PROSPECTS FOR THE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY IN CORPORATE INFORMATION SYSTEMS

Yurii Tulashvili, Iurii Lukianchuk and Viktor Kosheliuk

Department of Computer Sciences, Lutsk National Technical University, Lutsk, Ukraine

ABSTRACT

Over the past decade, blockchain technology has undergone rapid development and is recognized as one of the pivotal information technologies driving industrial transformation. Today, blockchain technology offers a promising solution to the problems faced by corporate information systems. Namely, with the help of appropriate measures of anonymization and preservation of confidentiality, the blockchain enhances data security, reduces the risk of unauthorized access, and ensures user privacy in corporate systems. Blockchain technology increases transparency, allowing users to monitor and verify the content of information, assess the integrity of data stores. In recent years, blockchain has become a subject of interest for state governments, multinational corporations, and major financial institutions. Today, considerable attention is paid to the development of private (corporate) blockchains. This article examines the prospects and development of blockchain technology in corporate information systems. The study is aimed at providing additional clarity regarding the concept of blockchain applications in corporate information systems. Existing enterprise applications cannot operate seamlessly with traditional transactional requirements when integrating blockchain technology. Therefore, they will have to be modified with inclusion in the existing data storage for asynchronous interaction with distributed nodes of the blockchain. A scheme of the principle of interaction of nodes - storages that support data synchronization and their current states are proposed. This scheme is based on a blockchain structure centered around cloud storage as a corporate document circulation system. Consensus to include a new entry - Byzantine fault tolerance. Blockchain nodes receive a parametric weight for decision making.

KEYWORDS

Blockchain, Consensus, Corporate Systems, Security

1. INTRODUCTION

In the modern world of digitization, the technology of the digital "ledger," known as Distributed Ledger Technology (DLT), is finding increasing application. In the work "Distributed Ledger Technology Systems: A Conceptual Framework," Michel Rauchs and his co-authors [1] describe DLT as multi-party systems that operate in an informational environment without a central operator or the delegation of managerial authority to anyone. Such decentralized systems provide access to the distributed ledger to all participants, regardless of whether they may be unreliable or malicious. Thus, the information is accessible to all who wish to view it, but it can only be added according to certain rules. Therefore, in their view, blockchain technology is a subset of the broader DLT universe. Blockchain is a continuous sequential chain of blocks containing

 DOI:10.5121/ijci.2025.140305

information, constructed according to specific rules. Blockchain technology uses a distributed data structure containing chains of hash-linked data blocks.

Lin William Cong and Zhiguo He, in their work "Blockchain Disruption and Smart Contracts," define blockchain as a decentralized form of distributed ledger technology [2]. According to them, blockchain is a decentralized ledger exchanged through secure channels. Blockchain is a decentralized digital ledger maintained by all computers within the information system. It provides many functions, such as distributed data storage, anonymity, data obfuscation (protection from viewing and tampering), shared ledgers, and autonomously maintains an ever-growing list of public records in information blocks.

In a special issue of Oracle [3], blockchain technology is considered a revolutionary way to manage decentralized data. Essentially, it is a data ledger that is copied to multiple locations, called nodes, which operate without mandatory trust in one another. The technology is based on ensuring that data remains consistent across all nodes, creating trust between business parties even when they do not know each other. The idea behind blockchain is to ensure data integrity without relying on a central authority. This approach can be called decentralized trust through data reliability [4].

Over the past decade, blockchain technology has undergone rapid development and is considered one of the key fundamental information technologies driving information transformation in the manufacturing sector. Today, blockchain technology is seen as a promising solution for many problems faced by corporate information systems. Specifically, by decentralizing the network, ensuring cryptographic data security, and implementing operational rules defined in smart contracts, blockchain enhances information security, reduces the risk of unauthorized access, and ensures the confidentiality of corporate system users. Blockchain technology ensures transparency in corporate information systems, allowing users to track and verify information content and assess the integrity of data storage. This is achieved through regular blockchain monitoring, which enables the retrieval of corporate information and verification of its accuracy and presence in data storage. This approach provides high protection against fraud. Since blockchain is a decentralized network with no centralized administration, for successful task resolution in corporate information systems, all nodes or the majority of them must participate and agree on decisions.

Existing corporate information systems cannot continue to operate according to traditional transaction requirements. They must be modified to meet modern requirements by integrating blockchain technology. Corporate information systems will include blockchains containing comprehensive data on existing data storages, ensuring asynchronous interaction of all system participants in the form of distributed blockchain nodes. The introduction of corporate information systems for document management is particularly relevant.

