DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

A Proposed Authentication Method for Document in Blockchain Based E-Government System

Zainab A. Kamal[1], Rana.F. Ghani[2]

[1,2] Computer Science Department, University of Technology, Baghdad, Iraq

[1]cs.19.33@grad.uotechnology.edu.iq, [2]110016@uotechnology.edu.iq

Abstract—*the primary concerns with manual transactions include corruption, lack of transparency, fraud, and mismanagement of distribution operations, all of which are created by traditional centralized applications, necessitating the migration to blockchain technology. In this work, a system is presented to secure and monitor correspondence between several nodes and store it in a decentralized database in order to secure distributed ledger transactions and safeguard against fraud and tampering when transactions are shared by multiple parties. The hashing that blockchain technology delivers in each transaction ensures a high level of security. The hashing associated with each transaction confirms all sending and receiving transactions. When a transaction is sent from one node to another, the other node checks the hash accompanying the transaction to see if it came from a registered node or an external node. Within the blockchain system, the nodes will check transaction correspondences. The system has demonstrated its effectiveness by delivering a more secure messaging system with high credibility and tamper resistance. In addition, the time it takes to authenticate will be in real time.*

Index Terms*— Blockchain, Consensus procedure, Hashing, Blockchain in Governance.*

I. INTRODUCTION

In communications networks, nodes are either distributed or end point. Each node in the network needs to define the node in the network and need to define the referred protocol within the network. In a distributed system, the nodes are either clients, servers, or peers and the peers can work as a client and sometimes as a server.

A distributed system is one in which the components are spread among multiple computers connected by a network. The system's components are interacting together for achieving a common aim. There are three benefits of using a distributed system: **- No global clock, concurrency of components, independent failure of components**. Distribution: - Means the decentralized distribution divided into **two classes: peer to peer distribution (full distribution) and client / server distribution**. Peer to peer systems have been used in a variety of applications [1], [2].

Architecture peer to peer :- (Unstructured) network, (Structure) network and (Hybrid) network.

(**Unstructured) network: -** It is made up of nodes randomly connecting to each other (Gossip, Gnutella, and Kazaa are instances of unstructured protocols). Unstructured networks are simple to construct since there is no imposed structures, and due to the fact that all peers in networks play the same role, they are particularly important in the face of high rates of disturbance (meaning various peers frequently join and leave the network).

(**Structure) network: -** Even in the case when a resource or a file is exceedingly scarce, any node may efficiently search the network for it. Each file's ownership is assigned to a peer using a hash function.

Hybrid peer to peer network: - It's a network that combines client-to-server and peer-to-peer

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

networks. There is a central server which assists peers in locating one another. This paradigm makes trade-offs between the unstructured peer-to-peer network's paths between nodes and the central functionality offered via a server-client network. Hybrid networks now outperform unstructured networks since specific operations, like search, need a central function, yet also take advantage of the unstructured networks' central assembly of nodes [3]. One of the peer-to-peer applications is **Bitcoin: -** It is a crypto currency which was created in the year 2008 via an unknown individual or group of individuals. When it was first carried out as an open-source application in 2009, the currency began to be applied. Also, bitcoin is specified as a decentralized digital currency that does not have a central bank or single official. It could be sent directly from one user to another on the Bitcoin network with no intermediaries. In addition, transactions are verified and encrypted through network nodes before being recorded in a distributed public ledger known as the blockchain [4].

Blockchain is considered as a promising file used to resolve a wide range of services, including public services and smart contracts. The security services, IoT, and other government data can benefit from blockchain technology [5]. Blockchain is considered as a highly important approach for public services which can have an impact on associations and businesses that rely on peer-to-peer networks [6], [7]. Many studies have been devoted to many issues related to blockchain and its use in e-governance

Ølnes and Jansen 2017 [8], in this study, the researchers believe that one should look beyond currency applications to see how blockchain could be used in government activities like safe document handling and digital identity management. Also, it examines the utilization of blockchain as a platform for various electronic-government applications, as well as a growing and supporting infrastructure, through demonstrating that blockchain has the ability to authenticate numerous permanent documents. It underlines the need of a realistic approaches through illustrating several application scenarios.

Terzi, Tzovaras and Votis, 2019 [9], the researcher presented how the blockchain works with artificial intelligence to enhance strength and security through two scenarios. The first is the smart cities' governance with Information and Communication Technology (ICT) through the Internet of Things. To efficiently practice the available energy strategies through the devices installed in the staff residences that produce energy. The management, sustainability and efficiency of national energy is done by registering it in the blockchain base. The second scenario adopts e-health and control of the high costs of health care by providing electronic health solutions using ICT, for example, providing chatbots (they support the patient by completing forms and submitting them to government departments).

ZHANG and XUE, 2019 [10], this study presents a complete description regarding the blockchain's privacy and security. It includes a poll that allows users to learn more about the blockchain's understanding, privacy, and security. Also, it presents the major security features which are supported as basic building blocks and requirements for Bitcoin, like cryptocurrency systems, succeeded by an understanding of mixing protocols, chain storage, consensus algorithms, and anonymous signatures in terms of the features, concepts, systems, and technologies.

