Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MANIPULATION PREVENTION IN GOLD AND MINERAL PARTICLES PRODUCTION USING BLOCKCHAIN AND SMART CONTRACTS

[1] MAHMOUD ABD ELNABY A. HEGAZY,[2] SHEREEN A. TAIE,[3] SHEREEN A. HUSSIEN

[1] Information System Department Faculty of Computers and Information, Fayoum University, Fayoum, 63511, Egypt
[2] Computer Science Department, Faculty of Computers and Information, Fayoum University, Fayoum, 63511, Egypt
[3] Computer Science Department, Faculty of Computers and Information, Fayoum University, Fayoum, 63511, Egypt

E-mail: [1] ma4241@fayoum.edu.eg, [2] sat00@fayoum.edu.eg, [3] sam26@fayoum.edu.eg

ABSTRACT

Blockchain technology has an effective role in multi-step transactions. Blockchain technology availability of new solutions and innovations has made a real change in busines. Smart contracts are computer protocols designed to facilitate and verify the agreements among multiple users automatically when certain conditions are met. With the rapid advance in blockchain technology, smart contracts are being used to serve a wide range of purposes ranging from self-managed identities on public blockchains to automating business collaboration on permissioned blockchains. They contribute in the development of many decentralized applications for all domains. The gold particles and precious metals production from rocks is one of the fields that can be improved by using Blockchains. This paper provides a model based on the private blockchain permissioned system in recording and monitoring the results of the mineral exploration process in rocks and the result of the process data analysis of atomic absorption to prevent any manipulations. It is implemented with Hyperledger fabric platform based on consensus Federated Byzantine Agreement (FBA). It achieves a remarkable level of scalability, transparency and safety.
Keywords: *Manipulation Prevention, Previous Metals, Blockchain, Smart Controls*

1. BACKGROUND

A blockchain is a chain of blocks that contain information [1]. The three main components of blockchain are the following:-

1.1 Blocks

A ledger can be defined as a book where transactions are recorded. Think of blocks as pages in a ledger. Several data blocks form a chain and hence the name "blockchain" is created. These blocks contain all the unvalidated transaction data created by network users. Furthermore, all the information stored by blocks is cryptographically encrypted. The blocks are closed right after the information is validated by the network. As more transactions pile up, new blocks will be created and the process will be repeated. Each block contains this information:-

- Nonce: A 32-bit whole number that was generated randomly during block creation.
- Hash: The nonce is used to generate a 256-bit number aka a hash. Both the nonce and the hash are used to identify that block as part of a particular cryptocurrency's network.
- Transactions: A list is created to contain all the transactions stored inside a block.

1.2. Miners

The creation of blocks is done by miners who use sophisticated software that was developed specifically to solve complex math problems. A miner's block is added to the chain when the miner can find a nonce that generates a correct hash. If a block is successfully mined, the nodes inside will accept the change and a financial reward will be given to whoever was involved in the mining process. Mining cryptocurrencies that exist on the blockchain such as Bitcoin require large amounts of time and computational power. An interesting thing to know is that there are some blockchains known as "permissioned

blockchains" which do not necessarily need miners to create blocks. This is because they are programmed in such a way that nodes can find the best block for themselves.

1.3. Nodes

A blockchain network cannot function without transparency. That's why nodes are used to maintain copies of the blockchain. These nodes are inter-connected and regularly exchange information with each other so that they are constantly updated. By storing and preserving all the data inside a blockchain, nodes can be thought of as the framework for an entire blockchain.

2. INTRODUCTION

The concept of blockchain technology is derived, whereby a digital stored ledger is a series of data blocks without a central system, after each transaction distributed across the entire network is verified [1].

Blockchain has many important advantages, such as transparency, immutability, reliability and enhanced security [2]. Blockchain blend both encryption and consensus algorithms and peer-to-peer networks to verify the validity of the transactions concluded [1] All participating nodes on the network must reach a consensus, in order to add new transactions to the ledger and verify whether the transaction is legitimate or not. All these steps depend on consensus algorithms. In addition, blockchain's dependence on decentralization is a key factor in its performance (e.g., execution time, latency, throughput, scalability) [2].