The goals of this work are to analyze the state of development of corporate systems based on blockchain technology and to propose an architecture for a universal decentralized corporate information system that would be sufficient for accounting and monitoring document circulation.

2. ORIGINS OF BLOCKCHAIN TECHNOLOGY

The name "blockchain" derives from the fact that all data is stored in blocks, and each block is linked to the previous one, forming a chain-like structure. A node can create and add new blocks to the blockchain only by adhering to specific consensus rules agreed upon with other nodes [3].

2.1. The Essence of Blockchain Technology

Blockchain technology has undergone several stages of development, each characterized by specific technological and conceptual changes:

- The Emergence of Blockchain Technology (2008-2009). This period is characterized by the creation of Bitcoin, the first cryptocurrency. The catalyst was the publication of the article "Bitcoin: A Peer-to-Peer Electronic Cash System" under the pseudonym Satoshi Nakamoto in 2008. Satoshi Nakamoto is the pseudonym of an individual or group of people who developed the Bitcoin cryptocurrency protocol and created the first version of the software. The article outlined the principles of the fully decentralized Bitcoin electronic cash system. In early 2009, the first version of the decentralized Bitcoin payment network was launched.
- Software Expansion (2010-2013). The emergence of Bitcoin led to the creation of other cryptocurrencies and the first attempts to build systems for various purposes based on blockchain. This period is characterized by experiments with different concepts and technologies.
- Expansion of Technology Functionality (2014-2016). During this period, blockchain platforms began to emerge, allowing the creation of smart contracts and decentralized applications (DApps). For example, Ethereum is a prominent example of such blockchain platforms.
- Institutional Adoption (2017 - Present). In recent years, blockchain has become a subject of interest for governments, corporations, and financial institutions. Today, significant attention is being paid to the development of private (corporate) blockchains. Parallel to this, research is being conducted on the application of blockchain technology in various sectors such as finance, healthcare, logistics, and more. One of the main challenges facing blockchain technology is scalability and the ability to interact between different blockchain networks. Therefore, research on scalability and interoperability is gaining particular importance. At this stage of technology development, solutions to these problems are actively being sought through inter-chain interaction protocols, among others.

2.2. Corporate Information Systems Using Blockchain Technology

On the IBM blog, the essence of corporate blockchain is discussed in a discursive form [5]. A corporate blockchain refers to a database system or a decentralized ledger. Corporate blockchains represent innovative systems of protocols that are decentralized and use cryptographic methods to ensure data confidentiality and security.

A number of authors study the operation of corporate information systems using blockchain technology across various business sectors. For instance, Don Tapscott and Alex Tapscott, the authors of the book "Blockchain Revolution," highlight the potential of blockchain technology to transform the financial system and various aspects of business, including corporate system models [6]. In their book "Blockchain and the Law: The Rule of Code," Primavera De Filippi and Aaron Wright explore the legal aspects of using blockchain technologies in corporate structures [7]. William Mougayar, the author of the book "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology," investigates various aspects of implementing blockchain technologies in business, including opportunities for corporate information systems [8]. Skiner K., in his book "ValueWeb: How FinTech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value," examines the impact of blockchain

technology on the financial system and the opportunities for developing corporate financial structures [9].

According to the authors [10], blockchains have the potential to transform the future institution into a digitized decentralized network of stakeholders. They argue that blockchains can facilitate the formation of a new organization without top management or organizational hierarchy. Blockchains provide the possibility for new types of organizations to evolve based on a distributed decentralized structure. The importance of smart contracts is emphasized for implementing a system of trust regulation within the corporate system.

In the work [11], it is stated that corporate blockchain is significantly more productive than traditional business systems, starting with processes that involve multiple parties, each of which requires access to the same data but may have slightly different or outdated information that requires constant reconciliation. The various types of corporate blockchains are considered, depending on how open or closed they are, allowing participants to perform the core tasks of the blockchain, which include executing transactions on it and verifying the accuracy of each block added to the blockchain. The main types of blockchains are analyzed [11]:

