentication for baking system.

In this paper, the blockchain for letter of guarantee in financial management is described in detail. Based on the infrastructure of banking system, we proposed a blockchain based user authentication for LoG. We also analyzed its performance through various design metrics.

The rest of the paper is organized as follows: Section II reviews the related to blockchin for financial management, Section III presents the design architecture of the Blockchains in banking system; Section IV discusses the user authentication of the proposed blockchain for letter of guarantee in banking infrastructure; Section V describes performance metrics comparison of proposed work with other state-of-literatures; and Section VI reaches our conclusions.

2.0 RELATED WORK ON BLOCKCHAIN FUNDAMENTALS

Bitcoin was first introduced in 2009 based on Blockchain technology. This is the first virtual electronic cash, which is transfer between peer-to-peer networks. Approximately, 28.5 million electronic wallets are transferred in bitcoin network [11]. The specialty of Blockchain technology performs efficient transactions without the need of centralized trust authority system. These coin exchanges are stored in a ledger which is controlled by a set of peers, like a decentralized peer-to-peer network [12]. Blockchain technology performs encryption based network verification before approving the coin exchange to ensure the security. The main advantage of Blockchain is the decentralized network, which is implemented such a way that no trust is needed. The security and reliability of these peer-to-peer networks are encrypted by mathematical equations [13]. Previously, the Blockchain networks mostly implemented for cryptocurrency transactions. The advance security in Blockchain allows the researcher to utilize this technology for other domain applications such as healthcare, IoT, etc.

The term blockchain is the distributed ledge technology based security model has gained it dominance to various field such as medical data, government ledge, and trading industries etc. the blockchain has already showcased its importance to handle major security problems to the all major fields like system security, accountability, transparency and cost. Every industry has brought blockchain security model to maintained ledge and improving the security of industry function.

Based on the nature of the application, Blockchain technology can be classified into three models:

- Public blockchain model
- Private blockchain model
- Consortium blockchain model

A) Public Blockchain

Public Blockchain, as the name implies, is open to the public and has no limitations on who can participate or be a node operator. No one has full control over the network on a public blockchain. Because a single person cannot modify the Blockchain, this assures data protection and immutability.

Public Blockchains are known to be fully decentralized because the authority on the Blockchain is evenly spread across each node in the network. Bitcoin, Ethereum, and Litecoin are all examples of cryptocurrencies that utilize public blockchains.

B) Private Blockchain

Who can access and participate in transactions and authentication on a Private Blockchain (also known as Permissioned Blockchain) is limited. The Blockchain can only be accessed by pre-approved organizations. These entities are selected by the relevant authority and granted authorization by the Blockchain developers throughout the development of the Blockchain application. If rights are needed to be granted to new users or revoked from an existing user, the Network Administrator can handle it.

C) Consortium Blockchain

Some nodes govern the consensus mechanism in Consortium Blockchain, while others may be authorised to participate in transactions. Consortium Blockchain is kind of a cross between public and private blockchains. It is public because different nodes share the Blockchain, and it is private because the nodes that can access the Blockchain are limited. As a result, it is both public and private. [14].

Crypto Blockchain: Instead of cash/cashless based money transactions, this will allows virtual cash transfer using crypto blockchain model. The crypto currency transaction only transfers the information data regarding the amount of money. These types of transactions are public blockchain based model to improve security and transparency. In these networks are decentralized to improve the security of each user associated with nodes. Mathematical models are applied to ensure the transparency of each node as well as currency transactions [15].

Business Blockchain: The blockchain technology is introduced for business related industrial operation management for device productions. Compared to previous models, this method provides secure contract blockchain for variety of business transaction. This secured system monitors the activities of ubiquitous devices, industrial production in real-time and financial data transfer [16]. The business blockchain model uses private or permissioned model. This will ensure the secure delivery and block system creation.