Ajao, Adedokun and Karngong, 2019 [11], this study describes a mechanism for monitoring and safeguarding the distribution records with regard to petroleum products in a decentralized ledger database. Blockchain was utilized for securing a distributed ledger transaction in a database, as well as to safeguard records from fraud, manipulation, and corruption via the chain's participants. Sha1 algorithm depending on the approved public blockchain was used for this secure distribution, and this remote method is developed into an in-vehicle model which records remote geolocation with the use of remote monitoring or GPS to gather real-time data. Due to the fact that it doesn't enable

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

any single thing to change the records, the system has been demonstrated to be secure, effective and simple to manage. It also supports the agreement of 75% of the chain' participants to change events.

Miquel Oliver and Ramalhinho,2020 [12], this research reveals how creative technologies and smart city concepts may assist society in meeting the day-to-day problems of increasing citizen awareness. Through utilizing ICT to improve cooperation, digital technologies can drive economic and social progress. Decentralized democracy has made use of blockchain as a fundamental instrument. The researchers analyzed open points and offers recommendations for the successful, transparent, and long-term use of technology in future cities.

Alexandra, Lovelle, Molano,2020 [13], the researchers explained how the blockchain records' management might help society meet its needs for participation, transparency, and cooperation, which are all based on automated transactions. This would reduce corruption and improve the transparency and efficiency of government services. The idea of using smart contracts (mechanisms which attempt to remove intermediaries for simplifying transactions) in public procurement is given special attention. Because of its versatility and present development in topics with comparable tasks, the researcher finishes with recommendations for using the blockchain in conjunction with smart contracts via the Ethereum or Link platforms.

Sladi´c, Milosavljevi´c, Nikoli´c, Sladi´c and Radulovi´c, 2021 [14], the researchers looks at how the Serbian Land Administration handles transactions and how current ledger technologies like blockchain help supporting the process. The implementation of the blockchain is analyzed to support transactions in land information systems, including real estate registry transactions. Transactions are tracked in an immutable manner and tampered with to increase security and thus increase transaction speed, efficiency and data integrity without affecting the laws.

Guarda, Augusto and Haz, 2021 [15], The researchers explained how blockchain may be used to benefit from resources while also removing several major issues like corruption and ensuring more efficient resource allocation and dissemination. The effect of blockchain on electronic governance is investigated by the researcher. The researchers discussed the evolution of electronic governance through time, which has been fueled by economic globalization and the rise of the Internet and its application in public administration. Blockchain was defined as a decentralized and extremely secure accounting system. Governments have generally been criticized for not knowing how to deal with some, but blockchain has the potential to bring about new changes.

E-governance refers to information and communication technology, in combination with the creation of information and communication technologies, such as distributed technologies that include collective commitment and joint creativity towards evidence-based decision-making and policy. Distributed ledger technologies can make a significant contribution to the public sector that makes them more open and more reliable. For a more cooperative ecosystem in services and the ability to record transactions to deal with the community with a more transparent vision [16],[17].

II. BACKGROUND (BLOCKCHAIN)

It's a distributed database that can handle a large number of records. A links and timestamp to preceding blocks are included in each one of the blocks. Another definition is an electronic record system for processing and recording transactions, which allows all parties to track information through a secure network [18].

All financial transaction, assets and expenses are preserved and similar to that. Through blockchains, it is possible to preserve stored data without modifying it. Satoshi Nakumato (whose purpose is to invent the currency, Bitcoin) originally mentioned blockchain in a 2009 research report. This technology allows users to make transactions with no intermediaries, and it is a decentralized technology (there is no one controlling the operations that occurs through it

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

following its implementation). There are no governmental bodies controlling the course of events Things and even companies managing and organizing work in them[19].

Blockchain technology is a type of cryptography (meaning that the data which is transferred or the money traded through it is anonymous). People in the blockchain are merely coders who create programs that execute any activity, function, or implementation using blockchain technology. Many layers make up a blockchain [20]:

- Ifrastructure (hardware)
- Networking (node discovery - propagation and verification)
- Consenuse (proof of work - proof of stack)
- Data (blocks-transaction)
- Application (smart contract)

A. Block

A block in blockchain is a collection of transactions that have been hashed as well as encoded in the Merkel tree, as shown in *Fig. 1*. Each one of the blocks contains a cryptography hash of the previous block in the chain, tying the two together. A chain is formed by the linked blocks. This recursive procedure verifies the integrity of each subsequent block, all the way back to the genesis block, which is the first block. Hash, preceding hash, and data are all included in each transaction [21], [22].