- Public blockchain, which does not require permission to join and is transparent to all participants. It is also the slowest because opening the blockchain consensus process to such a large number of participants makes data verification more exhaustive but also less vulnerable to hacking or control by a dominant individual. This type of blockchain is where cryptocurrency transactions take place.
- Private (permissioned) blockchain. Operating within a closed network, often under the control of a single organization, this type of blockchain typically has the same decentralization and peer-to-peer architecture as a public blockchain but on a much smaller scale, which enhances performance. Trust in a private blockchain is weaker than in a public blockchain because the owner or central node decides what is valid. Security may also be weaker since a small number of nodes can more easily dominate the consensus mechanism used to verify transactions. Most businesses deploy blockchains on a private basis.
- Hybrid blockchain, which combines aspects of both public and private blockchains. Organizations can use it to segment certain data and transactions within a permissioned scheme while maintaining a connection to the public side. The security risks and data integrity issues of a private blockchain are reduced by not allowing the owner to alter transactions, and the performance is generally better than that of a public blockchain. Users who join a hybrid blockchain maintain privacy until they conduct a transaction. This approach is justified for businesses with a broad client base.

In today's world, the future lies in the total digitization of information. The authors [12] suggest that successful firms integrate new technologies across all aspects of their organization and management to achieve the goal of complete digitization. Companies can leverage new technologies to create a more decentralized, direct, and inclusive corporate culture for all stakeholders, including investors, executives, managers, and employees, as well as early adopters, former employees, other companies, service providers, various levels of government, and society as a whole. Such a culture offers a competitive edge by attracting top talent, raising capital, forging partnerships, and thriving in today's highly competitive global markets.

3. ARCHITECTURE OF CONNECTION OF BLOCKCHAIN NODES TO CORPORATE SYSTEMS

The works [13, 14] discuss typical architectures of corporate information systems based on blockchain technology. The blocks of corporate information systems' blockchains organize data in a chronological order and are secured by cryptography. The blockchain adheres to a distributed ledger data structure, which is duplicated and distributed among the network users.

According to the authors [13], during development, it is crucial first to study the operationalization of the blockchain and establish the most suitable design for the current situation to build a blockchain-based architecture.

A blockchain consists of a sequence of blocks connected in a chain, as shown in Figure 1. Each block contains a set/package of transactions organized in the form of a Merkle tree (Tx_Root), where cryptographic hashes of the transactions are stored as headers for quick and easy verification of individual transactions within the block. Additionally, each block contains a timestamp indicating when the block was formed, the hash of the previous block (Prev_Hash), the block identifier/number, and the proof from the consensus algorithm (Nonce). The blocks are recorded in the distributed ledger based on consensus rules agreed upon by network partners. Furthermore, to understand the blockchain mechanism and the proposed structure, it is important to understand four key components of blockchain technology: the distributed shared ledger, smart contracts, permissions, and consensus.

Corporate blockchains widely employ smart contracts, whose purpose is to establish obligations and trust constraints between nodes. In essence, a smart contract is a blockchain-based program that autonomously executes when predefined conditions are met, eliminating the need for third-party intervention. This structure enables all parties in the transaction chain to fulfill their respective responsibilities, ensuring the legality and traceability of information flows (eg, Figure 1).

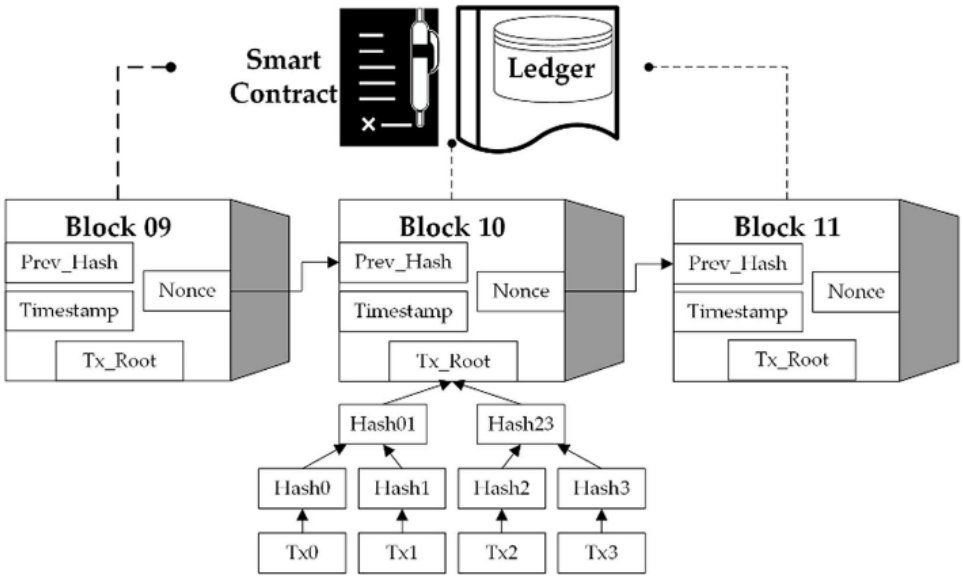

Figure 1. Stages of creating a new block using a smart contract [13]

