Journal of Information Systems Engineering and Management
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Digital Document Security System using Blockchain Technology

Muhammad Fachri[1], Haryono Soeparno[2]
Computer Science Departement, BINUS Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
muhammad.fachri003@binus.ac.id, haryono@binus.edu

ARTICLE INFO

Received: 12 Nov 2024

Revised: 27 Dec 2024

Accepted: 14 Jan 2025

ABSTRACT

Blockchain represents a groundbreaking innovation poised to streamline various human tasks and yield positive impacts, particularly in the realms of managing and safeguarding digital records and data. With the rapid advancement of technologies dedicated to digital document management and security, these digital assets have become prime targets for cyberattacks, potentially resulting in undesirable consequences such as data tampering and forgery. This research delves into the development of a robust digital document security system leveraging Blockchain technology tailored to meet the specific requirements of institutions. Utilizing the Enterprise Blockchain Design Framework, the study aims to ascertain the suitability of Blockchain implementation in current business processes. Subsequently, various popular Blockchain platforms are evaluated based on factors such as functionality, speed, transaction costs, and security. The findings from this selection process inform the design of a Digital Document Security Framework utilizing Blockchain technology, thereby enhancing the integrity and security of digital records.

Keywords: Blockchain, Digital document, Security, Enterprise Blockchain Framework, System design

INTRODUCTION

A crucial component of information management in all business sectors is the fundamental requirement for digital document protection. A digital document needs to be secured according to the following standards: non-repudiation, compliance, sufficiency, completeness, relevance, thoroughness, and correctness (SCHAUDER & KENNEDY, 1996). However, concerns regarding the authenticity of digital documents are frequently caused by security flaws in them, such as forgery, alteration, illegal access, unreliability, and difficulty in searching and accessing them. This is since digital documents are merely data and have no physical form, leaving them open to manipulation and improper management (Penubadi et al., 2023).

The trustworthiness and dependability of institutions or organizations are also enhanced by document security. Clients, consumers, or business partners who deal with organizations that can preserve the confidentiality and integrity of their papers feel more safe and secure. Establishing trust via document security can improve a company's standing and reach new markets. The lack of duplicate information detection in current models frequently results in scenarios where two employees utilize the same file concurrently but with different versions, generating severe disarray that jeopardizes data security and eventually lowers productivity within the company (Bernstein & Dayal, 1994). Additionally, centralized servers are used to store data in current models, which leaves the data on these servers extremely open to assault. Attacks on centralized systems sometimes involve digital copies of the original documents, which raises the risk of data loss and fabrication.

Blockchain technology has become a fascinating answer to these problems in recent years. The coordination, recording, and execution of transactions on the blockchain are unchangeable and tamper-proof, which makes it unique. Blockchain can be used as a platform to store different records of people, groups, and communities in the form of papers, identities, and digital assets because of its distinctive architecture (Zheng et al., 2017).

However, not every Blockchain platform can be used for this. When determining if a Blockchain platform is appropriate for securely protecting digital documents inside a company, there are a number of things to take into account. Thus, the purpose of this study is to present the backdrop of blockchain-based document security.

RELATED WORKS

Blockchain

Peer-to-peer (P2P) transactions between two system participants are made possible by blockchain and are then recorded in a distributed network. Disseminated Ledger Technology (DLT) is a technology that allows transactions to be shared and disseminated across all members of a decentralized distributed network, but it prevents transactions from being changed or removed (Simaiya et al., 2020). The peers connected in the network can conduct their transactions directly and will be verified consensually using algorithms within the network.

Previous study (Lin & Liao, 2017), indicates that there are six (six) key elements of blockchain:

a Decentralization: Distributed recording, storing, and updating of data is possible.

b Transparency: Every network member has access to the data stored on the Blockchain.

c Open Source: Every member of the Blockchain network has access to every record on the network.

d Autonomy: Every Blockchain node can safely move or change data.

e Immutable: No information on the Blockchain can be changed; it will remain unchanged forever.

f Anonymity: If one knows someone's Blockchain address, they can move data or transactions in an even more anonymous manner.

Despite these advantages, Blockchain has several drawbacks that should be taken into account (Drescher, 2017):

a Lack of privacy: All transactional information is disclosed.

b Security model: No one is liable for the account of a third party.

c Limited scalability: Standard Blockchain requires a lot of processing power to perform hash computations to decide whether to add a block to the ledger.

d High costs: Limited scalability problems lead to high capital costs: greater infrastructure investment is necessary for high computational resources.

e Hidden centers: Nodes that process transactions more quickly than others can handle a bigger volume of transactions.

f Lack of flexibility: Because altering a block will alter its hash value, each block cannot be changed.

g Critical size: Blockchain systems need to increase their number of nodes until the probability of a 51 percent attack (where 51 percent of its nodes are controlled by malicious actors) is low.

Blockchain Structure.

On the Blockchain, a block hash is also produced at the time of creation. The block hash will also change if the content inside is going to be added, removed, or altered. (Haber & Stornetta, 1991). As a result, it is extremely improbable that data from a block inside the Blockchain network will be altered or removed.

The Genesis block is the first block without a link to a previous block. It contains initial configuration data, such as protocol version, timestamp (block creation time), block creator information, and the hash of the previous block (usually set to zero), that forms the characteristics and key parameters of the Blockchain) (Koussema & Haga, 2020).

