Blockchain Application Concept in SSO Technology Context

Valeriia Balatska[1], Vasyl Poberezhnyk[1], Petro Petriv[1], and Ivan Opirskyy[1]

[1] *Lviv Polytechnic National University, Information Security Department, Lviv, 79000, Ukraine*

Abstract

With the increasing importance of security in digital transformation for companies, the challenge arises to ensure data protection and reliable user authentication, especially in the rapid development of web applications. Many users utilize identical credentials for login, creating significant risks to their security. This article explores the potential of utilizing blockchain technology in the context of Single Sign-On (SSO) systems. Single Sign-On provides users with the ability to authenticate only once and gain access to various digital resources. The problem statement encompasses current trends in security and access management, such as the risk of data compromise and inefficient information exchange between SSO systems. An integral component of the article involves the analysis of recent research and publications, focusing on expanding the applications of blockchain technology, developing decentralized identifiers, and integrating consensus technologies. The primary objective of the research is the development and implementation of technological solutions aimed at enhancing the security, resilience, and efficiency of SSO systems in the digital environment. Additionally, key research is examined, emphasizing the significance of blockchain utilization and innovations in user identification and authentication.

Keywords

Blockchain, SSO, protection of personal data, authentication, NFT, token.

1. Introduction

Over the last decades, technological progress has led to the expansion of the cyber world and the increase in volumes of digital interaction. In this context, the SSO system has become a crucial element in ensuring the efficiency and security of user authentication. However, the constant growth in the volume of digital and in-person services leads to the growth of access management and information protection tasks complexity [1, 2].

One innovative technology that has the potential to cover many of these challenges is blockchain. Considering the concept of applying blockchain in the scope of a possible SSO technology, we are opening a wide field of possibilities that unites security, decentralization, and smooth user experience.

In this paper, we explore the possibilities of improvements that blockchain technology can provide to authentication security, ensure decentralized access control, protect user data, and cover other aspects of SSO. Also, we will examine the impact of this technological symbiosis on the security of Internet interaction and the role it can play in the further development of the digital world.

By developing our understanding of the interaction between the blockchain and SSO, we discover how this integration can define new standards of security and efficiency in today's digital landscape [3–5].

Problem formulation. SSO systems are becoming vital in the context of the growing demand for digital services and web resources. However, existing authentication and access management methods and tools do not always meet the security and trust challenges that emerging in a digital environment. Issues such

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: valeriia.s.balatska@lpnu.ua (V. Balatska); vasyl.poberezhnyk@gmail.com (V. Poberezhnyk); petro.p.petriv@lpnu.ua (P. Petriv); iopirsky@gmail.com (I. Opirskyy)
ORCID: 0000-0002-6262-6792 (V. Balatska); 0000-0002-7523-2557 (V. Poberezhnyk); 0009-0000-7426-3696 (P. Petriv); 0000-0002-8461-8996 (I. Opirskyy)
© 2024 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3654/paper4.pdf

as the risk of identity compromise, centralized management, and data sharing between different SSO systems remain relevant.

Actual aspects of the problem:

1. Insufficient security: existing authentication methods may be vulnerable to various types of cyber-attacks, which endangers the confidentiality and integrity of user information.
2. Centralized systems: Centralized access control systems can become a point of vulnerability and contribute to the risks of unauthorized access or security breaches.
3. Inefficient data exchange: SSO implementation does not always ensure efficient exchange of authorization information between different systems, which can lead to delays and incorrect access management.

Considering the mentioned problems, the necessity of the development and implementation of new technological solutions becomes obvious. In particular, the integration of blockchain technology into the field of SSO can be a promising way of the security, stability, and authentication improvements in the digital space.

Recent research and publications analysis. The combination of SSO and blockchain technology can create an effective and secure solution for access management and personal data protection. Let's consider how these two technologies can work together to improve security and user experience.

Firstly, decentralized identity. The blockchain can provide the basis for creating decentralized identities that users can control. Each user can have a unique digital ID by storing it in a distributed blockchain ledger. Also, an important aspect is the security of credentials—the storage of identification data in the blockchain can increase the security of this data [6]. The usage of encryption and decentralization avoids centralized points of vulnerability and ensures reliable protection of identity data.

Secondly, decentralization of access control. The blockchain can help in the implementation of decentralized access control systems, where each node (user) has significant influence over setting access rights. This helps to reduce the risk of centralized attacks and increases the transparency of the whole system. The usage of blockchain for identification can include the use of zero-knowledge proofs and other methods that allow authentication without transmitting the information itself.

