

**ANALYSIS OF THE CAPABILITIES OF BLOCKCHAIN TECHNOLOGY
IN DATA MANAGEMENT**

Jakhongirbek Khabibullaev

*Tashkent University of Information Technologies
named after Muhammad Al-Xorazmiy,*

Norkuvvat Chunaev

*Tashkent University of Information Technologies
named after Muhammad Al-Xorazmiy.*

Annotation: *This paper discusses the issues of using blockchain technology for user authorization, such as limited scalability, high usage costs, limited interoperability, insufficient protection against cyberattacks, security and privacy issues, limited legal regulation, and low user awareness. The article describes ways to address these challenges, such as improving scalability, optimizing resource usage, developing interoperability standards, employing additional security measures, ensuring data confidentiality, creating new legal norms, and promoting user technical literacy. Using blockchain technology in user authorization can offer significant advantages, but it requires a thorough analysis of the problems, the development of appropriate solutions, and the provision of high levels of security and privacy when working with blockchain networks.*

Keywords: *blockchain technology, authorization, issues, solutions, security, privacy, interoperability, scalability.*

Introduction

Blockchain technology can be used for data management in various fields, including finance, logistics, healthcare, government, and others.

In the context of data management, blockchain can be used to create a distributed database that stores information without centralized control. Each participant in the network has a copy of the database and can add new records or verify existing ones.



Each record in the blockchain is protected by a cryptographic signature, making it immutable and impossible to hack. Thanks to this, data can be easily verified and traced back to its source, increasing transparency and reducing the possibility of manipulation.

The use of blockchain in data management can offer numerous advantages. For example, blockchain can help accelerate data processing and reduce data storage costs. It can also be used to ensure secure data exchange between network participants.

Additionally, blockchain can be beneficial in managing confidential data. Blockchain technology can provide secure access to confidential data, such as medical information, only to those with appropriate permissions.

Overall, the application of blockchain technology in data management can help improve the reliability, security, and transparency of data processing, which is an important factor in many areas of activity.

Data management is the process of collecting, storing, processing, and using data within an organization. The goal of data management is to ensure the correct use of data to support business processes, decision-making, and the achievement of organizational objectives.

Data management includes the following stages:

Data Collection: Gathering data from various sources, including both internal and external sources.

Data Storage: Storing data in secure repositories, such as databases or cloud platforms.

Data Processing: Processing data to extract the required information. This stage includes data transformation, aggregation, analysis, exploration, and more.

Data Usage: Using data for decision-making, supporting business processes, identifying trends, forecasting, and so on.

Data Protection: Ensuring data security and confidentiality in accordance with legislation and organizational policies.



Data Lifecycle Management: Planning, deployment, support, and decommissioning of data.

Data management involves using technologies, methodologies, and processes to ensure the efficient use of data and to mitigate the risks associated with their use. Additionally, data management includes managing metadata (data that describes other data) and data quality management.

Data management may also include processes for cleaning data from errors and duplicates, as well as establishing rules for data formatting and standardization. These processes are essential for ensuring data quality and proper use in business processes and decision-making. Overall, data management is a crucial component of managing an organization's information resources and serves as the foundation for effective business operations.

Advantages of applying blockchain in data management. The application of blockchain technology in data management can bring many advantages, including:

Decentralization. Decentralization in blockchain technology means that information is stored across multiple nodes in the network, and each node has access to this information. This ensures a more decentralized data management process and reduces dependency on centralized repositories, such as central servers and databases.

The concept of decentralization in blockchain technology is based on the principle of distribution. This means that each node in the network stores a copy of all the information in the block chain, ensuring high availability and system resilience.

Blockchain reduces the risks associated with a single point of failure and ensures a more reliable data management process, as each node in the network verifies and confirms every transaction. This makes data manipulation within the block chain impossible and reduces the risks of hacking and breaches.

Decentralization also provides a more transparent data management process, as each node has access to all the information in the block chain. This eliminates the need for intermediaries and increases the trust of participants in the data management process.



Overall, decentralization in blockchain technology ensures a more decentralized, reliable, transparent, and secure data management process, which can bring numerous advantages in various fields of activity.

Security. Blockchain uses cryptographic methods to protect data, making it reliable and resistant to hacking. Each block in the blockchain contains the hash code of the previous block, which ensures the immutability of the chain and prevents the possibility of manipulating data in past blocks.

Additionally, blockchain employs encryption algorithms that safeguard information from unauthorized access. Data in blockchain technology is stored in a distributed format, which reduces risks associated with a single point of failure and makes it impossible to hack the entire system.

Blockchain technology also uses digital signatures that allow for the authentication of data and its source. This provides a high degree of trust and protects against possible fraudulent schemes.

