IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART CONTRACT BASED APPROACH FOR FIXED DEPOSIT IN BLOCKCHAIN NETWORKS WITH REMIX IDE

Mr.Abhishek Rawat[1], Dr.Habib Ur Rahman[2],

Research Scholar[1], Professor[2]

Department of Computer Science and Engineering,

Kanpur Institute of Technology, Kanpur, Uttar Pradesh, India.

Abstract:

Blockchain technology has received a lot of attention recently due to its potential to create decentralized and secure data systems. This technology is a digital ledger technology that is tamper-evident and tamper-resistant, offering a new way of storing and sharing data. In this review, the author will summarize the present state of research on blockchain technology, including its applications and benefits, as well as potential pitfalls. The author will review the latest research on blockchain technology in different domain areas, comparatively finance, healthcare, and supply chain management, and provide insights into the future direction of this technology. The main functions of security deposits, such as the financial management system, computerized order entry system, and information interchange, have received a lot of attention in many pieces of literature. In this research paper, the author reviews the existing research papers and applications available for the security deposit using blockchain technology. The goal of this research paper is to give readers a thorough grasp of the state of blockchain technology research today and how it might affect a variety of fields.

Keyword- Blockchain technology, Ethereum, Remix IDE, Smart contract.

1. Introduction-

Without the need for a centralized authority, the distributed digital ledger known as blockchain uses complicated algorithms to record and verify transactions. The technology first gained attention as the underlying architecture for Bitcoin, the virtual currency that was first released in 2009 by an unidentified person or group using the pseudonym Satoshi Nakamoto. Since then, blockchain has evolved to become much more than just a tool for facilitating financial transactions [1]. It has the power to change a variety of businesses., from healthcare and energy to logistics and real estate, by improving transparency, security, and efficiency. At its core, blockchain is a decentralized database that is maintained and verified by a network of participants, called nodes, who jointly validate transactions and add them to the record in a transparent and tamper-proof manner [2]. A set of transactions are contained in each block of the chain, and once a block has been added, it cannot be changed or removed. without also modifying all subsequent blocks – a task that becomes increasingly difficult as more blocks are added. The capacity of blockchain to do away with the requirement for middlemen to validate transactions is one of its primary characteristics[3]. In conventional financial systems, banks and other financial organizations serve as middlemen between buyers and sellers, confirming the parties' names and creditworthiness and ensuring the secure transfer of payments. With blockchain, however, transactions can be verified and recorded directly on the ledger, eliminating the need for middlemen and reducing costs [4]. Another key benefit of blockchain is its strong security features. Each block in the chain is verified by multiple nodes, making it virtually impossible for

any one participant to alter the record without being detected [5]. In addition, the use of cryptography to secure transactions ensures that sensitive data remains private, even as it is shared across the network [6].

Perhaps most importantly, blockchain offers a new way of thinking about data and information sharing. By providing a decentralized, transparent, and secure way of recording and verifying transactions, it has the potential to fundamentally transform the way we exchange value and interact with each other online. Despite its many potential benefits, however, blockchain is still a relatively new technology, and many challenges must be overcome before it can achieve widespread adoption. These include technical hurdles, such as scalability and interoperability, as well as legal and regulatory issues surrounding the use of digital currencies and blockchain-based systems.

2. Research Background –

Stuart Haber and W. Scott Stornetta, two research scientists, created blockchain technology in 1991 [7]. To prevent anyone from being backdated or tampered with, they aimed to offer a computationally possible technique for time-stamping digital documents. To store the time-stamped documents, they created a chain of blocks that is cryptographically safe. The interest in blockchain technology has increased recently across a wide range of industries, including the healthcare system [8].. Blockchain is a distributed ledger technology that was originally developed for use in the cryptocurrency Bitcoin. It provides a secure and reliable way to maintain a record of transactions without the need for a central authority or trusted intermediary [9]. A blockchain is fundamentally a network of nodes that each hold a duplicate of the same data and functions as a decentralised database. Every time a new transaction is made, it is broadcast to the entire network, and each node on the network validates and records the transaction using a consensus algorithm [10].

