Developing of Blockchain Method in Message Interchange Systems

Vasyl Poberezhnyk[1] and Ivan Opirskyy[1]

[1]*Lviv Polytechnic National University, 12 Stepana Bandery str., Lviv, 79000, Ukraine*

Abstract

This paper examines the main blockchain and decentralized application features, their advantages and disadvantages for use in message interchange systems, and proposes a conceptual method of development of such systems. Performs analysis of such method and discusses its drawbacks while proposing methods of leveling of these drawbacks by using different types of nodes in the system or hybrid of Tor and XRP Ledger for solving issues and performs an examination of proposed methods.

Keywords

Blockchain, instant messaging, XRPL, Tor, privacy, DApp, decentralization, distributed network, hybrid network infrastructure.

1. Introduction

Cyberspace has a huge impact on life today, its capabilities are used for interaction between people or organizations, for education, recreation, or business, and in 2019, at the start of the COVID-19 pandemic, the use of cyberspace has allowed many businesses to continue operating due to massive introduction of remote access to workplaces [1]. However, cyberspace poses security challenges. For example, the integration of IoT [2] into life poses challenges because this technology is used both in personal life and in the activities of enterprises, which can be of interest to an attacker. Also, the use of e-mail or social networks carries risks for the user, such as sending spam or phishing messages [3] or distribution of ransomware [4], which businesses often fall victim to [5]. Threats can also be contained in transmission lines, as attackers can eavesdrop on the communication between two subscribers through the capture and processing of packets in the network, which can lead to loss of connection, data theft, or impersonation of the attacker as a legitimate participant in the exchange of information [6]. The use of instant messaging services has become especially popular nowadays, and various messengers have become an integral part of people's lives, for example, Messenger has 1.3 billion downloads, and WhatsApp has 2 billion [7]. However, despite the popularity of these services, they also pose various threats to users, and above all, this is a threat to user privacy. These services may collect personal information about users, for example, WhatsApp messenger [8] may collect the following types of data: phone number, email address, purchase information, geolocation, contact list, financial data, contact data, media content, identifiers, diagnostic data and usage data, and Messenger [9] in addition to the above: health data, search history, browsing history, sensitive data, and more. The storage of such data creates the threat of data leakage with personal information, which happened in 2019, when a vulnerability in Facebook (now Meta), which owns Messenger, stole the personal data of 533 million users [10]. Another example of a possible data leak is the discovered vulnerabilities in WhatsApp in 2022 [11], which allowed an attacker to gain access to remote code execution, which could provide an opportunity to steal user personal data. What's more, users may not even be aware that an app is collecting metadata about them or interested in what data is being collected about them, and the connection between social networks and messaging apps can increase the amount of information being collected about them. users [12].

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: vasyl.poberezhnyk@gmail.com (V. Poberezhnyk); iopirsky@gmail.com (I. Opirskyy)
ORCID: 0000-0002-7523-2557 (V. Poberezhnyk); 0000-0002-8461-8996 (I. Opirskyy)


Also, in a study [13] using the Lumen Privacy Monitor in applications such as Viber, Slack, and Ayoba, trackers and leaks of personal data were detected and the need for an approach to application development that would include privacy by default was emphasized.

In addition to disruptions and leaks of personal data, such services, in particular Zoom, have been used as part of an attack vector to distribute malware or exploit application vulnerabilities to gain unauthorized access to personal information and conference recordings [14].

Taking this into account, the development of cyber technologies, on the one hand, entails an improvement in computing capabilities, an increase in the number of opportunities for interaction between people and enterprises, and an increase in the number of services, and, in parallel, this development leads to an increase in the number of threats to participants in cyberspace. Therefore, the problem of cyber security occupies a significant place in the modern world [15].

In the field of cyber protection, several methods, methods, and means of protection are used to eliminate threats. An example of this can be the use of means based on neural networks [16] or the use of software decoys [17] to counter the attacker or study his actions.

Also, one of the ways can be the use of blockchain technology, which ensures the privacy of users [18]. Given the privacy threats mentioned earlier, this technology was chosen to analyze its potential for use in building messaging services.

This paper examines the main properties of blockchain technology and decentralized applications working in conjunction with blockchain. An analysis of the advantages and disadvantages of the technology for the implementation of the messaging service was carried out. The concept of the service construction method was developed, and the analysis of shortcomings was carried out. Methods of leveling these restrictions were also proposed and their comparison was carried out.