Thanks to this high level of security, blockchain technology can be used in various fields such as finance, medicine, logistics, government, and so on. For example, in the financial sector, blockchain can ensure the security and transparency of transaction processes, while in medicine it can protect patients' personal data.

Overall, blockchain technology provides a high level of data security, making it one of the most reliable and secure technologies for data management.

Transparency. Blockchain ensures transparency in the data management process, as every node has access to all the information in the blockchain.

Each block in the blockchain contains information about the transactions that have occurred within the network. Every participant in the network can view and verify each transaction and confirm its authenticity. This makes the data management process more transparent and allows network participants to better control their data.

Blockchain also provides transparency in terms of data accounting. The blockchain contains information about every change made to the data, which allows network participants to better monitor the data and track its history of modifications.



Transparency in blockchain increases trust among network participants and reduces the risks of potential fraudulent schemes. Additionally, blockchain technology can be used to ensure transparency in various areas such as voting, elections, government activities, and so on.

For example, in the government sector, blockchain can be used to ensure the transparency of the voting process and vote counting. Every network participant will be able to confirm that their vote was counted, which will increase trust in the voting process and reduce the possibility of fraud.

Blockchain provides high reliability and fault tolerance because it is distributed across many nodes, ensuring high availability and resilience. In a blockchain network, each node is a copy of the blockchain containing all information about transactions and data changes in the network. This ensures the reliability and fault tolerance of the blockchain network because if one node fails, the information does not disappear and remains available to other nodes. As a result, the blockchain network becomes more accessible and fault-tolerant.

Moreover, blockchain uses cryptographic methods to protect data, making it reliable and resistant to hacking. Each block in the blockchain contains the hash of the previous block, ensuring the reliability and integrity of the data in the network. If data in one block is altered, it will immediately be noticed by all network participants, who can reject this block as invalid.

Thus, blockchain ensures high reliability and fault tolerance, making it attractive for use in various fields where reliability and data availability are critical. For example, in the financial sector, blockchain can provide strong data protection and transaction reliability, which will increase market participants' trust and reduce the risks of potential fraud.

Cost Reduction. Using blockchain can reduce transaction and data management costs because it allows the elimination of intermediaries and automates processes through smart contracts.

In traditional data management and financial systems, intermediaries such as banks, government agencies, or intermediary companies are needed, which increases



the costs of transactions and data management. Blockchain allows the exclusion of intermediaries in the process, thus reducing transaction and data management costs.

Moreover, blockchain allows the automation of processes through smart contracts. Smart contracts are software codes that execute automatically when certain conditions are met. Smart contracts can be used to automate processes and reduce data management costs. For example, in the financial sector, smart contracts can be used for automatic transaction execution and management of financial flows without the need to involve intermediaries.

Data Privacy. Blockchain can ensure data privacy by encrypting information and controlling access to it. Data encryption in blockchain is performed using cryptographic methods that protect information from unauthorized access and forgery. In the blockchain network, each block contains a unique code, which is the result of hashing the data within that block.

If the data in a block changes, the code will also change, which will immediately become noticeable to all network participants. This ensures the reliability and integrity of data in the network.

Moreover, blockchain can enforce access control to data. Each network participant has a unique identifier that defines their access rights to the data within the blockchain network. This helps ensure data privacy and protects it from unauthorized access.

For example, in the medical field, blockchain can be used to store and transfer confidential medical data of patients, such as medical histories, test results, and more. Data encryption and access control help protect the confidentiality of medical data and ensure its secure transfer between doctors and patients.

Thus, blockchain can ensure data privacy through encryption and access control. This makes it attractive for use in various fields where protecting confidential data is critical, such as healthcare, finance, and others. Thanks to reduced costs in data management and financial operations, blockchain can lead to lower prices for goods and services, making them more accessible to consumers. This can increase market competition and improve the quality of goods and services.



Data Immutability. Blockchain ensures data immutability because each block is linked to the previous block through a hash function, making it impossible to alter data in past blocks.

A hash function is an algorithm that converts data of arbitrary length into a fixed-length string called a hash code. The hash function is used in blockchain technology to link blocks into a chain. Each block contains the hash code of the previous block, which guarantees the immutability of data in the chain.

If data in a block change, the hash code will also change, which will affect all subsequent blocks in the chain. This makes data tampering in previous blocks impossible and ensures data immutability in the blockchain network.

Data immutability is especially important in fields requiring a high degree of data accuracy, such as finance, where transaction data must be precise and unchangeable. It is also crucial in fields related to security and control, such as healthcare, where the inability to tamper with medical data is critically important.