The details of how the consensus algorithm operates vary depending on the blockchain implementation, but the basic idea is that nodes work together to come to a decentralized agreement about the state of the database. Blockchains are distinguished by this decentralised consensus mechanism, which makes sure that no single node may alter the database without the support of the other nodes in the network [11]. Another important aspect of blockchains is their use of cryptographic keys and digital signatures to authenticate transactions. Transactions on a blockchain are created using digital signatures that are generated using a private key, which is kept secret by the user. These digital signatures are then validated using the corresponding public key, which is widely available [12].

a) Blockchain Technology

Blockchain technology is a distributed, decentralised ledger system that enables peer-to-peer transactions that are safe, transparent, and effective without the use of middlemen like banks or governmental organisations [13]. The transactions are recorded in each block of the chain and protected using encryption in order to prevent tampering or unauthorised access [14]. The blockchain is a database that stores information electronically in a digital format and is shared among the nodes of a network. Each node can access the same information, and as new transactions occur, they are added to the most recent block in the chain, which is linked to the previous block, forming a chain of data known as the blockchain [15]. Each block in the chain contains a unique hash code that identifies it and ensures that it is tied to the previous and subsequent blocks. This creates a tamper-proof record of transactions and ensures that the chain remains secure[16]. These hash values are the output of a secured hashing algorithm, which produces hash values. Blockchain technology has the potential to revolutionise a wide range of industries, from finance and banking to logistics and supply chain management [17]. It is frequently connected with cryptocurrencies like Bitcoin. Because of the blockchain is decentralized, it is much more difficult for a single actor to manipulate or corrupt the data, making it more secure than traditional centralized database systems. Additionally, because every node has access to the same information, there is greater transparency and accountability in the system. Overall, blockchain technology represents a groundbreaking innovation that has the potential to transform a wide range of industries and revolutionize the way of storing and exchanging information [18]. As the audience can in Figure 1, how blocks are connected in blockchain and also this Figure represents the architecture of blockchain networks.

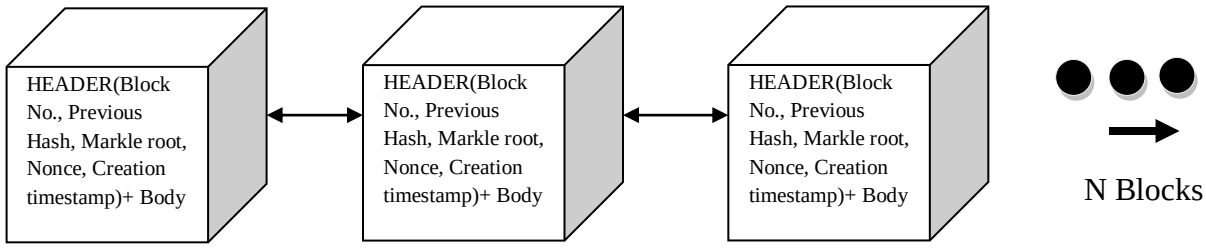

Figure: 1 Architecture of Blockchain

b) SHA-256

SHA-256 hashing algorithm is widely used in blockchain for calculating the hash value of the block. Secure Hash Algorithm 256, or SHA-256, is a patented cryptographic hashing algorithm. It was introduced in 2001 and is a member of the SHA-2 family of hash algorithms. A 256-bit (or 32-byte) hash value produced by the technique is specific to the input data [19]. In other words, while it is simple to calculate the hash of a given input, it is computationally challenging to produce the input from the hash value. This is because the technique is designed to be a one-way function. SHA-256 is widely used in many applications, including as a hash function in Bitcoin mining and in SSL/TLS security protocols used in web browsers. It has a high degree of collision resistance and is considered secure for most practical applications [20]. As the audience can see Figure 2, it is presenting the working of the SHA-256 algorithm, and how data is encrypted in a fixed output length.