The Blockchain contains confirmed transaction data in every block. A block is made up of a Block Header with:

a Block Version: Identifies the block validation rules that are adhered to.

b Merkle Tree Root Hash: The value of all hashes of transactions within the block.

c Timestamp: The current universal time, expressed in seconds since January 1, 1970.

d nBits: The desired bit threshold for a legitimate block hash

e Nonce: a 4-bit region that normally begins at 0 and grows with each hash computation.

f Parent Block Hash: a hash value of 256 bits that refers to the preceding block

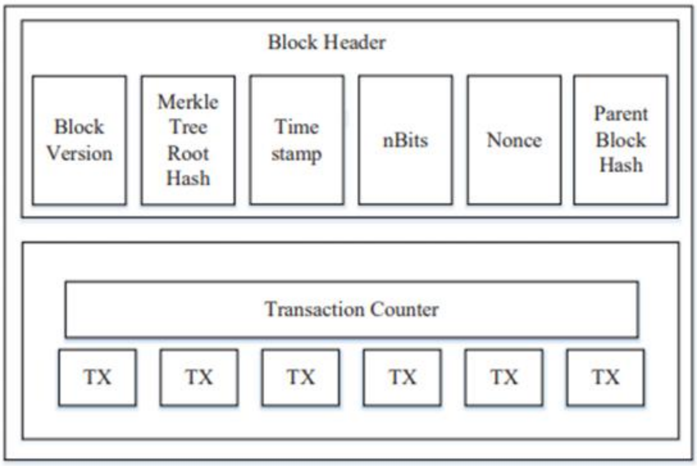


Figure 1 Block Structure

Consensus Mechanisms in Blockchain

Every node in a blockchain network that takes part in the consensus process has a copy of the whole blockchain. These nodes must decide whether a newly proposed transaction is legitimate and ought to be included in the following block. This procedure guarantees the data's consistency and integrity throughout the network (Laatikainen et al., 2023).

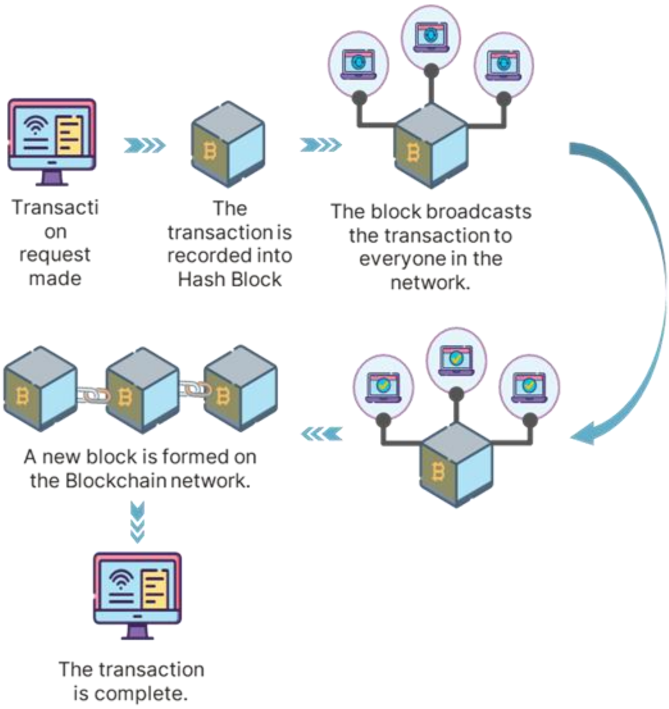
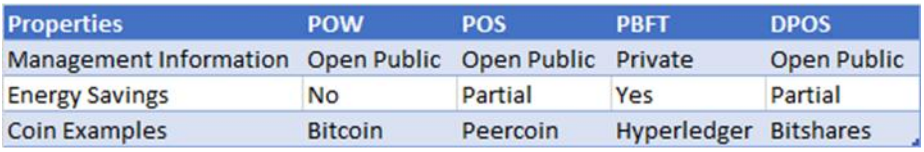

Transacti on request made
The transaction is recorded into Hash Block
The block broadcasts the transaction to everyone in the network.
A new block is formed on the Blockchain network.
The transaction is complete.

Figure 2 Blockchain Workflow

The consensus mechanisms vary depending on the type of Blockchain used. Several unique consensus mechanisms have been designed for Blockchain, such as Some common consensus mechanisms used.

Table 1 Consensus Mechanism Type



Properties	POW	POS	PBFT	DPOS
Management Information	Open Public	Open Public	Private	Open Public
Energy Savings	No	Partial	Yes	Partial
Coin Examples	Bitcoin	Peercoin	Hyperledger	Bitshares

Security and Data Integrity in Blockchain

Blockchain uses cryptography and collaboration to create trust, thereby eliminating the need for centralized institutions to act as intermediaries. Information on the Blockchain is stored in a ledger using cryptography (Guo & Yu, 2022).

Blockchain uses several cryptographic components such as:

a Public Key Cryptography: Used for digital signatures and encryption.

b Zero-Knowledge Proof: A concept wherein any person can use knowledge as long as they don't reveal who used it.

c Hash Function: A mathematical function that is one-way pseudo-random. Merkle Trees use hashing functions to create block header components.

