Security Model for a Central Bank in Latin America using Blockchain

Richard Romero[1], Raul A. Sanchez-Ancajima[2], Javier A. López-Cespedes[3], Miguel A. Saavedra-López[4*], Segundo Juan Sanchez Tarrillo[5] and Ronald M. Hernández[6]

[1]Universidad Estatal de Milagro, Milagro, Ecuador. rromeroi@unemi.edu.ec
Orcid: https://orcid.org/0000-0002-3387-6661

[2]Universidad Nacional de Tumbes, Tumbes, Peru. rsanchez@untumbes.edu.pe
Orcid: https://orcid.org/0000-0003-3341-7382

[3]Universidad Nacional de Tumbes, Tumbes, Peru. jlopezce@untumbes.edu.pe
Orcid: https://orcid.org/0000-0003-2560-1876

[4*]Universidad Continental, Cusco, Peru. saavedralopezmiguel@gmail.com
Orcid: https://orcid.org/0000-0002-4773-0647

[5]Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Peru. ssanchez@usat.edu.pe,
Orcid: https://orcid.org/0000-0002-6763-760X

[6]Universidad Privada Norbert Wiener, Lima, Peru. ronald.hernandez@outlook.com.pe
Orcid: https://orcid.org/0000-0003-1263-2454

Received: February 22, 2023; Accepted: April 03, 2023; Published: May 30, 2023

Abstract

Banking institutions in Latin America are the target of increasingly sophisticated and advanced cyber-attacks and threats, which increase every year and leave substantial economic losses, due to the high level of global interconnection and digitization of their operations. The objective of this work is to design a model to guarantee information security in a Central Bank in Latin America using Blockchain technology. Exploratory research, observation and inductive and deductive methods are used to propose Blockchain solutions in a Central Bank. The results are a model for secure transactions in Blockchain, Smart Contract functions and a data management process. It was concluded that the security model for a central bank provides high level of information management and storage of transactions in a secure and immutable way.

Keywords: Central Bank, Blockchain, Hyperledger, Ethereum, Latin America.

1 Introduction

Organizations belonging to Latin American countries have a low level of cybersecurity capacity to face the increasingly sophisticated and advanced attacks and threats, which increase every year and leave substantial economic losses. (Romero Izurieta, R., 2023). The banking sector is one of the first targets of cybercrime, because it handles money, with high level of global interconnection and digitization; that is why it is a sector that invests heavily in cybersecurity and tries to control the risks of cyberattacks

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 2 (May), pp. 117-127.
DOI: *10.58346/JISIS.2023.I2.007*

*Corresponding author: Universidad Continental, Cusco, Peru.

(Vedral, B., 2021). In 2020 the Bank for International Settlements reported that globally 36 central banks planned to implement central bank digital currency (CBDC); this decision also brings security risks to central banks, such as counterfeiting, fraud and cyber-attacks (Han, D., 2021). The benefits of implementing a digital currency are to improve financial inclusion and speed up the time of international transactions, but as disadvantages we have increased cyber security risks (Kesavaraj, S.V., 2022).

The accelerated development of new technologies such as Blockchain, Internet of Things, Big Data, Artificial Intelligence, has changed consumer behaviors and the business model of financial institutions, due to the ease and efficiency provided by these technologies, but as disadvantages brings fraud risks that can cause large financial losses. (Zhou, H., 2021). Blockchain technology allows to implement CBDC and decrease security problems, we have experience of many countries that have carried out projects with Blockchain with excellent results for their central banks (Sethaput, V., 2023).

This paper aims to propose a general conceptual model to ensure information security through the use of Blockchain technology of a Central Bank of a Latin American country. Why design a model for information security through Blockchain of a Central Bank of a Latin American country? To ensure that the Central Bank of any Latin American country performs secure and reliable transactions, mitigating cyber attacks and system vulnerabilities.

Exploratory research and observation are used to study the problem of implementing Blockchain technology in a Bank or institution. We also employ the inductive and deductive methods to general general and specific conclusions about the implementation of Blockchain in a Central Bank based on the literature review conducted.