Blockchain has been digitally transforming every enterprise in every industry. Blockchain's encryption technology and digital ledger allows secure storing and sharing of cryptocurrency. The blockchain was initially created confined only in Bitcoin transactions and with its evolution and scalability and application in many industrial and commercial [1]. Many fields have become dependent on the blockchain primarily, such as the financial fields, in order to reduce the costs of financial activities, enhance insurance policies, and enable exchanges without the involvement of a third party. In addition to the field of health care to reach the subjection of electronic medical records to oversight among many medical service providers. In addition to the logistical field, construction field, agriculture and food field, communications and many vital industries.

Blockchain provides security and transparency in business transactions, changes made to designs, documents and other business agreements. These aspects of blockchain make it useful and relevant to the mining industry. Recently, the digital mining is got the attention where not digging the ore at all and identifying the value in the ground. The digital tokens represent a green gold vault quantity (e.g. gram/oz of gold in the ground), gold that will never be mined, but traded on an exchange using digital tokens. This model has the potential to significantly disrupt the gold market. This paper focuses on applying blockchain technology in the production of gold and precious metals, which requires high accuracy and security. Since there is a lot of data from the rock analysis process, and to maintain the security and confidentiality of data from fraud or loss to actual production extracted.

3. RELATED WORKS

Block chain has been used in so many industries. It is used as a digital ledger that processes, verifies, and stores transactions on computers around the globe. Since a blockchain cannot be modified or interrupted, security is vastly improved as nobody can interrupt a transaction at any given time.

JAMEELA AL-JAROODI (2019) [1] have described the usages of the blockchain, opportunities, benefits, and challenges in general and specially its industrial applications in different domains. It examined its use in industry in the public financial industry, healthcare industry, energy industry, agriculture and food industries, robotics industry, Entertainment industry and other industrial fields. It is a technical challenge for safety, integrity and scalability.

CAIXIANG FAN (2020) [2] have discussed the analysis and performance evaluation of many types of distributed ledger technologies and the stages of their formation and compare them to each other. This analysis is performed in terms of application, execution, Data Layer, Consensus and Network.

SUPORN PONGNUMKUL (2017) [3] have focused on Performance Blockchain Platforms,

the comparison between Hyperledger Fabric and Ethereum (private deployment) mainly depends on Latency, execution time and throughput. The study has shown that HLF consistently succeeds on ETH across all metrics, but both platforms failed to assess them in terms of workload.

PURATHANI PRAITHEESHAN (2021) [4] have explained the provision of a technical solution to ensure the privacy and reliability of transaction data, Hyperledger Besu is an advanced Ethereum client. The purpose of choosing Hyperledger Besu to carry out smart contract transactions for a trustworthy lending system is to be easy to use for configuration and compatible with private and public chains. Experiments have been conducted for Hyperledger Besu performance measurements with additional security feature and also to face activities and harmful risks.

Cyril Naves Samuel (2021) [5] have Evaluated work performance and behavior between both Ethereum such as Geth, Open Ethereum (Parity) and Hyperledger Besu.

STEVEN GRAHAM (2019) [6] have explained the importance of blockchain in the construction industries and recording all information about projects from space, planning and project ownership. Moreover, it expands the knowledge of the construction industry using blockchain and demonstrates the results of companies using blockchain in construction projects the methodology currently in place in the construction industries is Site Sense. In short, it is based on recording all the building and construction industries and classifies all activities in the sequence related to the resource, The conjunction of blockchain.

JAMEELA AL-JAROODI (2019) [7] have shown the value blockchain in the industrial fields in facilitating the production process through the use of Digital Identities, Distributed Security for data, Smart Contracts and Micro-Controls. After using all these elements, all those who are concerned with viewing the data are enabled to record all the data, transaction and transparency. The most important industries that used blockchain in are Energy Related Applications, Logistics Management Applications, Manufacturing Applications, and pharmaceutical industries The results of relying on blockchain in those industries showed the results of access to safe and transparent production, cost reduction and production efficiency.

4. CLASSIFICATIONS OF DISTRIBUTED LEDGER TECHNOLOGIES (DLT)

DLTs are representing any ledger stored in a distributed manner and shared among a group of nodes or can refer to the participants according to ledger permissions.

DLTs were initially limited to cryptocurrencies such as Ethereum, Bitcoin and EOS but after the development of DLTS in 2019 they were used in many industries [7] and were classified as follows as shown in figure 1.