Blockchain Network

Ethereum is still the Blockchain application model used in the majority of Blockchain application research. But the authors of this research want to analyze three well-known Blockchain networks: Ethereum, Polygon, and Solana.

Ethereum is a decentralized Blockchain platform and the second-largest cryptocurrency globally by market capitalization. Ethereum creates a peer-to-peer network for the safe execution and verification of application code, as well as a secure digital ledger known as smart contracts.(Wood, 2014).

Polygon is a decentralized scalability solution specifically designed for the Ethereum network. It enables developers to connect Ethereum-compatible smart contracts to the Polygon platform and create decentralized applications (dApps) that can scale with low transaction costs (Kanani et al., 2021)

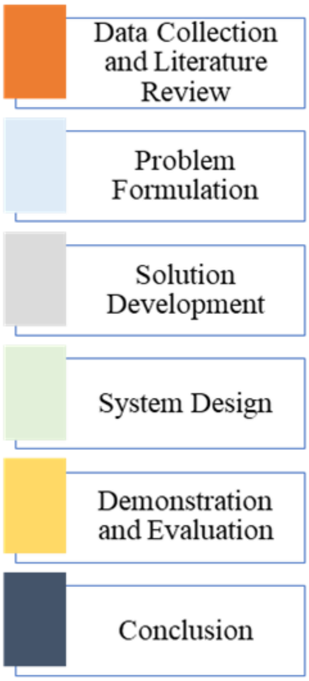
Solana was launched several years earlier than Polygon, although both networks were essentially developed in the same year. Solana was created to provide developers with a platform to build applications similar to Ethereum but with transaction capacity far exceeding Ethereum and almost matching Polygon's capabilities (Yakovenko, 2018).

Table 2 Comparison Table of Ethereum, Polygon, and Solana

Parameter	Ethereum	Polygon	Solana
Token	ETH	MATIC	SOL
Establishment	2013	2017	2017
Programming Language	Solidity	GoLang, Solidity, Viper	Rust, C, C++
Transaction per Second	13 -15	65.000	50.000 – 65.000
Consensus Mechanism	POW (Proof of Work)	POS (Proof of Stake)	Proof of Stake and Proof of History
Architecture	Stateful Architecture	Multichain Architerture	Stateless Architecture
Scalability	Limited Scalability	High Scalability	High Scalability
Gas Fee (Depend on Coin price)	8 - 30 USD	0.0004-0.0006 USD	0.001-0.005 USD)

METHOD

The method used in this research is DSRM (Design Science Research Method). The DSRM methodology focuses on developing innovative solutions for specific problems, carried out through a design and implementation process. The adaptation of the provided guidelines is shown in Figure 3.



Data Collection and Literature Review

Problem Formulation

Solution Development

System Design

Demonstration and Evaluation

Conclusion

Figure 3 Research Stage

Figure 3 research stages can be explained as follows:

a Data Collection and Literature Review: To comprehend the approaches that have been employed in the past, data collecting and literature reviews are carried out.

b Problem Formulation: Understanding the problems based on the knowledge gathered from the earlier phases is the problem formulation that will be investigated in this study.

c Solution Development: This stage is where the challenges that need to be solved are developed.

d System Design: To create a design for protecting digital documents using Blockchain technology, the system design uses a Framework design for Blockchain technology.

e Demonstration and Evaluation:

The developed prototype is tested and its performance is discussed during the demonstration and evaluation stage.

f Conclusion: The last phase in the DSRM process, known as the conclusion stage, is used to compile the findings from the demonstration and evaluation stage.

Data Collection Methods and Problem Formulation.

This research seeks data on existing document security systems through Primary Data and Secondary Data, to understand the current business processes and systems in place at the institution, as well as to establish a foundation for the proposed system. Primary Data is obtained through interviews with selected respondents, while Secondary Data is gathered from existing literature. The list of questions that the researcher posed to the respondents can be seen in Table 3.

Table 3 List of Interview Questions

No	Question
1	Do you have any experience related to the current system?
2	How is the process of storing all data within the current application?
3	What are the obstacles or issues that have been faced in issuing the current system?
4	Are many parties involved in the system?
5	Are all parties involved trusted parties?
6	Is there a possibility of malicious activity or attacks?
7	Is a trusted intermediary needed in the system?
8	Is immutable data needed?
9	Are the rules used uniform?
10	Are the rules regarding the workflow in the process often changing?
11	Can data in the system become public data or be viewed by anyone?
12	What is the business process in issuing letters within the application?
13	What security challenges does the application face?
14	What are the expectations for the development of the application?

The data is collected from employees and administrative staff. Participants are selected using expert sampling, designed to provide information related to the existing system and the issues faced, as the participants are those who have the status, experience, or knowledge required for the purposes of the research.

Solution Development and Designing a Blockchain Model.

To identify the most suitable Blockchain implementation for a specific scenario, a flowchart or diagram can be created. This flowchart should help governments/companies determine the right type of Blockchain to solve existing problems (Nodehi et al., 2022).