2. Basics of Blockchain Technology

A blockchain is a list of records, also known as cryptographically linked blocks, each of which contains a hash of the previous block, a timestamp, and transaction data (Fig. 1).

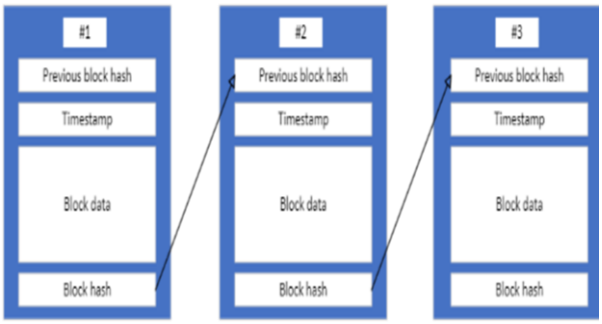

Figure 1: Representation of blocks and their linkage in blockchain by hash

A block's hash is calculated from the data content, and the timestamp identifies that the data in the block was real at the time the block was created. The presence in the block of the hash of the previous block allows linking the block in one chain with previous blocks, which allows tracking any changes made to one of the blocks in any version of the blockchain since the chain with changes will be different from the version that every node in the network has. Therefore, the availability of each node's copy of the blockchain makes it possible to identify unauthorized changes in a certain chain and discard them. This possibility is available since the blockchain is a distributed network, by its very nature, which provides several advantages, such as:

- In a distributed network, it is easy to keep track of changes that are happening because they propagate relatively quickly among distributed network participants.
- Each node in the blockchain network must maintain a registry and participate in the verification of transactions.
- Absence of intermediaries in the blockchain.
- The addition of a new block occurs after it is checked by other network nodes.
- The addition of a new block occurs after approval by the majority of network nodes.
- In a blockchain network, all nodes are equal and will not receive any special treatment or favors from the network, that is, so each node must follow a standard procedure to add a new block to the network [19–22].

Considering the peculiarities of blockchain technology, it can be considered as a kind of database, which, of course, will have certain differences from the classic databases. In classic databases, such as SQL databases or NoSQL databases, there are users with administrator rights who, on the one hand, perform database administration functions, and on the other hand,

can make changes to the database without the knowledge of other users. However, due to its decentralized nature, blockchain does not have such users. What's more, decentralization means that not only there are no users with administrative rights, but there is also no control center in the blockchain. In addition, decentralization provides the following advantages:

- A blockchain network is less prone to failure due to the decentralized nature of the network.
- An attack on the system is more expensive for hackers, due to the need to obtain large computing capabilities, so the probability of an attack is lower.
- The absence of intermediaries in the network reduces additional risks associated with the involvement of a third party. Changes in the blockchain are easier to trace and more obvious.
- Network users are in control of their assets, so there is no need for third-party developers to maintain and manage assets.

Another key factor in the ability to use a blockchain as a database is that it stores all the changes that have occurred in it since the beginning, meaning that any block in the blockchain can be viewed at any time, and information about the changes can be obtained. For example, after consideration of a block from the Ethereum blockchain with id: 16445636 in the screenshot below (Fig. 2), the transactions that were added to this block can be seen.