The results are a model for secure transactions in Blockchain, general functions of the Smart Contract and a flowchart of the data management process. It is concluded that the proposed security model based on Blockchain for a Central Bank, guarantees the security and reliability of information, in transactions and storage of the banking system.

2 Materials and Methods

Materials

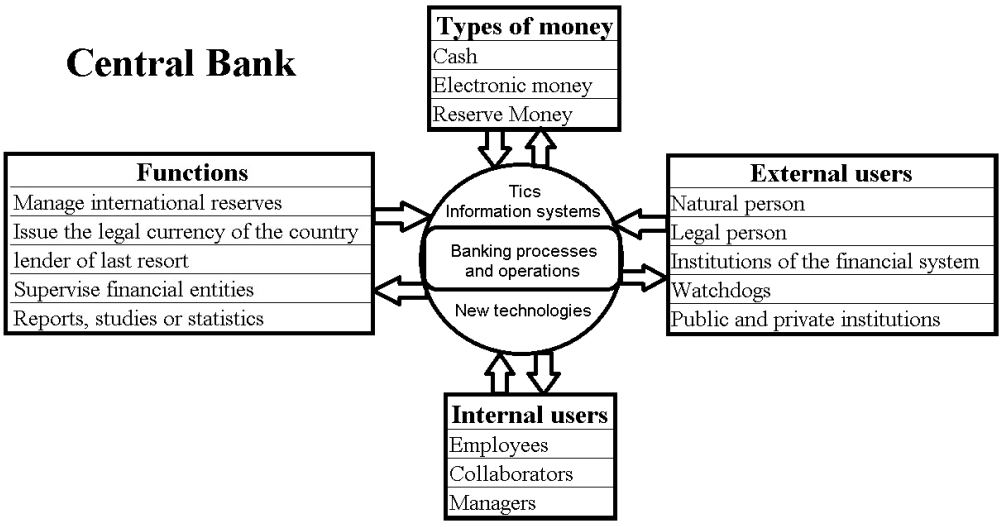

Figure 1: Central Bank Interaction with Users

Central Bank

In general terms, the functions of a country's central bank are: to issue legal tender, manage international reserves, serve as lender of last resort and banker to credit institutions, regulate currency, international exchange and credit, and serve as fiscal agent of the government; these functions may vary from country to country. (Bjerg, O., 2017). The role and functions of central banks have undergone changes throughout history, pointing towards digitization and total globalization of their activities, such as the issuance and supply of money and the flow of credit in an economy; the application of disruptive technologies such as Blockchain are fundamental to fulfill the functions of central banking (Mehrotra, A., 2021). Fig. 1 shows the interaction of the Central Bank with internal and external users, which, through its processes and operations with the help of ICT, information systems and new technologies can successfully provide its functions considering different types of money.

One of the global trends of Central Banks is the creation of digital currency, taking advantage of Blockchain features to manage and monitor transactions; since 2020 when Bahamas implemented its CBDC, other countries followed this initiative, such as Jamaica, Dominica and Grenada, which are from the Caribbean. By 2022, 105 countries are studying the feasibility of creating their CBDC, among them Brazil from Latin America; CBDC can improve financial inclusion and make international transactions in less time, but it has higher cybersecurity risks (Kesavaraj, S.V., 2022).

Blockchain Environment

Blockchain technology has been successfully tested in different areas, from finance, medicine, logistics, insurance, among others; banking has applied this disruptive technology in its products and services, taking advantage of its characteristics of being a decentralized, secure and reliable system to perform transactions without the involvement of intermediaries; central banks have implemented Blockchain for projects of: CBDC, payment clearing and settlement, asset transfer, audit trail, and standards enforcement. (Dashkevich, N., 2020). Blockchain has the ability to store data in unalterable blocks, related to its secure point-to-point applied to authorization and validation of decentralized transactions (Hosen, A.S., 2020).

Blockchain technology is a database that shares information in a distributed environment, where nodes/participants are involved, containing encrypted information and identification to create a secure blockchain (Han, J., 2021). Blockchain is used to record, validate and secure peer-to-peer transactions, Hyperledger is one of the most widely used Blockchain platforms in organizations for a private network, with Smart Contract facilitates the fulfillment of agreements between two parties (Rabbi, M., 2021). Ethereum is also a recognized platform for global payments, open source, which also allows to execute Smart contract (Joseph, S., 2021).