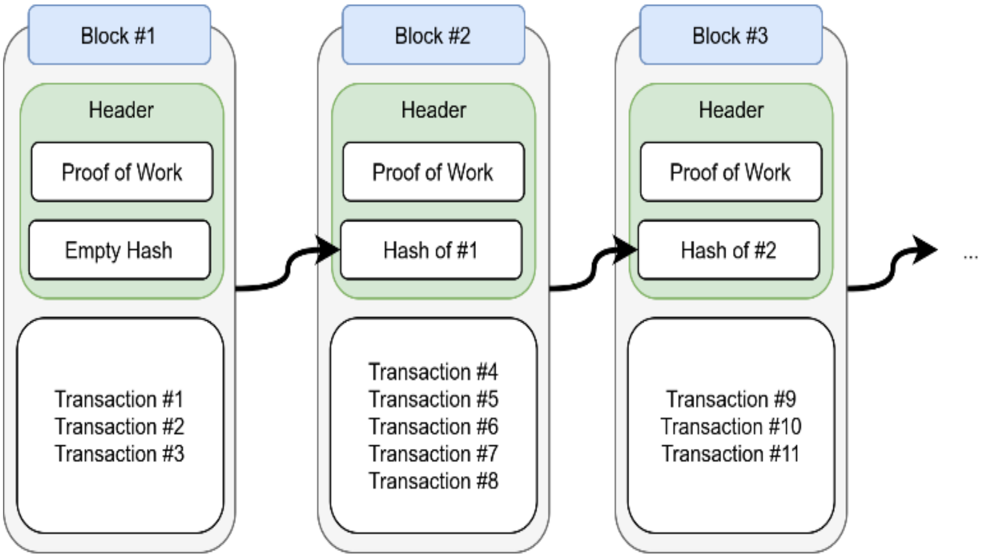

FIG. 1. BLOCKCHAIN STRUCTURE.

Blockchain advantage

- Decentralized network that does not belong to anyone, but rather is the property of its users.
- Open source.
- The level of safety is high and protection is high.
- The thought of breaking into the system is nearly impossible.
- Because persons are merely encrypted codes in the system, it provides a high level of confidentiality and privacy to its users.

As a result, no one can access the personal information of another user.

Blockchain disadvantage

– The absence of supervision represents, in one way or another, an opportunity and arena

Received 06/December/2021; Accepted 10/April/2022

for the work of the birds of darkness.

– Need expensive devices and great energy. Need very expensive appliances and a great deal of energy [23].

B. Hashing

Hashing is a cryptographic function that creates a unique fixed length hash code for any input such as an image, text or video. The entry every time will give the same output if the change is not made to the entry. It will always produce the same hash symbol (for example, if one of the lowercase letters is changed and converted to a capital letter, it will give a completely different and unique hash).

For blocks, transactions are stored in the block create a unique hash token. A block uses hash codes to link the blocks together. The blocks are added one by one in a linear chronological order, and each of them contains its own hash code and the previous block code, and this links the blocks together to form a chain [24],[25]. This interdependence of blocks is shown in *Fig. 2*.

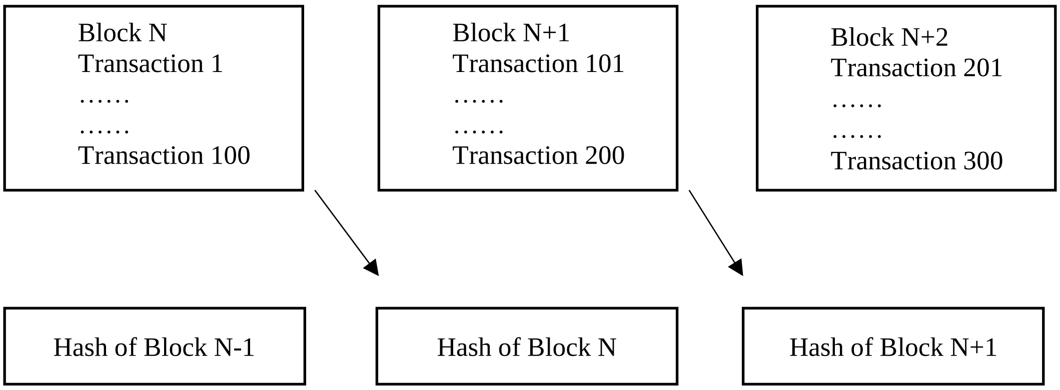

FIG. 2. THE INTERDEPENDENCE OF BLOCKS.

If someone tries to change the contents of a block in any way, then he or she must change the hash values for the content and for the block. The change can be detected easily because it will be evident that the change occurred in the hash because the nodes are responsible for verifying transactions and blocks [26], [27].

There are three principles for transactions.

Transaction is immutable

- The blocks are linked together using unique hash codes.
- Any change in the entry leads to a change in the breakdown of the transaction.
- Through the contract consensus process, the contract will realize that the block has been tampered with and will reject it.

C. Consensus Procedure

It's difficult to obtain consensus across untrusted nodes in a blockchain network. There is a group of Byzantine generals who lead a portion of the Byzantine army, which is going to if a portion of the general's attacks the city. The generals must agree on whether or not to launch an attack. It's possible that there will be traitors. Various judgments can be sent to different generals by a traitor. It is difficult to reach consensus in an untrustworthy environment, which is an issue with the block chain. Because the nodes do not need to trust the other nodes, we need some protocols [28].

– **Proof of work: -** Evidence-based consensus algorithm. Its concept is based on determining which node will get the right. This consensus was used in Bitcoin. If there is a transaction due to many nodes, then from the transaction that will put the transaction in the block, noting that the ledger will be meaningless if the transactions are repeated. It is important to reach an agreement, as the Prof. of Work tries to solve this problem.