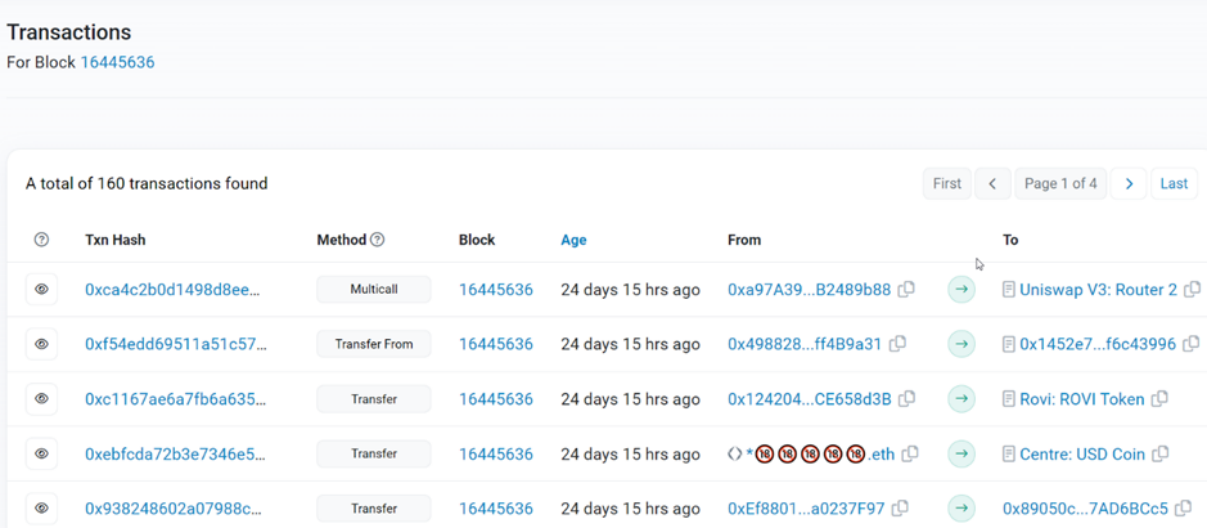

Figure 1: Transactions that are stored in the Ethereum blockchain block

Moreover, such a property of the blockchain as immutability allows us to make sure that the stored data is complete and permanent. Also, any verified entries are irreversible and cannot be changed. This means that anyone on the network will not be able to edit, change or delete it.

Therefore, considering these factors, it can be assumed that the blockchain can provide a quality basis for building a messaging service, providing the prerequisites for storing information in a reliable place and protecting it from forgery or unauthorized change.

Another important component for the operation of a service based on the principle of decentralization is Decentralized Applications (DApp), the principles of which will be discussed in the next section.

3. DApp Basics

DApps are decentralized applications that run on decentralized systems like Ethereum, Solana, Tron, etc. Their feature is that, as in the case of the blockchain, there are no servers, and all calculations are carried out by the nodes of the network in which the DApp works. In addition, the application must ensure the fulfillment of several requirements [23]:

1. The DApp must be open source, self-contained, and no single user must hold most of the tokens. All changes to the application must be implemented through consensus among participants and based on their suggestions.
2. The data and results of the application's operations must be stored in a

cryptographically secure form and stored on a public blockchain.

3. Tokens should be used to reward users who keep the network running and provide access to service to users.

4. Tokens must be generated by a decentralized application according to standardized cryptographic algorithms. These tokens are to be used as proof of value for investors. For example, the reward of miners in the Bitcoin network.

Such applications can be used to decentralize various functions and services, ranging from entertainment, such as the game CryptoKitties [24], which is one of the oldest attempts to use technology in the field of entertainment, to the decentralization of various financial transactions, health care or conducting elections. For example, the Pancakeswap platform was created for decentralized exchange transactions with cryptocurrencies, such platforms are known as DeFi (Decentralized Finance) [25] and work on the Binance smart chain blockchain and currently have a capitalization of 700 million US dollars [26] at this moment. In healthcare, there are platforms such as MedRec [27], which uses the blockchain for medical data access and access management, providing patients with a complete immutable history and easy access to their medical information across all medical facilities that use the service.

Also, such applications can be used to ensure transparency of supply chains by clearly recording the movement of resources between and within the chain participants. Moreover, the DHL company in its overview of blockchain perspectives [28] believes that blockchain can help achieve cost savings by providing more economical, more automated, and error-free processes. And add transparency and predictability to logistics operations, which can speed up the physical flow of goods and can help create sustainable, large-scale supply chains and help fight counterfeiting. For example, blockchain technology has been applied to increase trust in halal meat suppliers in Indonesia [29].

Table 1 shows the advantages and vantages of using decentralized systems.

Table 1
Advantages and disadvantages of centralized and decentralized systems

Analysis process	Centralized	Decentralized
Advantages	Full control over the program and its execution. Can handle a larger volume of traffic. Easy to update as the update is automatically sent to the user's device.	Due to decentralization, user data is not at risk in the event of a data leak or hacking attempt. Ability to work when one or more nodes fail. Resistance to censorship. Decisions regarding the system are made collegially. System nodes are equal in rights. Immutability of already saved data.
Disadvantages	In the event of a system error, the service may stop working until the problem is resolved. Additional costs for server protection.	Difficulty in updating and correcting errors due to the decentralized nature. Low suitability for use in performance-intensive systems as DApp transactions are typically slower. Large memory costs to keep a copy of the blockchain in each node.