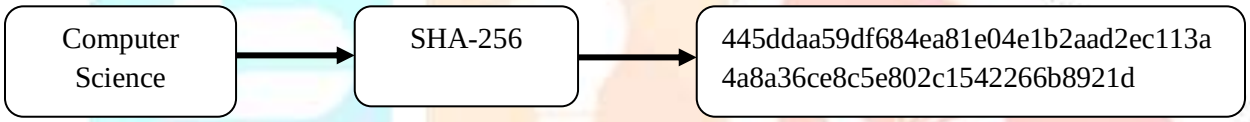

Figure: 2 Hash Function

3. Problem Statement-

I. Poor Assets management and high cost and taking more time in documentation and storing records manually.
II. High risk of data loss and data redundancy as a result of different fixed deposit schemes at various banks across the country.
III. Achieving a reliable database over multiple geographical regions is very difficult, especially for relational database systems.

4. Proposed Research Methodology Implementation

In this study, the author creates a smart contract on remix ide by using Ethereum cryptocurrency where the three identities - User, Bank management, and financial management service provider will register themselves. In this framework, the user provides his details like name, age, adhar number, contact details, address, etc. The Bank management provides his details like Bank registration number, Bank name, bank schemes, and facilities that are available for the User. The other finance management service provider enters his details and also provides the fixed deposit scheme details. When a user wants to invest his finance in any fixed deposit scheme then the user can check and choose the bank's services or other financial services schemes. After that, the selection of schemes the user invests his finance in the schemes according to the detail of the schemes. The scheme detail, the section has much information about the schemes such as time boundation for finance and the minimum investment that information is provided by banks and other financial management service providers. Because of the automated nature after the completion of fixed deposit time, the investors get their investment with the interest rate in their private address which address is used to invest the finance in the schemes by the banks or other finance management service providers. If the user wants his investing finance before the time boundation, the user can break his fixed deposit after completion of some authentication process in this case if user authentication is valid then the user will receive his invested finance without interest, and in this case, the bank management and other financial management services provider will also deduct some cost of your holds money for the security reason. As the audience can in Figure 3 is the working flow chart of the proposed framework.

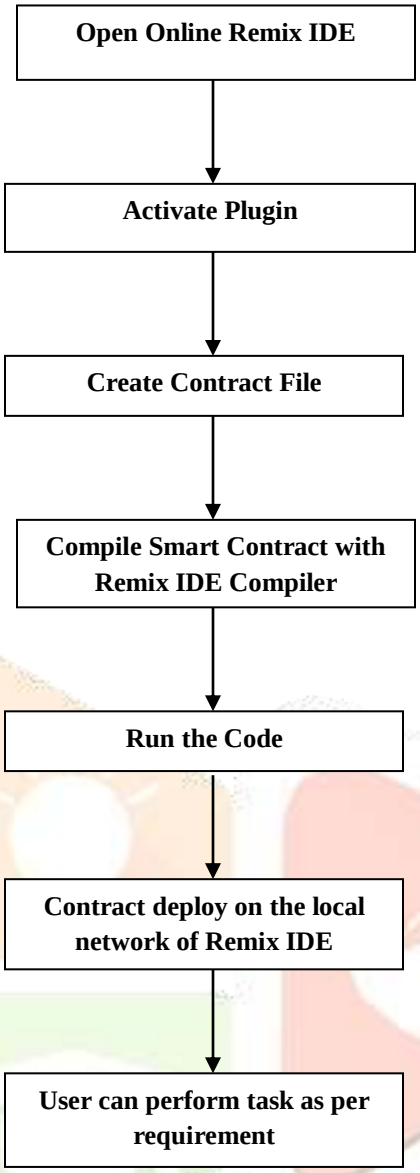

Figure 3. Work flow chart of proposed framework

5. Proposed research method

The author used the Remix IDE, the Ethereum blockchain, and the smart contract to build this framework. This framework's smart contract code is written in the solidity language..

5.1 Ethereum

Decentralised applications (DApps) and smart contracts can be developed on Ethereum, a decentralised blockchain-based platform. A distributed ledger known as a blockchain securely and openly records transactions and data. The Ethereum blockchain is distinctive in that it enables decentralised application development and data storage on the blockchain [21]. Ethereum was created in 2014 by Vitalik Buterin, who was inspired by Bitcoin's blockchain but wanted to create a platform that could execute more complex transactions beyond just transferring cryptocurrency. For transactions and to run smart contracts, Ethereum uses its own cryptocurrency known as Ether (ETH). It also introduces the idea of "gas," a unit used for determining how much computational work is necessary to carry out a transaction or a smart contract [22].