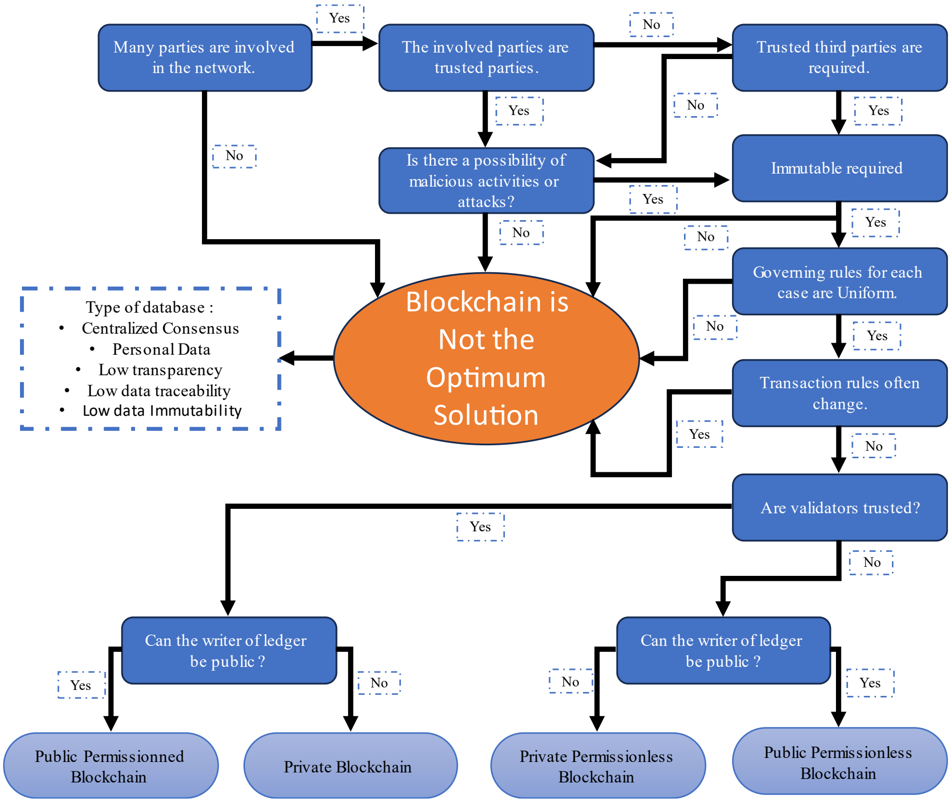

Many parties are involved in the network.
Yes
The involved parties are trusted parties.
No
Trusted third parties are required.
Yes
No
Yes
No
Is there a possibility of malicious activities or attacks?
Immutable required
Yes
No
Yes
No
Type of database :
Centralized Consensus
Personal Data
Low transparency
Low data traceability
Low data Immutability
Blockchain is Not the Optimum Solution
Governing rules for each case are Uniform.
No
Yes
Transaction rules often change.
Yes
No
Are validators trusted?
Yes
No
Can the writer of ledger be public ?
Yes
No
Can the writer of ledger be public ?
No
Yes
Public Permissionned Blockchain
Private Blockchain
Private Permissionless Blockchain
Public Permissionless Blockchain

Figure 4 Enterprise Blockchain Design Framework

Selecting the appropriate option is essential to the execution of any Blockchain project. In order to create a Blockchain ecosystem that is both relevant and ideal in comparison to centralized databases, and to ascertain which type of Blockchain is most appropriate for use, the Enterprise Blockchain Design Framework is employed (Anjana et al., 2019). The author tried to make a comparison between Public Blockchain and Private Blockchain, as indicated in Table 4, in order to further elucidate the choice of Blockchain type to be employed.

Table 4 Comparison of Private and Public Blockchains

Comparison Basis	Public Blockchain	Private Blockchain
Access Rights	Any entity can participate	Limited (Only for specific entities)
Network Participants	Do not know each other	Know each other
Decentralization	Decentralized	More towards Centralization
Speed	Slow	Fast
Transaction per second	Fewer transaction	More compared to public
Security	Public Blockchain networks are more secure due to the larger number of nodes (validators).	Private Blockchains are more vulnerable to manipulation. It is easy for someone with access to manipulate them.
Energy Consumption	More Energy Consumption	Less Energy Consumption
Consensus Algorithms	Proof of Work (POW), Proof of Stake (POS)	Proof of Elapsed Time (PoET), Raft, dan Istanbul BFT.
Network Attacks	Almost impossible to attack, as the validators of Public Blockchain are unknown	Validators of Private Blockchain are clearly known by each entity, making it susceptible to attacks
Digital Coins	Required	Not Required
Example Networks	Bitcoin, Ethereum, Solana,dll	R3, EWF, B3i, HyperLedger, etc

Evaluation Method.

The evaluation within DSRM aims to determine the progress made in designing, building, and utilizing the DSRM artifact in relation to the problems faced. To assess how much progress has been achieved, the evaluation must be conducted with evaluation criteria. In this research, the evaluation criteria adopted are the DSR evaluation and adapted by the researcher, as shown in Table 5.

Table 5 DSR Artifact

Elemen	Goal	Environment	Structure	Activity	Evolution
Efficacy					
Fit With Organization					
Consistency					
Efficiency					
Learning Capability					

Goal: To what extent does the system design produce the desired effect in achieving the goal (objective).

Environment: The criteria for this element is the extent to which the system design is consistent with people, organizations, and technology.