The decentralized nature of blockchain allows the creation of immutable event logs that are easy to verify, enabling audits and establishing trust in user behavior. Moreover, the efficient data exchange mechanism between SSO systems can be established by using the blockchain as an intermediate platform for the secure and efficient exchange of authentication information between different SSO systems, which will ensure seamless authentication and access management [7].

The main idea is that blockchain can be used for the creation of secure, decentralized, and transparent identification and access systems that increase trust and protect users' data.

The purpose of the article. The purpose of this paper is to thoroughly research and analyze the possibilities of blockchain usage in the scope of SSO technology to overcome the indicated problems and create a more secure and efficient environment for Internet users. The main objectives of the article are:

- The overview of blockchain technology, its basic principles, and benefits of blockchain technology in the context of security and reliability.
- The analysis of the SSO technology: analysis of the current state of the SSO technology, its advantages, and limitations, particularly from a security perspective.
- The identification of the problems related to the current methods of authentication and access control on the Internet, in particular from the point of view of security, convenience, and reliability.
- The role of blockchain in the SSO: explores the possibilities of using blockchain technology to improve the SSO process, including overcoming identity conflicts and improving security.

Development of the concept: the concept of using the blockchain to improve the SSO is outlined, including technical and functional aspects.

2. The Analysis of SSO Technology

2.1. Simplification of Authentication and Data Management through SSO

SSO is a mechanism that allows users to sign into multiple applications, services, or websites while using a single set of credentials. This approach is convenient for users because there is no necessity to remember several different sets of credentials or authenticate multiple times. While users have one strong password instead of many, they are less likely to choose a weak password over a strong one or use the same password for different services, which is considered a common cause of cyberattacks [8].

The next important benefit is improved user control. SSO systems enable IT administrators to better control access to applications and services. They can easily check and manage user rights, which significantly reduces the risk of unauthorized access. This is especially important in organizations where access to confidential information is strictly regulated.

Moreover, the usage of SSO provides efficient login processes. The SSO provides fast and seamless access to various applications and services. This is especially important in industries such as healthcare or law enforcement, where quick access to information can be critical. Instead of spending time entering passwords for each service, users can start working immediately.

Finally, the key benefit of SSO is improved security. Because users need to remember fewer passwords, they tend to choose more complex and secure passwords. In addition, since there is only one entry point, it is easier to protect against cyber-attacks. Companies can use additional security measures, such as multi-factor authentication, making the system even more secure [9].

However, SSO, or the single sign-on system, despite its advantages, has certain drawbacks that are important to consider when implementing and using it.

One of the key disadvantages is that due to its nature, SSO creates a single point of failure. If the SSO provider goes down for some reason or experiences technical problems, it may lead to loss of access to all connected applications and services. This is a critical risk, especially for organizations that depend on continuous access to their applications.

Another drawback is limited support for some applications. Not all applications and services support SSO, which may encourage users to have separate accounts for those applications. This partially removes the advantage of single sign-on because users still need to remember several logins and passwords [10].

One more problem is related to the risks of shared computer usage. In environments where computers are shared, such as libraries or educational institutions, there is a risk of unintentional access to someone else's account unless the user is logged out.

In addition, there is a serious risk of credentials being stolen in case of data leakage. If an SSO account has been compromised, attackers gain potential access to all associated services and applications. This can lead to a large-scale leak of confidential information.

Another potential drawback is the complexity of the integration of SSO with existing security systems in some organizations. Implementing SSO can require significant technical effort to integrate with different systems and platforms, especially in large or complex IT infrastructures.

All in all, SSO can limit the ability to customize security policies for individual applications. In some cases, the standardization of security settings through SSO may not consider the unique requirements of certain applications, which may pose a risk to data and information security.

The integration of blockchain technology into the SSO system offers unique solutions to existing shortcomings and provides new functionality.

2.2. The Blockchain Integration with SSO

First and foremost, blockchain creates a centralized yet distributed ledger that simplifies the process of managing accounts. This reduces the risks associated with a single point of failure since the data is now distributed and does not depend on a single server or provider [10].

The distribution of data in the blockchain also reduces its vulnerability to attacks.

Attacking a system where information is stored in many nodes at the same time is much more difficult than a centralized system with a single entry point. This is especially important given the risks of compromising SSO accounts, which can give access to a wide range of services and applications.