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

The nodes which will participate are referred to as miners, and information is added to the transaction and it is hash. SHA-256 algorithm is used. All participants must continuously calculate the hash value. Although many miners may participate in verification and creation of transactions, only the first to solve will become the winner and will receive a surprise, creating a block of 12.5 BTC. The basic purpose of proof of work is that miners must expend significant computational resources for solving the problem and that just one miner is going to be a winner [29].

– **Practical Byzantine Fault Tolerance (PBFT):-** With the existence of shaded or malicious nodes, tolerance of Byzantine error indicates to communicating an agreement of viewpoints between at least two nodes which securely interact via a distributed network. Also, the replication algorithm is considered to be error-tolerant. It is supposed to be a high-execution consensus which may rely on a group of untrusted nodes in the network and expects that a few nodes are false or dishonest. The nodes are arranged in a sequential manner, with one serving as the leader and the rest serving as backup copies. Because the contract talks with other nodes for proving the origin (the integrity and origin of the message), decisions are taken by most of the votes [30].

– **Proof of Stack: -** It is a more energy-efficient option. The miner doesn't have to waste a lot of computational power for solving a mathematical puzzle which depends on the presence of nodes with enough system shares for participating in the block creation process. The likelihood of receiving the opportunity is totally dependent on the wealth of the participating nodes, which eliminates the possibility of malicious activity on the network. The auditor is selected based on how much of the network he owns. It removes peer competition, and the auditor after that uses his share and places a bet on a block. The auditor collects transaction fees included in the block if it is accepted. Proof of Stack has more sustainability than Proof of Work since it saves more energy while also delivering better productivity and latency, yet it has drawbacks. Because the validator is chosen based on bets, the richer node might have a better chance of verifying the block's legitimacy and so becoming more influential in the network. It's possible that this will result in unequal distribution.

Advantage and disadvantages Consensus algorithms

In **terms of managing the identity of the node** in the (POS and POW), the nodes can leave and join the network as they like either in PBFT It must be the node Known for choosing leaders

In **terms of energy saving**, the adapters and the work consume a great deal of electricity as for the proof and stack, it does not consume energy As for PBFT It does not need any mining and can save electricity greatly [31].

III. THE PROPOSED SYSTEM

This section describes the entire proposed System and implementation on distributed network with chains of operation that is shown in *Fig. 3*.

A. System Architecture

This section describes the network architecture made up of system entities.

System Entities

This section describes the basic entities of the proposed system

- **Peers:** refers to the registered members of the network and who are connected to each other.
- **Private Blockchain:** It refers to the type of peer-to-peer blockchain that is of the private type.
- **Chains build on SQL database:** It is the build blockchain on of a SQL database in which transactions are stored between registered employees across the network.
- **Smart Contract:** A program that is executed automatically and the contract is redeemed according to the listed conditions.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

The system will be a distributed system between more than nodes. The nodes in the network will send receive transaction between them. Any movement in the system from sending and receiving will be recorded and placed in the blockchain But before sending and receiving any transaction in the system represent (propose transaction), The node from which the transaction was received will be checked.

In order not to allow foreign nodes to enter the system and impersonate the sender.

B. ***Chains of operation*:-**The system will consist of four axes.

- The authentication stage base on registration: - register node in the system.
- Transaction propose stage :- propose transaction
- Authentication stage base on transaction: Sending and receiving transaction between nodes after authentication And make sure that the node that sends the transaction is registered in the system
- Storing transaction stages: sending and receiving transaction and store in the blockchain.

a- Before sending transaction from node to another node (the authentication stage):-

Before the propose transaction by a particular node, to decide on it, an authentication is made for the nodes. Authentication is done by logging into the node's page by registering the user and password in the system .

b- Transaction propose stage: -

Propose transaction from register node in the system**.**

c- Authentication stage base on transaction:-

After a transaction is proposed by a specific node registered in the system and fill the transaction by data , the correspondence process takes place between the shared node in order to make a decision regarding the proposed transaction, as shown in *Fig. 4*.

- **Node sending:-**

The authentication stage takes place before any process of sending transactions by sending a file that contains (encrypted data from transaction propose, hash)

The encrypted data is for the transaction propose by the node that is trying to send the transaction, and this same encrypted data will be generated from it a hash, In addition to a code suggested by the node that sends the data and distributed to all nodes that want to receive the data

So the file will consist of a hash as well as encrypted data and code number.

- **Node receiving:-**

When the node is received on a file (contains encrypted data for the proposed transaction, and hash)

The receiving node of the data will decryption after entering the correct code

Agreed upon between the parties.