Blockchain in Central Bank

Literature review of articles pertaining to the topic of financial sector security using Blockchain technology was conducted: They propose a Central Bank Digital Currency System (CBDC) using Blockchain, with a transparent unspent transaction output approach (Islam, M.M., 2022). They present a three-layered architecture to address all CBDC processes, using Blockchain (Han, X., 2019). They propose generic framework for CBDCs using DLT platform for a financial services case. (Opare, E.A., 2020). They propose a hybrid Blockchain system with a modular network for CBDCs, with data storage in slices to improve network concurrency (Zhang, J., 2021). They analyze cybersecurity benefits and risks, and their economic and financial impacts of implementing a CBDC, in addition, cryptographic

solutions are presented (Kesavaraj, S.V., 2022). They developed a two-tier architecture for improving CBDC electronic cash processes and account and currency management (Liu, Y., 2022). They present CBDC founded on Cosmos blockchain employing the Inter-Blockchain Communication protocol. (Han, J., 2021). They analyzed the effects of implementing CBDC with Bitcoin distributed architecture. (Yang, J., 2020). Developed a management accounting system of commercial banks using Blockchain technology conjugating performance and intelligent data management, to improve the management level and competitiveness (Han, J., 2021). They analyze risk control, Blockchain technology adoption and countermeasures in the implementation of CBDC (Zhang, X., 2020). They evaluate the main internal and external aspects to implement CBDC in developing countries, to have an efficient payment system and monetary policy, financial inclusion and illicit activity monitoring (Syarifuddin, F., 2023). They present a two-layer CBDC environment, the wholesale distribution layer using Blockchain and the retail user layer using tokenization (Kumar, S., 2021). They analyze the money laundering scenarios of China's CBDC, the anonymous transaction scenario and the real-name transaction scenario (Li, Z., 2022). They use the advantages of Blockchain to create a development project management process in a Bank, to improve the transparency of public money allocation (Arantes, G.M., 2018). They present a Time Banking system through Blockchain, using smart contracts, to improve the use of digital currencies (Lee, Y.T., 2020). They implement security evaluation to the insurance trading chain via partially decentralized Blockchain (Liu, Y., 2019). They analyze Blockchain technology to improve authentication processes in public and private organizations (Mamunts, D.G., 2018). Investigate defense tools in banking systems, using tokenless Blockchain technology (Popova, N.A., 2019). They present a CBDC architecture using Blockchain technology, to manage payments more quickly. (Sun, H., 2017). They designed a scalable Panda model of CBDC, which employs efficient consensus protocols. (Tsai, W.T., 2018). They propose improved system performance through parallelized in-memory processing to enhance Blockchain transactions (Wang, Q., 2019). Examine the basic architecture and security flaws of the Blockchain platform layers. (Zhang, P., 2020). proposes a blockchain-based trusted data management scheme (called BlockTDM) in edge computing to solve the above problems, in which we proposed a flexible and configurable blockchain architecture including mutual authentication protocol, flexible consensus, smart contract, block and transaction data management, blockchain node management and deployment (Zhaofeng, M., 2019).

Methods

A literature review of scientific articles on information security models and banking transactions using Blockchain was carried out. The structure and general functions of central banks in Latin American countries were studied. The proposed security model guarantees monetary transactions, increases reliability among the actors of the banking process. Scientific articles proposing robust storage systems, which improve data confidentiality and privacy, were taken as a basis. (Zhaofeng, M., 2019), models of value transfers proposed for banking entities with Blockchain technology. (Mamunts, D.G., 2018).

A Blockchain environment is proposed to ensure the security and reliability of transactions and storage. We recommend Blockchain Hyperledger / Ethereum platforms to improve the security and management of data storage and digital transactions of the bank. A digital transaction management process is developed.