The key mechanism in the operation of these applications is consensus in the network, which allows you to confirm the newly added block and consider it legitimate. Examples of obtaining consensus in the network are discussed in the next section.

4. Basics of the Consensus Mechanism

One of the key aspects of blockchain technology is determining which node publishes the next block. This is solved by implementing one algorithm out of many possible consensus algorithms. For public blockchain networks, there are usually many publishing nodes competing simultaneously to publish the next block. They usually do it to get a reward. In general, this

mechanism allows you to confirm that the changes made to the network are legitimate.

When a node joins the blockchain network, it must agree on the initial state of the system. This is recorded in a single pre-configured block, the genesis block (i.e. the first block in the blockchain). Each blockchain network has a published genesis block, and each block must be added to the blockchain after it is based on an agreed-upon consensus algorithm. However, regardless of the algorithm, each block must be valid and, accordingly, it can be independently verified by each blockchain node. By combining the initial state and verifying each block, nodes can independently agree on the current state of the blockchain. On the other hand, if two valid chains were provided for a full node, a common mechanism in almost all blockchain networks is that the "longer" chain is assumed to be the correct chain to depend on since it was longer worked on [30].

For example, the first algorithm was Proof of work [31] used in Bitcoin and Litecoin, the idea of which was to perform complex mathematical calculations to solve a problem, the solution of which gave the node that found the solution the right to add a block to the network and receive a reward for their work.

Another possible option is Proof of stake [32], which is used in Ethereum [33]. Unlike the PoW algorithm, a node uses the available number of tokens to add a block to the network. That is, a larger number of tokens at a node gives it a greater chance of being chosen to validate transactions and add a new block to the network, and the need to have a large number of tokens reduces the probability of an attack on the network, due to the economic impracticality for an attacker.

5. Algorithm Development

Using the possibilities provided by blockchain technology and decentralization, a messaging service can be built. This service will have an information exchange scheme similar to the passage of a transaction in the blockchain, and since the blocks can contain not only information about the transaction but theoretically any information that meets the requirements for the block, then the information sent to the recipient can also be stored there.

The messaging algorithm will consist of the following steps:

1. User A wants to send a message to User B.
2. Message data adds to the block.
3. The message block is sent to all network nodes for validation.
4. Network nodes confirm the legitimacy of the new block.
5. A new block is added to the blockchain.
6. User B receives a message from a new block in the blockchain.

The schematic image of the algorithm is displayed in Fig. 3.

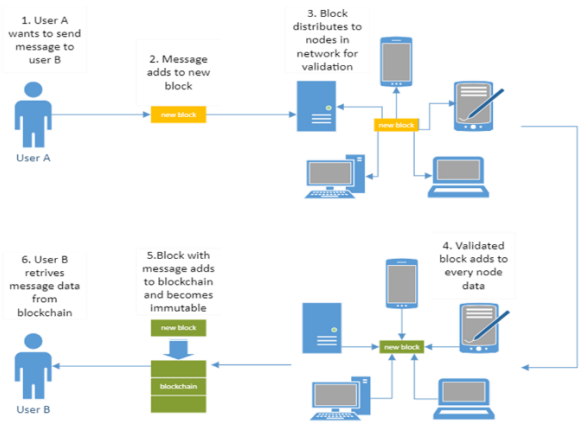

Figure 3: Scheme of the transaction in the blockchain

Table 2 shows the advantages and disadvantages of using this method.

Table 2
Advantages and disadvantages of using blockchain for messaging

Analysis process	Blockchain method usage
Advantages	Anonymity Decentralization Immutability Equality of nodes Transparency
Disadvantages	The need for additional cryptographic protection of messages. Message size limit. The complexity of implementing media files. exchange. Blockchain size. Load on nodes. Lack of ability to organize real-time messaging.

First, one of the disadvantages will be that the messages stored in the blockchain will be available for viewing by all participants of such a

service, and not only the participants of the correspondence, since the block data, as discussed earlier, is stored in a viewable form for all participants.