A permissioned blockchain model has been implemented for different business network with use of hyperledge [17]. This model developed for the Fabric [18] business frameworks. Depending on the nature of business the variety of frameworks and consensus algorithm [19] are introduced for developing hyperledge. Generarally, the hyperledger structure is the basement for the blockchain model to solve decentralized related security problems [20]. The generic architecture of permissioned Blockchain is shown in Figure 1. Blockchain architecture is created using peers interconnections and these peers are independent systems. Here the blockchain models are responsible for security of transactions and preserve the distributed ledger. Security and data maintains are entirely depends on the chain code which must be installed on each peer systems. Basically, chain code is a hash programming to define the secure transactions between peers. This secures transactions codes are stored back into the common ledger which is also integrated with peers. The modified chain code consist the following details of peers, i.e., lot timeout configuration and Membership Service Provider (MSP).

3.0 BLOCKCHAIN FOR FINANCIAL MANAGEMENT

A letter of guarantee (LoG) is an agreement bond generated by a bank on behalf of one of their clients who has engaged into a deal with a supplier to goods or services. Even if the bank clients defaults, the LoG assure the provider supplier know that they will receive payment. A LoG can only be obtained if the client applies for it.

The LoG application process can be transformed by using blockchain technology to make it totally paperless, electronic, and transparent. Because the blockchain environment is secured by permissioned peer to peer network, which includes respectable banking institutions and this transparency remove fraud and forgery. This results in a highly secure framework for data writing and retrieval, and also provides storage for network transaction which is irreversible, auditable record. Blockchain based LoG ledger is not controlled by a central organization.

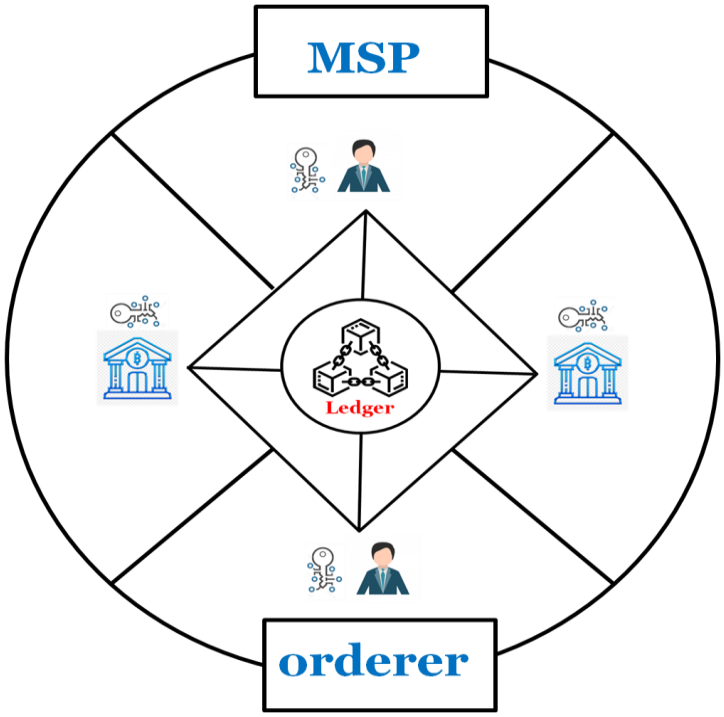

Fig. 1: Peer-to-Peer Communication in Permissioned Blockchain.

Banking systems that are heavily depend on paper, particularly those that involve back-and-forth agreements between clients, are ideal candidates for digitization and blockchain. The paper-based operations in the banking systems are associated with the risk of fraud, this leads for blockchain even stronger [21], [22], [23], [24], [25]. The bank guarantee, often known as a letter of guarantee, is one such an instrument.

The financial institution guarantees make it easier to do business by establishing confidence between two clients, such as a vendor and a goods buyer or a property-owner and a renter. If the buyer or the renter fails to make payment, the financial institution assurances that the recipient will be reimbursed. A LoG also covers performance, ensuring that the recipient is protected in the event that the other client fails to deliver a product [26], [27], [28].

While the idea of a bank agreement is regular across the business, the implementation is anything but each banks have their own set of rules, forms and procedures. Before achieving an agreement, there may be several drafts and consultations, and if adjustments are needed, the entire process must be repeated. Overall, the bank guarantee of one page bond can take up to a month.