3 Results

The results generated in this work are:

a) Model for Secure Transactions using Blockchain

To obtain the security that guarantees optimal protection of a central bank, we designed a six-layer modular security model, where each layer specializes in a particular task, combating and preventing potential attacks and cyber threats. Fig. 2 shows the security model for the transactions of a central bank in a Latin American country. The six layers of the proposed security model are detailed below:

User layer: the central bank system interacts with internal users, who are employees, managers and collaborators of the central bank; external users are also involved, which can be a natural or legal person that uses the information and services of the central bank, such as institutions of the financial system, control bodies, public companies, citizens in general. The user layer interacts with the application layer to obtain the information and services requested by authenticated users, and interacts with the Blockchain layer to ensure security (Jung, S.W., 2022).

Application layer: provides network services to the banking transaction software applications used by users. The application layer is related to the Blockchain layer for key management, digital signature, transaction creation, among other functions.

Business layer: contains the banking application logic of the application layer. It interacts with the application layer and the database layer to process user requests.

Storage layer: it is the repository of the data recorded by the databases and the Central Bank's IT system; it corresponds to the physical storage of data and is related to the data management layer and the Blockchain layer. For the functional part of the system requirements, it is related to the business layer.

Database administration layer: generally there are database management systems (DBMS), which are specialized software that allow database administration, i.e., making configurations, managing information, performing transactions, managing users, roles and permissions. This layer is closely related to the storage layer and also interacts with the user, application and business layers and, in terms of security, with the blockchain layer.

Blockchain layer: This layer makes use of all the functionalities to guarantee the security provided by the Blockachain platform, both in user authentication, banking transactions, data storage, smart contracts, etc. To implement this Blockchain layer, a hybrid scheme is proposed using two platforms: Hyperledger for the authentication of internal users of the Central Bank and local Banks that have been granted their respective system authentication credentials; with the Ethereum platform for the authentication of external users, who process their authentication credentials through Smart Contract, according to the rules and conditions regulated by the Central Bank.

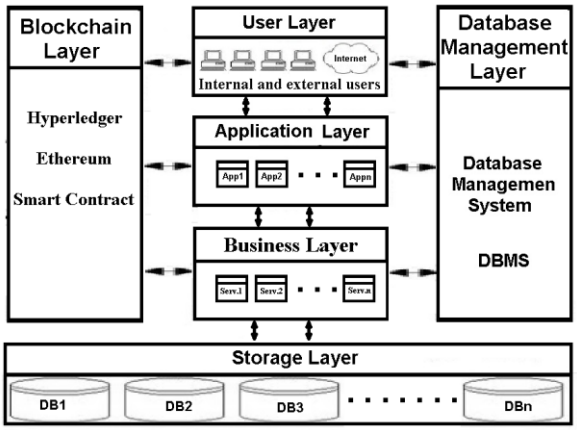

Figure 2: Architecture for Transaction Security Management

b) Smart Contract Functions

In order to achieve the objectives of the proposed model it is necessary to make use of the Smart Contract functions of Blockchain Ethereum, for the services and transactions of the Central Bank with its external users, in this way we automate the operations and create an account for each user. Fig. 3 shows the general transactional scheme of the Central Bank, using Smart Contract, the transaction starts with the access to the system of a registered user who uses his private key that is created with the new transaction, for which a Smart Contract is generated with the necessary data of issuing user, receiving user, account, amount and other agreements. This Smart Contract is added to the Blockchain network, once the public key and other transaction data are validated, it is sent through the network to the receiving user's address.

This transactional scheme using Blockchain's Smart Contract ensures the traceability of the movements made by users and increases confidentiality, through the use of public and private keys that are the Blockchain network identifications, using cryptographic methods to encrypt and decrypt messages through a mathematical algorithm. Smart Contract increases security by verifying compliance with the policies implemented in the central bank system.

