Protocol Storage of Notary in Blockchain For Guaranteeing Legal Protection of Personal Data of All Parties

Rico Aldy Munafan[1], Nuzulia Kumala Sari[2], Samuel Saut Martua Samosir[3]

University of Jember, Indonesia

DOI: https://doi.org/10.47772/IJRISS.2026.100500730

Received: 12 May 2026; Accepted: 18 May 2026; Published: 11 June 2026

ABSTRACT

The notary protocol storage in its implementation is still done in a non-digital manner, with physical deeds stored in special archive cabinets or using iron safes placed in the notary's office. This method of document storage has been in place for a long time and is considered secure. However, with the advancement of technology, the conventional storage model is beginning to be questioned in terms of its relevance. If the notary protocol is stored conventionally in large quantities and must retain documents for many years, even for a lifetime, and after the notary has passed away, the protocol must also be handed over to another notary, this creates a significant administrative burden and requires a large amount of space. Therefore, there is an urgency to consider digital storage alternatives. Thus, the purpose of the research is to determine whether notary protocol storage can be done on the blockchain and to understand the concept of future legal protection for personal data of the parties involved in notary protocol storage on the blockchain. This research uses normative legal research methods or Legal Research.The approach used in this research is the legal approach, the conceptual approach, and the comparative approach. The legal materials of this research consist of primary legal materials, secondary legal materials, and non-legal materials. Based on the discussion in this research, several main findings were obtained: First, the blockchain-based storage system essentially has characteristics that are in line with conventional storage systems. Both aim to preserve the existence, integrity, and authenticity of documents, thus, the application of blockchain in notary protocol storage is feasible, as long as there is clear legal backing. Secondly, the concept of future legal data privacy protection for parties in blockchain- based notary protocol storage in Indonesia must be established through regulations that clearly allow for the digital storage of notary protocols, recognizing digital notary documents as authentic acts with evidence strength equivalent to physical authentic acts, the existence of adequate digital infrastructure, and integrated legal systems.This protection is not only technical but also normative in ensuring the privacy rights of the parties involved.

Keywords: Notary, Protocol Storage, Blockchain

INTRODUCTION

A notary is a public official who is authorized to create authentic deeds, ensure the authenticity of the date of creation, store the deeds in the notary's protocol, and provide official copies.[1] Law No. 30 of 2004 on Notaries, as amended by Law No. 2 of 2014 on Notaries, in Article 1 paragraph (1) states that a notary is a public official who has the authority to create authentic deeds and has other authorities as stipulated in the Notary Law or other laws.[2] Referring to Article 1868 of the Civil Code, an authentic notary deed plays an important role in the Indonesian legal system because an authentic deed is a perfect proof that guarantees legal certainty and protection for the parties involved.

In performing his duties, a notary is required to keep records as a form of notary protocol. The notary protocol, based on Article 1 paragraph (13) of the Notary Office Law, is a collection of documents that must be kept and maintained by the notary based on the provisions of the laws and regulations because it is a state archive.[3] Therefore, the storage of the notary protocol is not only related to the interests of the notary and the parties involved, but also to the interests of the state to ensure the authenticity of legal documents, so the notary protocol is not just an administrative record, but also part of the state archives that are attached to the notary's position.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue V May 2026

Protocol storage for notaries is generally still done manually, by securely storing minutes of the act. This is important, considering that the data in the notary protocol includes information about the personal data of the parties involved in legal acts before the notary. As stated in Article 16 paragraph (1) letter a of the Notary Position Law, notaries are required to act honestly, diligently, independently, impartially, and to protect the interests of the parties involved in legal acts. As stated in Article 16 paragraph (1) letter f of the Notary Position Law, maintaining confidentiality and protecting personal data of the parties is a notary's duty, thus notaries not only act as notary public but also as guardians of legal data security and confidentiality.[4]

The first paragraph of Article 1 of Law Number 27 of 2022 concerning Personal Data Protection states that personal data is any data about an individual that can be identified or identifiable by itself or by combining it with other information, either directly or indirectly through electronic or non-electronic systems.[5] Personal data recorded in authentic deeds is personal information that contains the identities and interests of the parties, such as name, place and date of birth, gender, address, occupation, and identification numbers, which are an inseparable part of the notary protocol. With this, notaries bear a great responsibility in maintaining the security of this data, as the storage of notary protocols contains a legal protection dimension for the personal data of the parties.

Protocol storage for notaries in its implementation is still done in a non-digital manner, with physical deeds stored in special archive cabinets or using iron safes placed in the notary's office or other locations that have been notified to the Notary Supervisory Board.[6] This method of document storage has been in place for a long time and is considered secure because it is resistant to fire, water, and risks of damage or theft. However, with the advancement of technology, the conventional storage model is beginning to be questioned in terms of its relevance. If protocol storage for notaries is done conventionally in large quantities and must store documents for many years, even for a lifetime, and after the notary has passed away, the protocol must also be handed over to another notary, this creates a significant administrative burden and requires a large amount of space. Therefore, there is an urgency to consider digital storage alternatives.