Regulating and digitizing the complete paper work and introducing a blockchain technology for letter of guarantee can improve the following:

- Peer to peer communication with streamline
- Avoiding the costs of photocopy, circulating, and exchanging LoG documents
- Eliminate the risk of data error and manipulation of documents

- Transparent process with decentralized control

Limitation of letter of guarantee

Bank fee: A letter of guarantee process includes the extra cost to business. All banking system are charging a fee for giving LoG service and it will be modified if the clients wanted to add extra features. This leads additional burden for small and medium scale clients.

Messaging Fees: All banking system uses the software based intra network for transmitting messages. This increase the charges based on the size, type of data. Intra network data transfer is time consuming process with less security.
Risk of Misuse: A letter of guarantee some time creates data manipulation risk to the distributor. Without knowing this issue the bank has to release payment to the retailer. Hence it can create manipulation of goods services which is different from the actual cost.

Currency Risk: A letter of guarantee comes with the currency transfer risk of forex. This should be varied up on the trading of currency in the global market. There will be some variation in the overall cost of LoG than actual transfer cost.

4.0 PROPOSED DETERMINISTIC ENCRYPTION ALGORITHM BASED DECENTRALIZED USER AUTHENTICATION SCHEME FOR LETTER OF GUARANTEE

This section discusses the proposed decentralized architecture and user authentication scheme for Letter of Guarantee in detail. The developed decentralized network for the banking system employs a deterministic encryption algorithm based user authentication of LoG [29]. The proposed system eliminates the paper based LoG transfer between different entities and also reduces the overall cost. Hence, our proposed user authentication scheme improves the system security, efficiency and reduces the computational overhead.

A. System Architecture

Deterministic encryption algorithm based decentralized user authentication scheme for financial management network is shown in Figure 2. The proposed blockchain based decentralized network consists of four entities namely Buyer, LoG issuing bank, LoG advising bank, and seller.

The buyer is customer to get letter of guarantee from issuing bank. Buyer is the responsible trader for repaying amount to the seller. The duty of LoG issuing bank is to maintain the records of both the buyer and seller. LoG issuing bank is also to take full responsible for buyer regarding to proper transfer of funds. Advising bank is one entity to acts as a brokerage between seller and LoG bank issuing. In this matter, the LoG advising bank is responsible for the proper release of fund transfer to the seller. Seller is the responsible distributor for delivering goods to the buyer. There is a smart contract between buyer, seller, Issuing bank and advising bank. In this process, we proposed decentralized user authentication scheme for LoG. Because all the record available in the LoG with high security.

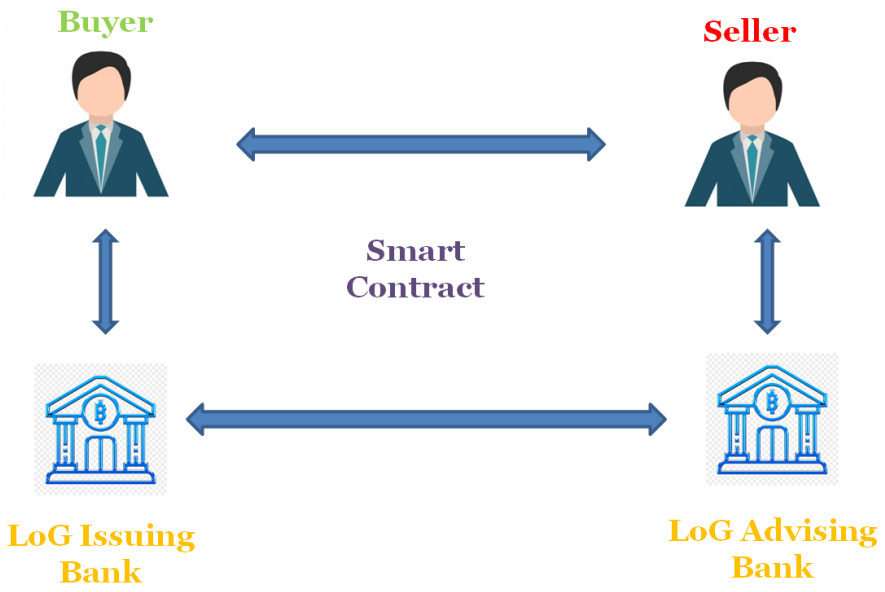

Fig. 2: Decentralized user authentication scheme for financial management network.