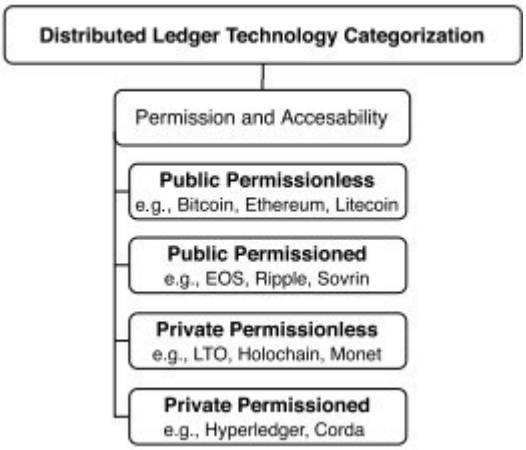

Figure 1: *Categories of distributed ledger technologies.*

DLTs become classified as permissioned and permissionless, according to ledger permissions. They can be divided into Public and private based on access to the ledger. Public ledgers enable all subscribers to validate, read and add transactions; they are open and available host a node to all participants without prior consent. Private ledgers can only be accessed by who has been approved with prior permission based on the permissions and accessibility of to the ledger. Table 1 shows the validity of each type of distributed ledger technologies.

Table 1: Comparative analysis of many consensus protocols in permissioned blockchain [11]

Categories of DLTS	The Validity
Public permissionless ledgers	No restrictions on all participating parties.
Public permissioned ledgers	The identity of the participants must be known but anyone can read and Validation of ledger.
Private permissionless ledgers	Participants' identities are not known but pre-approved.
Private permissioned ledgers	Determines access on Pre-certified participants and participants' identities Be known.

5. DLTS ABSTRACTION LAYER

In oracle blockchain Guidebook [8] General organizational structure to blockchain is designed with five layers. First application layer, second execution layer, third data layer, fourth consensus layer and Fifth network layer as shown in figure 2

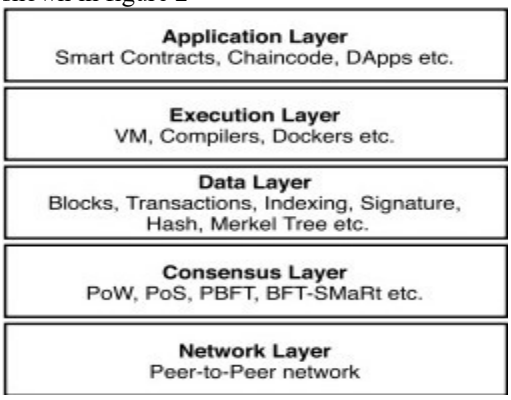

Figure 2: layers model for DLTs

5.1 Application Layer

This Layer includes many crypto currencies, smart contracts and all decentralized applications. Smart contracts are based on the idea of computer protocol, which consists of a set of rules that depend on certain conditions. If these conditions are met, the transaction is completed and the contract is executed through execution layer. The contract is published on one of the platforms that use blockchain technology such as, Ethereum, Hyperledger and other, which are available for many decentralized applications [9].

5.2 Execution Layer

The execution layer is responsible for the executing of the contract and EVM is developed to operate smart contracts code. There are several languages for writing smart contracts, such as Solidity, JavaScript and other.

5.3 Data Layer

Data layer is responsible for implementing smart contracts and connecting blocks that contain transactions together. As a result, Data is compiled in a "block", that is added to a blockchain and linked to the previous dataset. Hyperledger Fabric and Ethereum use a two-layer data structure to coordinate the block's content.

5.4 Consensus Layer

The consensus protocol is the most critical layer as it is the core of the DLT system. It defines the rules and mandates that all nodes follow them to reach an agreement called transaction confirmation. There are many consensus protocols, the most widespread is proof of work (POW). It has been used in many blockchain networks due to its advantages in high security, integrity and decentralization but one of the major disadvantages of its poor efficiency in Transaction Processing. To tackle this problem, many other consensus protocol have been proposed, including proof of stake (PoS), proof of authority (PoA) and proof of elapsed time (PoET). There are also some hybrid DLTs that combine different many types of consensuses. For example, Tendermint combines PBFT and PoS.

5.5 Network Layer

A peer-to-peer (P2P) network is the basis of the DLT system because it is responsible for inter-node communication, As node discovery, block creation, and block addition are done through this layer The most important requirement to be provided in P2P network are stability and speed. If one of these factors is not available, this may reflect negatively on DLT performance.