The Digital Age has brought about very significant changes in all aspects of life, including the legal field. Digitalization has enabled various administrative activities and public services to shift from conventional systems to electronic systems. The digital transformation aims to enhance convenience, effectiveness, efficiency, and security in various fields.[7] For example, in the context of archiving, the physical storage systems of several state institutions are beginning to be replaced by electronic archives or e-archives, which aligns with Article 40 paragraph (2) of the Records Management Law, which allows for the digital storage of records as long as the principles of authenticity, integrity, security, and accessibility are met.[8]

This development presents a significant opportunity for notaries to adapt to digital systems, particularly in relation to data archiving or protocol storage. Although currently still using conventional storage systems, with the advancement of technology and the need to streamline notaries' work, as well as the effectiveness and efficiency in storing notarial protocols, it is not impossible in the future to integrate digital methods by leveraging blockchain technology as an alternative storage method for notarial protocols.[9]

Blockchain is a digital storage system or known as a decentralized and encrypted ledger, where data is stored in the form of blocks connected by a digital chain, as well as verified by many computers. 10 Each block will contain related data, transaction records, or protected information by a cryptographic system, so that the data stored in the blockchain cannot be changed or deleted without being detected by the system. With this system, blockchain can ensure data security, confidentiality, authenticity, and integrity, because this technology is not centralized or centralized but decentralized and spread across several systems, so every change must be approved by all networks or consensus. Therefore, blockchain technology is starting to be used in various fields to store important data such as financial transactions, digital certificates, or legal documents, because this technology is transparent, cannot be manipulated, and has an audit trail that can be accountable.[11]

Blockchain technology is highly relevant when applied in the notary profession, particularly for recording important data such as personal data and all transactions between parties in notary protocol storage, which requires high security and authenticity levels.[12] This aligns with the Notary Position Law in Article 15 paragraph (3) which states that notaries have other authorities regulated in laws and regulations.[13] in this article it does not

explicitly mention the application of blockchain, but it gives other authorities to notaries, which can be interpreted as notaries are allowed to perform their duties and authorities digitally, including the storage of notary protocols on blockchain.

Several developed countries have already applied blockchain technology in the field of notarization. One example is Italy, which has developed a digital notary system by leveraging this technology to ensure the authenticity of documents.[14] This fact demonstrates that blockchain has global relevance in modern notarial systems, which can serve as a reference for Indonesia to develop similar regulations.

However, as of now, there are no clear regulations governing cyber notaries in Indonesia, particularly regarding the use of blockchain technology in storing notary protocols. Therefore, there is a need for new discussions or regulations that are relevant to technological advancements and the times, so that notaries can provide effective and efficient legal services to the public. This raises legal issues regarding whether notary protocols can be stored on blockchain and what legal protections are in place for the privacy of parties involved in storing notary protocols on blockchain.

The purpose of this research is to determine whether notary protocols can be stored on a blockchain and how the legal protection of personal data of the parties involved in the storage of notary protocols on a blockchain can be ensured.

RESEARCH METHODOLOGY

This study employs a normative legal research methodology, also known as Legal Research, which involves analyzing and examining the substance of laws and regulations, as well as theoretically-oriented literature related to the researcher's legal issues and problems concerning the legal protection of personal data of parties stored in notary protocols on the blockchain. The approach used in this thesis is the legal approach, the conceptual approach, and the comparative approach. The legal materials for this research consist of primary legal materials, secondary legal materials, and non-legal materials. The collection of legal materials for this thesis is conducted using a systematic literature review method obtained from books, research findings, expert opinions, journals, and articles. For the analysis of legal materials, a deductive approach is used, starting from a general issue or problem, which is then followed by drawing conclusions and reaching specific conclusions regarding the legal issues that are the focus of the research

RESULTS AND DISCUSSION

Storage of Notary Protocols Using Blockchain Technology

Blockchain based storage systems inherently share characteristics with conventional storage systems. Both aim to preserve the existence, integrity, and authenticity of documents. The fundamental difference lies not in functionality but in storage medium and the mechanisms of access. In conventional systems, notary protocols are stored physically in a secure vault or specific archive room, safeguarded for security.[15] Meanwhile, in blockchain systems, storage is conducted digitally using cryptographic mechanisms, hashes, and interconnected data distribution, making alterations difficult to execute without detection.[16]