The proposed scheme includes all entities to the smart contract in order to create agreement between seller and buyer. Hence, the letter of guarantee provides the complete details of smart contract with high security. The following section presents the Deterministic encryption algorithm [31] based decentralized user authentication scheme for LoG using blockchain technology.

B. User authentication phase

A detailed description of user authentication scheme presents in this section. There are several processes to be followed by seller and buyer, before added to smart contract. First process is to create user authentication for customer using deterministic encryption algorithm. The pseudo code for proposed user authentication model is shown in Table 1.

Table 1: Deterministic Encryption Algorithm (DET) for User Authentication

Deterministic Encryption Algorithm (DEA) for User Privacy
Input data: User ID (UIDi), DEA_Cipher, DEA_Password
Output: The user selection result
1. **for** i=0 to N-1 **do**
2. selection_result.add(UID[i]);
3. **if** UID[i]= DET_cipher in DET_Password **then**
4. selection result.add(DET_cipher);
5. **return** the selection_result;

Authentication phase is started with the input data such as user ID, Cipher text and password. Then user account created with help of algorithm. In this step the proposed algorithm is used to encrypt the user account and also provide the password for access. This process will be followed whenever the system wants to create new account. Hence, each customer has its own password for user authentication. This gives two factor authentications for LoG as well as financial institutions.

The customer records are encrypted using algorithm and then it is added to the blockchain network. In this smart contract the banking system uses the permissioned blockchain network for their control of security and also avoids

the data loss. Hence, the buyer and seller access the smart contract through user authentication and the permissioned blockchain model gives the authorization via proof of work.

C) Key Management and Authorization Phase:

Whenever a registered customer wants to communicate with banking system corresponding to the same blockchain network, it requires encryption keys for the secure data transmission. For that, deterministic encryption algorithm generates a cipher text. Then it encrypts the customer password using public key of the smart contract to which it belongs. It also sends the proof of work with the above customer details for authorizing itself to the blockchain network. The permissioned blockchain based banking systems generate the N number of public key/private key pairs and the hash values using the proof of work. At the same time, the bank issues a transaction to the customer to store hash value, the current timestamp and validity of key. Once the transaction is authorized by all user of the network such as LoG issuing bank and LoG advising bank, bank encrypts the private and public key set and signs LoG, then transfer to customer.

5.0 PERFORMANCE EVALUATIONS

To evaluate the performance of proposed user authentication for LoG we compared security measures with other blockchain models. In order to overcome the security issues of blockchain-based user authentication, we propose to merge banking system and customer records to authenticate user login. In the decentralized user authentication scheme proposed to enhance the privacy of customer details. The main reason to introduce deterministic encryption algorithm based user authentication for banking system is to eliminate the security attacks.

In order to measure the effectiveness and security of the proposed decentralized user authentication scheme for LoG, in this section, we compared the common security necessities and attacks in financial applications with existing schemes. The security comparisons of different scheme results are shown in Table 2. Our proposed user authentication for LoG is more comprehensive in terms of security.

Table 2: Comparison of Various security models in Blockchain

Parameters	**Ref[17]**	**Ref[18]**	**Ref[19]**	**Ref[20]**	**Proposed**
User Privacy	✓	✓	✓		✓
DoS	✓	✓		✓	✓
Scalability	✓		✓	✓	✓
Sybil	✓	✓	✓		✓
User Authentication			✓	✓	✓
Decentralization	✓	✓	✓	✓	✓

In this section we analysis the performance of user authentication for LoG based on the computation cost, average transaction time and throughput. In banking system, the determination of customer verification depends on the output of user authentication. In this experiment, the system evaluates the computation cost of deterministic encryption algorithm when the number of customers is fixed as 50.