Structure: Structure can be measured by completeness, simplicity, clarity of style, level of detail, and consistency. To what extent can the structure of the system design address the strengths and weaknesses of the current structure?

Activity: Activities can be characterized by completeness, accuracy, performance, and efficiency. This criterion relates to dynamic aspects such as speed, which highly depends on the ratio of system usage activities.

Evolution: Evolution is characterized by the system's ability to learn. The author defines evolution as the capability to respond to environmental fluctuations, such as technological advancements.

RESULT AND DISCUSSION

The results of the system analysis obtained through the process of data collection and fact interpretation conducted at the Ministry of Public Works and Housing regarding the Building Permit Application System aim to identify issues and provide solutions that can assist and enhance all components within the system.

Current System Overview

The Building Permit Application System (SIMBG) is a system for managing building permit documents throughout Indonesia.

Currently, SIMBG facilitates the issuance of Building Permits (PBG), Certificates of Feasibility for Function (SLF), and Certificates of Ownership for Buildings (SBKBG) across all regions of Indonesia.

The Building Permit (PBG) is a permit granted by the local or central government to building owners to construct new buildings, modify, expand, reduce, and/or maintain buildings in accordance with the applicable technical standards for buildings. Meanwhile, the Certificate of Feasibility for Function (SLF) is a certificate issued by the local or central government to declare the suitability of the building's function before the building is utilized.

The Ministry of Public Works and Housing, along with related agencies across all provinces in Indonesia, issues documents such as Building Permits (PBG), Certificates of Feasibility for Function (SLF), and Certificates of Ownership for Buildings (SBKBG), which are then stored in the SIMBG application. The responsibilities for issuing these documents are divided as follows: the issuance of regular Building Permits (PBG) is the responsibility of the local government, while the issuance of Special Function Building Permits (PBGFK) is the responsibility of the Ministry of Public Works and Housing (Kementerian PUPR). This means that PBGFK can only be issued by the Ministry of PUPR, after which it is entered into the SIMBG application system.

Interview Results

Based on the results of the interviews conducted, here are the generalizations of the issues identified from the users of the SIMBG application:

a. All SIMBG data is stored using a centralized storage system, making this platform a very easy target for attacks. There have been instances of web attacks on the SIMBG application, resulting in the loss of data within the application.

b. The Certificate of Feasibility for Function (SLF) is a certificate that must be renewed every 5 to 20 years, necessitating a history of previous SLF issuance.

c. There are still challenges within the data structure of the SIMBG application, leading to some data redundancy, where the same data is recorded in two identical data variables.

Proposed System

In this research, the researcher aims to propose a system that can serve as a solution to the problems previously discussed. The system design will encompass several aspects, including:

a. Decentralization: Data storage will be decentralized, meaning that data storage will not be conducted in a centralized system but will instead utilize a Blockchain network that is most suitable for addressing the current issues.

b. Trusted Third Party: The system will include a trusted third party responsible for executing and validating the documents within the application.

c. Cryptography: The system will incorporate a strong cryptographic algorithm with a high level of security. Each piece of data entering the application will have its own transaction hash.

d. High Scalability: By using the appropriate consensus mechanism, Blockchain technology can handle a large volume of transactions and rapid transaction growth while maintaining integrity, security, and the fundamental principles of decentralization.

Workflow of the System

The workflow for the system will be designed as follows:

a. Uploading Files

A file that has been authorized by each Entity's internal regulatory authority is uploaded using the same template. The logic of the system will be based on this policy.

b. Hashing Process

The document will first go through a hashing procedure that generates a hash code, QR code, date and time, transaction code, block code, and user ID before it is placed in the blockchain.

c. Storing Documents

The certificate will be kept in IPFS (Inter Planetary File System), the document will be kept in the Blockchain network, and the CID (Central Identifier) will be kept in the Blockchain as well.

d. Document Verification

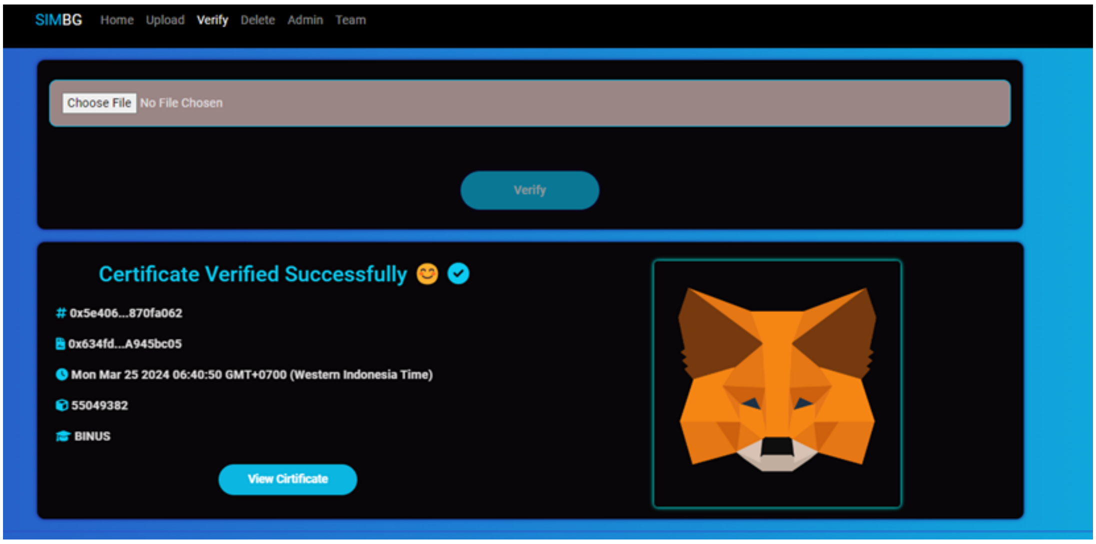
The document must first be posted to the Blockchain in order for it to be verified. Verification of the papers posted to the Blockchain is limited to registered CIDs.

e. Sharing Documents

Users who have successfully authenticated will view all of the certificates they have created on a dashboard page.