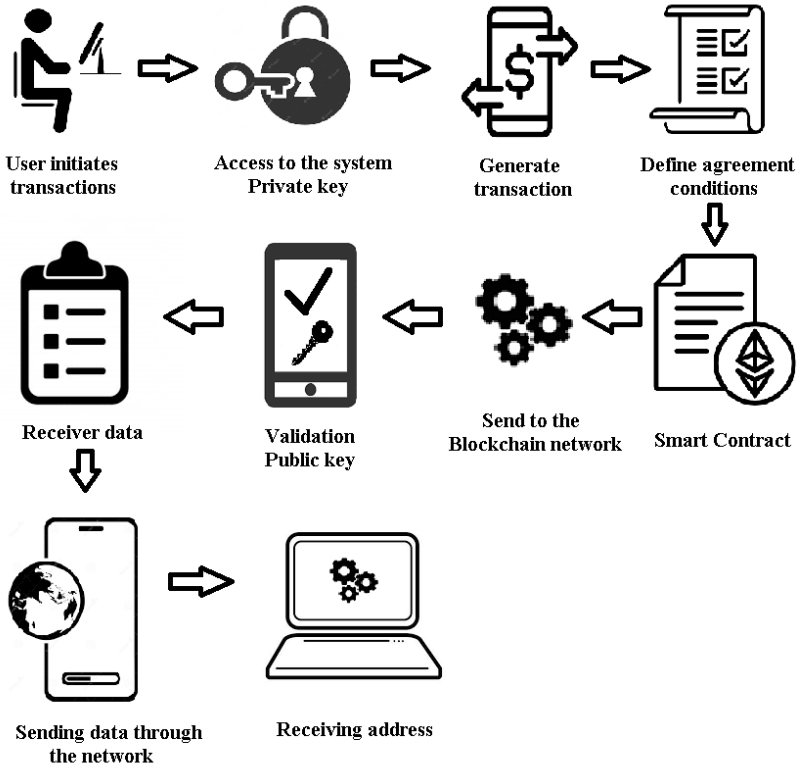

Figure 3: Transactional Scheme Smart Contract

c) Data management procedure

Fig. 4 shows the procedure for the security management of transactions generated by the Central Bank's clients, which guarantees the security of transactions through the Blockchain network. As we observe in the flowchart, to enter the system the validation of private keys is performed, after the system validates the access, it allows the user to generate a new transaction, otherwise the user's connection is prevented; the user generates a new transaction and the system verifies the data, terms and conditions; if it does not

comply with the terms and conditions the system terminates the transaction; if it complies with the terms and conditions the system asks the user for the data of the user receiving the transaction and requests the public key generated by the Blockchain manager; then, a connection is made with the Blockchain network to register the transaction generated and the process ends. With this process, the proposed model guarantees the security of Central Bank transactions, verifying the identity, terms and conditions.