The process of storing data in a blockchain is not done directly, like saving a file in a folder on a computer. Instead, the data to be stored is first processed using a cryptographic hash function. The blockchain process begins with a transaction request, which is recorded as a data block. The created transaction is first broadcast across the blockchain network for validation. Next, the network or the majority of nodes in the blockchain network validates whether the transaction is accepted or not. If the transaction is successfully validated, it is added to a transaction block; this block is then chained to the previous one, and the transaction is confirmed.[17]

Along with the transaction, a cryptographic hash is also added to the new block. The hash acts as a link connecting the blocks together. If the contents of a block are altered whether intentionally or unintentionally the hash value changes, providing a way to detect data tampering. Thus, blocks and the chain are securely linked

and cannot be edited. Each additional block reinforces the verification of the previous block and, ultimately, strengthens the entire blockchain.[18]

Based on the above discussion, it can be concluded that blockchain technology has a highly robust security system for protecting the data it contains, including the personal data of the parties involved, because the security system in blockchain technology is built on a combination of a decentralized system, cryptographic mechanisms, immutability, and a collective verification process through consensus. In a blockchain system, data is not stored on a single central server but is distributed across multiple nodes in the network, thereby preventing the risk of data leaks resulting from cyberattacks on a single point of failure. Furthermore, every piece of data is first processed through a cryptographic hash function that converts the information into a unique code that cannot be reversed to its original form; thus, this system ensures the confidentiality of personal data because if it is forcibly accessed, the information within the blockchain data will automatically become corrupted and unreadable.

The use of private and public keys also provides strict access control, ensuring that only authorized parties can access the data. Furthermore, the immutable nature of the system ensures that recorded data cannot be deleted, altered, or manipulated without the approval of the network majority, and any changes are recorded in a new block without erasing the previous history, thereby preserving the authenticity and integrity of the data. The consensus mechanism, which involves multiple nodes in the verification process, also prevents abuse or domination by a single party, as every transaction must receive collective approval before being recorded on the blockchain. The traceability feature also allows all activities related to the data to be traced chronologically, thereby enhancing accountability and transparency in the management of personal data. Thus, this demonstrates that blockchain technology functions not only as a data storage system but also as an effective personal data protection system, as it is capable of comprehensively ensuring the integrity, confidentiality, and security of data aspects that are highly relevant in the context of notarial protocol storage, given that such documents contain sensitive legal information and hold significant value.

Thus, blockchain can be projected as a future notary protocol storage system that replaces conventional physical-based storage systems. However, during the transition phase, blockchain can still be used as an archival duplication (backup) system to ensure the sustainability and security of documents. This model actually strengthens document protection because it can prevent loss due to physical damage, natural disasters, fires, or theft. The implementation of blockchain-based systems offers guarantees of data integrity, authenticity, and availability that, technically, even surpass conventional systems. Therefore, from a technical and functional perspective, digital blockchain-based notary protocol storage is not only compatible with conventional storage goals but also superior in terms of security and efficiency.

In a normative sense, the opportunity for the digital implementation of notary protocol storage has gained legal grounds in various laws and regulations. Firstly, in Article 15 paragraph (3) of the Notary Position Law, it is emphasized that notaries have other authorities regulated in laws and regulations.[19] This provision opens up an interpretation space that notaries' authorities can develop following legal and technological advancements, including in providing legal services and electronic transactions. Thus, this norm can be interpreted as an entry point for the digital storage of protocols as long as it does not conflict with other more specific provisions.

Second, Article 5 paragraph (1) of the Electronic Information and Transactions Law affirms that electronic information or electronic documents are legal evidence.[20] Indeed, in Article 5 paragraph (4) of the initial version of the ITE Law (Law No. 11 of 2008), there is an exception for documents that according to the law must be made in the form of a notarial act. However, through the latest changes in Law No. 1 of 2024, this exception was removed, thus opening up space for notaries to create or authenticate documents electronically, as well as their storage.

Third, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions emphasizes that reliable, secure, and responsible electronic systems have legal force.[21] As long as the blockchain system meets the principles of reliability, integrity, information security, and personal data protection, then there is no regulatory prohibition on using it as a storage medium.

Fourth, Article 12 of the Company Documents Law states that company documents can be transferred to other media, including electronic media, as long as their validity and integrity can be guaranteed.[22] This norm indicates

that Indonesian law generally recognizes the principle of media conversion (media conversion), as long as the authenticity and integrity of the documents are maintained, a characteristic that actually becomes the advantage of the blockchain system.

Five, Article 77 of Law No. 40 of 2007 on Limited Liability Companies explicitly allows the conduct of RUPS through electronic means such as teleconferences or video conferences.[23] This provision demonstrates that Indonesian corporate law has recognized the use of digital technology in corporate legal practice, including that which intersects with the notary's authority.