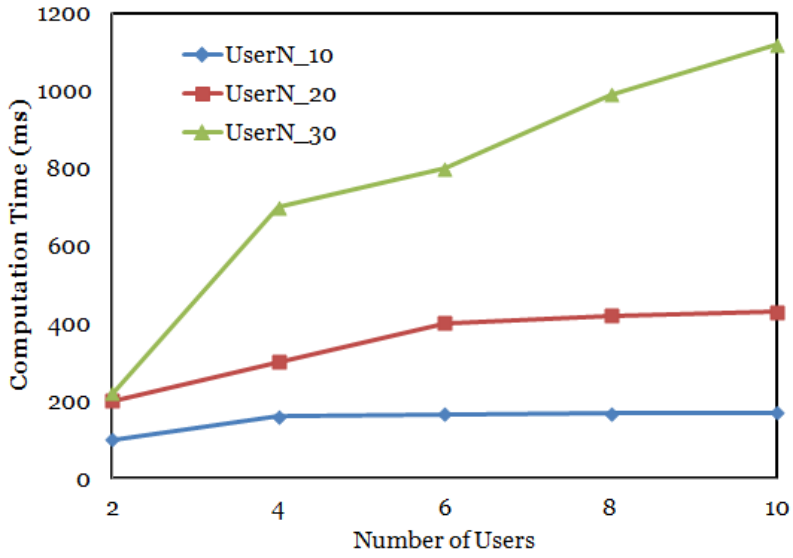

Fig. 3: Computation time of user authentication when number of customer is 50.

The proposed smart contract system repeats this test 10 cycles and final evaluation results are shown in Figure 3. From the result, banking system observing that as the number of customer added, the computation cost will be increased.

In banking system, the customer transaction will be submitted to the permissioned blockchain network. To get the average transaction time of customer transactions and throughput within a specific time period, we evaluate the timing of transaction latency and throughput with fixed number of customer. For this experimental test, we evaluate the results with the number of customer is set to 10 and 20 respectively. From figure 4, 5, 6 and 7, we conclude that when the number of customer increases then the average transaction time is uptrend and throughput is in downtrend.

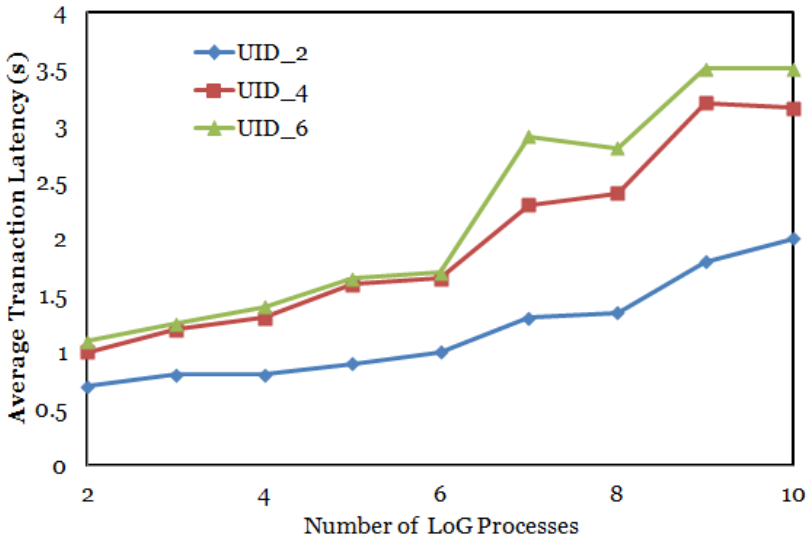

Fig. 4: Average transaction latency test results when N = 10.

