Enhancing Data Security by Blockchain Technology: Investigating The Effective Execution of Digital Transformation Initiatives in Indonesia

Tito Wira Eka Suryawijaya [1], Mochammad Eric Suryakencana Wibowo [2]

[1] [2] Universitas Dian Nuswantoro
[1] tito.wes@aol.com, [2] ericsuryaa@gmail.com

ABSTRACT

Digital transformation has affected various aspects of our lives, starting from the way we communicate, work, shop, and do business. In Indonesia, the use of blockchain technology for data security has great potential to increase security and transparency in data management. The use of blockchain technology for data security is an interesting and innovative solution. However, amidst the great potential benefits, the use of blockchain technology also carries risks and challenges that cannot be ignored. The research methodology was carried out using a qualitative descriptive approach by analyzing data and information obtained from reliable sources such as journals, books, articles, reports and official documents related to digital transformation and the implementation of blockchain technology in Indonesia. In addition, this research also involves interviews with experts and practitioners in the field of technology and digital transformation in Indonesia. The concept of data security includes three main aspects: confidentiality, integrity and availability of data. Data confidentiality relates to the privacy and confidentiality of data from unauthorized parties. Information categorized as confidential includes personal data, health data, financial data, company confidential data, and government data. The Indonesian government has paid attention to this potential and issued regulations and strategies to increase the use of blockchain technology in government and private sector operations. Several projects using blockchain technology in Indonesia have been carried out, such as verifying and validating educational certificates, storing medical data, and using cryptocurrency as a means of payment.

Keywords: *digital transformation, blockchain, data security, Indonesia*

Transformasi digital telah mempengaruhi berbagai aspek kehidupan kita, mulai dari cara kita berkomunikasi, bekerja, berbelanja, dan berbisnis. Di Indonesia, penggunaan teknologi blockchain untuk keamanan data memiliki potensi yang besar untuk meningkatkan keamanan dan transparansi dalam pengelolaan data. Penggunaan teknologi blockchain untuk keamanan data merupakan sebuah solusi yang menarik dan inovatif. Namun, di tengah potensi manfaat yang besar, penggunaan teknologi blockchain juga memiliki risiko dan tantangan yang tidak dapat diabaikan. Metodologi penelitian dilakukan dengan menggunakan pendekatan deskriptif kualitatif dengan menganalisis data dan informasi yang diperoleh dari sumber-sumber terpercaya seperti jurnal, buku, artikel, laporan, dan dokumen resmi yang berkaitan dengan transformasi digital dan implementasi teknologi blockchain di Indonesia. Selain itu, penelitian ini juga melibatkan wawancara dengan para ahli dan praktisi di bidang teknologi dan transformasi digital di Indonesia. Konsep keamanan data mencakup tiga aspek utama: kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan data berkaitan dengan privasi dan kerahasiaan data dari pihak-pihak yang tidak berkepentingan. Informasi yang dikategorikan sebagai rahasia meliputi data pribadi, data kesehatan, data keuangan, data rahasia perusahaan, dan data pemerintah. Pemerintah Indonesia telah memperhatikan potensi ini dan mengeluarkan peraturan dan strategi untuk meningkatkan penggunaan teknologi blockchain dalam operasi pemerintah dan sektor swasta. Beberapa proyek yang menggunakan teknologi blockchain di Indonesia telah dilakukan, seperti memverifikasi dan memvalidasi ijazah pendidikan, menyimpan data medis, dan menggunakan mata uang kripto sebagai alat pembayaran.

Kata-Kata Kunci: *digital transformation, blockchain, data security, Indonesia*

Introduction

Digital transformation has affected various aspects of our lives, starting from the way we communicate, work, shop, and do business (Panggabean, 2022). This is because digitization has made it easier and faster to collect, store and process data. In the digital era, data is one of the most important assets for organizations and individuals. Data is a source of information that is used to make important decisions, generate added value for companies, and drive innovation (Jurnal Entrepreneur, 2022). Therefore, data security is very important and critical in digital transformation. In Indonesia, digital transformation is experiencing rapid development. The Indonesian government has issued various initiatives to encourage digital transformation in Indonesia, such as the 1000 Digital Startup National Initiative, the 100 Smart City National Movement, and others (Saefudin, 2022). However, even though digital transformation can provide many benefits to the Indonesian economy, there are security risks that must be faced. The problem of data security has become a very serious problem worldwide. Data can be accessed by unauthorized parties and used for harmful purposes. Some examples include identity theft, fraud, using data to commit crimes, and others. Therefore, a strong security system is needed to protect data from these risks (Situmeang, 2021). In this context, blockchain technology offers an interesting solution to the problem of data security in digital transformation. Blockchain is a decentralized technology that allows transactions between two parties who do not trust each other without involving a third party. The data in the blockchain is stored decentralized across the network, so that it cannot be changed by one party without the consent of the entire network. Blockchain can also increase transparency and accountability in data management.

Data security in digital transformation is very important because data can be accessed by unauthorized parties and used for harmful purposes (Nugroho et al., 2021; Situmeang, 2021). In this context, blockchain technology can improve data security in several ways First, the blockchain allows data to be stored in a decentralized and encrypted manner, thereby increasing data security. Because data is not stored centrally, it is difficult for people to steal data or change it without the consent of the entire blockchain network. Second, in blockchain technology, every transaction and data can be verified by all parties involved. This increases transparency and reduces the risk of fraud. Thirdly, the verification and validation process in blockchain technology is very efficient and fast, as it does not require intermediaries or third parties.