Here is a table comparing some blockchain platforms:

Table 1

Comparison of Some Blockchain Platforms

Platform	Scalability	Transaction Processing Speed	Privacy Level
Ethereum	Medium	Medium	Low
Hyperledger Fabric	High	High	High
Corda	High	Very High	High

Disadvantages of Using Blockchain in Data Management. Despite the analyzed advantages, the blockchain technology itself, like any other, has its own drawbacks and limitations. Let us consider some of them:

Limited Scalability. The limited scalability of blockchain is related to the fact that each node in the network must process and store all the data transmitted through the network. This means that as the number of nodes and the volume of data to be processed increases, scalability issues arise.



In the financial sector, data volumes can be enormous, so blockchain networks may face scalability problems. For example, Bitcoin can process only about 7 transactions per second, which is insufficient to handle a large number of transactions in the financial sector.

However, there are technical solutions to increase the scalability of blockchain networks, such as improvements in consensus algorithms, parallel data processing, and the use of multi-layer networks. For example, Bitcoin's second-layer network — the Lightning Network — allows for fast and cheap micro-transactions, which can significantly increase the network's scalability.

High Energy Consumption. When blockchain networks operate, a large amount of energy is used to process transactions and create new blocks. This is because each node in the network must perform complex computations to verify transactions and generate new blocks.

This can become a problem from both an environmental and cost perspective. The high energy consumption of blockchain networks can lead to increased carbon dioxide emissions and negatively impact the environment. Additionally, the energy demands may make blockchain technology inefficient and uneconomical for some applications.

However, there are various studies and developments aimed at reducing the energy consumption of blockchain networks. For example, using more efficient consensus algorithms, such as Proof of Stake, can significantly lower the energy consumption of blockchain networks. Furthermore, new solutions are emerging in the form of green blockchain networks that use renewable energy sources, such as solar and wind power, to run their nodes.

Low Transaction Processing Speed. Blockchain networks can be slow in processing transactions because each node must confirm and verify the transaction before it is recorded in the next block of the chain. This process can take several minutes or even hours, depending on the network's load.



This can be problematic in applications that require high transaction processing speed. For example, in the financial sector, fast transactions can be critically important, especially during periods of high trading volume.

However, technical solutions are being developed to improve transaction processing speeds in blockchain networks. For example, many developers are working on mechanisms such as sharding and sidechains, which can improve the throughput of blockchain networks and increase transaction processing speeds. Additionally, consensus algorithms like Proof of Stake can also provide faster transaction processing.

Complexity of Use. Blockchain is a relatively new technology that requires certain knowledge and skills for its use. Working with blockchain networks requires an understanding of cryptography basics, distributed ledger technology, and transaction processing procedures. This can be challenging for ordinary users who lack experience with technical systems.

Moreover, using blockchain may require specialized programming skills and network management abilities, which can be difficult for beginners. This can hinder the adoption and widespread use of blockchain technology in society.

However, efforts are underway to simplify blockchain technology usage, such as developing more user-friendly interfaces and creating convenient tools for blockchain network development and management.

Low Level of Privacy. Public blockchain networks, such as Bitcoin, are characterized by an open structure where all participants can view transactions and data in the blockchain. This means that data in such networks may be accessible to the public, which is not always desirable, especially for business clients and other organizations that require a higher level of privacy.

However, there are also private blockchain networks that provide a higher level of data privacy. In such networks, access to data is controlled and restricted, and only authorized participants can view or modify the data. These private networks may be more suitable for use in business and other fields where data confidentiality is critically important.



Immutability of Data. The inability to change data stored in a blockchain network can be a drawback in certain situations. For example, if incorrect data is entered by mistake, it remains immutable and cannot be changed. This can also be problematic in cases where data needs to be updated, such as changes in regulatory rules or corrections of errors in contracts.

However, blockchain networks have mechanisms to address this issue. For example, networks based on blockchain smart contracts may include data modification functions that can be invoked only by certain users with the appropriate access rights. There are also blockchain networks with multi-signature features, where data changes can be made only with the consent of several network participants. Overall, immutability is an inherent characteristic of blockchain technology that ensures data reliability and integrity in the network.

Conclusion

This work has reviewed the advantages and disadvantages of using blockchain technology in data management, as well as the challenges and solutions related to its use in user authorization. It was identified that blockchain networks may face problems such as scalability issues, high operational costs, limited interoperability, insufficient protection against cyberattacks, security and privacy concerns, limited legal regulation, and low user awareness.

Solutions proposed include using segmented blockchain networks, cloud computing, protocol standardization, multi-factor authentication, private blockchain networks, and user education. It is important to consider technical, economic, and legal aspects while ensuring a high level of security and privacy when working with blockchain networks.