The work [14] reveals the typical role of nodes in blockchain architecture. The task of nodes is to maintain the reliability of the data stored in the blockchain. The more nodes a blockchain has, the

more decentralized it becomes, making it resilient to threats such as system failures or power outages. When a new piece of data (block) is added to the blockchain, the node will transmit this block to other nodes in the network. Nodes are typically classified into the following categories (eg, Figure 2):

- Full node - Every participant can run their own node with a complete copy of the blockchain.
- Light nodes - Lightweight clients do not store full copies of the blockchain but interact with the network using full nodes. Light nodes typically contain the block header, which allows them to maintain and verify the validity of previous transactions. The information stored in the block header usually includes the block timestamp and a unique identification number (also known as a nonce).
- Mining node - Full nodes that can record transactions to the blockchain (in cryptocurrency systems). In corporate blockchains, witness nodes are full nodes that participate in the consensus.

All nodes are interconnected. With such a set of elements, the blockchain network architecture becomes more resilient. Most users utilize lightweight clients or web wallets for transactions.

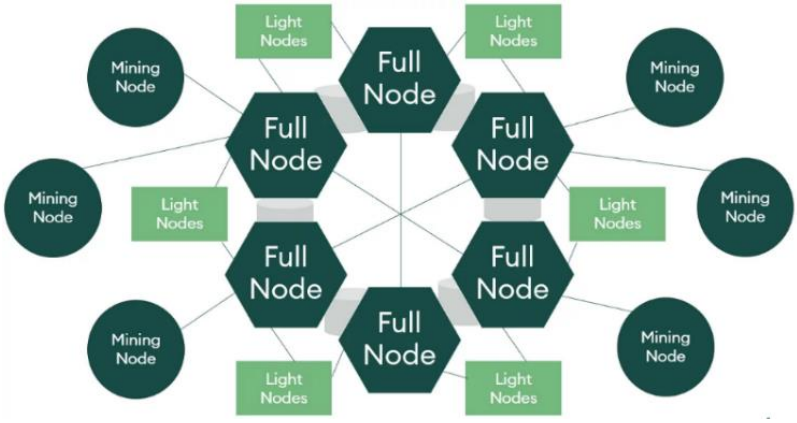

Figure 2. Overall architecture of blockchain nodes [14]

The key difference between mining and running a full node is that a miner must run a full node to determine the criteria (consensus) for valid transactions. The role of miners is to complete tasks such as finding a nonce.

In article [15], an analysis is conducted of the architectures of well-known medical data management information systems based on blockchain technology. The most relevant for corporate information systems is the block diagram (eg, Figure 3) of blockchain generation. DynamiChain [16] implements the processes of forming a new block according to consensus rules. In this process, a participant called Data Provider1 in Org1 attempts to send their data to an institution in Org3 according to the dynamic consent system via Dapp1. First, Data Provider1 requests the creation of a transaction to send data through Dapp1 (step a). Upon receiving the transaction creation request, Dapp1 generates a transaction containing a message to send the data and sends the transaction to the supporting node Peer3. Peer3 can be connected to Dapp1 after passing the certification process using Data Provider1's certificate. After connection, Dapp1 calls the chaincode update function set in Peer3 and requests the execution of the chaincode (step b). Upon receiving the transaction from Dapp1, Peer3 models the chaincode by referencing the World State DB and checks the read/write set results to determine if it is validated (step c). If the

transaction execution result is valid and Peer3's validation is passed, Peer3 sends the results and Peer3's digital certificate to Dapp1 (step d). After receiving the modeling results from Peer3, Dapp1 checks if the read/write set values match the expected values and verifies the received digital certificate from Peer3. After verification, Dapp1 broadcasts the transaction, containing Peer3's digital certificate and the read/write results, to node Orderer1 for block creation (step e). Orderer1 determines the timestamp fields required for ordering transactions and instructs the inclusion of these transactions in a block to create the final blocks (step f). After that, Orderer1 delivers the created blocks to all peer users in the network (step g). Each node receiving the final block performs verification by running the Validation System ChainCode (VSCC) to validate the results and certificates of all transactions within the block. If the verification process is successful, all nodes update the distributed ledger stored in their local storage (step h). Peer nodes complete the distributed ledger update process by sending the results of the updated distributed ledger to Dapp1 (step i).