Enter of the data it into the hash generation algorithm if the output hash is the same as the hash sent in the file

So the contract deals with the valid node registered in the system

d- Build blockchain

Every transaction that is proposed will be record in the blockchain and every authentication between the nodes to send and receive this transaction will also be recorded. So that each node will have the same transaction with the hash and the previous hash except for the first node will contain only the transaction and the hash. And it is easy to track any transaction and know it in any existing node.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

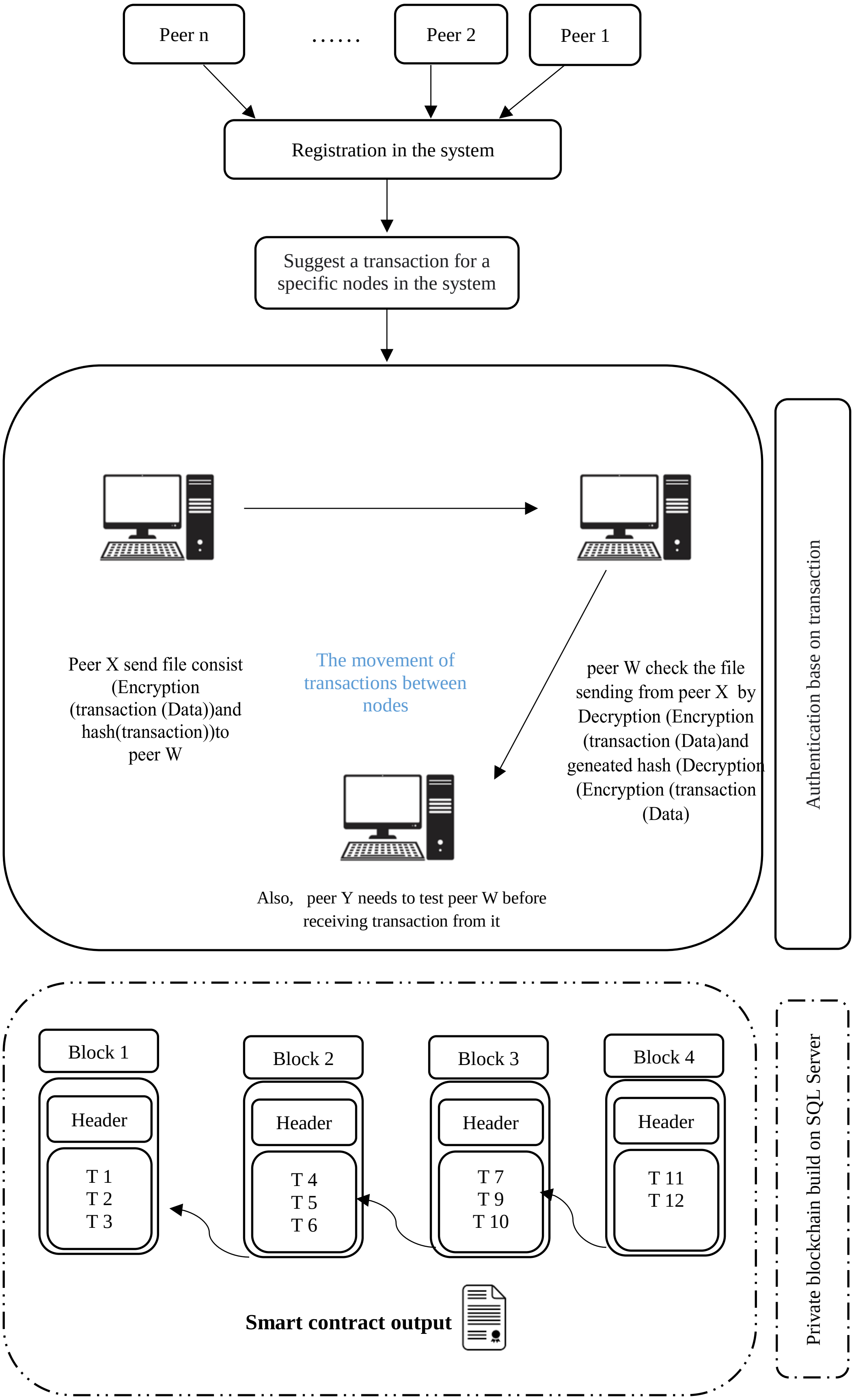
Peer n
......
Peer 2
Peer 1
Registration in the system
Suggest a transaction for a specific nodes in the system
Peer X send file consist (Encryption (transaction (Data))and hash(transaction))to peer W
The movement of transactions between nodes
peer W check the file sending from peer X by Decryption (Encryption (transaction (Data)and geneated hash (Decryption (Encryption (transaction (Data)
Also, peer Y needs to test peer W before receiving transaction from it
Authentication base on transaction
Block 1
Header
T 1
T 2
T 3
Block 2
Header
T 4
T 5
T 6
Block 3
Header
T 7
T 9
T 10
Block 4
Header
T 11
T 12
Smart contract output
Private blockchain build on SQL Server