Application Design.

In order for the application to function effectively, a front end that focuses on operational simplicity while placing Blockchain technology behind the scenes is necessary.



Certificate Verified Successfully 😊 ✓

0x5e406...870fa062

0x634fd...A945bc05

Mon Mar 25 2024 06:40:50 GMT+0700 (Western Indonesia Time)

55049382

BINUS

Figure 5 Frontend display

First, users will not use a traditional username and password for login, but instead will use Metamask as a replacement. Metamask is used because, in order to log in and perform all functions on the Blockchain, an Address and Private Key from the Blockchain are required. An illustration of Metamask as a substitute for the conventional username and password system can be seen in Figure 6.

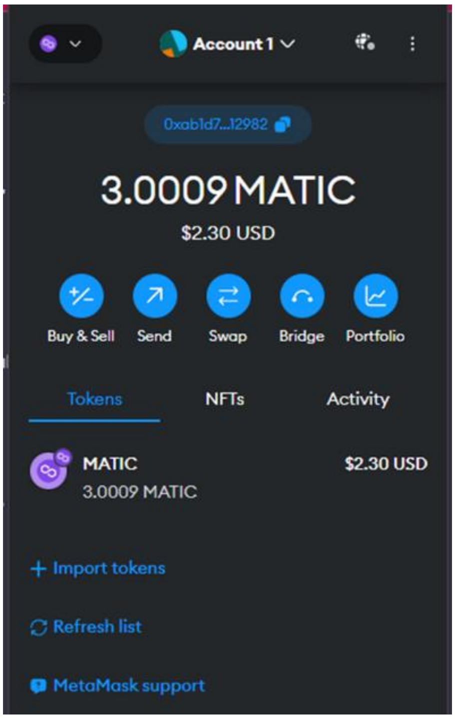


Figure 6 Metamask Wallet

The system will check the user's level within the application, specifically whether the user is an application admin or a regular user. This can be accomplished by verifying the functions embedded in the Smart Contract that has been created.

Data Structure

Blockchain will serve as the database of the system using the Polygon Blockchain network and the Proof of Work consensus concept it employs. The decentralized repository compatible with the Polygon Blockchain in a peer-to-peer manner is IPFS (Interplanetary File System). The IPFS protocol creates a decentralized file storage system on a peer-to-peer network. In IPFS, every data block is identified through cryptographic hashing mechanisms contained within each block. In simpler terms, each file can be accessed through its hash address.

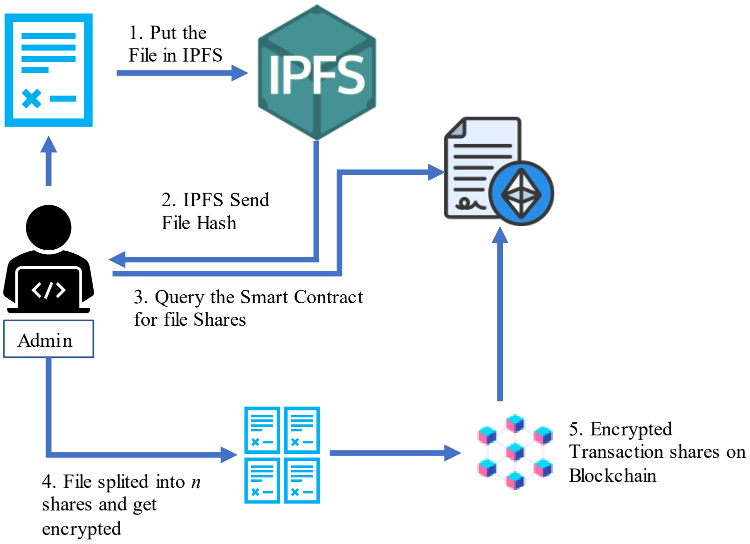

1. Put the File in IPFS
IPFS
2. IPFS Send File Hash
3. Query the Smart Contract for file Shares
Admin
4. File splited into *n* shares and get encrypted
5. Encrypted Transaction shares on Blockchain

Figure 7 How IPFS Works

The data in the Blockchain structure is separated into multiple essential components, including Address data, which indicates the attributes of the parties involved, Transaction Date, which logs the time of the transaction, Hash data, which shows the history of each block, and Previous Hash data, which connects one block to another. Instead of using user IDs and passwords, users get a Wallet Address by using Metamask, a browser extension application. This new paradigm in online access security not only offers users increased convenience but also raises the bar for security.