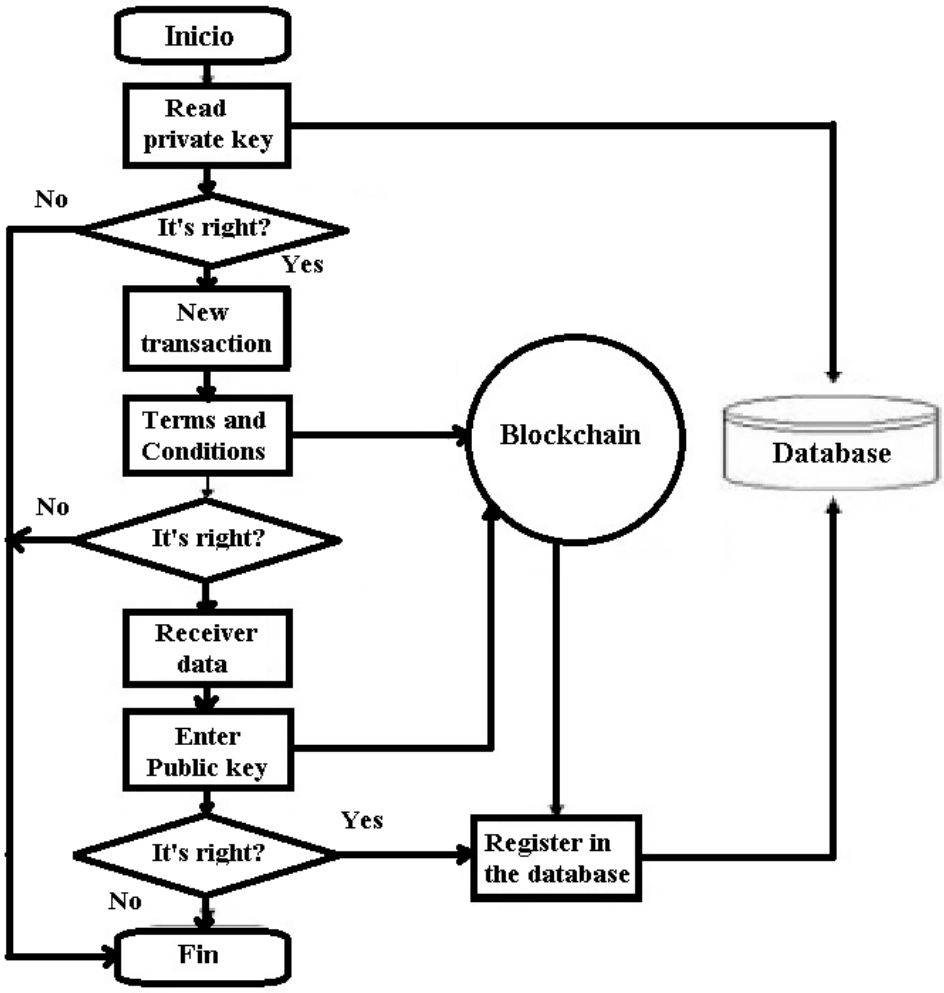

Figure 4: Data Management Procedure

4 Discussion

The proposed model improves security for Central Bank transactions, both of digital money movements, of the information stored in the system, the administration of internal and external users of the central bank, to ensure security from start to finish of each transaction through the use of Blockchain.

The information management model and functions defined in the Smart Contract ensure traceability and safeguard information in an effective and leak-free manner; the transactional functions and algorithm complement the security prototype with the connection in the database and the connection to Blockchain; the model in hybrid Blockchain and the data model focus on maintaining a management of information that are generated in the interactions with the system to increase the security and immutability of the information.

In the literature review we found scientific articles with similar models that developed systems using Blockchain technology for the security of their transactions, user management, data tracking according to the roles of each user, information availability, among others.

This proposal does not determine the budget, time and resources for the implementation of the proposed model, since it varies according to the conditions of the Central Bank of each country.

5 Conclusions and Future Work

As future work we should evaluate the proposed security model for a Central Bank by simulating or experimenting with Blockchain, with a dataset provided by a Central Bank.

It was concluded that the information security model for Central Bank transactions provides improvements in the management and storage of transactions in a secure manner.

With the Smart Contract functionality, traceability and security is generated throughout each transaction, of the information generated and stored in the nodes; the hybrid Blockchain network provides greater security and reliability in the transaction system from the issuing user to the receiving user of the transaction.

The proposed security model improves the management of users and their accounts in the database, through the storage of their records in the Blockchain network, which are generated after the registration in the conventional database.

References

[1] Arantes, G.M., D'Almeida, J.N., Onodera, M.T., Moreno, S.M.D.B.M., & Almeida, V.D.R.S. (2018). Improving the process of lending, monitoring and evaluating through Blockchain Technologies: an application of Blockchain in the Brazilian Development Bank (BNDES). *In IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1181-1188.

[2] Bjerg, O. (2017). Designing new money-the policy trilemma of central bank digital currency, 1-57.

[3] Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain application for central banks: A systematic mapping study. *IEEE Access*, *8*, 139918-139952.

[4] Han, D. (2021). Analysis on risks and Development Countermeasures of Central Bank digital RMB issue. *In IEEE International Conference on Public Management and Intelligent Society (PMIS)*, 250-254.

[5] Han, J. (2021). Intelligent Data Management System and Performance Joint Blockchain Model for Commercial Bank Management Accounting. *In IEEE Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 1525-1528.

[6] Han, J., Kim, J., Youn, A., Lee, J., Chun, Y., Woo, J., & Hong, J.W.K. (2021). Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain. *In IEEE 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 303-308.

[7] Han, X., Yuan, Y., & Wang, F.Y. (2019). A blockchain-based framework for central bank digital currency. *In IEEE International conference on service operations and logistics, and informatics (SOLI)*, 263-268.

[8] Hosen, A.S., Singh, S., Sharma, P.K., Ghosh, U., Wang, J., Ra, I.H., & Cho, G.H. (2020). Blockchain-based transaction validation protocol for a secure distributed IoT network. *IEEE Access*, *8*, 117266-117277.