Also, usage of the blockchain greatly improves the scalability of SSO systems. Due to its distributed nature, blockchain can easily handle large numbers of users and services without the need to centralize data and request processing.

In addition, the blockchain provides a high level of transparency and traceability. Every transaction, including changes to access or credentials, is recorded and auditable. This adds an element of accountability and helps prevent unauthorized access.

Decreased dependence on service providers is another important advantage. Using blockchain can reduce the need for external SSO providers, giving organizations more control over their identity and access systems.

Thus, the application of blockchain in SSO provides new opportunities for improving the security, efficiency, and reliability of access management systems, while solving several existing problems associated with traditional methods of identity management.

In the context of SSO technology, blockchain can help create a secure and efficient authentication mechanism. Each node of the blockchain network will store and maintain user authentication information. This allows the usage of a secure registration and authentication process, as well as managing access to various resources [11]. Information stored in the blockchain can be reliably protected from interference or alteration, providing a high level of security for users' data.

In a blockchain-based SSO system, each user can have a unique identifier that is stored in a distributed blockchain database. When a user logs in to any of the resources, a request is made to the blockchain to validate the authentication data.

This approach has several advantages:

- Data security—blockchain uses cryptographic methods to ensure security, making it resistant to hacking.
- Decentralization—saving authentication information is distributed among network nodes, making possible attacks more difficult.
- Efficiency—the authentication process is carried out once and data about it is recorded in the blockchain, avoiding re-entering credentials for each resource.

This approach can find its application in various industries, from access control in corporate systems to secure login to online services.

SSO authentication, as described previously, is the process of logging into a network once and then gaining access to all other systems on the same network using the same credentials. A user can log in once and access all systems associated with their account. SSO authentication is used for cloud applications, web applications, mobile applications, and more. Additionally, companies can create a customized login environment with login policies, access controls, and access auditing using SSO.

In case of the blockchain usage in SSO, the users' credentials are stored in a decentralized ledger, which means that the data is stored on a network of computers (nodes) rather than on a single server. This decentralized data storage makes information more secure and less vulnerable to cyber-attacks.

If a hacker tries to break into a network, he will have to break into every single computer in the network, which is much more difficult than breaking into a single computer. The system owner can also decide whether to change access rights to user data.

2.3. Protecting Personal Data in Government with Blockchain and SSO

The use of SSO and blockchain technology to protect personal data in government can bring several significant benefits, such as increased security, decentralization, auditing, and efficiency.

The blockchain allows personal data to be stored and processed in an encrypted and secure environment. The data can be distributed across the network in a secure format, making it less vulnerable to potential cyberattacks. Blockchain can serve as the basis for creating a decentralized access control system for public services. Each user can have a unique identifier and control

their permissions, reducing the risk of centralized vulnerability points.

An important step is the introduction of Zero-Knowledge Proof. Using the "Zero-Knowledge Proof" or other cryptographic methods allows you to prove authenticity without transmitting the information itself. This can be useful for identity verification without details disclosure. Blockchain technology provides the possibility of the creation of event logs that are immutable and auditable. This assists in managing, tracing, and identifying anyone who accessed personal data, when, and how.

Moreover, the blockchain can solve the problem of data duplication in different government systems. A distributed database can provide a single and up-to-date set of data. SSO and the blockchain can facilitate effective data recovery after possible disasters or cyberattacks. The blockchain can provide data backup and recovery while preserving integrity. The usage of single sign-on and blockchain technologies can facilitate the integration and exchange of data between different government services, simplifying the processes of processing and sharing information.

It is important to take into account the challenges of regulation, privacy, and the introduction of new technologies in public administration. The specific legal environment and security standards that apply to public institutions should also be taken into account.

Table 1

The combination of SSO and blockchain technology for personal data protection in government introduces several advantages and disadvantages