FIG. 3. PROPOSE DISTRIBUTED NETWORK BLOCKCHAIN.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

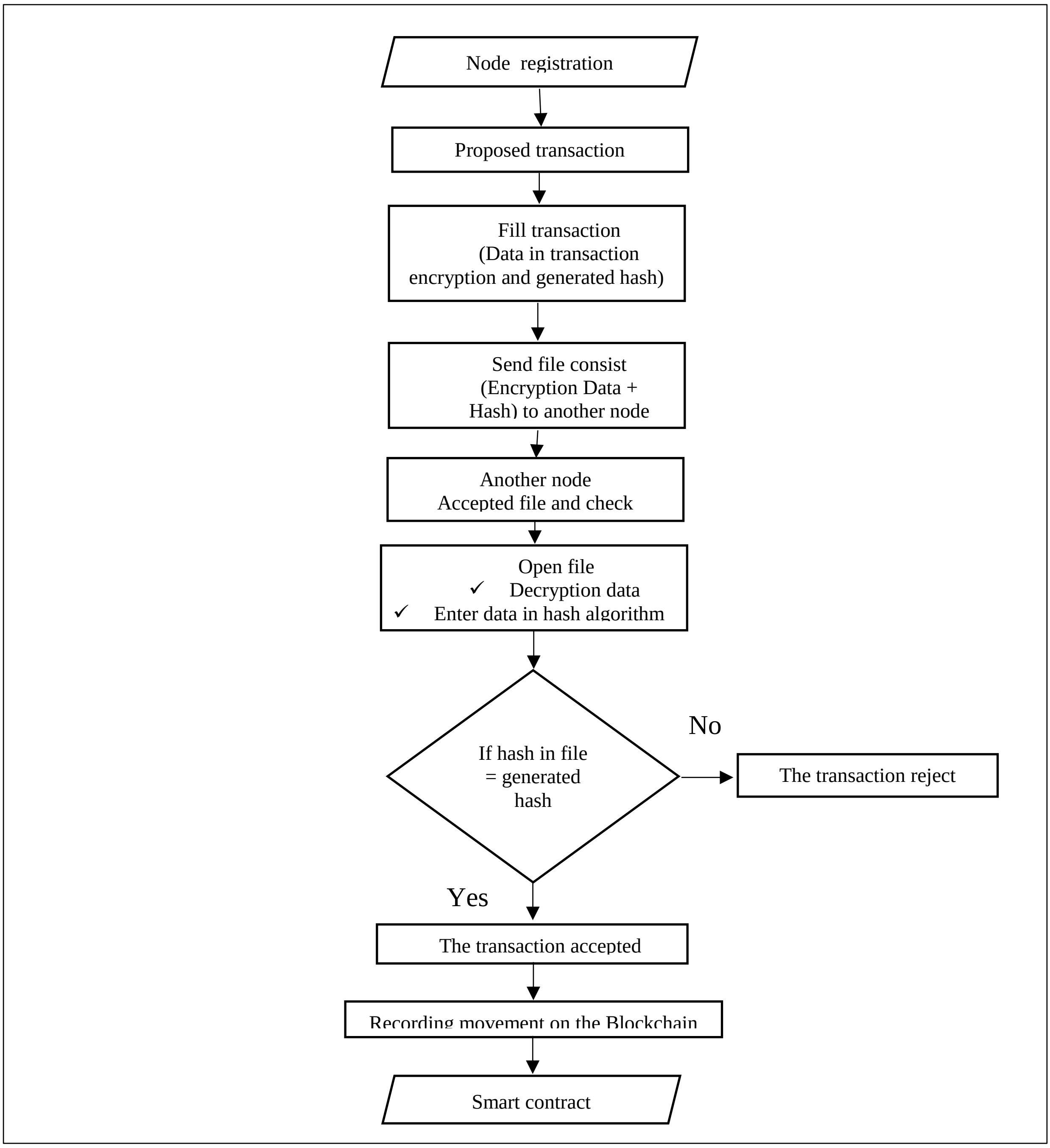

FIG. 4. BLOCK DIAGRAM AUTHENTICATION PROCESS BETWEEN NODES IN DISTRIBUTED SYSTEMS.

```
Algorithm blockchain based authentication System
Input:  Data(propose transaction);
Output: Smart Contract;
Begin
1: Authentication baseon peers regestration in the system (Username ,
     Password);
2: Proposed Transaction by specific peers: proposed
     transaction(Data)→  Encryption (transaction (Data))and hash(transaction);
3: Authentication base on transaction proposed
     a.peer x send file consist (Encryption (transaction (Data))and
       hash(transaction))to peer w;
```

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

```
    b. peer w check the file sending from peer x by Decryption (Encryption
      (transaction (Data)and geneated hash (Decryption (Encryption (transaction
    (Data)
if the generated hash by peer w = hash found in file send by peer x→
    Accepted transaction;
Else
   Reject transaction;
The same operations are repeated In order for all peers to participate in the
same transaction; // all peers;
4: record any movement in blockchain all distributed ledger in peers; // from
     The cloud;
Return Smart contract(Transaction);
```

IV. RESULTS

The system proposed by C# has been implemented to make peer-to-peer communication among three sockets on the laptop computer.containing: -

The processor consumed in this sheet is the Intel Pentium i76500U processor that runs at 2.50GHz 2.70GHz • 8 GB RAM. 64-bit, it was the OS (Window 10). The Blockchain is implemented using SQL Server Management Studio 2019.

The proposed system was applied in one of the municipal directorates of the countries of Iraq. Where was the work of a private blockchain network consisting of a group of nodes. Each node is a represent client/server.

Proposed system was analyzed in terms of strengths, which are represented by several steps that included:-

A- ***Time required to propose a transaction:*** Transaction suggestion will be in real time as shown in Table I.

TABLE I. THE TIME TAKEN TO OPEN A TRANSACTION

Node	Time Execution
Node1	0.00

B- ***Dependence of performance on the number of transactions per second:-***The performance of the blockchain network depends on the number of transactions processed per second. Transactions are verified in a second or less and it depends on the number of validators in the network. The more auditors there are, the more there will be delays in the network, while the more appropriate the number, the better the verification of transactions.