The limitation of the size of the message follows from the limitation of the size of the block itself, for example, in the Bitcoin network the size is 1 Mbyte, and in the Ethereum network there is no actual limitation, however, for a larger size, you will have to pay an additional amount for processing—a gas fee, which will again limit the size of the message. This limitation also leads to another drawback—the difficulty in implementing the exchange of media files. Such exchange will be impractical through the blockchain itself, as the size of media data such as voice messages, images, or videos is too large to exchange through the blockchain, and their storage in the blockchain will involve the use of large amounts of memory, which will increase the size of the blockchain.

Also, with the growth of the number of users and the data they exchange, the size of the blockchain itself will grow, which will increase the load on the nodes themselves and take up a large amount of memory. This factor can lead to the impossibility of using mobile devices to access the network due to the too large size of the blockchain.

However, the biggest disadvantage of such a system would be that it would be virtually impossible to ensure instant messaging, as blocks would only enter the network after a new block has been found and then verified by network nodes and added to the blockchain. After that, the addressee will be able to download a new block and receive a message. In addition to this, the transmission of the message will also require some token expenditure, as the nodes of the network must receive a reward for finding a new block. These shortcomings encourage the search for methods of their leveling, which will be considered in the next section.

6. Bypassing the Limitations of the Proposed Method

The use of blockchain for messaging has several disadvantages that make it much more difficult to use it in this direction. However, these limitations can be leveled in ways, the concepts of which will be given below.

General access to messages. This drawback can be circumvented by cryptographic protection of the data content. The use of additional protection of messages will also entail an additional expenditure of resources for cryptographic transformations and the need for a mechanism for exchanging keys between dialogue participants.

Sharing media files. One of the solutions to the problem of exchanging such data can be the use of IPFS platforms, which allow you to store media data in a decentralized manner, and to exchange them, send the addressee to the file itself, and the hash of the file to search for it in IPFS. However, if we are talking about the exchange of important documents, then storing them in the blockchain will ensure their integrity and availability, however, as in the case of messages, they will be available to all participants of the service, not only participants of the dialogue. Also, such documents will most likely have a size limit to prevent excessive use of space in the blockchain or the ability to fit the file itself into the allowed block size.

Blockchain size and node load. To combat the excessive size of the blockchain, the "zeroing" method can be used, when certain set sizes are exceeded. The idea is that when the blockchain reaches a certain size, block data is deleted from it, and only proof of work and block hashes are kept preserving the blockchain. However, this approach is not optimal, since the information contained in it will also be lost when the blockchain is zeroed. Ultimately, deleted data can be stored separately from the blockchain to ensure access to it.

Although the proposed method of building a messaging service based on blockchain is real for implementation and will provide access to the benefits provided using blockchain technology, its shortcomings force us to look for other approaches for solving the problem of using blockchain in such systems.

7. Usage of Nodes of Various Types

One of the possible ways to circumvent the shortcomings is the implementation of the service based on nodes of different types (Fig. 4). Conventionally, they can be divided into nodes of the following types:

- Full nodes—nodes that will contain all functionality.
- Archive nodes—nodes that will contain a copy of the blockchain.

- lightweight nodes are nodes that will contain only blocks containing information that is relevant only to this node.

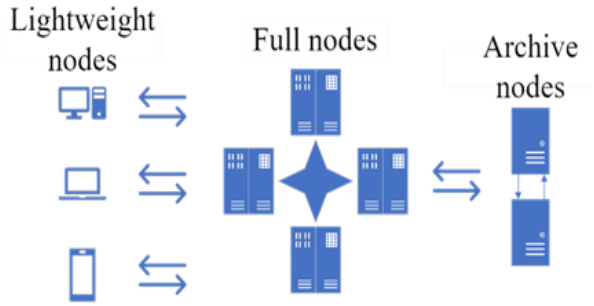

Figure 2: Schematic representation of the implementation of a network based on mixed nodes

In this approach, lightweight nodes can be considered as a conditional client application, and the algorithm itself will have the following steps:

1. User A wants to send a message to user B.
2. If user A is a full node, the user participates in the creation of a new block, if not, the user delegates to a full node.
3. The new block is validated by full nodes and added to the blockchain.
4. Archive nodes are synchronized with the new state of the blockchain.
5. light blocks get a new block if it contains information that applies to them.