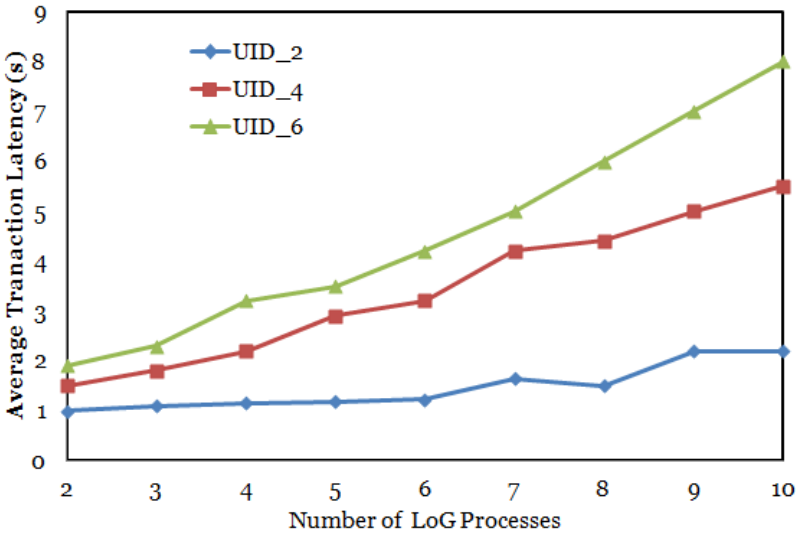

Fig. 5: Average transaction latency test results when N = 20.

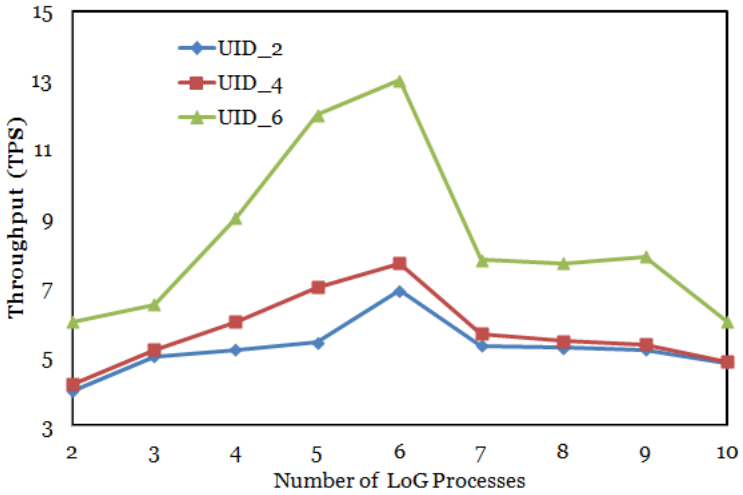

Fig. 6: Throughput test results when N = 10.

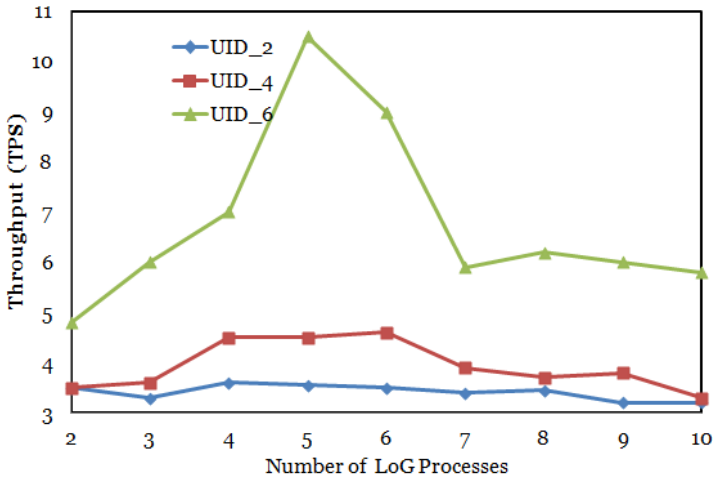

Fig. 7: Throughput test results when N = 20.

Finally, the experimental results shows that the computation cost of the proposed authentication increases due to the rising of number of customer added to the blockchain network. Overall the proposed authentication scheme most suitable for banking system to issue the LoG contract in right time.