[9] Islam, M.M. (2022). A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs. *IEEE Transactions on Services Computing*, *1-15*.

[10] Joseph, S., & Karunan, S. (2021). A Blockchain Based Decentralized Transaction Settlement System in Banking Sector. *In IEEE Fourth International Conference on Microelectronics, Signals & Systems (ICMSS)*, 1-6.

[11] Jung, S.W. (2022). Universal Redactable Blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *13*(4), 81-93.

[12] Kesavaraj, S.V., Jakhiya, C.M., & Bhandari, C.N. (2022). A Study on Upcoming Central Bank Digital Currency: Opportunities, Obstacles, and Potential FinTech Solutions using Cryptography in the Indian Scenario. *In IEEE 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-10.

[13] Kumar, S. (2021). Permission blockchain network based central bank digital currency. *In IEEE 4th International Conference on Computing, Power and Communication Technologies*, 1-6.

[14] Lee, Y.T., Lin, J.J., Hsu, J.Y.J., & Wu, J.L. (2020). A time bank system design on the basis of hyperledger fabric framework. *In IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1-3.

[15] Li, Z., Zhang, Y., Wang, Q., & Chen, S. (2022). Transactional Network Analysis and Money Laundering Behavior Identification of Central Bank Digital Currency of China. *Journal of Social Computing*, *3*(3), 219-230.

[16] Liu, Y., Ji, Q., Zheng, Q., Wu, H., Wang, Z., & Xiong, G. (2019). Security Assessment of a Partially Decentralized Blockchain System. *In IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 242-247.

[17] Liu, Y., Ni, J., & Zulkernine, M. (2022). AT-CBDC: Achieving Anonymity and Traceability in Central Bank Digital Currency. *In ICC IEEE International Conference on Communications*, 4402-4407.

[18] Mamunts, D.G., Marley, V.E., Kulakov, L.S., Pastushok, E.M., & Makshanov, A.V. (2018). The use of authentication technology blockchain platform for the marine industry. *In IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 69-72.

[19] Mehrotra, A., & Munjal, A. (2021). Leveraging Technology in Central Banking: Macroeconomic Forecasting & Managing Volatility. *In IEEE International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 323-328.

[20] Opare, E.A., & Kim, K. (2020). A compendium of practices for central bank digital currencies for multinational financial infrastructures. *IEEE Access*, *8*, 110810-110847.

[21] Popova, N.A., & Butakova, N.G. (2019). Research of a possibility of using blockchain technology without tokens to protect banking transactions. *In IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 1764-1768.

[22] Rabbi, M., Hradoy, P.M., Islam, M.M., Islam, M.H., Akter, M.Y., & Biswas, M. (2021). BLS: Bank Loan Sanction Using Blockchain Authenticity, Transparency and Reliability. *In IEEE International Conference on Electronics, Communications and Information Technology*, 1-5.

[23] Romero Izurieta, R. *et al.*, (2023). Prototype to Identify the Capacity in Cybersecurity Management for a Public Organization. *Advances in Science, Technology and Engineering Systems Journal*, *8*(1), 108-115.

[24] Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). *Cluster Computing*, 1-15.

[25] Sun, H., Mao, H., Bai, X., Chen, Z., Hu, K., & Yu, W. (2017). Multi-blockchain model for central bank digital currency. *In IEEE 18th International conference on parallel and distributed computing, applications and technologies (PDCAT)*, 360-367.

[26] Syarifuddin, F. (2023). Optimal Central Bank Digital Currency (CBDC) Design for Emerging Economies.

[27] Tsai, W.T., Zhao, Z., Zhang, C., Yu, L., & Deng, E. (2018). A multi-chain model for CBDC.