However, the use of blockchain technology also carries some risks, such as dependency on the technology, security risks, and scalability limitations. If the blockchain technology experiences problems or failures, the data and transactions stored in the blockchain will also be affected. In addition, security issues are also a major risk in using blockchain technology for data security. Even though blockchain technology is considered very safe, it does not rule out the possibility of attacks that can successfully penetrate its security system. Several types of attacks that can occur on the blockchain include 51% attacks, double-spending attacks, sybil attacks, and others. A 51% attack occurs when an attacker manages to control more than 50% of the power of the blockchain network (Trinowo, 2020). By controlling more than 50% of the power of the network, attackers can fake transactions and change the records of transactions that have been done previously. This can undermine data integrity and threaten data security in the blockchain. A double-spending attack is an attack where an attacker tries to make the same transaction twice using the same crypto asset. In the blockchain, every transaction must be verified and approved by the entire network. However, in a double-spending attack, the attacker tries to fake a transaction and send the same cryptocurrency to two different addresses simultaneously. This can result in significant financial loss for the party receiving the crypto asset. A sybil attack is an attack in which an attacker tries to take over the blockchain network by creating multiple fake identities. In a sybil attack, the attacker creates many fake identities that appear to originate from many different network nodes. This can make attackers have greater power in the network and can falsify transactions and data (Bashar et al., 2022).

Apart from security risks, the use of blockchain technology in digital transformation also has limitations in terms of scalability. Blockchain technology is limited in the scale and capacity of transactions that can be handled. This becomes a challenge when used in implementing large and complex digital transformations (Lin & Liao, 2017; Bashar et al., 2022). Although there are several blockchain technologies developed to increase scalability, further research and development is still needed to increase the capacity of transactions that can be handled.
Although the use of blockchain technology has some risks and limitations, this technology can provide significant benefits for data security in digital transformation. In implementing blockchain for data security, it is important to choose the type of blockchain that best suits the needs of the organization and consider the benefits and risks associated with using blockchain. In addition, it is also important to consider the need for integration with existing systems and the ability to overcome the limitations of blockchain technology (Lin & Liao, 2017; Liu et al., 2019).

In the context of digital transformation in Indonesia, the use of blockchain technology for data security has great potential to increase security and transparency in data management. However, the use of blockchain technology in digital transformation in Indonesia is still relatively new and limited. A number of companies and institutions in Indonesia are starting to consider using blockchain in their business, but many still do not understand the full potential and drawbacks of this technology (Liu et al., 2019). Apart from that, there are still different views between regulators and industry players regarding the use of blockchain and cryptocurrency (Manurung & Wijoyo, 2021). Several regulators in Indonesia such as Bank Indonesia and the Financial Services Authority (OJK) have a skeptical view of the use of cryptocurrencies and are tightening related regulations. This can affect the development of the blockchain ecosystem in Indonesia and hinder the adoption of this technology (Centre for Innovation Policy and Governance, 2018).

Apart from that, technical and infrastructure issues are also a challenge for blockchain development in Indonesia. Availability of adequate infrastructure, availability of human resources with expertise in blockchain, as well as support from financial institutions and government are important factors in the development of blockchain technology. The technical problems that arise in the development of blockchain in Indonesia include limited network scale, dependence on internet networks that are not always stable, and limitations of the technology used in blockchain transactions. Nonetheless, blockchain technology has great potential to improve data security in digital transformation in Indonesia. Various industries and sectors involved in digital transformation, such as banking, logistics and government, can take advantage of this technology to increase the security of their data. In the banking sector, blockchain can be used to secure financial transactions and minimize the risk of fraud and financial crimes. In the logistics sector, blockchain can be used to ensure the safety and reliability of goods delivery and minimize the risk of loss or damage to goods. In the government sector, blockchain can be used to increase transparency and accountability in data management, as well as minimize the risk of corruption.

However, the implementation of blockchain in digital transformation in Indonesia needs to be done carefully and considering various factors. Some factors to consider include using the right technology, choosing a reliable blockchain vendor or platform, and understanding data security and privacy. In addition, there needs to be cooperation between regulators, industry players, and academics to ensure successful and sustainable adoption of blockchain in Indonesia. In this regard, it is important for leaders and decision makers in Indonesia to understand the potential and risks associated with blockchain technology, as well as make the necessary efforts to support the development of the blockchain ecosystem in Indonesia. This can be done through investing in blockchain research and development, establishing regulations that facilitate the use of blockchain, and providing adequate infrastructure and human resources (Bashar et al., 2022).

In the context of digital transformation in Indonesia, the use of blockchain technology for data security is an interesting and innovative solution. However, amidst the huge potential benefits, the use of blockchain technology also brings risks and challenges that cannot be ignored (Argani & Taraka, 2020; Bashar et al., 2022). Therefore, in this research, we will discuss and analyze in depth the benefits and risks of using blockchain technology in increasing data security in digital transformation in Indonesia. Through this research, we hope to provide new insights and contribute to the development of effective and efficient data security solutions in Indonesia.

Research Methods

The research methodology was carried out using a qualitative descriptive approach. This research was conducted by analyzing data and information obtained from trusted sources such as journals, books, articles, reports and official documents related to digital transformation and the implementation of blockchain technology in Indonesia. In addition, this research also involved interviews with experts and practitioners in the field of technology and digital transformation in Indonesia (Kim et al., 2017).

The initial phase of the research was carried out by collecting and reviewing literature related to digital transformation and blockchain technology in Indonesia, as well as analyzing regulations and strategies that have been issued by the Indonesian government regarding the implementation of blockchain technology. After that, the researchers conducted interviews with experts and practitioners in the field of technology and digital transformation to get a broader and deeper perspective on the implementation of blockchain technology in Indonesia. The results of this research are then analyzed and compiled into a conclusion regarding the potential and challenges of implementing blockchain technology in digital transformation in Indonesia, as well as recommendations that can be made by the government and the private sector to maximize the benefits of blockchain technology in digital transformation in Indonesia (Moleong, 2014) .

Result and Dicussion

The development of digital technology has made it possible for data to be accessed, shared and stored easily and efficiently. However, this development also raises increasingly complex and diverse data security risks (Bashar et al., 2022). Data security is important because data is a very valuable asset for organizations and individuals. Data can be used to influence decisions, generate added value, and provide a competitive advantage. Therefore, data security must be taken seriously and integrated into all aspects of digital transformation (Manurung & Wijoyo, 2021; Maulani et al., 2023).