Advantages	Disadvantages
Identity and electronic document management. The use of blockchain can simplify the identification and management of electronic documents. Citizens can have digital identifiers that prove their identity, which can be used in various government systems and services.	Risk of personal information leakage. Attackers can use identifiers for unauthorized access or data leakage. Dependence on technical means. Failure or malfunction of SSO or blockchain hardware can lead to access problems.
Ensuring privacy. It's important to consider privacy practices in the context of blockchain and SSO. Techniques such as anonymizing data, using private blockchain solutions, or encryption can help keep personal information confidential.	Lack of absolute anonymization. Not all data anonymization methods can guarantee absolute privacy and anonymity. Controversial private blockchain, the use of a private blockchain may raise questions about its true independence and privacy.
Standardization and the legal environment. It is important to consider the standards and legal environment surrounding the use of blockchain technology in public institutions. Defining standards for data processing, storage, and exchange can help to ensure that systems are secure and interoperable.	Slow standard-setting process. The process of defining and adopting standards can be lengthy and protracted. Outdated standards and changes in the technological environment can make established standards obsolete, requiring constant updating.
Integration with existing systems. When implementing SSO and blockchain, it is important to consider the possibility of integration with existing government information systems. Ensuring compatibility and ease of implementation can help avoid difficulties in transitioning to new technologies.	Integration with existing systems can be complex and require significant resources and time. The transition to new technologies may be accompanied by temporary disruptions that may affect government services.
Benefits for citizens. It is important to emphasize the benefits for citizens in using these technologies. Simplifying access to government services, and increasing security and control over their data can make these technologies more acceptable to the general public.	Some citizens may find it difficult to use new technologies or may not see the benefits of using them. Citizens may express concerns about security and privacy in the context of SSO and blockchain.
Efficient resource management. The use of blockchain technology in government can help to manage resources efficiently and avoid unnecessary duplication and data loss.	The costs of implementing and maintaining technology can be significant and require significant investment. Government staff may require additional time and training to adopt new technologies.
Training and awareness. Implementation of new technologies requires training and awareness raising of staff on data security and the benefits of using SSO and blockchain technologies.	Some employees may be resistant or disapproving of the need to learn and use new technologies. Low levels of information literacy among citizens may make it difficult to adopt new technologies.

The integration of SSO and blockchain technologies in government can help address security, efficiency, and transparency issues in the processing and storage of citizens' data. However, it is important to maintain a balance between security and convenience to ensure successful implementation and adoption of the technologies.

The introduction of SSO and blockchain technology in the public sector can face several issues and challenges that should be considered during the design and implementation of the system. Government agencies often use different information systems and platforms [12]. Integration of SSO and blockchain technology may face challenges

in terms of compatibility and interoperability with existing systems.

Also, ensuring a high level of data security and confidentiality is a critical task for government agencies. It is important to examine and address possible risks associated with the storage and processing of sensitive information. The introduction of new technologies requires training and adaptation of staff. Public services may face challenges in terms of lack of awareness and resistance to change among staff.

An important issue is that changes in existing legislation and the regulatory environment may be necessary to comply with and legally use new technologies. This may require time and effort to amend legislation. Legislative issues related to the introduction of SSO and blockchain technology in public government may include several aspects related to the legal environment and regulation.

It is important to determine whether there are necessary legislative changes or support for the introduction of new technologies. This may include developing new laws or adapting existing ones to take into account the specifics of SSO and blockchain technologies. Determining the responsibility of the parties in case of possible data security incidents or breaches. This includes defining the responsibilities of government agencies, technology providers, and possibly even citizens in the case of problems [13].

Many jurisdictions have strict laws and regulations governing the privacy and protection of personal data. While introducing new technologies, it is important to determine if they are consistent with these requirements and how to ensure compliance. Determine the status of electronic documents and digital identifiers used in the system. This may include the legalization of electronic signatures and other issues related to the legal force of electronic documents.

In turn, it is important to consider the issue of public trust in new technologies and security measures. Active communication with the public and taking their views into account can be key to successful implementation. Legislation should define the rights and obligations of users in the context of SSO and blockchain technologies. This may include issues of authorization, access management, and retention of rights. The introduction of the blockchain may require transparency and openness in addressing issues of data legitimacy and integration. Legislation may define rules for auditing and verifying transactions.

While implementing new technologies, the huge number of users and processing of large amounts of data can create challenges in scaling the infrastructure and ensuring the system's resilience. The use of blockchain to create virtual identifiers may raise issues related to the fairness, validity, and reliability of such identifiers [14].

Taking these challenges into account and actively managing them can help create a successful and effective SSO and blockchain system in a state government. In addition, it is important to engage all stakeholders and develop strategies to address specific challenges that may arise when implementing new technologies.