In IEEE 5th International Conference on Dependable Systems and Their Applications, 25-34.
[28] Vedral, B. (2021). The Vulnerability of the Financial System to a Systemic Cyberattack. *In IEEE 13th International Conference on Cyber Conflict (CyCon)*, 95-110.
[29] Wang, Q., Jia, Z., Wang, T., Shen, Z., Zhao, M., Chen, R., & Shao, Z. (2019). A highly parallelized PIM-based accelerator for transaction-based blockchain in IoT environment. *IEEE Internet of Things Journal*, *7*(5), 4072-4083.
[30] Yang, J., & Li, Z. (2020). Impact of Bitcoin's Distributed Structure on the Construction of the Central Bank's Digital Currency System. *In IEEE Fourth International Conference on Inventive Systems and Control (ICISC)*, 829-832.
[31] Zhang, J., Tian, R., Cao, Y., Yuan, X., Yu, Z., Yan, X., & Zhang, X. (2021). A hybrid model for central bank digital currency based on blockchain. *IEEE Access*, *9*, 53589-53601.
[32] Zhang, P., & Zhou, M. (2020). Security and trust in blockchains: Architecture, key technologies, and open issues. *IEEE Transactions on Computational Social Systems*, *7*(3), 790-801.
[33] Zhang, X. (2020). Opportunities, challenges and promotion countermeasures of central bank digital currency. *In IEEE Management Science Informatization and Economic Innovation Development Conference (MSIEID)*, 343-346.
[34] Zhaofeng, M., Xiaochang, W., Jain, D.K., Khan, H., Hongmin, G., & Zhen, W. (2019). A blockchain-based trusted data management scheme in edge computing. *IEEE Transactions on Industrial Informatics*, *16*(3), 2013-2021.
[35] Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet financial fraud detection based on a distributed big data approach with node2vec. *IEEE Access*, *9*, 43378-43386.

Authors Biography

Richard Romero Izurieta

Doctor in Applied Mathematical Statistics from the National University of Tumbes, Master in Information Systems with mention in Data Science, Computer Engineer from the Escuela Superior Politécnica del Litoral, Master in Business Administration with mention in International Business from the University of Guayaquil. He has 20 years of professional experience in the IT area, carrying out technological projects for different public and private companies. He also has 10 years of experience in university teaching, where he has directed undergraduate and graduate theses.

Raul A. Sanchez Ancajima

Degree in Mathematics from the Faculty of Sciences of the National University of Piura (UNP), Peru (2004). He obtained a Master's degree in Science with a major in Applied Mathematics from the National University of Piura (UNP), Peru (2011). D. in Mathematics from the National University of Trujillo (UNT), La Libertad, Peru (2021), with an internship at USP in Brazil. Senior Lecturer at the National University of Tumbes, Peru. My research interests are focused on Artificial Intelligence, Optimization Methods and Fractional Calculus.

Javier Ausberto López Cespedes

Public accountant and business administrator, master's degree in economics with mention in business management and doctorate in administration. With teaching experience in undergraduate and postgraduate courses, work experience as president of the Admissions Executive Committee, director of the Office of Marketing and Development of the Graduate School and president of the Research Committee of the Faculty of Economics at the National University of Tumbes. Also, former president of the Board of Directors of the Peru-Ecuador Border Development Corporation (CODEFRO). Currently Vice Rector of Research at Universidad Nacional de Tumbes.

Miguel A. Saavedra-Lopez

Doctor in Psychology from Universidad César Vallejo (Trujillo - Peru), in 2023. Dean of the Regional Board of Directors of Tumbes - College of Psychologists of Peru (2020 - 2022). Qualified as a RENACYT researcher by the National Council of Science, Technology and Technological Innovation (CONCYTEC). Currently teaching at the National University of Tumbes and Continental University (Peru), director of the International Journal of Social Sciences (RICSO). Interest in research related to mental health, artificial intelligence and scientific production.

Segundo Juan Sanchez Tarrillo

Doctor in Education, Master with mention in Research and University Teaching. Professor of the Faculty of Humanities and academic coordinator of the graduate school of the Catholic University Santo Toribio de Mogrovejo. He is a specialist in Historical-Social Sciences and Philosophy, developing formative undergraduate research subjects that culminate in essays, opinion articles, projects and theses, as well as educational planning, pedagogical management and active strategies.

Ronald M. Hernandez

Doctoral student in Education. Master in Education and Bachelor in Psychology. Qualified researcher in RENACYT Level II. Undergraduate and graduate university professor. Adjunct editor of national and international scientific journals. He has published more than 100 scientific articles in journals indexed in Scopus, Web of Science and SciELO.