Sixth, Minister of Communication and Informatics Regulation No. 11 of 2018 gives a strategic role to notaries as parties that can be designated as the registration authority in the issuance of electronic certificates.[24] Even notaries are given the authority to verify identities and inspect documents. This shows that, regulatory-wise, notaries have been recognized as part of the national electronic system ecosystem.

In connection with Hans Kelsen's theory of legal certainty, law is a statement that emphasizes the aspect of should or das sollen, law must be able to provide certainty through clear and systematic norms.[25] In addressing the need for technology to promote effectiveness and efficiency, law is required to remain relevant to the times. This relevance is important so that the law can continue to provide certainty, while also preventing the occurrence of legal vacuums as notarization practices develop in line with technological advancements.

From the perspective of legal utility according to Jeremy Bentham, law is considered good if it provides the greatest benefit to society (the greatest happiness for the greatest number).[26] Blockchain-based storage enhances the security of state archives, minimizes the risk of permanent loss, accelerates the verification process, and improves administrative efficiency. Therefore, the application of this technology not only meets the aspect of utility but also broadly supports public interests.

Thus, the application of blockchain is not a deviation from the existing legal system, but rather an evolution of the law in response to the development of information technology. Theoretically, it meets the legal certainty principle through systematic normative interpretation, and practically meets the legal benefit principle. Therefore, the problem of whether the storage of notary protocols on the blockchain is allowed can be answered that conceptually and in the direction of legal reform, such storage is possible to become the main system, as long as it obtains clear normative legitimacy within the legal framework. So legally, there is a chance for the application of blockchain technology in the storage of notary protocols in Indonesia. However, as of now, there is no explicit regulation governing this matter, so its application cannot be carried out optimally due to the lack of legal cover, especially if a dispute arises in the future. Furthermore, the main purpose of storing notary protocols is to secure legal documents that have perfect evidentiary power for the parties involved.Therefore, if storage is done digitally, there must be clear settings that allow the storage of notary protocols digitally, recognizing digital notary documents as authentic deeds with evidence strength equivalent to physical authentic deeds, as well as adequate digital infrastructure and integrated legal systems. In summary, blockchain can be used but with these conditions.

The Concept of Legal Protection for Personal Data of Parties in the Storage of Notary Protocols Based on Blockchain in Indonesia

The notary protocol storage system in Indonesia, as of now, is still primarily conducted in a conventional manner using physical documents.[27] The notary protocol, which includes the minutes of the act, the repertoire, the act register book, and other supporting documents, is stored by the notary as part of the state archives. This arrangement is as stipulated in Law No. 30 of 2004 on Notary Position, as amended by Law No. 2 of 2014, which states that the notary protocol is a collection of documents that are state archives and must be stored and maintained by the notary.[28] These provisions indicate that the notary protocol holds a very important position in the Indonesian legal system, as these documents not only function as administrative records but also serve as evidence with complete evidentiary power in civil law practice.

Despite this, the conventional system of storing notary protocols has various limitations in practice. The physical storage of documents is highly susceptible to various damage risks, caused by environmental factors such as

humidity, paper aging, fire, or natural disasters. Additionally, the continuous increase in the number of notary protocol documents over time also creates problems in archival management, particularly concerning storage space needs and the increasingly complex process of document organization.[29] In practice, it is not uncommon to find situations where the storage of notary protocol documents requires very large archival spaces and necessitates a fairly complex management system.

Another problem that often arises in conventional document storage systems is the limitation in the document retrieval process. When a minutes of meeting document is needed again, the retrieval process often requires a considerable amount of time because the archiving is still done manually.[30] This situation can certainly hinder the effectiveness of legal services to the public, especially when the document is needed in the evidentiary process in court or for other legal purposes. Therefore, it can be said that the conventional notary protocol storage system is not fully capable of ensuring the efficiency, security, and sustainability of managing notarial documents in the long term.

On the other hand, the development of information technology over the past few decades has brought significant changes in various public administration sectors, including in the field of archive management and legal document management. The use of digital technology in document storage essentially provides various benefits, both in terms of the efficiency of archive management and in terms of improving document security.[31] Through digital storage systems, documents can be stored in electronic form, thus no longer fully dependent on physical media that are susceptible to damage. Furthermore, digital systems also enable the implementation of various data security technologies such as encryption, user authentication, as well as stricter access control systems for confidential documents.

However, the implementation of a digital document storage system for notarial acts in Indonesia still faces various obstacles, particularly in the regulatory aspect. As of now, the Notary Act still classifies notarial protocols as physical documents that notaries are required to store as part of the state archives. There is no explicit regulation governing the possibility of storing notarial protocols in digital form. Furthermore, there is no specific regulation addressing the mechanism for protecting the personal data of parties involved in a digital protocol storage system.[32] This situation indicates that the current legal system is still not fully equipped to accommodate the development of information technology in notarial practice.