6.0 CONCLUSION

In this paper we proposed a decentralized user authentication scheme for letter of guarantee using blockchain-technology for banking system that reduces the costs of the transaction, and eliminates the need of paper to manage the customer records in the system. The proposed deterministic encryption algorithm based user authentication improves the security in the system and also conducts dynamic updates of public/private key pair of customers over time. Further, we develop a balockchain based proof of work to verify the customer details before signs to LoG contracts. Specifically, the LoG contracts implementation process employed a series of authentication steps and authorization that served to improve the system's applicability to a dynamic environment and to overcome the drawbacks of previously proposed schemes. We have addressed the benefits of user authentication with blockchain technology for banking system. Compared with other mechanism, our user authentication based blockchain model provides the better security in terms of decentralization, scalability, DoS and privacy.

REFERENCES

[1] Weking, J., Mandalenakis, M., Hein, A. et al. The impact of blockchain technology on business models – a taxonomy and archetypal patterns. *Electron Markets* 30, 285–305 (2020). https://doi.org/10.1007/s12525-019-00386-3

[2] Maicon Azevedo da Luz and Kleinner Farias. 2020. The Use of Blockchain in Financial Area: A Systematic Mapping Study. *In XVI Brazilian Symposium on Information Systems (SBSI'20). Association for Computing Machinery, New York, NY, USA,* Article 3, 1–8 (2020). DOI:https://doi.org/10.1145/3411564.3411579.

[3] Nakamoto, S., & Bitcoin, A. (2008). "A peer-to-peer electronic cash system. Bitcoin".–URL: https://bitcoin. org/bitcoin. pdf, 4.

[4] Xu, M., Chen, X. & Kou, G. A systematic review of blockchain. Financ Innov 5, 27 (2019). https://doi.org/10.1186/s40854-019-0147-z

.

[5] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Netw. Appl.* 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0.

[6] Feng T., Chen W., Zhang D., Liu C. (2020) One-Stop Efficient PKI Authentication Service Model Based on Blockchain. *In: Si X. et al. (eds) Blockchain Technology and Application. CBCC 2019. Communications in Computer and Information Science*, vol 1176. Springer, Singapore. https://doi.org/10.1007/978-981-15-3278-8_3.

[7] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah. 2020. Blockchain Technology for Cloud Storage: A Systematic Literature Review. *ACM Comput. Surv.* 53, 4, Article 89 (September 2020), 32 pages. DOI:https://doi.org/10.1145/3403954

[8] Uddin M, Salah K, Jayaraman R, Pesic S, Ellahham S. Blockchain for drug traceability: Architectures and open challenges. *Health Informatics Journal.* April 2021. doi:10.1177/14604582211011228.

[9] Yang Liu, Yuwen Zhang, Siyu Zhu, and Cheng Chi. 2019. A Comparative Study of Blockchain-Based DNS Design. *In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications (ICBTA 2019). Association for Computing Machinery, New York, NY, USA*, 86–92. DOI:https://doi.org/10.1145/3376044.3376057.

[10] Jabbar R, Kharbeche M, Al-Khalifa K, Krichen M, Barkaoui K. Blockchain for the Internet of Vehicles: A Decentralized IoT Solution for Vehicles Communication Using Ethereum. *Sensors* (Basel). 2020;20(14):3928. Published 2020 Jul 15. doi:10.3390/s20143928.

[11] Mattke, J., Maier, C., Reis, L., & Weitzel, T. (2020). Bitcoin investment: a mixed methods study of investment motivations. European Journal of Information Systems, 1-25.

[12] Hill, B., Chopra, S., Valencourt, P., & Prusty, N. (2018). "Blockchain Developer's Guide: Develop smart applications with Blockchain technologies-Ethereum, JavaScript", Hyperledger Fabric, and Corda. Packt Publishing Ltd.