The concept of data security includes three main aspects: confidentiality, integrity, and availability of data. Data confidentiality relates to the privacy and confidentiality of data from unauthorized parties. Information that is categorized as confidential includes personal data, health data, financial data, company confidential data, and government data (Centre for Innovation Policy and Governance, 2018). Disclosure of confidential information can adversely affect the interests of individuals or organizations. Therefore, efforts to maintain data confidentiality are very important in digital transformation (Panggabean, 2022). Data integrity is the quality of data that is maintained so that it remains correct, intact and valid. Data integrity includes data validity, data consistency, and data integrity. Loss of data integrity can result in data that is inaccurate, not true to reality, and results in wrong decisions. Therefore, maintaining data integrity is very important in digital transformation (Universitas Islam Indonesia, 2021).

Availability of data relates to the ability to access data easily and quickly by authorized parties. Availability of data is very important in the era of digitalization which is increasingly connected and requires data that is continuously updated. Low data availability can hamper business processes, interfere with decision making, and reduce organizational performance. Therefore, efforts to maintain data availability must be considered in digital transformation. In addition to the aspects of confidentiality, integrity and availability of data, the concept of data security also includes aspects of data reliability and speed. Data reliability relates to the accuracy and consistency of data used in business processes (Liu et al., 2019). Data speed relates to the ability to access data quickly and on time. In digital transformation, the reliability and speed of data becomes very important to ensure the right decision making and time efficiency.

Data security concept in digital transformation

In the era of growing digitalization, data is becoming the most valuable asset for organizations and individuals. Data is an important resource used to make the right decisions in business, help solve problems, identify trends, and improve operational efficiency. However, the use of digital technology also increases data security risks. Data security threats such as leakage, theft, manipulation and unauthorized use are increasing along with the development of technology. Therefore, the concept of data security is very important and crucial in the digitalization era (Lin & Liao, 2017).

The concept of data security includes three main aspects, namely confidentiality, integrity, and availability of data. Data confidentiality relates to maintaining data privacy from parties who are not entitled to access it. This includes preventing unauthorized access to data or unauthorized use of data (Centre for Innovation Policy and Governance, 2018). For example, a person's health data is very sensitive information and must be protected from unauthorized parties. Data integrity includes the authenticity and integrity of data processed and stored by the organization (Bashar et al., 2022). Data authenticity guarantees that data is not manipulated or changed without the knowledge or approval of the authorities. Data integrity guarantees that data is not damaged or lost during the process of storing or transmitting data. Data availability relates to data accessibility by authorized parties when needed. If data is not available when it is needed, the organization may lose business and customers may lose trust.

In digital transformation, the use of digital technologies such as cloud computing, big data, and internet of things (IoT) can increase organizational efficiency and productivity (Liu et al., 2019; Trinowo, 2020). However, the use of digital technology also increases data security risks. This emphasizes the importance of using the latest security technologies and implementing strict security practices in digital transformation. The application of the right security technology will ensure that important data and information are protected from unauthorized access or manipulation by unauthorized parties. In addition, the use of security technology will also help organizations comply with laws and regulations related to data security (Liu et al., 2019; Putra et al., 2019).

An effective data security strategy must include the use of appropriate security technologies, strict security procedures, security training for employees, and development of disaster recovery plans. Proper use of security technology includes the use of firewalls, data encryption, and multiple authentication technologies. A firewall is software or hardware that is used to limit access to a network and prevent attacks from unauthorized parties. Data encryption is the process of turning information into a secret code so that only authorized parties can read and access it. Two-factor authentication technology involves using two types of verification to confirm a user's identity before being allowed access to data or systems. An example is the use of passwords and codes sent to the user's mobile device (Lin & Liao, 2017; Jurnal Entrepreneur, 2022).

In addition to the right security technology, strict security procedures are also an important aspect of maintaining data security. This includes strict security policies, such as setting access rights and user control, as well as policies for using devices that are safe and updated regularly (Tashia, 2017). Security training for employees is also important to increase awareness of data security risks and help employees to recognize the signs of cyberattacks or other security threats. In addition, it is also necessary to develop a disaster recovery plan to deal with losses that may occur as a result of natural disasters or cyber attacks. The disaster recovery plan should include procedures to perform backup and restore *data*, system recovery, and business recovery. This plan must be tested and updated regularly to ensure that the organization is prepared for disasters or adverse events (Hoesada, 2023).

In the era of digital transformation, companies can face increasingly complex and increasing data security risks. Therefore, organizations must pay attention to the importance of data security in the use of digital technology. It is important to develop an effective data security strategy and continually update security technologies and practices to address existing risks. Thus, organizations can ensure data security and minimize risks to their business and reputation (Bashar et al., 2022).

Blockchain Technology: Definition, Characteristics and Advantages

Blockchain technology has been widely recognized in recent years, especially as the underlying technology behind cryptocurrencies such as Bitcoin (Azis et al., 2021). However, blockchain has much more potential than just being the basis for cryptocurrencies. Blockchain can be used for various other applications in various fields, such as banking, health, energy, and others. In the context of digital transformation, blockchain can also be used to improve data security in online transactions, centralized data processing, and digital data storage. One of the main advantages of blockchain technology is its ability to store and send data in a decentralized manner (Centre for Innovation Policy and Governance, 2018). This means that data is not centralized in one place, but spread across the network. Every time a transaction occurs, new data is added to the blockchain and stored at every connected network node. This means that data stored on the blockchain is much more secure than data stored centrally. If one node in the network has a problem or is attacked by hackers, data is still available on other nodes in the network (Liu et al., 2019; Argani & Taraka, 2020; Fazreen & Munajat, 2022).