Philosophically, laws should ideally provide the greatest possible benefits to society. This aligns with Jeremy Bentham's view that laws are good when they can provide significant benefits to society (the greatest happiness for the greatest number).[33] Therefore, laws must offer substantial benefits to society, especially amid the development of time and technological advancements. Laws should not lag behind but must adapt and cater to human needs. To achieve these goals, there must be legal certainty as the primary foundation.

According to Hans Kelsen, law is a hierarchical system of norms, so legal certainty can only be achieved if every legal action has a clear and definite normative basis.[34] This legal certainty will ultimately provide legal protection for legal subjects. Legal protection is an effort to protect individual interests based on legal provisions. Theoretically, legal protection, based on its source, is divided into two types: internal legal protection and external legal protection.

According to Moch. Isnaeni, internal legal protection is legal protection created by both parties in agreed-upon clauses.[35] Regarding this research, both parties, notaries and parties, have rights and obligations. Notaries are entitled to fees and are obligated to provide legal services and maintain the confidentiality of the deeds, whereas the parties are entitled to personal data protection and the authenticity of the deeds.

External legal protection is realized through the government's actions in establishing laws and regulations to protect the interests of every individual and prevent the occurrence of disputes or legal issues in the future.[36] This means that the law must be in place before any future issues arise. Therefore, due to the need for efficiency and effectiveness in storing notary protocols, technology is required to address this need, yet there are currently no clear regulations governing the digital storage of notary protocols on blockchain. Thus, the law should not lag behind the advancement of time, and there should be laws in place to address these issues, providing protection and preventing problems in the future.

According to Philipus M. Hadjon, legal protection based on its form is classified into two types: legal protection preventive aimed at preventing violations, and legal protection repressive aimed at resolving disputes that have already occurred. In its development, these two forms of protection can also be understood as direct and indirect legal protection, where direct protection is provided through clear legal norms, while indirect protection is provided through the mechanism of enforcing the law.[37] Thus, if the development of information technology in the storage of notary protocols can be accommodated through clear legal regulations, not only will legal certainty be created, but also optimal legal protection for the parties involved, so that ultimately the law can provide the greatest benefits to society.

Meanwhile, several countries have started developing digital document notarization systems as part of the legal administration modernization. One country that has implemented digital notarization documents is Italy. Through the regulations in Decree Law 7 March 2005, n. 82 on the Digital Administration Code, the Italian legal system has provided a legal basis for the use of electronic documents and the storage of documents in a digital system.[38] This regulation acknowledges that electronic documents equipped with digital signatures have legal force equivalent to conventional written documents. Furthermore, these regulations also provide a legal basis for storing electronic documents in a digital archive system, ensuring the authenticity, integrity, legibility, and security of documents over a long period.

The recognition of electronic documents in the Italian legal system is governed by an article 20 *Decreto Legislativo 7 marzo 2005, n. 82*, which reads:[39]

"*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile quando vi è apposta una firma digitale o un'altra firma elettronica qualificata*."

This means: "An electronic document satisfies the requirements for written form and has legal force as referred to in Article 2702 of the Civil Code if it bears a digital signature or other qualified electronic signature."

This provision indicates that electronic documents using digital signatures have the same legal force as conventional written documents as long as they meet the requirements set forth by laws and regulations. Provisions regarding the evidentiary weight of electronic documents are also regulated in Article 21 *Decreto Legislativo 7 marzo 2005, n. 82*, which states:[40]

"*Il documento informatico, cui è apposta una firma digitale o un'altra firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile*."

This means: "Electronic documents bearing a digital signature or a qualified electronic signature have evidentiary value as provided for in Article 2702 of the Civil Code."

This provision confirms that electronically signed documents may be used as valid legal evidence because they guarantee the identity of the signatory and the integrity of the document. Additionally, Article 22 *Decreto Legislativo 7 marzo 2005, n. 82* also addresses electronic copies of analog documents, which states:[41]

"*La copia informatica di un documento analogico ha la stessa efficacia probatoria dell'originale se la sua conformità è attestata da un pubblico ufficiale a ciò autorizzato."*

This means: "An electronic copy of an analog document has the same evidentiary value as the original document if its authenticity is certified by an authorized public official."

Digitalization in Italian notary practice is strengthened through regulations in Legislative Decree 2 July 2010, n. 110, which regulates the use of information technology in notarial activities.[37] This regulation provides a legal basis for the use of telematic tools in the execution of notarial duties, including the creation, transmission, and storage of notarial documents in electronic form. With these regulations in place, Italian notarial practice has begun to integrate digital technology into the management of legal documents, thereby improving administrative efficiency while enhancing document security.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue V May 2026

Provisions regarding the use of electronic documents in notarial activities are set forth in Article 47-bis *Decreto Legislativo 2 luglio 2010, n. 110*, which reads:[42]

"*L'atto notarile può essere formato come documento informatico ed è sottoscritto con firma digitale dal notaio e dalle parti, secondo le modalità previste dalla normativa vigente*."