C- ***- Transaction Throughput*****:** Total read operations divided by total duration in seconds is transaction throughput.

The read transfer rate is a measurement of how many read operations can be done in a given amount of time. It's measured in readings per second (RPS).

Total committed transactions divided by total time in second's equal's transaction throughput.

The transaction transfer rate is the rate at which valid transactions are processed by the blockchain in a given amount of time, and it does not indicate transaction transfer in a single node, but rather across all nodes. The time necessary to implement a number of transactions is shown in Table II.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

TABLE II. THE TIME IT REQIRED TO IMPLEMENT A NUMBER TRANSACTIONS

Number of Transactions	Time Execution
100	9 Min -540 Sec
500	47 Min – 2,820 Sec
1500	141 Min-8,460 Sec
2500	235 Min -14,100 Sec

***D- Attack*:-** Some potential attacks on the proposed system, including:-

- **Attack 51%:-** Through the proposed system, we made the implementation of the transaction and a decision on it by all people, and a smart contract is not implemented for an incomplete transaction that did not pass through all the contracts in order for a decision to be taken. This will not allow the contract to monopolize the transactions, but all the contracts will be equal in terms of tasks.
- **Double spend: -** Any proposed transaction will be examined if its proposal was previously submitted or not. And even in the case of proposing two transactions for the same person, the result will be the same because the benefit is not written by the node, but will be fetched directly from the data base by the system, and do not enter the node with that, so in all cases the answer will be the same.
- **Sybil’s Attack:-**It means flooding the network with nodes after entering with an assumed identity. The proposed system does not allow the contract to enter until after proving their identity. The nodes has no right to propose another node, so this attack is impossible to happen because it provides real authentication during the exchange of transactions and correspondence.

E- (Authentication):-The use of a credential between all the nodes and this authentication followed the conditions

➢ All nodes must be registered in the blockchain system

➢ All nodes must possess the agreed-upon digital code to be entered in the authentication stage followed in the system.

F- (Complexity):- The complexity is in two stages

The first stage includes data encryption (which is the citizen's form data and employee information) and the second stage includes the generation of a special hash for each form

➢ The data must be encrypted, as the nodes needs to know the key used to include it within the agreed encryption algorithm (the cryptographic algorithm was used AES).

➢ The file containing data and an encrypted hash is received

➢ After entering the code agreed upon between all the nodes.

➢ In case of entering the wrong code, the received encrypted file will be rejected.

If the correct code is entered, the encryption of the data inside the file will be opened, and this data that has been opened will be entered using the hash algorithm

If the hash extracted from the hash algorithm matches the hash sent in the file, then the node is registered correctly in the system.

If the hash generated does not match the hash in the file, the file will be rejected.

G- Tracking the events and work of the nod:-

➢ Any process of sending and receiving the transaction will be recorded within the shared server between the nodes.

➢ The chain of events and correspondence that took place between the nodes for each proposed transaction will be recorded in the blockchain.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

- Even if one of the blockchain records of the node is changed, it cannot change all records for all node, because each node has its own distributed ledger.

V. CONCLUSIONS

There are many serious security incidents due to falsification of transactions and denial of internal correspondence between the participating nodes within the same system for a decision on them. This proposal provides a secure decentralized ledger by tracking all the movements of sending and receiving the proposed transactions. Every time a transaction is sent and received between the nodes, it will be authenticated through several procedures to be followed, represented by encrypting the transaction data with the generation of a special hash for this data. This is done the provision of real authentication between the nodes participating in the system, through which the identity of the contract is revealed every time the system is entered and also every time the contract is concluded by proposing transactions. The proposed system has proven the extent of its sobriety and its strength against external attacks and intruders. In addition, the time spent during authentication and during the process of proposing a transaction within the blockchain does not take any time, but rather within real time.

REFERENCES

[1] W. J. Lutter "Bitcoin and the future of digital payments". The Independent Review, 20(3), 397-404. (2016).

[2] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey", IEEE Access, DOI: 10.1109/ACCESS.2019.2903554, vol. 7, pp. 36 500–36 515, 2019.

[3] M Sharples and J Domingue. "The blockchain and kudos: A distributed system for educational record, reputation and reward". In Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), DOI: https://doi.org/10.1007/978-3-319-45153-4_48, pages 490–496, Lyon, France, 2015.

[4] V. Morabito." Business Innovation through Blockchain: The B³ Perspective ", (pp. 41-59). Springer, Cham. (2017).

[5] Satoshi Nakamoto.2009."Bitcoin: A Peer-to-Peer Electronic Cash System", WWW.bitcoin.org

[6] M.Atzori, "Blockchain Technology and Decentralized Governance: is the State Still Necessary?" DOI: 10.22495/jgr_v6_i1_p, ISSN Online: 2306-6784 ISSN Print: 2220-9352, Journal of Governance and Regulation / Volume 6, Issue 1, 2017

[7] M Khayyat, F. Alhemdi2 and R.Alnunu3 "The Challenges and Benefits of Blockchain in E-government" IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020 on 29 May 2020.