Apart from that, the blockchain also has a strong encryption system. Any data stored on the blockchain is encrypted and can only be accessed by the person who has the correct encryption key. This ensures that data stored on the blockchain cannot be read by unauthorized parties, thereby increasing data security significantly. Blockchain also has a transparent nature which is very important in the context of digital transformation. Every transaction or block in the blockchain can be accessed and verified by all parties involved in the transaction. This means that transactions made on the blockchain can be monitored and verified by anyone, increasing trust and reducing the risk of fraud. In addition, the blockchain is also difficult to manipulate. Each block or transaction in the blockchain is linked to the previous and following blocks in chronological order (Lin & Liao, 2017; Azis et al., 2021). Every node in the network must approve and verify each new transaction before it is added to the blockchain. If there is an attempt to manipulate the data in one block, then the entire blockchain will be affected and will not be approved by other nodes in the network. Therefore, the blockchain is very safe from attempts to manipulate data by unauthorized parties.

The process of verifying and validating transactions in the blockchain is also very fast and efficient. This process does not require intermediaries or third parties such as banks or financial institutions, which can speed up transaction times and reduce costs associated with transactions. In the context of digital transformation, blockchain technology can be used to improve data security in online transactions. Today, many online transactions are carried out over networks that are vulnerable to hacker attacks. Personal data such as credit card numbers or other personal information can easily be stolen or hacked, causing financial and security losses. By using the blockchain, data stored on the network can be locked with a strong encryption system so that only people who have the encryption key can access and read the data. This means, data security can be significantly improved because only authorized parties can access data.

Apart from that, blockchain technology also allows data to be stored and shared in a safe and decentralized way (Pratiwi, 2022). In traditional systems, data is stored in a centralized database managed by one or several specific companies. This allows for greater security risks as the database can be accessed and manipulated by unauthorized persons. Blockchain also allows data to be stored in a decentralized manner. This means, data is not stored in a centralized point, but is stored across the blockchain network in a distributed manner. Thus, everyone connected to the network has the same copy of the stored data, and if one copy is subject to a cyber attack or other corruption, the other copy can still be accessed (AWS, 2023).

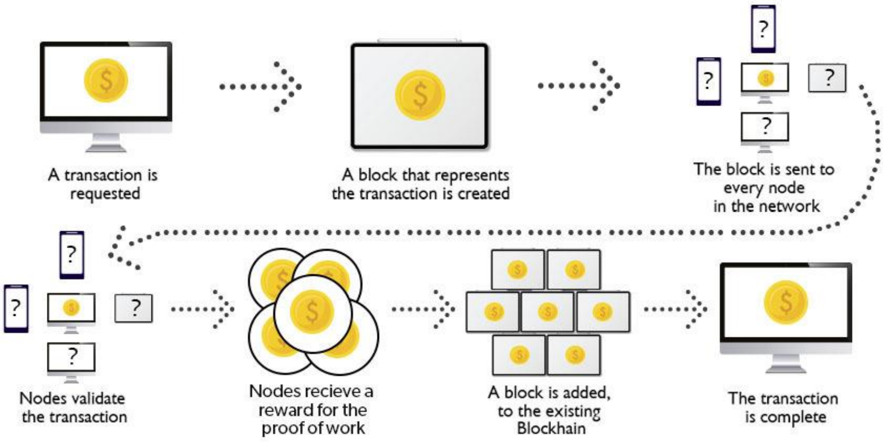
A transaction is requested
A block that represents the transaction is created
The block is sent to every node in the network
Nodes validate the transaction
Nodes recieve a reward for the proof of work
A block is added, to the existing Blockhain
The transaction is complete

Figure 1. Illustration of the Blockchain Framework

Source: Geeks for Geeks, 2023

Another advantage of blockchain technology is its ability to create high transparency in data processing. Each transaction or block in the blockchain is linked to the previous and subsequent blocks, making it difficult for unauthorized parties to manipulate the data. Thus, blockchain can help reduce the risk of fraud, and generate transparency and trust in the network. Not only that, blockchain technology can also be used in various sectors, including the financial, health, logistics, and others (Liu et al., 2019; AWS, 2023). For example, within the financial sector, blockchain can be used to increase transaction security and reduce costs associated with verification and validation processes. This can help reduce transaction costs and increase the speed of transaction completion. In the healthcare sector, blockchain can be used to strengthen medical data security and improve interoperability between different medical systems. Within the logistics sector, blockchain can be used to increase transparency and accountability in supply chains, which can help speed up the shipping process and reduce shipping costs (Pusat Inovasi Kota dan Komunitas Cerdas, 2021).

In addition, blockchain can also be used in IoT applications. The combination of blockchain and IoT can help improve security and privacy in processing data generated by IoT devices (Liu et al., 2019). For example, on the data collection system smart city, blockchain can be used to provide secure verification and validation of collected data. Even though blockchain offers many benefits, there are still some challenges that need to be overcome. One of the biggest challenges is the issue of scalability. In the blockchain, each transaction must be verified by the nodes in the network before being stored on the blockchain. This can slow down the process and increase transaction costs when the network is weak (Atmomintarso & Wirawan, 2021).

However, blockchain technology continues to experience significant development and performance improvements to date. Several innovations such as the new consensus algorithm and the use of side technologies such as*Lightning Network* has accelerated the process of verifying and validating transactions in the blockchain network, thereby reducing transaction costs and increasing the scale of use (Pluang, 2022). The use of blockchain technology in digital transformation is also not limited to the financial sector. Various industrial sectors are also starting to adopt blockchain technology to increase security and efficiency in their business processes. For example, in the logistics industry, blockchain technology can be used to track shipments more accurately and transparently. Data regarding goods delivery, starting from location, time, to delivery conditions, can be stored in the blockchain and accessed by all parties involved in the shipping process (Logistics Engineering, 2021; AWS, 2023).