Meaning: "Notarial deeds may be drawn up in the form of electronic documents and signed with digital signatures by the notary and the parties in accordance with the procedures set forth in applicable laws and regulations."

This provision indicates that the Italian legal system has recognized the possibility of drawing up notarial deeds in the form of electronic documents. The use of digital signatures by the notary and the parties is intended to guarantee the authenticity of the document, verify the signatories' identities, and preserve the integrity of the document's content, ensuring that the deed retains the same legal validity as a notarial deed prepared in the conventional manner. Further provisions regarding the electronic management of notarial documents are set forth in Article 47-ter *Decreto Legislativo 2 luglio 2010, n. 110*, which reads:[43]

"*Gli atti notarili formati come documenti informatici sono conservati mediante sistemi informatici che garantiscono autenticità, integrità, affidabilità e reperibilità nel tempo*."

This means: "Notarial deeds created in the form of electronic documents must be stored using an information technology system that guarantees the authenticity, integrity, reliability, and traceability of such documents over the long term."

This provision stipulates that notarial documents created electronically must be stored through an information technology system that meets certain security standards. The storage system must be capable of guaranteeing the authenticity of the documents and ensuring that they remain accessible and their validity verifiable over a long period of time. Furthermore, the use of telecommunications in notarial activities is also regulated in Article 52-bis *Decreto Legislativo 2 luglio 2010, n. 110*, which reads:[44]

"*Il notaio può utilizzare sistemi telematici per la trasmissione degli atti e dei documenti agli uffici pubblici competenti secondo le modalità stabilite dalla legge*."

This means: "Notaries may use electronic systems to transmit deeds and documents to the competent public authorities in accordance with the procedures established by law."

This provision indicates that Italian law permits notaries to use telematics to transmit notarial documents to government agencies, such as registry offices or other administrative bodies. The use of telematics aims to expedite administrative processes and improve the efficiency of legal services provided to the public.

The notarial practice in Italy shows that the digitization of notarial documents is an inevitable development in the modern legal administration system. Therefore, the development of a digital storage system for notary protocols has also become a necessity in the Indonesian notarial system, especially to address various problems in the conventional storage system.

As part of the concept of developing a future notary system, the implementation of a blockchain-based notary protocol storage system in Indonesia needs to be designed through an integrated system model that integrates information technology, personal data protection, and state supervision mechanisms.[45] This system model aims to ensure that the digitization of notary protocols not only provides efficiency in managing notary documents but also ensures the security of the documents and provides optimal legal protection for the personal data of the parties included in the notary documents.

In notarial practice, the documents contained in the notary's protocol generally contain various sensitive information, such as the identities of the parties, their residential addresses, identification numbers, as well as information regarding the rights and obligations of the parties in a legal act.[46] Therefore, if the storage system for notary protocols is developed in digital form, the system must be designed with strict attention to personal

data protection principles. This is important to prevent the misuse of data, leakage of personal information, or manipulation of documents that have evidentiary power in the legal system.

Conceptually, the design of a blockchain-based notary protocol storage system in Indonesia can be achieved through several integrated operational mechanism stages. The first stage is the Document Digitalization process. In this stage, every notary-made minutes of deeds are converted into electronic documents using specific formats predetermined by the state. This Digitalization process is not just about scanning physical documents into digital form, but also involves verifying the authenticity of the documents and adjusting their format to the electronic storage system to be used. The electronic documents produced in this process are then equipped with certified electronic signatures.[47] Where it functions to ensure the authenticity of the documents and to confirm the identity of the notary who made the deed.

The second stage is the process of forming the digital identity of the document. In this stage, the created electronic document will be processed through a cryptographic system to produce a unique hash value.[48] This hash value is the digital representation of the document in question, so each document will have a different digital identity from one another.

The third stage is the recording of digital document identities within a blockchain network. At this stage, the document's hash value is recorded in the blockchain network, which functions as a document authenticity verification system.[49] This recording creates a digital trail that cannot be unilaterally altered, ensuring the document's integrity remains intact.

The fourth stage is the secure storage of documents within a digital archival system. Electronic documents are stored in a digital storage system that is protected by layered security mechanisms such as data encryption, user authentication, and access control to the documents.[50]

The fifth stage is the implementation of a digital monitoring and audit system. In this system, every activity related to documents will be recorded in the form of a digital trail, making it possible to monitor the use of documents and prevent the misuse of access to personal data of the parties involved.[51]

Aside from the aforementioned system mechanisms, protection of personal data for all parties also needs to be supported by the implementation of several data protection principles. The first principle is the limitation of data recorded in the blockchain network so that it only records the digital identity of documents without directly including personal data of the parties. The second principle is the implementation of encryption technology to protect electronic documents stored in the digital archive system. The third principle is the implementation of access control mechanisms for notarization documents. The fourth principle is the implementation of the accountability principle in managing the digital notary protocol storage system.