5.2 Smart Contract-

A self-executing programme or piece of code known as a "smart contract" operates on a blockchain-based platform like Ethereum. A smart contract's main goal is to make transactions and agreements between parties more trustworthy by automatically carrying out the provisions of the contract when specific prerequisites are satisfied. It makes transactions more safe and transparent by doing away with the need for middlemen [23]. From straightforward financial transactions to intricate supply chain management procedures and decentralised applications, smart contracts can be used for a variety of tasks [24].

5.3 Remix IDE-

The open-source Remix IDE is an Integrated Development Environment (IDE) for creating smart contracts on the Ethereum network. With its quick development cycles and extensive library of plugins with simple Graphical User Interfaces (GUIs), it is easy to use. It enables developers to write, compile, and debug Solidity code and test smart contracts in real-time on an Ethereum virtual machine (EVM) before deploying them onto the blockchain [25]. Remix IDE is used by developers of all knowledge levels for the entire journey of smart contract development without requiring any setup. It is simpler to create, test, and deploy smart contracts on the Ethereum blockchain thanks to Remix IDE, a potent tool. It offers 15 private accounts for the blockchain deployment of the smart contract. Each account has 100 fictitious Ether. Figure 4 shows this to the audience.

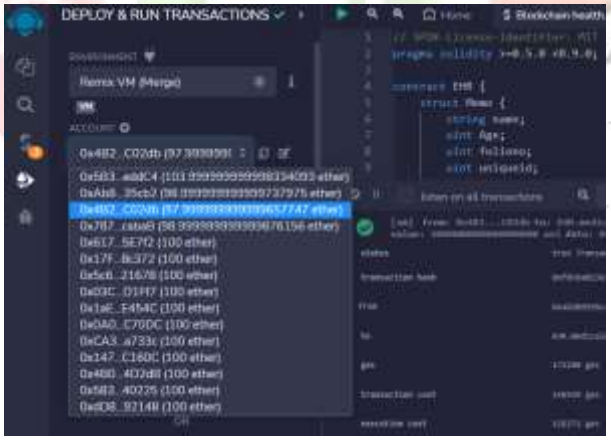

Figure 4. Fifteen private acconts of Remix IDE

6. System Architecture and Design-

The work done in the area of asset management utilising blockchain technology is included in this linked study. As mentioned author provides a certain solution for the previous problem which occurs in the paper-based industry or centralized asset management system. The proposed framework is implemented generally using Ethereum. The previous section of this paper also discusses Ethereum and its dependencies.

The most crucial component of any framework is its system design, which is created with the aid of model theory. The modules, architecture, and other components that make up the framework for the entire system to carry out the particular task are all included in this section. This framework's goal is to use blockchain technology to build a decentralised, secure, and smart contract system-based fixed deposit processing system. As shown in Figure 3, there are three layers present in the proposed framework. When combined, these layers would keep our system operating. The following explanations are provided for each of these levels' many ideas. The various user groups that interact with the proposed framework to carry out the task include investors, banks, the government, and other service providers of financial management.