3. Technology Capabilities in the Context of the SSO System

3.1. Blockchain Credentials

The use of blockchain for creating and storing credentials can offer several advantages. First and foremost, the use of blockchain technology will allow data to be stored immutably throughout its existence. That is, once such data is created and stored in the blockchain, it will not be possible to unauthorizedly change or delete it. The next advantage is decentralization, which will allow different network nodes to participate not only in creating or verifying such data but also in providing access to such records in the event of a failure of one or more network nodes [15].

Another important characteristic is the use of cryptographic mechanisms that allow such data to be used for the digital signing of documents or user identification. To do this, when creating credentials, it is enough to add the user's digital signature to them, which will allow them to be used in the future.

At the moment, various systems make it possible to create such credentials in the field of education [16], and their actual use prompts us to look for new ways to use these types of credentials, in particular, to explore the possibility of their use in SSO systems.

3.2. Distributed Access Logging System

Activity logging systems are an integral part of any system, including access control systems, which include SSO. Analyzing user actions allows the detection of unauthorized activities by finding anomalies in the users' behavior [17], atypical actions, unusual locations from which were obtained, etc., or by investigating attack vectors [18]. This system can be of great interest to an attacker. The CAPEC-161 family of attacks: Infrastructure Manipulation [19] are aimed at changing the system's infrastructure, in particular the CAPEC-268: Audit Log Manipulation [20] attack is aimed at altering the user action logs in the system. The idea of such an attack is that an attacker changes entries in the activity register to hide unauthorized actions in the system. There are several types of such manipulations: deleting logs, modifying logs, saving fake logs, and suppressing logging.

In this case, the use of blockchain technology will protect the logging system, the concept of which is depicted in Fig. 1, from unauthorized changes by using the very nature of the technology. Such a property as data immutability will make it possible to ensure that no stored data has been deleted, modified, or unauthorizedly added to previously stored records, since any change in the existing chain of blocks will be easily detected by changes in the block hash, which is formed based on the data stored in it, and the hash value itself is stored in the next block.

Although the use of this approach is quite attractive due to its protection against unauthorized changes, one should take into account the limitations of blockchain technology. For example, the size of the blockchain itself may become a limitation, which will grow with the number of records, since all data will be stored in the blockchain. This will lead to a constant increase in the load on the system and a decrease in performance over the time of existence of such a blockchain, since its size may negatively affect performance, in particular, the time to reach consensus in the network. In addition, the size of the blockchain itself will have a positive impact on the system's resistance to attacks, as making unauthorized changes will require the use of significant resources, making the attack non-profitable for the attacker.

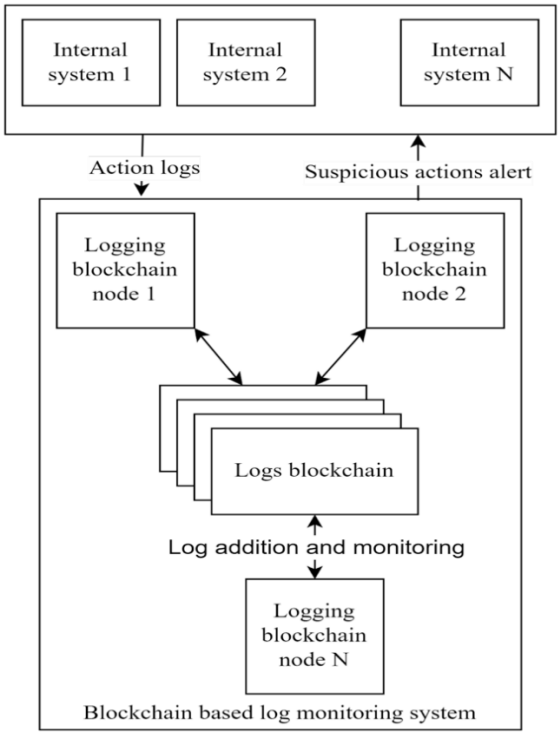

Figure 1: The concept of a blockchain-based monitoring system

3.3. Pseudo-Anonymous Credentials

In the context of blockchain, pseudo-anonymity means that a user's credentials and digital identifier are not directly linked, but can be linked using various methods and tools. Accordingly, there are various blockchain projects [21] that use more sophisticated cryptographic methods and tools to ensure greater user privacy.