In this approach, the main load falls on full nodes, since lightweight nodes contain only those blocks in which information is relevant to the node, and the entire blockchain is missing, which excludes their ability to participate in the creation of new blocks and their validation. Also, lightweight nodes will only be able to interact with full nodes to gain access to updates in the blockchain but will not be able to interact with each other. Since archive nodes are used to store a copy of the blockchain, it makes it easier to add a blockchain "zeroing" method, since there are already nodes in the network to store the data. Thus, archive nodes will have the blockchain in its full form, and full nodes will be able to work with a zeroed one.

However, the main disadvantage of this method will be the reduction of decentralization in the network, since part of the network will have more rights compared to others. For example, only full nodes will be able to perform validation, archive nodes will be able to store blockchain data or backup, and light nodes will only be able to receive and send messages. Also, the load on full nodes will increase due to the exit from the consensus algorithm of lightweight and archive nodes. Along with this, the addition of new types of nodes adds new points of vulnerability to the system.

8. A Hybrid of Tor and XRP Ledger

Another way to circumvent the limitations associated with the use of blockchain can be the creation of hybrid systems. One of them could be the use of a combination of Tor technology with the XRP Ledger. XRP Ledger does not use the blockchain itself, but rather the technology that was its predecessor (Distributed ledger). Unlike blockchain, distributed ledger technology does not use blocks, but operates on a log of records.

Another feature is that it does not need a full copy of the log history to work, but only an up-to-date version and the transaction time takes 3–5 seconds [34].

The scheme of work of the XRPL has the following form (Fig. 5):

- Clio server—an optimized server for working with HTTP and WebSocket.
- Rippled P2P is a peer-to-peer network that supports and validates the XRP Ledger.
- Data Base—contains the current version of data from the XRP Ledger.
- Client—the client part that works with data not directly, but through the Clio server.

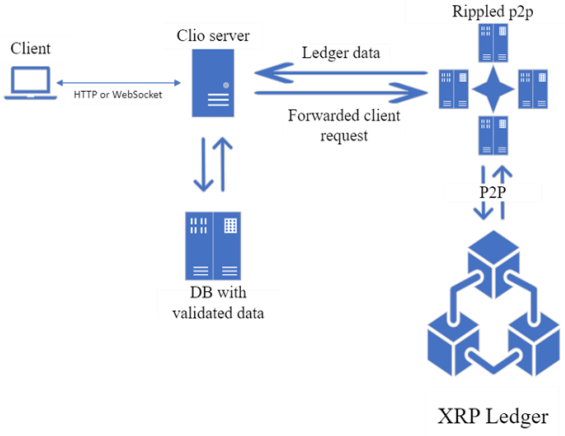

Figure 3: XRP Ledger operation scheme

The work algorithm based on XRPL will have the following steps:

1. User A wants to send a message to user B.
2. User A sends a request to Clio server.
3. Clio-server sends a transaction validation request to rippled p2p.
4. Rippled p2p validates the transaction and adds it to the XRP Ledger.

5. Clio-server receives updated data from Rippled p2p and updates the current version in the Database.
6. User B receives data from the Database via Clio-server.

By adding Tor technology to this scheme, it is possible to provide anonymity for endpoints. That is, in this case, communication between the client and Clio will take place through onion routing.

The advantage of this method is to reduce the time for the transmission of messages and reduce the load on the network nodes, since nodes only need to have the current version of the XRPL to work, and not the entire chain, as in the case of the blockchain.

Also, this method will have its drawbacks, the most important of which will be a decrease in the level of decentralization. Also, the use of Tor technology can lead to a decrease in the speed of passing requests between nodes, and malicious nodes can also participate in routing.

9. Conclusions

The paper considered the possibilities of using blockchain technology to build services for exchanging messages between network participants and proposed several methods of its implementation. It was stated that the use of the approach using the blockchain itself is possible, however, due to several features of the technology, its usage is impractical due to the possible sizes of the blockchain, the limitation of the size of the message to the maximum allowed block size in the network, and the growth of the load due to the growth of the blockchain itself.

Variants were proposed to circumvent the shortcomings of the method proposed in Chapter 5, in particular by using such methods as zeroing the blockchain when a critical size is reached, which on the one hand will reduce the load on nodes and increase the speed of information processing due to the reduction of the size of the blockchain itself, but at the same time will add the need to save data that was deleted from the blockchain in a separate place, which is not the best option and prompts the search for other solutions.