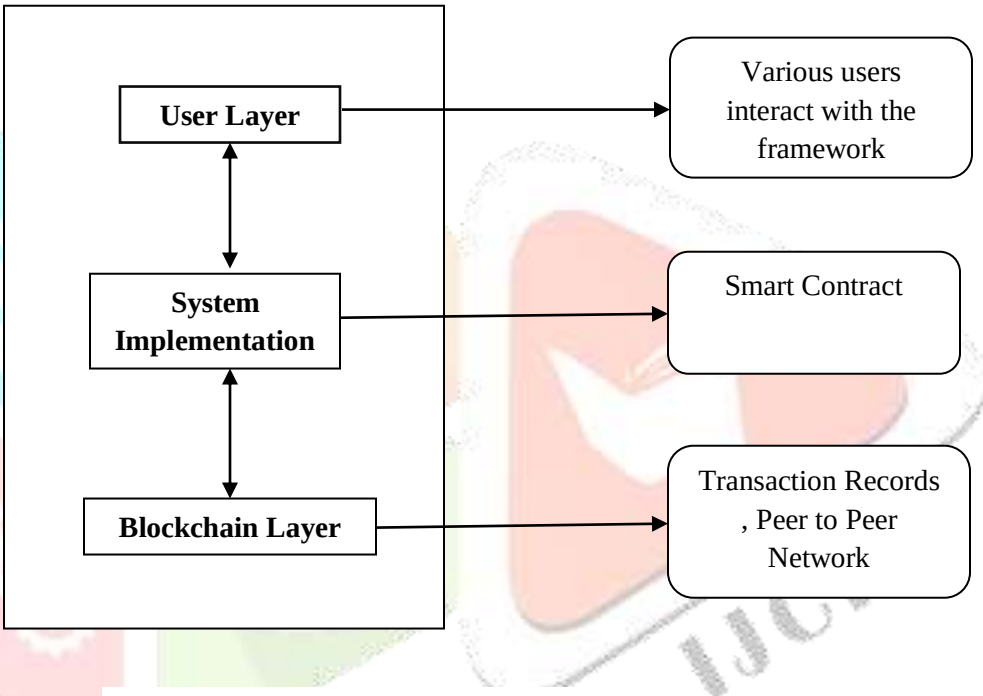

Figure 5. Layers of framework

6.1 User Layer

The users of this proposed framework could be Investors, Bankers, administrators, etc. The primary duties of the users would be to interface with the framework and carry out operations like reading, writing, and updating the records of the assets.. In this framework for performing any operation, the users must have an Ethereum account because every transaction consumes some charges, these charges are known as the gas price because this framework is based on blockchain technology. These charges are detected from the user's Ethereum account in the form of ether.

6.2 Blockchain Layers

The blockchain layer is the following layer in this suggested framework. The blockchain layer is made up of a few guidelines, codes, or techniques for interacting with the blockchain's working architecture. It consists of three things: transactions, consensus rules, and blockchain assets.

6.2.1 Blockchain Assets

The external user who can update and keep the record on the Ethereum blockchain processes the transaction there. The Ethereum blockchain treats these transactions as assets. These assets are bits of data that users can send to one another or store on the blockchain for later use.

6.2.2 Consensus Rules

In general, consensus criteria are followed by blockchain technology when calculating transactions. It uses a few consensus methods to accomplish this and keep the blockchain secure. The proof-of-work (PoW) consensus technique is used by the Ethereum blockchain. The justification for selecting this algorithm is that it upheld the trusted protocol, which is the agreement of all nodes connected to the blockchain network.

6.3 Transaction

The system consists many of transactions such as adding records, viewing records, and updating records. This proposed framework consist of three entities Investors, Banks Management, and other financial management service provider. All entities have different fields for Invetors there are several fields like ID, Name, Age, Contact, etc, and same as Bank Management has different fields such as Bank Name, Bank ID, Specification, etc and for the other finance management service providers entities have the Company name, registration number and the several details of the Investors such as fixed deposit details.

7. Result and Discussion-

From the above textual matter, it should be observed that Blockchain is an optimal solution for enhancing the confidentiality of the fixed deposit system. Table 1 illustrates the problems of the current fixed deposit system and the author assumes that this problem is reduce by blockchain technology in the future.
The Major findings obtained are shown below:

Sr No.	Issue	Solved in Blockchain (Recommendations/Assumptions)	Achievable Solution
1	Data is stored in centralized or paper Based Documentation	Data is stored in a decentralized and Encrypted manner	Yes
2	The risk of Data loss is very high	Minimum risk of data loss	Yes
3	The current fixed deposit system has no transparency	By the blockchain it provides transparency	Yes
4	Data is not tamper-proof	Data is tamperproof in blockchain	Yes
5	Operates by one authority	Operates by many authority	Yes

Table: 1

8. CONCLUSION AND FUTURE SCOPE

A fixed deposit system is a valuable financial tool for individuals and organizations looking to earn a stable return on their investments. With its fixed rate of interest and guaranteed returns, a fixed deposit provides security and peace of mind to investors. Additionally, it is a great option for those looking to save money for a specific duration of time, with the option to choose various maturity periods. Despite the limited liquidity and availability of flexible withdrawal options, a fixed deposit system remains a reliable and safe investment option for those seeking stable returns on their savings. The introduction of the fixed deposit system is described in section 1 and in section 2 the author described the research background of blockchain technology. Section 3 is related to the problem statement and section 4 narrates the proposed method to implement the fixed deposit system. section 5 has a description of the method and tools which is used to make the framework of the fixed deposit system and section 6 which is system architecture and design described the various layers of the proposed framework such as the user layer, system implementation, and transaction layer. The last section, the result, and discussion is described the final output of this proposed framework.