However, in the scope of developing an SSO system, this property of the technology can become one of the tools for building a logging system. Analyzing user activity in the activity log and detecting abnormal activity may indicate the presence of unauthorized actions. Although the user's identity cannot be established based on the user's crypto address alone, a separate database with user credentials will allow to identify the person who may be the intruder. In this case, pseudo-anonymity means that all actions are logged using only the user's crypto address, but there is a separate secure blockchain containing the user's credentials, which allows to identification of the user if necessary. This method of applying such a property is ambiguous since it does not guarantee

complete anonymity of system users and provides the ability to identify the user, but this is a necessary measure in the case of blockchain-based SSO, as it will create the possibility for attackers inside the system that their identity will be disclosed.

3.4. Organization of Access Control

Access separation is one of the key functional characteristics of any access control system and SSO in particular. In traditional systems, access control takes place on the side of the system that stores the separation rules and is responsible for their enforcement. When using the blockchain, the function of storing permissions can be transferred to the system users themselves, while the execution of access control rules and the issuance of new permissions can be left on the system side [22].

The following technologies can be used to ensure this approach: NFT, Smart contracts, and the use of different types of blockchains—open, closed, hybrid, etc.

Since NFT is a non-fungible token, unlike widely known cryptocurrencies, and can contain almost any information that is written to it, its use in the context of SSO systems can play the role of permissions to access certain internal services, the right to read or write information in systems, etc. The existence of smart contracts, i.e. self-executing code in the blockchain network, will allow the system to automatically determine the role of the user based on the tokens he or she has and provide access to restricted information. The possibility to store information with different levels of access in the blockchain network can be achieved precisely through the use of different types of blockchain networks. For example, public information can be stored on a public blockchain, which does not require any special access tokens (NFTs), restricted information can be stored on a private blockchain, the rules for access to which can be determined by the organization to which it belongs and, for example, require that the user already owns a certain type of access token, or a hybrid blockchain can be used, which combines the access control capabilities of a private blockchain with the ability to provide open access to public information. However, it should be considered, that the use of different types of blockchain will lead to a decrease in the level of decentralization of the system, as this approach will create users with special rights [23].

4. System Concept

The proposed concept will be based on the use of a combination of different types of blockchain to enable the creation of a blockchain-based SSO system. The key element is the combination of two types of blockchain, one of which will be used to store data about users and the other to store logs of their actions in the system to monitor activity in such a system. We believe, that the best choice of blockchain type to store user data is a hybrid blockchain. Since it will make it possible to store user data in a secure place, inaccessible from the outside, and at the same time make it possible to obtain an anonymized user ID with data on their access rights for access rights validation.

The type of blockchain used to store logs will be public, as it will allow anyone to check network activity and find anomalies that may indicate intrusion into the network.

The system algorithm will look like this:

1. The credentials provider creates the user's blockchain credentials and stores them in the hybrid blockchain, and transmits them to the user of the system.
2. If it is necessary to grant special rights, the provider creates an NFT with data on the user's special rights and transfers it to the user.
3. To log in to the system, the user sends an access request to the access controller, which acts as an SSO gateway.
4. The access controller requests the adapter to the hybrid blockchain to verify user rights.
5. In case of successful validation, the user gains access to the system, and a corresponding entry is made in the public log blockchain. In case of unsuccessful validation, the user is not granted access, and a corresponding entry is made in the log blockchain.

When a user accesses internal systems, the corresponding records are entered into the log blockchain.