Such solutions can be the creation of a system based on various nodes or the creation of a hybrid network based on Tor and Ripple.

The advantages of the approach based on different types of nodes will be a reduction in the load on nodes due to their distribution into different types and, if necessary, a simplified application of blockchain zeroing due to the presence of archive nodes in the network. The disadvantage of this approach is a decrease in the level of decentralization along with the addition of additional points of vulnerability due to the presence of new types of nodes.

The advantages of the method based on the hybrid approach are the reduction of the transaction time and network load due to the distribution of tasks in the network, the interaction between the client and the Clio server through the HTTP or WebSocket standards, as well as increasing the level of anonymity using Tor technology. However, this method has its drawbacks, mainly a decrease in the level of decentralization and an increase in the time for processing requests through routing in the Tor network, as well as the presence of possible malicious nodes during routing.

Comparing them, you can see that both methods allow you to bypass the limitations of the application on mobile devices, due to the creation of lightweight nodes in the first option, and in the second, the introduction of client applications into the network. Also, these methods offer the creation of nodes responsible for validating transactions, however, in the first option, they can also act as a “client”, while reppledp2p is only engaged in XRP Ledger support. Also, the hybrid option offers communication between the client and the Clio server through already standard protocols, while the approach based on different types of nodes requires the development of a communication procedure between light nodes and full ones.

Also, these methods will have certain difficulties in implementation, for example, a hybrid approach will require the development of a method of protecting archival nodes since they will contain the entire history of the blockchain, which is considered legitimate, and their compromise will lead to the compromise of the entire network. The method based on the hybrid approach uses Tor technology, which simultaneously provides privacy for client applications and the Clio server, and also introduces the possible presence of malicious nodes in the Tor network itself, so the data that flows between them should also be additionally protected.

Therefore, it can be concluded that the development of a method for exchanging messages based on blockchain technology requires compromise solutions, since the use of

only the blockchain itself is not the best option due to its peculiarities, while the use of proposed methods contains both advantages and disadvantages. Moreover, the type of information which will circulate in the network must be considered. For example, the exchange of media data through the blockchain network is impractical due to the sharp increase of the blockchain itself and the limitation of the block size, therefore, for the exchange of such data, it is necessary to use additional services and integrate them into the network.

10. References

[1] A. Lashitew, When Businesses Go Digital: The Role of CEO Attributes in Technology Adoption and Utilization During the COVID-19 Pandemic, Technol. Forecast. Soc. Ch. 189 (2023) 122324. doi:10.1016/j.techfore.2023.122324

[2] N. Khan, A. Awang, S. Karim, Security in Internet of Things: A Review, IEEE Access, 10 (2022) 104649–104670. doi:10.1109/access.2022.3209355

[3] F. Jáñez-Martino, et al., A Review of Spam Email Detection: Analysis of Spammer Strategies and The Dataset Shift Problem, Artif. Intell. Rev. 56 (2023) 1145–1173. doi: 10.1007/s10462-022-10195-4

[4] D. Dobhal, et al., Machine Learning for Cyber Security (2022) 41–70. doi: 10.1515/9783110766745-003

[5] B. Luuk et al., Protecting Your Business against Ransomware Attacks? Explaining the Motivations of Entrepreneurs to Take Future Protective Measures Against Cybercrimes Using an Extended Protection Motivation Theory Model, Comput. Secur. 127 (2023) 103099. doi:10.1016/j.cose.2023.103099

[6] A. Cinar, T. Kara, The Current State and Future of Mobile Security in the Light of the Recent Mobile Security Threat Reports. Multimed. Tools Appls. 82 (2023) 20269–20281. doi:10.1007/s11042-023-14400-6

[7] Whatsapp, WeChat and Meta Messenger Apps—Global Usage of Messaging Apps, Penetration and Statistics. Messengerpeople by Sinch. URL: https://www.messengerpeople.com/global-messenger-usage-statistics

[8] WhatsApp Messenger. App Store. URL: https://apps.apple.com/ua/app/whatsapp-messenger/id310633997