Functions within the application can be executed on the Blockchain using Smart Contracts that are registered beforehand on the Blockchain network. Remix.ethereum.org is one of the applications used to register Smart Contracts on the Polygon network. This registration enables the application's front end to interact with the Blockchain. Smart Contracts registered on a network will have a Smart Contract ABI (Application Binary Interface) used to call functions from the application and connect to the Polygon Blockchain network. The data structure of the application can be described as follows:

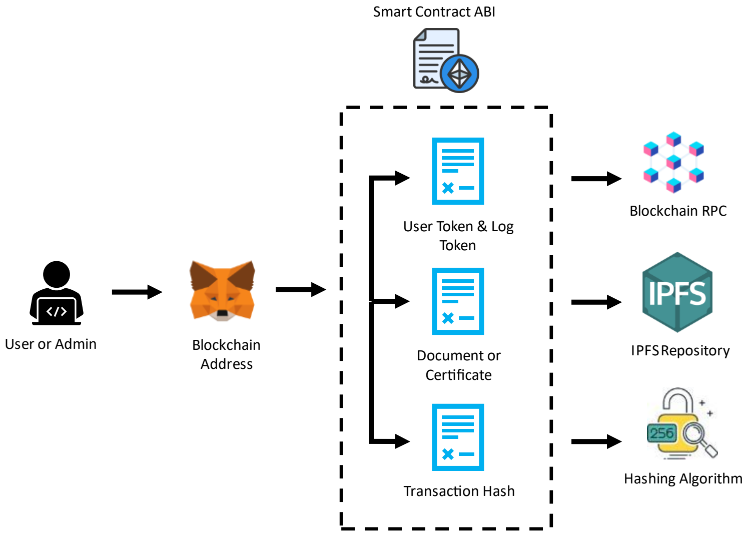
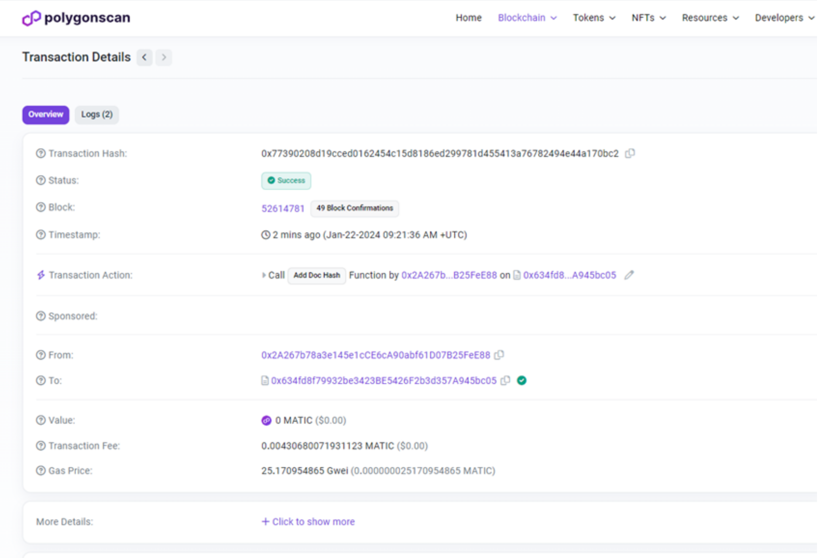


Figure 8 Data Structure Design

Every transaction that occurs within the Blockchain is recorded into the Blockchain network and stored in the Blockchain's repository. Each transaction can be tracked using a Transaction Hash on the explorer of each Blockchain. In this research, the author uses the Polygon Blockchain network, so transactions can be checked through one of Polygon's explorers, namely Polygonscan. All transaction details are recorded in the Blockchain, including fees, timestamp, block information, and transaction type, as shown in Figure 9.



Transaction Details

Transaction Hash: 0x77390208d19cced0162454c15d8186ed299781d455413a76782494e44a170bc2

Status: Success

Block: 52614781 49 Block Confirmations

Timestamp: 2 mins ago (Jan-22-2024 09:21:36 AM +UTC)

Transaction Action: Call Add Doc Hash Function by 0x2A267b...B25FeE88 on 0x634fd8...A945bc05

Sponsored:

From: 0x2A267b78a3e145e1cCE6cA90abf61D07B25FeE88

To: 0x634fd8f79932be3423BE5426F2b3d357A945bc05

Value: 0 MATIC ($0.00)

Transaction Fee: 0.00430680071931123 MATIC ($0.00)

Gas Price: 25.170954865 Gwei (0.000000025170954865 MATIC)

More Details: + Click to show more

Figure 9 Blockchain Hash Transaction

Security Design Evaluation

To understand the advantages of Blockchain in protecting digital documents, it is important to evaluate how this technology responds to various threat scenarios. In terms of security evaluation of the system design that has been created, the author attempts to develop several common cyberattack scenarios and how the system will implement its defense mechanisms against those attacks. Some of the scenarios the author uses are.

a. Sybil Attack

- Scenario: An attacker attempts to take over the network by creating numerous fake identities to impersonate legitimate network members.
- Blockchain Response: Decentralization and consensus protocols like Proof of Work (PoW) or Proof of Stake (PoS) make this attack impractical and extremely costly. The attacker would need to control more than 50% of the nodes in the Blockchain network to manipulate it.

b. Man-in-the-Middle (MitM) Attack

- Scenario: An attacker intercepts and modifies data during transmission.
- Blockchain Response: Data transmitted through the Blockchain network is encrypted, and each block contains the hash of the previous block, ensuring data integrity and security.

c. Distributed Denial of Service (DDoS) Attack

- Scenario: An attacker tries to overwhelm the network with excessive traffic, rendering it unavailable.
- Blockchain Response: Decentralization makes DDoS attacks less effective, as Blockchain has no single point of failure. An attack on one or two nodes in a network will not affect the entire network.

d. Phishing Attack

- Scenario: An attacker tricks users into revealing personal information such as private keys.
- Blockchain Response: Multi-factor authentication (MFA) is used within Blockchain, and in addition to passwords, Blockchain has implemented paraphrases. The use of hardware wallets also helps protect personal information from phishing attacks.