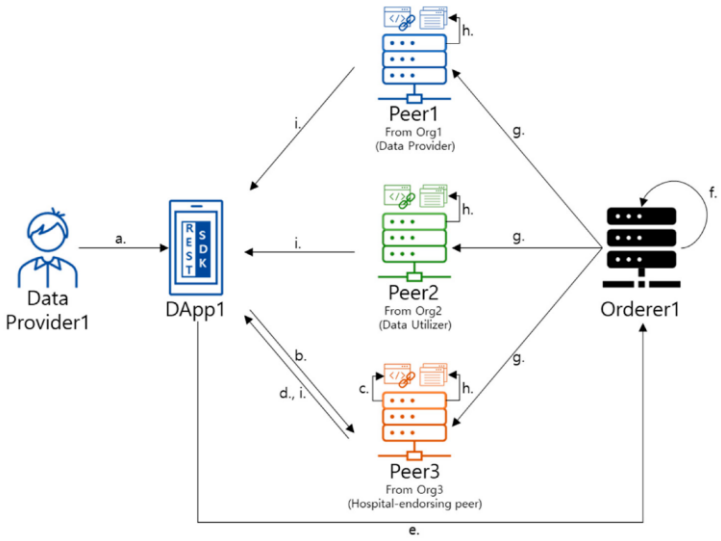

Figure 3. Dynamic consensus algorithm [16]

The examined works reveal the fundamental principles of corporate systems using blockchain technology, namely: decentralization and transparency, cryptographic security, consensus, and the use of smart contracts.

Organizations developing or providing services through corporate information systems based on blockchain technology must strictly adhere to these principles. This will enable them to ensure high operational efficiency of these systems, security and transparency of data and asset exchange, expand their information influence in the market, reach a larger number of consumers, and use any payment systems for processing payments for products and services.

Let’s describe the proposed scheme of the corporate information system and the principles of interaction of its network nodes using blockchain technology (eg, Figure 4), which are designed for interaction with the corporate data storage. This scheme is based on a blockchain structure, focused on interaction with a cloud storage system as a corporate document management system.

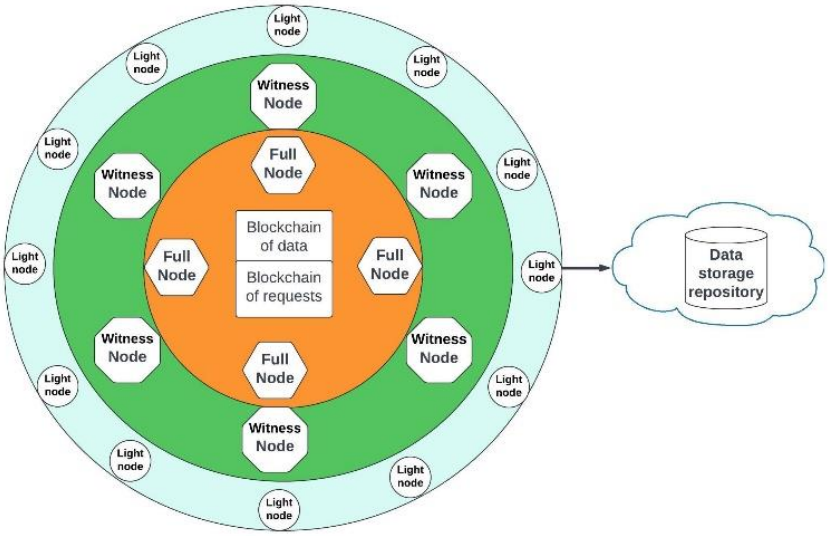

Figure 4. Corporate document management information system scheme

Let us elaborate on the principles of node interaction in the network of the proposed corporate document management information system scheme using blockchain technology.

3.1. Decentralization and Transparency

Decentralization and transparency within the corporate document management information system are achieved by broadly including nodes. Each node in the system is assigned its own priority rank for access to information. A regular node (Light Node) is granted rights to create requests, view information based on access levels, and add documents to the system as needed. Nodes responsible for data validation (Witness Nodes) are typically selected from the middle management of the organization, participate in the consensus process, and can record transactions to the blockchain. Full Nodes with a complete copy of the blockchain have full rights to use the system. The system's transparency is ensured by allowing any internet user to access the institution's publicly available resources using the corporate document management system built on blockchain technology.