References.

1. Verma, R., Dhanda, N., & Nagar, V. (2022, July). Application of Truffle Suite in a Blockchain Environment. In Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021 (pp. 693-702). Singapore: Springer Nature Singapore.
2. Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. International Journal of Information Management, 52, 101940.
3. Lu, N., Chang, Y., Shi, W., & Choo, K. K. R. (2020). CoinLayering: an efficient coin mixing scheme for large scale bitcoin transactions. IEEE Transactions on Dependable and Secure Computing, 19(3), 1974-1987.
4. Tripoli, M., & Schmidhuber, J. (2018). Emerging Opportunities for the Application of Blockchain in the Agri-food Industry.
5. Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia computer science, 123, 116-121.
6. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.
7. ELBUZ, A., OSMANOGLU, M., & TANRIOVER, O. O. (2019). Designing a secure blockchain-based trading platform for internet of things. Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, 61(1), 102-110.
8. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes, 10(9), e003800.
9. Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. International Journal of Information Management, 39, 1-4.
10. Angrish, A., Craver, B., Hasan, M., & Starly, B. (2018). A case study for Blockchain in manufacturing:"FabRec": A prototype for peer-to-peer network of manufacturing nodes. Procedia Manufacturing, 26, 1180-1192.
11. Chen, R. R., Chen, K., & Ou, C. X. (2023). Facilitating interorganizational trust in strategic alliances by leveraging blockchain-based systems: Case studies of two eastern banks. International Journal of Information Management, 68, 102521.
12. Mehbodniya, A., Webber, J. L., Neware, R., Arslan, F., Pamba, R. V., & Shabaz, M. (2022). Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data. Expert Systems, 39(10), e12978.
13. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22, 14743-14757.
14. Bhattacharjya, A., Kozdrój, K., Bazydło, G., & Wisniewski, R. (2022). Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics*, *11*(16), 2560.
15. Pal, K. (2020). Internet of things and blockchain technology in apparel manufacturing supply chain data management. *Procedia Computer Science*, *170*, 450-457.
16. Iftekhar, A., Cui, X., Hassan, M., & Afzal, W. (2020). Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety. *Journal of Food Quality*, *2020*, 1-14.
17. Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., & Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry?. *Journal of industrial information integration*, *17*, 100125.
18. Chin, T., Wang, W., Yang, M., Duan, Y., & Chen, Y. (2021). The moderating effect of managerial discretion on blockchain technology and the firms' innovation quality: evidence from Chinese manufacturing firms. *International Journal of Production Economics*, *240*, 108219.
19. Al-Odat, Z. A., Ali, M., Abbas, A., & Khan, S. U. (2020). Secure hash algorithms and the corresponding FPGA optimization techniques. *ACM Computing Surveys (CSUR)*, *53*(5), 1-36.
20. Gad, A. H., Abdalazeem, S. E. E., Abdelmegid, O. A., & Mostafa, H. (2020, October). Low power and area SHA-256 hardware accelerator on Virtex-7 FPGA. In *2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)* (pp. 181-185). IEEE.
21. Jain, A., Tripathi, A. K., Chandra, N., & Chinnasamy, P. (2021, January). Smart contract enabled online examination system based in blockchain network. In *2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-7). IEEE.
22. Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105-117.
23. Guadamuz, A. (2019). All watched over by machines of loving grace: A critical look at smart contracts. *Computer Law & Security Review*, *35*(6), 105338.
24. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.
25. Amir Latif, R. M., Hussain, K., Jhanjhi, N. Z., Nayyar, A., & Rizwan, O. (2020). A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia tools and applications*, 1-24.