To effectively implement such a system in notary practice in Indonesia, explicit regulatory support is needed, which should regulate the storage of notary protocols in digital form. This regulation should include acknowledgment of electronic notary protocols as part of state archives, provisions regarding secure digital storage systems, and mechanisms for protecting the personal data of parties mentioned in notarial documents.

Thus, the concept of implementing a blockchain-based notary protocol storage in Indonesia is not only an innovation in technology, but also a part of the development of the notarial legal system aimed at improving document security, efficiency in archival management, as well as legal protection for personal data of the parties involved in notarial documents.

CONCLUSION

Based on the analysis and discussion in this thesis, the researcher can draw the following conclusions:

Blockchain-based storage systems inherently share characteristics with conventional storage systems. Both aim to preserve the existence, integrity, and authenticity of documents, thus, blockchain can be envisioned as a future notary protocol storage system replacing conventional physical-based storage systems. During the transition phase, blockchain can still function as an archival duplication (backup) system to ensure the sustainability and

security of documents. However, as of now, there are no explicit regulations governing this, so its implementation cannot be optimal due to the lack of legal framework, especially if disputes arise in the future. Additionally, the primary goal of notary protocol storage is to secure legal documents that have perfect evidentiary strength for the parties involved. Therefore, if storage is done digitally, there needs to be explicit regulations allowing for digital notary protocol storage.The acknowledgment of digital notary documents as authentic deeds with evidence strength equivalent to physical authentic deeds, along with the existence of adequate digital infrastructure and integrated legal systems, allows for the use of blockchain. However, this should be done under certain conditions, in line with Hans Kelsen's view on the importance of legal certainty through clear and systematic norms, as well as Jeremy Bentham's perspective that law is effective when it provides significant benefits to society.

The concept of future legal data privacy protection for parties in the storage of blockchain-based notary protocols in Indonesia must be built through regulations that clearly allow for the digital storage of notary protocols, recognizing digital notary documents as authentic documents with evidence strength equivalent to physical authentic documents, having adequate digital infrastructure, and integrated legal systems. This protection is not only technical but also normative in ensuring the privacy rights of parties, achieved by limiting data recorded in the blockchain to only recording the digital identity of documents (hash) without directly including personal data, accompanied by encryption application, strict access control, and accountability mechanisms through digital audit systems. Like Italy, which has implemented digital document storage for notarization through the Decree Law 7 March 2005, n. 82 on the Digital Administration Code, which has provided a legal basis for the use of electronic documents and digital document storage, strengthened through regulations in Decree Law 2 July 2010, n. 110 regarding the use of information technology in notary activities. The concept of future legal data privacy protection for parties in the storage of notary protocols on blockchain, also aligns with Isnaeni's view in external legal protection theory, that the government should be able to provide legal protection for the community through legislation to prevent legal issues in the future, on the other hand, the law is also required to continuously adapt to the times to provide great benefits, as stated by Hans Kelsen in his theory. However, according to Jeremy Bentham, all of this can be achieved if the law is regulated clearly and firmly so that it can provide legal certainty for all individuals.

REFERENCE

1. Anggriani, Sufy, Rizki Savira Firdaus, and Windy Amanda Siwi Suherlan. (2023). Analysis of Electronic Storage of Notary Protocols, Notaire, Vol. 6. No. 3, p. 438.
2. Augusta, Muhamad Oka, Celline Putriana Oktaviandi Syeira, and Angga Hadiapurwa. (2022). The Use of Blockchain Technology in Education and Productivity," Jurnal Ilmiah Pendidikan Teknologi Informasi 2: 438.
3. Decree Law 7 March 2005, n. 82, concerning the Digital Administration Code.
4. Fadhilah, Daniyah, Hasyan and Fifiana Wisnaeni. (2014). Utilization of Artificial Intelligence and Blockchain in the Preparation of Notary Deeds in Indonesia, Notarius, Vol.17, No.1, p. 433.
5. Fariz Fadlillah, Muhammad. (2024). The Impact of Digital Technology Development on the Role of Notaries, Saturnus: Jurnal Teknologi Dan Sistem Informasi, Vol. 2. No. 3, 49.
6. Government Regulation of the Republic of Indonesia No. 71 of 2019 on the Implementation of Electronic Systems and Transactions.
7. Heriyanti. (2016). Legal Protection for Notaries Accused of Committing Criminal Acts in Creating Authentic Deeds, Yustisia Jurnal Hukum, 95. 2.
8. Irwan. (2024). The Use of Blockchain Technology in International Trade Transactions. Thesis. Makassar, Master's Program in Management, Faculty of Economics and Business. Hasanuddin University.
9. Isnaeni, Mochammad. (2016). Introduction to Property Security Law. Surabaya: PT. Revka Petra Media.
10. Karlina, Tiara. (2024). Application of Blockchain Technology in Notary Protocol Storage, Badamai Law Journal, Vol. 9, No. 1, 125.
11. Khanza, Moudy and Siti Hoesin. (2024). Authority and Responsibility of Notaries Related to Evidence Submitted by the Parties for the Implementation of Joint Agreement Letters (Case Study of the Medan State Court Decision No. 693/PDT.G/2021/PN MDN). Indonesian Notary, Vol. 3.