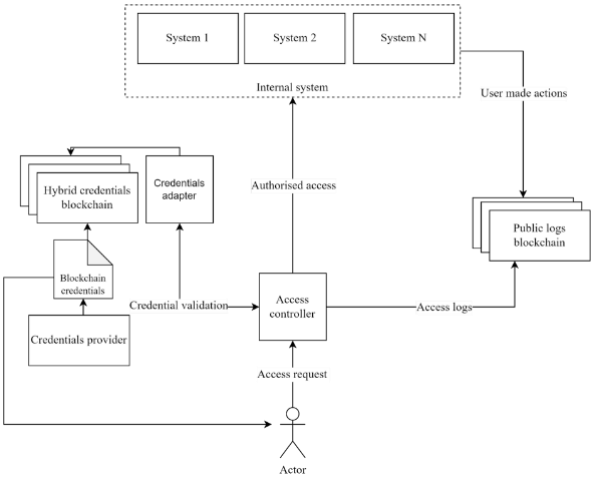

Figure 2: Conceptual scheme of the system

An analysis of the advantages and disadvantages is presented in Table 2**.**

Table 2
Analysis of the advantages and disadvantages of the proposed system

Advantages	Disadvantages
Absence of a central point of vulnerability.	Increased system load with an increase in the number of users.
Equality of nodes in the network.	Increased system load with an increase in the number of stored logs.
The ability to securely store user data.	Decrease in performance with the growth of the blockchain size.
Anonymization of login data.	A need to find niche specialists to develop and maintain the system.
Reducing the load on the network by using separate blockchains to store user credentials and log their actions.	Existence of users with special rights in the network.
Low possibility of making unauthorized changes to the network.	Decreased decentralization due to the use of a hybrid blockchain.
No possibility of unauthorized changes in user activity logs.	Possible difficulty in developing multi-factor user authentication.
	A need to develop a mechanism for removing users' special rights.
	A need for highly qualified developers to provide a secure mechanism for logging actions.

This approach allows to separation of the processing of user data and the action log, which reduces the load on the system and speeds up the login process since the creation of new users will not overlap with the entry creation in the action log. Also, the use of the credentials adapter will allow to transfer of only information about the identifier and access rights to the access controller, and all personal data will remain within the hybrid blockchain network.

Given the advantages of such a system, it may be of interest for further research and developing ways to implement such a system. Special attention will be required to find solutions to the disadvantages of such a system.

One of the key disadvantages of such a system is the increasing load on the system as the network grows, as the decrease in performance will directly affect the ability to use such a system in real projects, as the long time for a user to log in and record their actions in logs can become an insurmountable obstacle to the implementation of such a system. One possible way to overcome the problem is to use such an SSO system only for critical objects of the overall system, where it is necessary to ensure the highest level of control over user actions. Another way would be to use XRPL [24, 25] technology, which allows for fast processing of requests and is a precursor to blockchain technology which uses a distributed ledger system. However, the use of this technology can also lead to the need to find niche specialists, develop a mechanism for its harmonization with the network, etc.

Another disadvantage of the system is the need to create users with special rights and the use of blockchain types that reduce the level of decentralization. However, these are disadvantages without which the development of this system will be impossible since their very existence makes it possible to delimit access and store credentials in a secure place.

The next challenge is creating a mechanism for removing special rights from users. This can be done by providing access to resources through burning NFT tokens after a single access to resources or creating tokens with a limited lifespan. However, this approach will create an increased load on the network, as it will generate additional transactions when granting and redeeming such tokens from the user.

Also, the relatively low number of blockchain specialists may lead to the involvement of insufficiently qualified personnel, which may lead to problems in the system architecture, additional vulnerabilities, etc.

Another challenge is the possible difficulty in implementing the development of multi-factor authentication. This attention should be paid, as the theft of a user's crypto wallet may lead to free entry into the network for intruders, since in this approach the very existence of a crypto wallet with credentials is

an authentication factor, and the availability of additional mechanisms to confirm the user's authenticity is a necessity to protect against such situations.

In general, when using blockchain technology in SSO systems, it should be considered as a possible addition to the existing system, not as an alternative to traditional systems. In particular, the availability of a blockchain version of the event log can be a secure alternative to conventional access logs, as such a log will be protected from unauthorized tampering with log entries, making it impossible to hide abnormal activities in the network, which will make it easier to identify the intruder. Or using the blockchain as a repository of user credentials, which can simplify the exchange between different institutions and eliminate the need for multiple duplications of user data, make changes to them in one place, and allow users to control these changes and see the party that changed them. The use of blockchain technology at this stage of its development can be seen as an experimental addition to existing systems and as a basis for further research on this topic.

5. Conclusions

The study emphasizes that the blockchain, due to its decentralized nature, can solve the problems associated with centralized SSO authentication systems. This avoids one central point of vulnerability and contributes to a higher level of user data protection.

The main aspect of the study is to thoroughly examine and compare the benefits of blockchain and traditional SSO methods. The results show that blockchain not only provides a high level of security but also helps to avoid problems such as concurrent access and identity conflicts.

A detailed review of technical aspects of the blockchain-based SSO implementation was provided, including the development of a distributed blockchain-based SSO concept, which will ensure the possibility of storing identity and access control information. This can greatly improve the process of authentication and user data management.

The results of the analysis of SSO technology show that, despite its advantages in simplifying access, there are security and privacy issues. The use of blockchain can help solve these issues by providing a secure and reliable authentication mechanism.

Additionally, it is important to note that blockchain can be a fundamental element in solving the problems of identity conflicts that often arise in traditional SSO systems. Its ability to provide a single and reliable record of user information can help create a single point of authentication without the risk of a security breach.