6. PROPOSED METHODOLOGY

This research applies a model based on the gold mine's blockchain for gold and precious metals production with preserving it form manipulation and theft. Moreover, it seeks to increase the safety rate in production and transparency in transaction and achieve the desired actual production goal. Figure 3 shows the main steps in the model architecture.

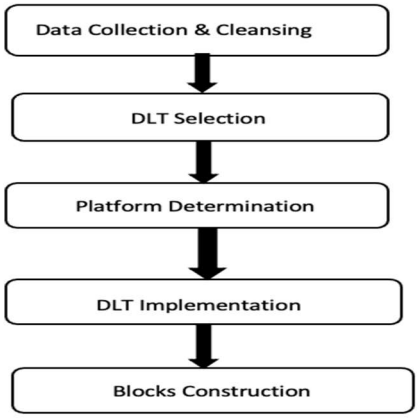

Figure 3: System Architecture

6.1 Data collection and cleansing

The data consists of different types of rock Produced for many precious metals. Include sequence number, sample number, type of each rock, latitude and longitude coordinates, the used method in the production process the atomic absorption through which the extraction is made Gold, silver, copper, lead, zinc, cobalt and nickel. The collected data may be having flaws or not in a proper format. So a data cleansing is the most important step of preprocessing because it will ensure that given input data is ready to use. data must be ensured its correctness and integrity before using it in the system. And so, cleansing it to avoid any errors, irrelevant, missing or distorted values. Also it reduces the costs of storing and analysing data easily and in a proper way.

6.2 DLTs Selection

Private blockchain permissioned is used in the industry and production of gold in mines, as it strengthens security by allowing only authorized persons make the transactions. In contrast, the public blockchain faces a major consensus challenge as must all nodes work together simultaneously otherwise there is a slow update of transactions made on the entire network.

Furthermore, authorized blockchain doesn't have the problem, as the nodes work together to move the updates faster. On the other hand, permissioned networks have their own pre-determined nodes for validating transactions There are many common permissioned blockchain frameworks. They include Quorum, Hyperledger, Corda, etc.

6.3 Platform Determination

When choosing a private framework for a certain usage purpose, it's important to identify some factors like society, activity, and the technology credence or even the essential performance. Evaluation Performance among different types permissioned blockchain platforms between Quorum, Corda, Ethereum and Hyperledger [10]. Latency, Throughput and scalability are the basic standards in the platforms that must be taken into account in evaluation.

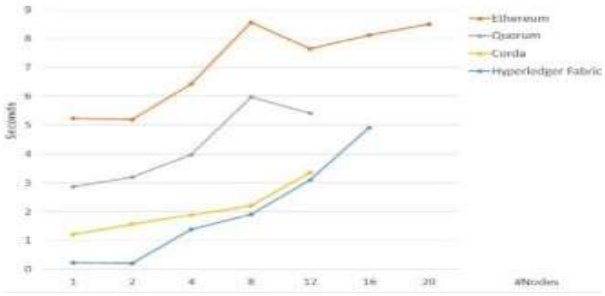

Figure 4: Comparison of Latency Sample Quorum, Corda, Ethereum and Hyperledger Fabric platforms (Nodes)

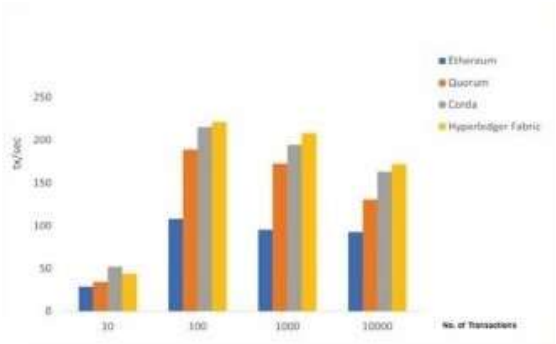

Figure 5: Comparison of throughput Sample Quorum, Corda, Ethereum and Hyperledger Fabric platforms (Transactions)

Fig. 4 and Fig. 5 show the comparison of latency and throughput between Quorum, Corda, Ethereum and Hyperledger fabric platforms. It's noticed that Hyperledger Fabric surpasses

Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ethereum and Quorum to a large extent but partially better than Corda.

6.4 DLT Implementation

Hyperledger Fabric simplifies a short Latency period while processing transactions equated with other permitted platforms. Thus, this platform is qualified for providing better throughput as well. The empirical observations expose that Hyperledger Fabric is performing better than other private platforms because of its straightforward, dynamic and effective modular consensus approach. Scalability can be evaluated for Hyperledger Fabric platform by changing the number of nodes and by monitoring scalability analysis by the same measures as scalability and latency by using two different sets of transactions (1000Tx and10000Tx). This experiment proves that the network can expand to up to 16 nodes due to communication among nodes in the consensus protocol [10].