3.2. Cryptographic Security

Protection of corporate and personal data in the system should be given special attention. The most attractive method is access control through encryption [17]. The work proposes an approach that involves a blockchain-based access control cipher for protecting personal data. This approach creates a rules table with three elements (Three factors) that are pre-shared between the data provider (in our case, nodes with document upload rights) and the data user (in our case, any node that requests document viewing). The proposed approach includes the creation of a rules table, encryption for data storage, and decryption for authorized data access. Figure 5 provides a complete overview of the proposed approach.

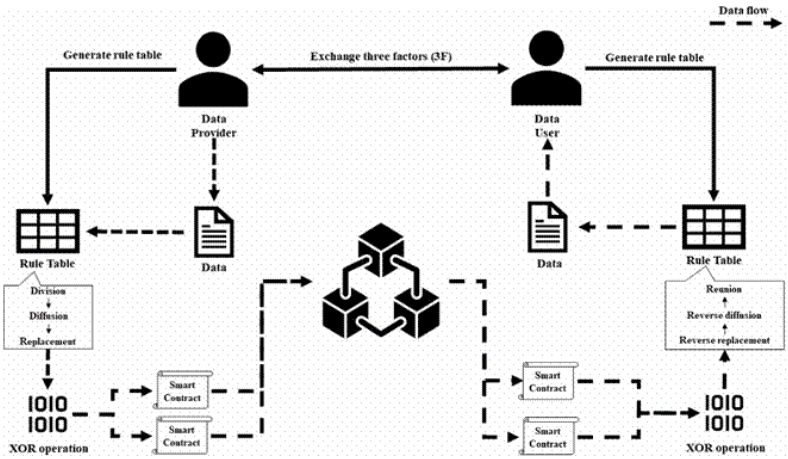

Figure 5. The process of interaction of nodes in the system [17]

This blockchain-based access control approach uses a substitution cipher based on a rules table.

3.3. Consensus

Blockchain technology is characterized by several features that make it unique: decentralization (ensuring no single entity has full control over the blockchain), consensus (requiring agreement among nodes to add a transaction to the blockchain), cryptography (employing cryptographic mechanisms to protect transactions from tampering), and immutability (ensuring that once a transaction is added to the blockchain, it cannot be altered or deleted—only new transactions or information can be appended) [18].

The proposed corporate information system scheme utilizes a technique based on involving data providers, who are users of the network system, in the consensus decision-making process (Witness Node), thus eliminating any administrative intervention.

This scheme is based on a blockchain structure that integrates cloud storage as a corporate document management system. Consensus on the inclusion of a new record is achieved through Byzantine Fault Tolerance (BFT). Blockchain nodes are assigned parametric weights for decision-making.

BFT consensus protocols, as a core component of blockchain, directly influence the practical applicability of blockchain technology. The classical Byzantine consensus under Byzantine fault tolerance mode must satisfy certain properties. Specifically, the Byzantine consensus problem guarantees the combination of three properties [19]:

- Agreement, where no two correct replicas reach different decisions;
- Termination, where all correct replicas eventually have a decision;
- Validity, where the decision is proposed by some replicas.

The BFT algorithm must guarantee the correctness of the following two properties:

- Safety is the property that if any two correct replicas reach a decision, both must reac the same decision [20].

- Liveness is the property that the consensus protocol makes progress in the current view and transitions to a new view, meaning that clients will eventually receive responses to their requests [21].

3.4. Smart Contract

The corporate document management system leverages blockchain technology to automate the consensus process using smart contracts. The node performing the transaction must, according to specific rules defined in the rule table, conduct it for approval among other nodes, after which a new block is created and added to the blockchain. Depending on the type of transaction whether it is a data request or the upload of a document to the cloud storage a block will be formed in the request blockchain or the data blockchain (eg, Figure 6).