In the context of developing the concept, it is important to consider cooperation with key players in the blockchain and identity space to ensure standardization and interoperability between different platforms and services.

In general, the introduction of blockchain into SSO technology can open up new opportunities for creating a safe, reliable, and innovative online environment.

References

[1] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7390–7404.

[2] K. Khorolska, et al., Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7426–7437.

[3] R. Marusenko, V. Sokolov, P. Skladannyi, Social Engineering Penetration Testing in Higher Education Institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147. doi: 10.1007/978-3-031-36118-0_96.

[4] R. Marusenko, V. Sokolov, V. Buriachok, Experimental Evaluation of Phishing Attack on High School Students, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 668–680. doi: 10.1007/978-3-030-55506-1_59.

[5] R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, Advances in Artificial Systems for Logistics Engineering, vol. 135 (2022) 583–594. doi: 10.1007/978-3-031-04809-8_53.

[6] P. Yawalkar, et al., Integrated Identity and Auditing Management Using Blockchain Mechanism, Measurement: Sensors 27 (2023). doi: 10.1016/j. measen.2023.100732.

[7] L. Stockburger, et al., Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation, Blockchain: Research and Applications 2(2) (2021). doi: 10.1016/j.bcra.2021. 100014.

[8] SSO Benefits. SSO Login: Key Benefits and Implementation (2016). URL: https:// auth0.com/blog/sso-login-key-benefits-and-implementation/

[9] M. Ahmed, M. El-Gendi, M. El-Khodar, Single Sign-On: A Critical Analysis of Security and Privacy (2019).

[10] D. Vujičić, D. Jagodić, S. Ranđić, Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview, 17th International Symposium Infoteh-Jahorina (INFOTEH) (2018) 1–6. doi: 10.1109/infoteh.2018.8345547.

[11] Y. Ezawa, et al., Designing Authentication and Authorization System with Blockchain, 14th Asia Joint Conference on Information Security (2019) 111–118. doi: 10.1109/asiajcis.2019.00006.

[12] W. Ao, et al., A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography, 2nd International Conference on Computer and Communication Engineering Technology (CCET) (2019) 90–95. doi: 10.1109/ccet48361.2019.8989361.

[13] MultiChain | Open Source Blockchain Platform. URL: https://www.multichain. com

[14] K. Sultan, U. Ruhi, R. Lakhani, Conceptualizing Blockchains: Characteristics and Applications, 11th IADIS International Conference on Information Systems (2018) 49–57.

[15] V. Poberezhnyk, I. Opirskyy, Developing of Blockchain Method in Message Interchange Systems, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems Vol. 3421 (2023) 148–157.

[16] V. Poberezhnyk, V. Balatska, I. Opirskyy, Development of the Learning Management System Concept based on Blockchain Technology, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 143–156.

[17] M. Wurzenberger, et al., Analysis of Statistical Properties of Variables in Log Data for Advanced Anomaly Detection in Cyber Security, Comput. Secur. 137 (2024). doi: 10.1016/j.cose.2023. 103631.

[18] J. Li, R. Zhang, J. Liu. ConLBS: An Attack Investigation Approach Using Contrastive Learning with Behavior Sequence, Sensors 23(24) (2023). doi: 10.3390/s23249881.

[19] CAPEC-161: Infrastructure Manipulation (2018). URL: https://capec.mitre.org/ data/definitions/161.html

[20] CAPEC-268: Audit Log Manipulation (2018). URL: https://capec.mitre.org/ data/definitions/268.html

[21] V. Maksymovych, et al., Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs, Appl. Sci. 12(3) (2022). doi: 10.3390/app12031519.

[22] V. Maksymovych, et al., Combined Pseudo-Random Sequence Generator for Cybersecurity, Sensors 22(24) (2022). doi: 10.3390/s22249700.

[23] O. Harasymchuk, et al., Generator of Pseudorandom bit Sequence with Increased Cryptographic Security, Metallurgical and Mining Industry 5 (2014) 25–29.

[24] M. Touloupou et al., Benchmarking Blockchains: The case of XRP Ledger and Beyond, Hawaii International

Conference on System Sciences. (2022). doi: 10.24251/hicss.2022.730.

[25] D. Perez, J. Xu, B. Livshits, Revisiting Transactional Statistics of High-scalability Blockchains, IMC '20: ACM Internet Measurement Conference (2020). doi: 10.1145/3419394.3423628.