[13] Yifan Mao, Soubhik Deb, Shaileshh Bojja Venkatakrishnan, Sreeram Kannan, and Kannan Srinivasan. 2020. Perigee: Efficient Peer-to-Peer Network Design for Blockchains. *In Proceedings of the 39th Symposium on Principles of Distributed Computing (PODC '20). Association for Computing Machinery, New York, NY, USA,* 428–437. DOI:https://doi.org/10.1145/3382734.3405704.

[14] Rahmadika S, Rhee K-H. Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management.* January 2018. doi:10.1177/1847979018790589.

[15] Tredinnick L. Cryptocurrencies and the blockchain. Business Information Review. 2019;36(1):39-44. doi:10.1177/0266382119836314.

[16] Julie Frizzo-Barker, Peter A. Chow-White, Philippa R. Adams, Jennifer Mentanko, Dung Ha, and Sandy Green. 2020. Blockchain as a disruptive technology for business: A systematic review. *Int. Inf. Manag*. 51, C(Apr 2020). DOI:https://doi.org/10.1016/j.ijinfomgt.2019.10.014.

[17] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[18] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," *in Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA),* pp. 1–8, November 2018.

[19] M. Shen, H. Liu, L. Zhu et al., "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[20] M. Li, H. Tang, A. R. Hussein, and X. Wang, "A sidechainbased decentralized authentication scheme via optimized twoway Peg protocol for smart community," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 282–292, 2020.

[21] David Heald & Ron Hodges (2018) Accounting for government guarantees: perspectives on fiscal transparency from four modes of accounting, *Accounting and Business Research*, 48:7, 782-804, DOI: 10.1080/00014788.2018.1428525.

[22] Leone P., Panetta I.C., Porretta P. (2013) Credit Guarantee Institutions, Performance and Risk Analysis: An Experimental Scoring. *In: Falzon J. (eds) Bank Stability, Sovereign Debt and Derivatives. Palgrave Macmillan Studies in Banking and Financial Institutions. Palgrave Macmillan, London.* https://doi.org/10.1057/9781137332158_6.

[23] Franklin Allen, Elena Carletti, Itay Goldstein, Agnese Leonello, Moral Hazard and Government Guarantees in the Banking Industry , *Journal of Financial Regulation*, Volume 1, Issue 1, March 2015, Pages 30–50, https://doi.org/10.1093/jfr/fju003.

[24] Aslanova, Kemale. (2014). The Impact of Globalization on Bank Guarantees: *Changing Role of Letter of Guarantee in Banking.* 10.1007/978-3-319-01125-7_15.

[25] Zhang C, Hu N. A New Method for Computing Letter of Credit Risks. *SAGE Open.* October 2020. doi:10.1177/2158244020970214.

[26] Anatolevich, Vladimir & Шеверева, Елена & Burmistrova, Mikhailovna & Nikolay, & Bodin, Borisovich & Alexander, & Chursin, Alexandrovich & Shevereva, Aleksandrovna. (2018). A letter of credit as an instrument to mitigate risks and improve the efficiency of foreign trade transaction *Carta de crédito como instrumento para mitigar riesgos y mejorar la eficiencia de la transacción de comercio exterior*. Vol. 39 (06) Year 2018.

[27] Jalilian, N., Zanjirchi, S.M. and Goh, M. (2020), "Interactive scenario analysis of banking credit risks in intuitive fuzzy space", *Journal of Modelling in Management*, Vol. 15 No. 1, pp. 257-275. https://doi.org/10.1108/JM2-01-2019-0011.

[28] Han, C.-R., Nelen, H. and Joo, M.Y. (2015), "Documentary credit fraud against banks: analysis of Korean cases", *Journal of Money Laundering Control*, Vol. 18 No. 4, pp. 457-474. https://doi.org/10.1108/JMLC-12-2014-0048.

[29] Brakerski, Zvika & Segev, Gil. (2011). Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting. *Journal of Cryptology*. 27. 543-560. 10.1007/978-3-642-22792-9_31.

[30] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *in Proceedings of Advances in Cryptology- EUROCRYPT'99*. Springer, 1999, pp. 223–238.