12. Kristanto, Kiki, et al. (2024). Legal Transformation in the Era of the Blockchain Technology Revolution, the Addition of Sodium Benzoate and Potassium Sorbate (Anti-Inversion Agents), and Stirring Speed as Methods to Inhibit the Inversion Reaction in Sugarcane Juice. Medan: PT Media Penerbit Indonesia.
13. Küzecİ, Elif. (2022). Personal Data Protection Law, Introduction to Turkish Business Law, 458.
14. Law of the Republic of Indonesia No. 2 of 2014 on Amendments to Law No. 30 of 2004 on the Office of the Notary.
15. Law of the Republic of Indonesia No. 40 of 2007 on Limited Liability Companies, 2007, Article 77.
16. Law of the Republic of Indonesia No. 43 of 2009 on Archiving, Article 40(2).
17. Law of the Republic of Indonesia No. 8 of 1997 on Corporate Documents, 1997.
18. Law of the Republic of Indonesia Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions, 2024, Article 5 paragraph (1).
19. Legislative Decree 2 July 2010, n. 110, containing provisions on the electronic public document drawn up by the notary, in accordance with Article 65 of Law 18 June 2009, n. 69
20. Makarim, Edmon. (2012). Notaries and Electronic Transactions: A Legal Study on Cybernotaries or Electronic Notaries. Depok: PT Raja Grafindo Persada.
21. Marzuki, Peter Mahmud. (2008). Introduction to Legal Science. Jakarta: Kencana, 2008.
22. Noer, Zakiah. Yuli Fajriyah. (2021). Notary Liability Regarding Notarial Protocols as State Archives, Jurnal Pro Hukum, 2: 80.
23. Paul, PK et al. (2022). Blockchain Technology and its Types: A Short Review. International Journal of Research Publication and Reviews 3: 195.
24. Putri, Juandela Herina. (2021). Design and Implementation of Blockchain Technology in Productive Waqf Transactions, Jakarta, Department of Computer Science, Faculty of Science and Technology, State Islamic University Syarif Hidayatullah.
25. Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 11 of 2018 Concerning the Implementation of Electronic Certification, 2018.
26. Ridwan, Mochamad. (2021). The Impact of Blockchain Technology Implementation on the Efficiency of Notarial Services in the Digital Era in Kediri City, Thesis, Semarang: Master's Program in Notarial Science, Faculty of Law, Sultan Agung Islamic University.
27. S. Skachkova, O. T. V. Chugurova, and E. Kh. Gubaydullina. (2020). Digital Notaries as a Key Element of the Digital Economy: International Experience, 360–66.
28. Saidin ok. (2013). Legal Aspects of Intellectual Property Rights. Jakarta: Rajawali Pers.
29. Shenti Agustini, Autia Kurnia Putri Hapsari, and Emiliya Febriyani. (2024). "The Right to Formal Education for Child Victims of Rape: The Urgency of Reforming the Child Protection Law," Jurnal Yustisia Tirtayasa, 4: 18–41.
30. Siddiqui, Shahbaz et al. (2024). Smart Contract-Based Adaptive Security Governance Architecture for Smart City Service Interoperability, Sustainable Cities and Society 113: 567.
31. Sinaga, Benny. (2023). The Principle of Public Benefit in Tax Amnesty: Lessons from Indonesia, Journal of Tax Law and Policy 3: 155.
32. Sjaifurrachman, Habib Adjie. (2011). The Notary's Accountability in the Preparation of Deeds. Bandung: Mandar Maju.
33. Solehudin, Dede, and Gunawan Djajaputra. (2023). Storage of Notarial Protocols in Cloud Storage within the Cyber Notary Concept, Journal of Society and Technology (SOSTECH), 1: 82.
34. Usman Noor, Muhammad. (2020). The Implementation of Blockchain in the Archival World: Opportunities, Challenges, Solutions, or New Problems, Khizanah Al-Hikmah: Journal of Library Science, Information, and Archival Studies, Vol. 8, No. 1, 89.