6.5 BLOCKS CONSTRUCTION

After the data collection and cleansing process, DLTs appropriate selection and platform determination phases are done. Finally, Blocks of secured data are constructed each block contains its hash number and some other details, as shown in Figure 6.

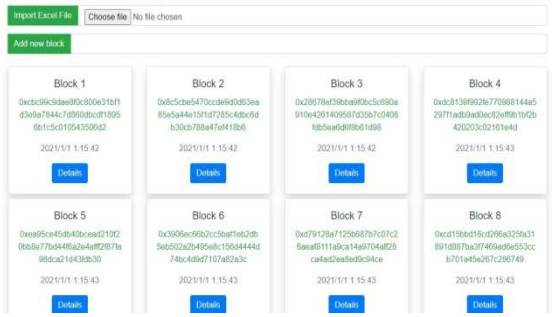

Figure 6: Blocks Construction

7. OPTIMIZED CONSENSUS ALGORITHM

After comparing several platforms, it is found that HLF is best in scalability, latency and throughput but better results can be obtained by choosing the suitable consensus protocol in comparison with other protocols based on the nature of gold mines.

Table 2 sheds light on the fact that each consensus protocol has advantages and disadvantages. However, what determines the use is the nature of work. Apparently, Federated Byzantine Agreement (FBA) overcomes PoA in some aspects including Throughput and Scalability [11].

Table 2: Comparative Analysis Of Many Consensus Protocols In Permissioned Blockchain [11]

Protocols Characteristics	dBFT	pBFT	FBA	PoA	Paxos	Raft
Security	Byzantine if f < 33.3%	Byzantine if f < 33.3%	Byzantine if f < 20%	Byzantine if f < 49%	Only from crash fault	Only from crash fault
Mutual trust	Nodes choose who to trust	Based on node selection	Flexible trust	Based on identity	Complete in terms of good intentions	Complete in terms of good intentions
Throughput	High	Moderate	High	Low	Moderate	Moderate
Scalability	High	Limited	High	Low	Limited	Limited

8. DISCUSSIONS AND RESULTS

Blockchain is a technology that allows for data to be validated and subsequently stored as an immutable ‘block’ on a collectively owned and distributed digital database. The resulting blockchain is immutable because every block is validated based on previous blocks, making it very difficult to alter. Blocks are validated either by an algorithm or a third party in the field. Both Hyperledger Fabric v1.0 and Hyperledger Fabric v0.6 will be applied to data for gold and precious metals mines. In order to demonstrate the superiority of either, in terms of latency, throughput and scalability.

.

8.1 EVALUATING LATENCY

Figure 6 shows the difference in the average latency by increasing the number of transactions between 1000 to 10000 transactions. The results indicate that Hyperledger Fabric v0.6 takes much longer time when the number of transactions increases compared to Hyperledger Fabric v1.0.

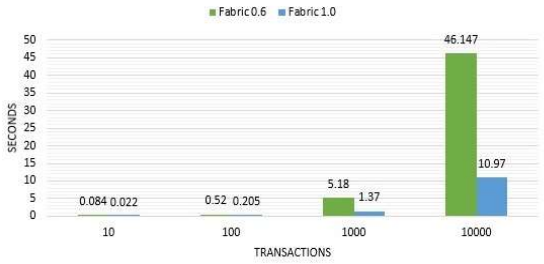

Figure 7 Average latency

8.2 EVALUATING THROUGHPUT

The results indicate that Hyperledger Fabric v1.0 has a higher throughput than Hyperledger Fabric v0.6, the reason for this is that the higher the number of transactions, the higher the Throughput speed in Hyperledger Fabric v1.0. Conclude that the difference in transactions per second (TPS) increases with the increase in the number of transactions.