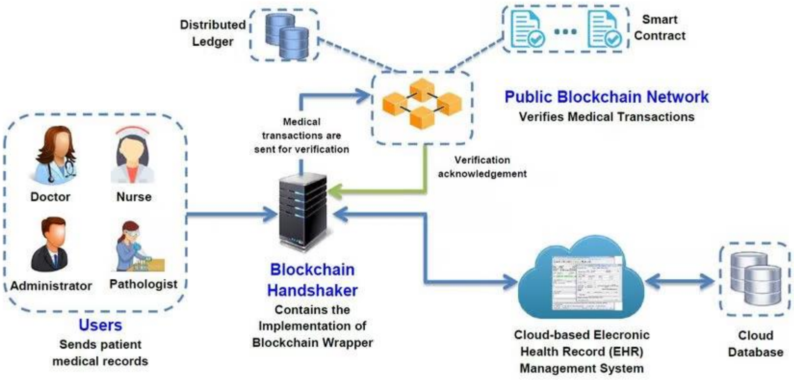
Distributed Ledger
Smart Contract
Public Blockchain Network
Verifies Medical Transactions
Medical transactions are sent for verification
Verification acknowledgement
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records
Blockchain Handshaker
Contains the Implementation of Blockchain Wrapper
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Figure 2. Blockchain for Health Sector

Source: AppMaster, 2023

Meanwhile, in the health sector, blockchain technology can be used to store and share patient medical data safely and encrypted. This can improve the security and privacy of patient medical data, as well as facilitate the process of sharing medical data between various parties involved in patient care. In Indonesia, several companies and institutions have started to adopt blockchain technology in their digital transformation. For example, Bank Indonesia (BI) has launched a blockchain-based digital payment system called Bank Indonesia Payment System (BI-PS). This system enables fast, safe and cost-effective payment transactions through blockchain technology (Bank Indonesia, 2020). Even though the use of blockchain technology is increasingly widespread in Indonesia, there are still some challenges and obstacles that need to be overcome. One of the main challenges is the lack of understanding and awareness about blockchain technology among the public and businesses. This can hinder the adoption of blockchain technology in various business sectors.

In addition, unclear and consistent regulations are also an obstacle to the use of blockchain technology in Indonesia. Even though BI has launched regulations regarding the use of blockchain technology, there are still many institutions and companies that do not fully understand and implement these regulations. However, even though there are still some challenges that need to be overcome, the use of blockchain technology in digital transformation in Indonesia continues to grow and shows great potential to improve security and efficiency in various industrial sectors (Bashar et al., 2022). With innovation and better understanding of blockchain technology, it is hoped that the use of this technology will be more widespread in the future.

Blockchain Implementation in Digital Transformation in Indonesia

In the era of digital transformation, the use of blockchain technology in Indonesia provides great potential in increasing data security and efficiency in various sectors (Argani & Taraka, 2020). The Indonesian government has launched various initiatives to strengthen the use of digital technology in the country, such as the use of blockchain technology for the verification and validation of educational certificates, medical data storage, and payment systems. Nonetheless, the implementation of blockchain technology in Indonesia still faces several challenges, such as unclear regulations, limited infrastructure, and a lack of understanding of blockchain technology (Centre for Innovation Policy and Governance, 2018).

One of the projects using blockchain technology in Indonesia is a solution for verifying and validating educational certificates (Argani & Taraka, 2020). The Indonesian government has worked with several blockchain companies to develop this solution. By using blockchain technology, the process of verifying and validating educational certificates can be carried out quickly and efficiently. This solution provides benefits for parties who require verification of educational certificates, such as those who are recruiting employees. The fast and accurate process of verifying educational certificates can also help reduce the risk of fraud in the recruiting process. Apart from that, blockchain technology is also used in storing medical data in several hospitals in Indonesia (Hoesada, 2023). By using blockchain technology, patients can access their medical data safely and conveniently, and doctors and hospitals can obtain medical data quickly and efficiently. Medical data security is very important in maintaining patient confidentiality and preventing manipulation or alteration of medical data. In the payment sector, blockchain technology is used in the use of cryptocurrency or tokens as a means of payment.

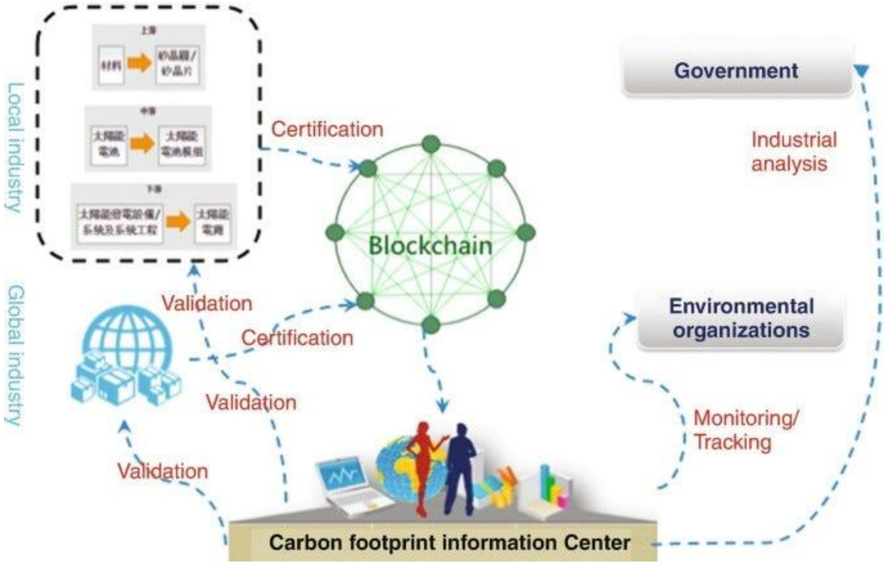

Figure 3. Blockchain Framework for Public Policy
Source: Liu et al., 2017

One example of the use of blockchain technology in payment systems in Indonesia is the Tokocrypto platform. This platform allows users to buy and sell cryptocurrencies easily and safely (Azis et al., 2021). In addition, the use of cryptocurrency can also facilitate international trade, because transactions using cryptocurrency can be carried out quickly and safely without the need for intermediaries. Although the use of blockchain technology in Indonesia offers many benefits, its implementation still faces several challenges. One of the challenges faced is unclear regulations such as regulations regarding taxes and data security (Atmomintarso & Wirawan, 2021; Budhijanto, 2023).