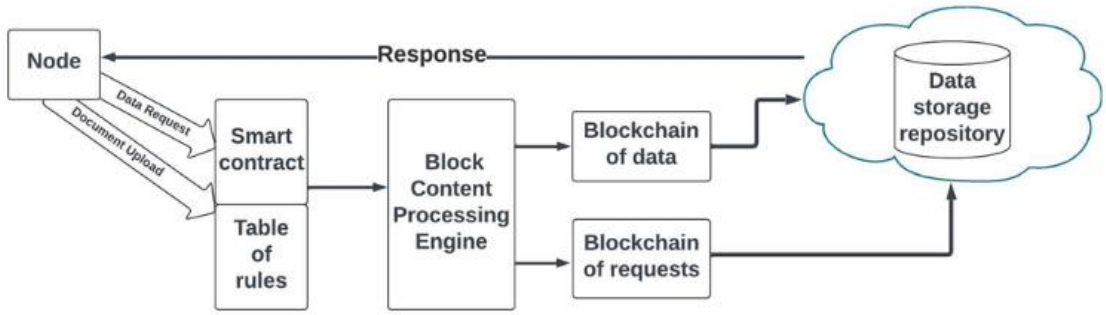

Figure 6. The process of interaction of nodes in the system

Nodes interact with one another and the data storage, ensuring network integrity and enabling making it possible to add data about new documents in real time in the corporate information system through blockchain-based data synchronization.

Using this approach, we practically implement a corporate information system for document management of the department of an educational institution using blockchain technology. In it, we proposed such a smart contract with the following sequence of actions:

- light node (student submitting work to the archive) registers and logs into the system;
- light node chooses the witness node (the teacher checking the work) and collaborates with him until the document is fully ready;
- light node transmits a witness node document. The right to include information about the document in the blockchain and to archive it is exclusively granted to the witness node, which according to Istanbul BFT becomes the leader, namely the initiator node;
- the leader of the witness node forms a block of information, generates an initial cryptographic hash of the current block and sends it to the witness nodes that have copies of the full blockchain and participate in the consensus;
- witness nodes that have copies of the full blockchain check the sent new hash to block of information on the consensus to cryptographic hash from the previous block and generate permission to include the current block;
- 6) each witness node sends its permission to the leader witness node, which records the consensus on including the current block. Having received 2/3 n +1 correct answers, it sends COMMIT to all system nodes to include the current block in the blockchain;
- witness nodes leader uploads the finished document to the repository.

- Implementating of a smart contract to form a requests blockchain is similar to the formation of a data blockchain. The witness-leader node provides access to the document to other nodes.

The interaction of nodes with each other and the data store makes it possible to maintain the integrity of the network and receive information about document updates and their review in the corporate information system by synchronizing the blockchain with the current state.

4. CONCLUSION

The proposed corporate document management system, leveraging blockchain technology, ensures decentralization and data integrity for the storage and retrieval of institutional documents. To automate the consensus process through smart contracts, the system employs a dynamic consensus algorithm based on the BFT consensus protocol. Nodes in the system interact according to the smart contract, the conditions of which are outlined in the rule table.
Future research and implementation of the corporate document management system will focus on comparative studies of dynamic consensus algorithms and BFT protocols to enhance the efficiency and robustness of blockchain protection mechanisms.

REFERENCES

[1] Michel Rauchs, Andrew Glidden, Brian Gordon, et al. Distributed ledger technology systems: a conceptual framework[M]. University of Cambridge. Judge business school, 2018: p. 15-17. https://ssrn.com/abstract=3230013 (accessed November 10, 2024).

[2] Lin William Cong, Zhiguo He. Blockchain disruption and smart contracts. NBER working paper series. http://www.nber.org/papers/w24399 (accessed November 11, 2024).

[3] Michael G. Solomon. Enterprise Blockchain For Dummies. Oracle Special Edition. John Wiley & Sons, Inc., Hoboken, New Jersey, 2019. https://www.oracle.com/a/ocom/docs/cloud/enterprise-blockchain-report.pdf (accessed November 23, 2024).

[4] Nguyen Truong, Gyu Myoung Lee, Kai Sun, Florian Guitton, YiKe Guo. A blockchain-based trust system for decentralised applications: When trustless needs trust. 2021. https://doi.org/10.1016/j.future.2021.05.025

[5] Ariel Zetlin-Jones, Bryan Routledge. What is a corporate blockchain? 2019. https://www.ibm.com/blog/what-is-a-corporate-blockchain

[6] Don Tapscott, Alex Tapscott. Blockchain Revolution. How the technology behind Bitcoin is changing money, business, and the world. Penguin Random House LLC, New York, 2016. P. 324. https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf

[7] De, Filippi, Primavera. Blockchain and the Law: The Rule of Code. Harvard University Press, 2018. https://ebin.pub/blockchain-and-the-law-the-rule-of-code-0674976428-9780674976429.html (accessed December 1, 2024).