[9] Messenger. AppStore. URL: https://apps.apple.com/app/messenger/id454638411

[10] A. Holmes, 533 Million Facebook Users' Phone Numbers and Personal Data Have Been Leaked Online, Business Insider. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[11] Critical WhatsApp Vulnerabilities Patched: Check You've Updated!, Malwarebytes. URL: https://www.malwarebytes.com/blog/news/2022/09/critical-whatsapp-vulnerabilities-patched-check-youve-updated

[12] L. Zhang, Q. Ji, F. Yu, The Security Analysis of Popular Instant Messaging Applications, 2017 International Conference on Computer Systems, Electronics and Control (2017). doi: 10.1109/iccsec.2017.8446863

[13] A. Kalapodi, N. Sklavos, The Concerns of Personal Data Privacy, on Calling and Messaging, Networking Applications, Communications in Computer and Information Science, Singapore (2021) 275–289. doi:10.1007/978-981-16-0422-5_20

[14] V. Susukailo, I. Opirskyy, S. Vasylyshyn, Analysis of The Attack Vectors Used by Threat Actors During the Pandemic, in: IEEE 15th International Conference on Computer Sciences and Information Technologies (2020). doi: 10.1109/csit49958.2020.9321897.

[15] S. Yevseiev, et al., Synergy of Building Cybersecurity Systems: Monograph, PC Technology Center (2021).

[16] A. Mustapha, et al., Detecting DDoS Attacks Using Adversarial Neural Network, Comput. Secur. 127 (2023) 103117. doi:10.1016/j.cose.2023.103117

[17] S. Vasylyshyn, I. Opirskyy, V. Susukailo, Analysis of the Use of Software Baits as a Means of Ensuring Information Security, in: IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (2020) 242–245. doi:10.1109/CSIT49958.2020.9321925

[18] F. Chentouf, S. Bouchkaren, Security and Privacy in Smart City: A Secure E-Voting System Based on Blockchain, Int. J. Electr. Comput. Eng. 13(2) (2023) 1848. doi:10.11591/ijece.v13i2.pp1848-1857

[19] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.
[20] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
[21] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.
[22] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks 47(3) (2016) 308–316.
[23] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks 47(3) (2016) 308–316.
[24] I. Bashir, Mastering Blockchain: Distributed Ledgers, Decentralization and Smart Contracts Explained, Packt Publishing, 2017.
[25] M. Smith, The Spectacular Collapse of Cryptokitties, IEEE Spectrum, 59(9) (2022) 42–47. doi:10.1109/mspec.2022.9881234
[26] D. Metelski, J. Sobieraj, Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations, Int. J. Financ. Stud. 10(4) (2022) 108. doi:10.3390/ijfs10040108
[27] PancakeSwap Price Today, CAKE to USD Live, Marketcap and Chart, CoinMarketCap. CoinMarketCap. URL: https://coinmarketcap.com/currencies/pancakeswap
[28] Blockchain In Logistics Perspectives on the Upcoming Impact of Blockchain Technology and Use Cases for the Logistics Industry, DHL. URL: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf
[29] A. Azaria et al., MedRec: Using Blockchain for Medical Data Access and Permission Management, in: 2nd International Conference on Open and Big Data (2016). doi: 10.1109/obd.2016.11
[30] J. Hidayati et al., Transparent Distribution System Design of Halal Beef Supply Chain, Uncertain Supply Chain Manag. 11(1) (2023) 31–40. doi:10.5267/j.uscm.2022.12.003
[31] M. Mahmood, N. Al Dabagh, Blockchain Technology and Internet of Things: Review, Challenge and Security Concern. Int. J. Electr. Comput. Eng. 13(1) (2023). 718. doi:10.11591/ijece.v13i1.pp718-735
[32] J. Soria, J. Moya, A. Mohazab, Optimal Mining in Proof-Of-Work Blockchain Protocols, Financ. Res. Lett. 53 (2022) 103610. doi:10.1016/j.frl.2022.103610
[33] S. Yan, Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake, 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI), Zakopane, Poland, August 2022. doi:10.1109/icdacai57211.2022.00098
[34] Y. Hsain, N. Laaz, S. Mbarki, Ethereum's Smart Contracts Construction and Development using Model Driven Engineering Technologies: A Review, Procedia Comput. Sci. 184 (2021) 785–790. doi:10.1016/j.procs.2021.03.097