This condition can be confusing for companies wishing to adopt blockchain technology, as they are unsure about the tax implications and other legal aspects. Another challenge is that digital infrastructure is still limited in Indonesia, especially in remote areas. Fast and stable digital infrastructure is very important in adopting blockchain technology, because blockchain technology requires fast and stable internet access. The lack of adequate digital infrastructure can make it difficult to implement blockchain technology, which requires fast and stable internet access (Atmomintarso & Wirawan, 2021; Iswanto et al., 2022). This issue is of concern to the Indonesian government, and currently various efforts are being made to increase internet access in all regions of Indonesia. One of the initiatives undertaken is the Palapa Ring program, which aims to build internet network infrastructure throughout Indonesia. In addition, the government also plans to build a national data center to facilitate centralized and secure data storage.

Apart from infrastructure challenges, the lack of understanding of blockchain technology is also a problem in adopting this technology in Indonesia. Some people may still perceive blockchain as a technology that is too complex and difficult to understand (Maulani et al., 2023). To overcome this problem, the government and the private sector need to increase education and outreach campaigns about blockchain technology and its benefits to society. Training and courses on blockchain can be provided to students, students and the general public to increase understanding and awareness of this technology.

In addition, unclear regulations are also a challenge in adopting blockchain technology in Indonesia. Even though the Indonesian government has issued several regulations related to blockchain technology, there are still many regulations that are unclear and need to be clarified. Several things that need to be regulated include data security, consumer protection, and taxes (Nugroho et al., 2021; Pusat Inovasi Kota dan Komunitas Cerdas, 2021). Clear and transparent regulations will provide legal certainty and facilitate the use of blockchain technology in Indonesia.

To accelerate the adoption of blockchain technology in Indonesia, the government and the private sector need to continue to encourage and support the use of this technology. Governments can provide incentives for companies and startups developing blockchain solutions, such as lower taxes or easier access to funding (Atmomintarso & Wirawan, 2021; Saefudin, 2022). In addition, the government can work with blockchain companies in developing blockchain solutions that suit the needs of the Indonesian people. Meanwhile, the private sector can also play an active role in adopting blockchain technology. Enterprises can develop blockchain solutions to improve data security, improve operational efficiency, and reduce costs. In addition, companies can adopt blockchain technology in payment and trading systems (Sutandi, 2018).

Overall, the implementation of blockchain technology in digital transformation in Indonesia has great potential to improve data security and operational efficiency (Trinowo, 2020; AWS, 2023; Maulani et al., 2023). Even though there are still some challenges, such as limited infrastructure, lack of understanding of blockchain technology, and unclear regulations, the government and the private sector can work together to overcome these challenges and accelerate the adoption of blockchain technology in Indonesia (Nugroho et al., 2021). With the adoption of the right blockchain technology, Indonesia can become an important player in the global blockchain ecosystem and strengthen its position as a country undergoing rapid digital transformation. Apart from the challenges faced, the implementation of blockchain technology in digital transformation in Indonesia also has the potential to provide great benefits. The use of blockchain technology in digital transformation can increase efficiency, transparency and data security in various sectors, such as the financial, health and education sectors (Pluang, 2022). The implementation of blockchain technology can also help increase citizen involvement in government processes, such as through a secure and transparent electronic voting system. The Indonesian government has also realized the huge potential of blockchain technology in digital transformation. The Indonesian government has committed to increasing the use of blockchain technology in various sectors, such as in building Smart City and digital payments. The Indonesian government has also collaborated with various blockchain technology companies in promoting the use of blockchain technology in Indonesia (Saefudin, 2022).

In addition, a number of research and educational institutions have also begun to develop research and teaching on blockchain technology in Indonesia. It is hoped that this will increase the understanding and skills of the Indonesian people in utilizing blockchain technology to face digital transformation challenges (Pusat Inovasi Kota dan Komunitas Cerdas, 2021; Iswanto et al., 2022). In a global context, the implementation of blockchain technology in digital transformation is becoming a growing trend worldwide. Developed countries, such as the United States and China, have developed initiatives and projects to use blockchain technology in various sectors. Indonesia needs to continue to develop and increase the use of blockchain technology in digital transformation so that it is not left behind by other countries (Liu et al., 2019). Overall, the implementation of blockchain technology in digital transformation in Indonesia has great potential to improve data security and efficiency, as well as enable the creation of new innovations in various sectors.

Despite facing challenges, the Indonesian government and various stakeholders need to continue to develop and promote the use of blockchain technology so that Indonesia can fully benefit from digital transformation (Centre for Innovation Policy and Governance, 2018; Panggabean, 2022).