This evaluation demonstrates that Blockchain technology has a strong ability to protect digital documents from various security threats. By implementing mechanisms such as decentralization, encryption, hashing, and consensus protocols, Blockchain offers a comprehensive and reliable solution. However, it is also important to continue raising awareness and improving security practices among users to ensure maximum protection. Through a combination of advanced technology and education, Blockchain is poised to become a key pillar in securing digital documents in the modern era.

CONCLUSION

Conclusion

Based on the results of the research conducted, the researcher presents the following conclusions. Determining the most appropriate type and kind of Blockchain for securing digital documents requires a deep understanding of the business processes, needs, and characteristics of the system to be implemented. The integration of Blockchain must take into account factors such as the desired level of decentralization and the required level of security.

The proposed design in this study has taken into account the factors of security needs and the efficiency of the selected Blockchain by conducting an in-depth understanding of the existing business processes. The implementation of the Enterprise Blockchain Design Framework (EBDF) has also been carried out to determine the suitability of Blockchain implementation with the ongoing business processes. The system design results are evaluated directly using DSR evaluation criteria.

Although the evaluation has been conducted and shows results that meet expectations, several factors still limit the author's ability to perform a comprehensive evaluation of every possible condition that may arise.

Recommendations

This study offers a preliminary understanding of a decentralized blockchain-based smart contract and Key Infrastructure digital document security system. Moving forward, collaboration among multiple stakeholders is imperative to better align the provided system with specific needs.

Given Indonesia's current absence of a private Blockchain network offering full control by the Blockchain owner, the system design proposed in this research utilizes a public Blockchain. However, public Blockchain may not always be optimal for all current business activities. Nevertheless, the limitations of public Blockchain, such as its openness and transaction costs, could potentially be mitigated or adjusted once Indonesia establishes its own blockchain network or domestic blockchain in the future.

REFERENCES

[1] Anjana, P. S., Kumari, S., Peri, S., Rathor, S., & Somani, A. (2019). An efficient framework for optimistic concurrent execution of smart contracts. *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 83–92.

[2] Bernstein, P. A., & Dayal, U. (1994). An overview of repository technology. *VLDB*, *94*, 705–713.

[3] Drescher, D. (2017). Planning the Blockchain. In D. Drescher (Ed.), *Blockchain Basics: A Non-Technical Introduction in 25 Steps* (pp. 57–62). Apress. https://doi.org/10.1007/978-1-4842-2604-9_8

[4] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, *3*(2), 100067.

[5] Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document*. Springer.

[6] Kanani, J., Nailwal, S., & Arjun, A. (2021). Matic whitepaper. *Polygon, Bengaluru, India, Tech. Rep., Sep*.

[7] Koussema, R. A., & Haga, H. (2020). Design and Implementation of Highly Secure Residents Management System Using Blockchain. *Journal of Computer and Communications*, *8*(9), 67–80.

[8] Laatikainen, G., Li, M., & Abrahamsson, P. (2023). A system-based view of blockchain governance. *Information and Software Technology*, *157*, 107149.

[9] Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, *19*(5), 653–659.

[10] Nodehi, T., Zutshi, A., Grilo, A., & Rizvanovic, B. (2022). EBDF: The enterprise blockchain design framework and its application to an e-Procurement ecosystem. *Computers & Industrial Engineering*, *171*, 108360.

[11] Penubadi, H. R., Shah, P., Sekhar, R., Alrasheedy, M. N., Niu, Y., Radhi, A. D., Tharwat, M., Tawfeq, J. F., Gheni, H. M., & Abdulbaqi, A. S. (2023). Sustainable electronic document security: a comprehensive framework integrating encryption, digital signature and watermarking algorithms. *Heritage and Sustainable Development*, *5*(2), 391–404.

[12] SCHAUDER, C., & KENNEDY, J. A. Y. (1996). Records Management in Australia: An Overview. *Records Management Journal*, *6*(3), 161–172. https://doi.org/10.1108/eb027094

[13] Simaiya, S., Lilhore, U. K., Sharma, S. K., Gupta, K., & Baggan, V. (2020). Blockchain: A new technology to enhance data security and privacy in Internet of things. *Journal of Computational and Theoretical Nanoscience*, *17*(6), 2552–2556.

[14] Wood, E. (2014). A secure decentralised generalised transaction ledger, ethereum proj. *Yellow Pap*, *151*(1).

[15] Yakovenko, A. (2018). Solana: A new architecture for a high performance blockchain v0. 8.13. *Whitepaper*.

[16] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564.