[8] S. Ølnes, A. Jansen,"Blockchain Technology as s Support Infrastructure in e-Government ", https://hal.inria.fr/hal-01702985, 16th International Conference on Electronic Government (EGOV), Sep 2017, St. Petersburg, Russia. pp.215-227, ff10.1007/978-3-319-64677-0_18ff. ffhal-01702985f.

[9] S.Terzi, K. Votis, D. Tzovaras,"Blockchain 3.0 Smart Contracts in E-Government 3.0 Applications", October 2019, Project: Blockchain for Software Quality.

[10] R. Zhang, R. Xue, and L. Liu,"Security and Privacy on Blockchain", LING LIU, School of Computer Science, ACM Computing Surveys, Vol. 1, No. 1, Article 1. Publication date: January 2019. https://doi.org/10.1145/3316481.

[11] L. Adewale Ajao, J.Agajo, E. Adewale Adedokun and L. Karngong,"Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry", Published: 2019, 2, 300–325; doi:10.3390/j2030021.

[12] T.Oliveira, M.l Oliver and H. Ramalhinho, "Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain", Published: 7 April 2020, Sustainability 2020, 12, 2926; doi: 10.3390/su12072926.

[13] Casallas, Lovelle and Molano," Smart Contracts with Blockchain in the Public Sector", | Published 31 July 2020,DOI: 10.9781/ijimai.2020.07.005.

[14] G.Sladi´c, B. Milosavljevi´c, S. Nikoli´c, D. Sladi´c and A. Radulovi´c, "A Blockchain Solution for Securing Real Property Transactions: A Case Study for Serbia", Published: 15 January 2021, https://doi.org/ 10.3390/ijgi10010035.

[15] T.Guarda, M. Augusto, L. Haz1 and J.Nafría,"Blockchain and Government Transformation", 130, pp 88-95, 2021, DOI: 10.1007/978-3-030-68285-9_9.

Received 06/December/2021; Accepted 10/April/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.10

[16] D. Allessie, M.Sobolewski and L. Vaccari." Blockchain for digital government", ISSN 1831-9424, DOI: 10.13140/RG.2.2.34874.85449, European Commission, Joint Research Centre, Digital Economy Unit (JRC/B6), MAY 2019.

[17] Z.Kamal and R.Ghani," E-government based on the blockchain technology, and the evaluation of its transaction through the number of transactions completed per second", ISSN 2303-4521, http://dx.doi.org/10.21533/pen.v10i1.2726, Periodicals of Engineering and Natural Sciences, Vol. 10, No. 1, February 2022, pp.620-631.

[18] C. Brunner, F. Knirsch and D. Engel." SPROOF: "A platform for issuing and verifying documents in a public blockchain,
DOI:10.5220/0007245600150025,Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Puch bei Hallein, Austria, ", JAN 2019.

[19] Z.Kamal and R.F.Ghani," Data retrieval based on the smart contract within the blockchain", ISSN 2303-4521 ,DOI: http://dx.doi.org/10.21533/pen.v9i4.2353, Periodicals of Engineering and Natural Sciences, Vol. 9, No. 4, October 2021, pp.491-507.

[20] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends", DOI: 10.1109/BigDataCongress.2017.85 in 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, pp. 557–564, JUN 2017.

[22] Z.Kamal and R.F.Ghani," A proposed hash algorithm to use for blockchain base transaction flow system", ISSN 2303-4521, DOI: http://dx.doi.org/10.21533/pen.v9i4.2401, Periodicals of Engineering and Natural Sciences, Vol. 9, No. 4, October 2021, pp.657-673

[23] G. O. Karame and E. Androulaki, "Bitcoin and blockchain security". Artech House, 2016.

[24] H.Samir, M.Alrawi" Message Authentication Using New Hash Function", DOI: 10.22401/JNUS.19.3.20, Sep 2016

[25] T.Abbas and A.Abdulmajeed," Identifying Digital Forensic Frameworks Based on Processes Models", DOI: 10.24996/ ijs.2021. SI.1.35, Iraqi Journal of Science, 2021, Special Issue, pp: 249-258.

[26] S. Makridakis and K. Christodoulou "Blockchain: Current Challenges and Future Prospects/Applications"; doi: 10.3390/fi11120258on 12 December 2019.

[27] H. Yu, Z. Yang, and R. O. Sinnott, "Decentralized big data auditing for smart city environments leveraging blockchain technology, DOI: 10.1109/ACCESS.2018.2888940" IEEE Access, vol. 7, pp. 6288–6296, 20 December 2018.

[28] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), https://doi.org/10.1145/357172.357176, vol. 4, no. 3, pp. 382–401, 1982

[29] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends", DOI: 10.1109/BigDataCongress.2017.85 in 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, pp. 557–564, JUN 2017.

[30] F. Saleh, "Blockchain without waste: Proof-of-stake,"27 JUN 2018.

[31] S. Almajali "Blockchain Technology Consensus Algorithms and Applications: A Survey", Princess Sumaya University for Technology, Amman, Jordan, DOI: 10.3991/ijim.v14i15.15893, on 13 September 2020.

Received 06/December/2021; Accepted 10/April/2022