[8] Vitalik Buterin, William Mougayar. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. 2016. https://publicism.info/business/ blockchain/4.html

[9] Skiner K. ValueWeb: How Fintech Firms are Using Bitcoin Blockchain and Mobile Technologies to Create the Internet of Value / K. Skiner. – Singapore: Marshall Cavendish International, 2016. – 424 p.

[10] Dulani Jayasuriya Daluwathumullagamage, Alexandra Sims. Blockchain-Enabled Corporate Governance and Regulation. 2020. https://www.mdpi.com/2227-7072/8/2/36/pdf?version=1593311974

[11] David Essex. Blockchain for businesses: The ultimate enterprise guide. 2023 https://www.techtarget.com/searchcio/Blockchain-for-businesses-The-ultimate-enterprise-guide (accessed December 3, 2024).

[12] Mark Fenwick, Wulf A. Kaal, Erik P.M. Vermeulen. Why 'Blockchain' Will Disrupt Corporate Organizations. 2018. https://www.ecgi.global /sites/default/files/working_papers/documents/finalfenwickkaalvermeulen.pdf

[13] Tarun Kumar Agrawal, Vijay Kumar, Rudrajeet Pal, Lichuan Wang,Yan Chen. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. 2021. https://www.sciencedirect. com/science/article/pii/S0360835221000346 (accessed December 5, 2024).

[14] Yves Longchamp, Sau rabh Deshpande, Ujjwal Mehra. Classification and importance of nodes in a blockchain network. 2020. https://aminagroup. com/research/classification-and-importance-of-nodes-in-a-blockchain-network/

[15] Vitalii Osyadlyi, Artem Moskalenko. System of medical data management based on blockchain technologies. International Scientific-technical journal «Measuring and computing devices in technological processes» 2022, Issue 2. pp.29-38. https://vottp.khmnu.edu.ua/index.php/vottp /article/download /45/45

[16] T. Kim, S. Lee, D. Chang, J. Koo, T. Kim, K. Yoon, I. Choi. DynamiChain: Development of Medical Blockchain Ecosystem Based on Dynamic Consent System. Appl. Sci. 2021, 11(4), 1612; https://doi.org/10.3390/app11041612

[17] Jungwon Seo, Sooyong Park. SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse. Future Generation Computer Systems 151 (2024) 85–97. https://www.sciencedirect.com/science/article/pii/S0167739X23003552?via%3Dihub (accessed December 15, 2024).

[18] Dasha Antsipava, Joanna Strycharz, Eva A. van Reijmersdal, Guda van Noort. What drives blockchain technology adoption in the online advertising ecosystem? An interview study into stakeholders' perspectives. Journal of Business Research 171 (2024) 114381. https://doi.org/10.17605/OSF.IO/DFK7G

[19] Gang Wang. oK: Understanding BFT Consensus in the Age of Blockchains. Cryptology ePrint Acrchive. 2021-07-05. https://ia.cr/2021/911

[20] L. Lamport, "The part-time parliament," in Concurrency: the Works of Leslie Lamport, 2019, pp. 277–317.

[21] Y. Lu, Z. Lu, and Q. Tang, "Bolt-dumbo transformer: Asynchronous consensus as fast as pipelined BFT," arXiv preprint, 2021. https://doi.org/10.48550/arXiv.2103.09425

AUTHORS

Prof. D.Sc. Yurii Tulashvili, Department of Computer Science, Lutsk National Technical University, Lutsk, Ukraine. Field of scientific interests: mathematical modeling of complex systems, software development and analysis algorithms, study of the effectiveness of the use of computer information technologies in education, science and production**.**

Iurii Lukianchuk in 2012 received the scientific degree PhD of technical sciences from the Lutsk National Technical University. From 2012 to 2016, he worked at the Lutsk National Technical University at the Department of Instrumentation, from 2020 to the present, as an associate professor of the Department of Computer Sciences. Scientific interests are aimed at the development of software for modeling technological processes, research of innovative technologies in education and production, design, development and maintenance of software.

PhD. Viktor Kosheliuk Candidate of Technical Sciences, associate professor, Faculty of Computer and Information Technologies, Department of Computer Science, Lutsk National Technical University, Lutsk, Ukraine. Field of scientific interests: information systems design, analytics of information security, cloud technologies, cyber security of information technologies, incident handling and response.