Benefits and Risks of Using Blockchain for Data Security

The use of blockchain technology in enhancing data security has a number of significant benefits. First, this technology provides better data security compared to conventional technology. In blockchain technology, data is stored in a decentralized and encrypted manner, thereby increasing security and minimizing the risk of tampering or manipulating data. The data stored in the blockchain also has a high level of integrity, because every transaction and data entered into the blockchain cannot be changed or deleted without the consent of all parties involved (Pluang, 2022). On the other hand, blockchain technology also provides higher transparency in every transaction or data that is made (Panggabean, 2022; Maulani et al., 2023). Because all transactions and data can be verified by all parties involved, the risk of fraud or fraud can be significantly reduced. This can provide benefits for various sectors, such as the financial or logistics sector, which require accurate and reliable transactions or data. Blockchain technology also provides efficiency and speed in the data verification and validation process (Lin & Liao, 2017; Fazreen & Munajat, 2022). In blockchain technology, every transaction can be verified quickly and efficiently, without the need to go through intermediaries or third parties. This can reduce costs and time required in the data verification and validation process, as well as speed up transaction time. However, the use of blockchain technology also has some risks that need to be considered. One of them is the dependence on the blockchain technology itself. If this technology encounters a problem or failure, then the data and transactions stored in the blockchain will also be affected. In addition, security risks are also a major concern in the use of blockchain technology (Bashar et al., 2022). Even though this technology is claimed to be safe, it does not rule out the possibility of attacks that can successfully penetrate its security system (Lin & Liao, 2017; Liu et al., 2019). Scalability limitations are also a challenge in the use of blockchain technology. This technology has limitations in the scale and capacity of transactions that can be handled. This becomes a challenge when used in implementing large and complex digital transformations (Maulani et al., 2023). Therefore, it is necessary to carry out careful planning and management in the use of blockchain technology in implementing digital transformation (Panggabean, 2022). Overall, the use of blockchain technology in enhancing data security provides significant benefits, such as better data security, transparency, efficiency, and speed. However, the use of blockchain technology also comes with risks, such as dependency on the technology, security risks, and scalability limitations. Therefore, it is necessary to carry out careful planning and management in the use of blockchain technology in implementing digital transformation in Indonesia (Liu et al., 2019; Panggabean, 2022).

Conclusion

In the era of rapid digital transformation, the use of blockchain technology has great potential to improve data security and reduce the risk of manipulation or alteration of data by unauthorized parties. The Indonesian government has noticed this potential and issued regulations and strategies to increase the use of blockchain technology in government and private sector operations. Several projects using blockchain technology in Indonesia have been carried out, such as verifying and validating educational certificates, storing medical data, and using cryptocurrency as a means of payment (Manurung & Wijoyo, 2021).

Nonetheless, the implementation of blockchain technology in Indonesia still faces several challenges, such as unclear regulations, limited infrastructure, and a lack of understanding of blockchain technology. To overcome these challenges, the Indonesian government needs to improve regulations and policies related to blockchain technology, especially those related to taxes and data security (Maulani et al., 2023). In addition, the government needs to improve digital infrastructure in Indonesia, especially in remote areas, so that the implementation of blockchain technology can run smoothly. Apart from the government, companies in Indonesia also need to pay attention to the use of blockchain technology to improve data security in their operations. Increasing understanding of blockchain technology also needs to be done through education and outreach to the public. On the other hand, blockchain technology companies also need to pay attention to Indonesia's large market potential and start expanding their business to Indonesia (Centre for Innovation Policy and Governance, 2018). An increase in the number of blockchain technology companies in Indonesia can open up new opportunities in the use of blockchain technology and encourage the growth of the digital economy in Indonesia (Panggabean, 2022). In conclusion, the use of blockchain technology in digital transformation in Indonesia has great potential to improve data security and promote digital economic growth (Pusat Inovasi Kota dan Komunitas Cerdas, 2021). Nonetheless, the implementation of blockchain technology still faces several challenges that need to be overcome by the government and companies in Indonesia (Putra et al., 2019; Saefudin, 2022). With joint efforts, the use of blockchain technology can be properly integrated into digital transformation in Indonesia and bring benefits to the people and economy of Indonesia as a whole.

References

Argani, A., & Taraka, W. (2020). Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi. Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi, 1(1). https://doi.org/10.34306/abdi.v1i1.121

Atmomintarso, B. E., & Wirawan. (2021). Sistem Pelaporan Pajak Pertambahan Nilai pada Web dengan Menggunakan Teknik Blockchain. JURNAL TEKNIK ITS, 10(2), 175-181. https://media.neliti.com/media/publications/499988-none-094e50e4.pdf

AWS. (2023). Apa itu Teknologi Blockchain? - Penjelasan tentang Blockchain - AWS. Amazon AWS. Retrieved February 9, 2023, from https://aws.amazon.com/id/what-is/blockchain/

Azis, M. T. E., Apriani, ,. R., & Kamal, M. F. (2021). PERLINDUNGAN HUKUM INVESTASI MATA UANG DIGITAL (CRYPTOCURRENCY). Jurnal Pemikiran dan Penelitian Ilmu-ilmu Sosial, Hukum, & Pengajarannya, 16(2). https://ojs.unm.ac.id/supremasi

Bank Indonesia. (2020). Sistem Pembayaran & Pengelolaan Uang Rupiah. Bank Indonesia. Retrieved February 24, 2023, from https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/default.aspx

Bashar, H. S., Purnamasari, H., & Priyanti, E. (2022). ANALISIS PENERAPAN BLOCKCHAIN DI INDONESIA, MENUJU REVOLUSI PELAYANAN PUBLIK DAN KEARSIPAN. NUSANTARA (Jurnal Ilmu Pengetahuan Sosial), 9(8). http://dx.doi.org/10.31604/jips.v9i8.2022.3023-3029

Budhijanto, D. (2023, January 24). Blockchain Law, Pelindungan Data Pribadi dalam Ekonomi Digital. Hukumonline. Retrieved Februari 10, 2023, from https://www.hukumonline.com/berita/a/blockchain-law--pelindungan-data-pribadi-dalam-ekonomi-digital-lt63cf37949e450/

Centre for Innovation Policy and Governance. (2018). Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia Usulan Desain, Prinsip, dan

Rekomendasi Kebijakan. Ditjen Aptika. Retrieved Desember 12, 2022, from https://aptika.kominfo.go.id/wp-content/uploads/2018/12/Kajian-Kominfo-CIPG-compressed.pdf

Fazreen, T., & Munajat, M. D. E. (2022). Solusi Pemanfaatan Teknologi Blockchain Untuk Mengatasi Permasalahan Penyaluran Dana Bantuan Sosial Covid-19. JANE (Jurnal Administrasi Negara), 12(2). https://jurnal.unpad.ac.id/jane/article/view/35133

Hoesada, J. (2023). Disaster Recovery Planning: Manajemen Bencana Administrasi dan Akuntansi. CRMS. Retrieved February 14, 2023, from https://crmsindonesia.org/publications/disaster-recovery-planning-manajemen-bencana-administrasi-dan-akuntansi/