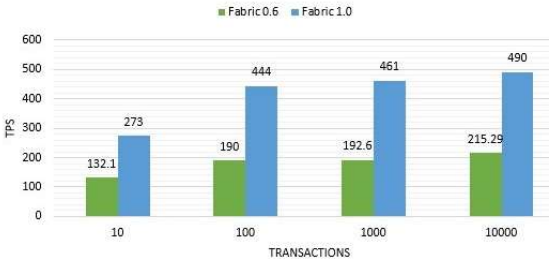

Figure 8 Average Throughput

8.3 EVALUATING SCALABILITY

Latency measurement depends on the change in the number of nodes with the continuation of the Latency and Throughput with the execution of 100 to 10,000 transactions, and one of the features of Hyperledger Fabric v1.0 is that it maintains the same range of performance across all rating scales, regardless of the number of nodes in the network.

9. CONCLUSION

Rocks go through number of phases to produce the final form of gold and precious metals such as atomic absorption and fire analysis. The results of each phase are issued in the form of numbers that are confirmed and given to the decision-makers to complete the production process. The traditional follow-up method allows tampering, damaging or losing data. In this paper, a blockchain model is presented with Private blockchain permissioned DLT which records all the results from the blockchain network in the form of blocks and each block is linked to what precedes it which guarantee data consistency and data manipulation prevention. Blockchain is authorized in the process of producing gold and precious metals. Moreover, it turns out that the core of any DLT is the consensus protocol. It is responsible for verifying every new block added to the blockchain as well as the agreement of all nodes on the transactions that take place in the blockchain. Hybrid between platform Hyperledger Fabric v1.0 and consensus protocol (FBA) is the most appropriate, to be used that provides a single entity from controlling the production process of gold and precious metals. As a result, the utmost degree of security, confidentiality and documentation of production process data can be reached.

REFERENCES:

[1] J. Al-Jaroodi and N. Mohamed, “Blockchain in Industries: A Survey.” IEEE Access, vol. 7, pp. 36500-36515, 2019.

[2] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, “Performance evaluation of blockchain systems: A systematic survey,” IEEE Access, vol. 8, pp. 126927–126950, 2020.

[3] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, “Performance analysis of private blockchain platforms in varying workloads,” 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017.

[4] P. Praitheeshan, L. Pan, and R. Doss, “Private and trustworthy distributed lending model using Hyperledger Besu,” SN Computer Science, vol. 2, no. 2, 2021.

[5] C. N. Samuel, S. Glock, F. Verdier, and P. Guitton-Ouhamou, “Choice of ethereum clients for private blockchain: Assessment from proof of Authority Perspective,” IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021.

[6] S. Graham, “Implementation of Blockchain Technology in the Construction Industry,” DigitalCommons@CalPoly, 2019.

[7] J. Al-Jaroodi and N. Mohamed, "Industrial applications of Blockchain," IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019.
[8] V. Acharya, A. E. Yerrapati, and N. Prakash, Oracle Blockchain Quick Start Guide: A practical approach to implementing blockchain in your enterprise. Birmingham: Packt Publishing, 2019.
[9] M. Alharby and A. van Moorsel, "Blockchain Based Smart Contracts: A Systematic Mapping Study." Computer Science & Information Technology (CS & IT), 2017.
[10] A. A. Monrat, O. Schelen, and K. Andersson, "Performance evaluation of permissioned Blockchain Platforms," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020.
[11] N. Z. Tomić, "A review of consensus protocols in permissioned blockchains," Journal of Computer Science Research, vol. 3, no. 2, 2021.
[12] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study." Telematics and Informatics, vol. 35, no. 8, pp. 2337-2354, 2018.
[13] P. Chapman, D. Xu, L. Deng, and Y. Xiong, "Deviant: A Mutation Testing Tool for Solidity Smart Contracts." 2019 IEEE International Conference on Blockchain (Blockchain), 2019.
[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." 2017 IEEE International Congress on Big Data (BigData Congress), 2017.
[15] N. M.Hamza, S. Ouf, and I. M.El-Henawy, "A proposed technique for enhancing the mining process in blockchain architecture," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020.
[16] D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," 2018 International Symposium on Electronics and Smart Devices (ISESD), 2018.
[17] R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh, and B. M. Kumar, "Decentralised applications using ethereum blockchain," Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 2019.
[18] V. Lakhanpal and R. Samuel, "Implementing Blockchain Technology in Oil and Gas Industry: A Review,", 2018.
[19] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles." Computers & Electrical Engineering, vol. 83, p. 106582, 2020.
[20] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, "Performance analysis of hyperledger fabric platforms," Security and Communication Networks, vol. 2018, pp. 1–14, 2018.
[21] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," 2019 IEEE International Conference on Blockchain (Blockchain), 2019.