Iswanto, Putri, N. I., Munawar, Z., Komalasari, R., & Widhiantoro, D. (2022). Pemanfaatan Teknologi Blockchain di Bidang Pendidikan. ematik : Jurnal Teknologi Informasi Komunikasi (e-Journal), 9(2), 171-181. https://doi.org/10.38204/tematik.v9i2.1082

Jurnal Entrepreneur. (2022). Sistem Informasi Manajemen dan Manfaatnya bagi Perusahaan - Mekari Jurnal. Jurnal.id. Retrieved Februari 13, 2023, from https://www.jurnal.id/id/blog/mengenal-sistem-informasi-manajemen-dan-manfaatnya-bagi-perusahaan/

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of Qualitative Descriptive Studies: A Systematic Review. Wiley Online Library, 40(1), 23-42. https://doi.org/10.1002%2Fnur.21768

Lin, I. -C., & Liao, T. -C. (2017). A Survey of Blockchain Security Issues and Challenges. Airiti Library, 19(5). http://dx.doi.org/10.6633/IJNS.201709.19(5).01

Liu, K.H., Chang, S., Huang, W., & Lu, I. (2017). The Framework of the Integration of Carbon Footprint and Blockchain: Using Blockchain as a Carbon Emission Management Tool. Technologies and Eco-innovation towards Sustainability I. https://www.semanticscholar.org/paper/The-Framework-of-the-Integration-of-Carbon-and-as-a-Liu-Chang/111fe0f01f3edea408954912379158 91ee9daf5a#cited-papers

Liu, C. H., Lin, Q., & Wen, S. (2019, June). Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning. IEEE Transactions on Industrial Informatics, 15(6), 3516-3526. https://doi.org/10.1109/TII.2018.2890203

Manurung, R., & Wijoyo, H. (2021). Sistem Informasi Akuntansi Cryptocurrency Bitcoin. Insan Cendekia Mandiri, indonesia.

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi. Jurnal Sosial dan Teknologi (SOSTECH), 3(2). https://sostech.greenvest.co.id/index.php/sostech/article/view/634/1006

Moleong. (2014). Metode Penelitian Kualitati. Remaja Rosdakarya. Bandung.

Nugraha, J. P., Kurniawan, A. P., Putri, I. D., Wicaksono, R. K., & Tarisa. (2022). Penerapan Blockchain Untuk Pencegahan Sertipikat Tanah Ganda Di Kementerian Agraria Dan Tata Ruang/Badan Pertanahan Nasional. Jurnal Widya Bhumi, 2(2). https://doi.org/10.31292/wb.v2i2.43

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 1(2). https://doi.org/10.15294/ipmhi.v1i2.53698

Panggabean, A. N. (2022, October). Memahami Dan Mengelola Transformasi Digital. OSF Preprints. https://doi.org/10.31219/osf.io/s36wq

Pluang. (2022). Mengenal Konsep Algoritma Konsensus Dalam Blockchain. Apakah Itu? Pluang.com. Retrieved February 18, 2023, from https://pluang.com/id/blog/resource/mengenal-konsep-algoritma-konsensus

Pratiwi, L. L. (2022). Implementasi Blockchain Pada Akuntansi Dan Audit Di Indonesia. Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 4(6). https://doi.org/10.32670/fairvalue.v5i01.873

Pusat Inovasi Kota dan Komunitas Cerdas. (2021, October 13). Penerapan Teknologi Blockchain pada Industri Kesehatan. PIKKC. Retrieved February 5, 2023, from https://citylab.itb.ac.id/pikkc/2021/10/13/penerapan-teknologi-blockchain-pada-industri-kesehatan/

Putra, H. F., Wirawan, W., & Penangsang, O. (2019). Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid. E-Jurnal ITS, 8(1). http://dx.doi.org/10.12962/j23373539.v8i1.38525

Saefudin. (2022, December 2). Gerakan Smart City sebagai Muara Kemajuan Transformasi Digital Indonesia. Ditjen Aptika. Retrieved January 4, 2023, from https://aptika.kominfo.go.id/2022/12/gerakan-smart-city-sebagai-muara-kemajuan-transformasi-digital-indonesia/

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. SASI, 27(1). https://doi.org/10.47268/sasi.v27i1

Soemitra, A., & Adlina. (2022). PERLINDUNGAN KONSUMEN TERHADAP KEBOCORAN DATA PADA JASA KEUANGAN DI INDONESIA. Jurnal Insitusi Politeknik Ganesha Medan, 5(1). https://polgan.ac.id/jurnal/index.php/juripol/article/view/11538

Sutandi. (2018). Pengaruh Big Data Dan Teknologi Blockchain Terhadap Model Bisnis Sektor Logistik Dengan Pendekatan Business Model Canvas. Jurnal Logistik Indonesia, 2(1). https://doi.org/10.31334/jli.v2i1.214.g139

Tashia. (2017, June 29). Keamanan Jaringan Internet dan Firewall – Ditjen Aptika. Ditjen Aptika. Retrieved February 11, 2023, from https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/

Teknik Logistik. (2021, July 19). Pemanfaatan Blockchain dalam Dunia Logistik - Teknik Logistik. Teknik Logistik. Retrieved February 24, 2023, from https://tekniklogistik.ittelkom-pwt.ac.id/pemanfaatan-blockchain-dalam-dunia-logistik/

Trinowo, L. E. (2020). Blockchain Proof-of-Work Threat: 51% Attack. Budi Rahardjo. Retrieved January 12, 2023, from http://budi.rahardjo.id/files/courses/2020STEI/18217018_Makalah_Luthfi_Eko_Trinowo.pdf

Universitas Islam Indonesia. (2021, June 7). Blockchain Tingkatkan Keamanan Data Dari Peretasan - UII. Universitas Islam Indonesia. Retrieved Januari 11, 2023, from https://www.uii.ac.id/blockchain-tingkatkan-keamanan-data-dari-peretasan/