Analysis of the Potential Implementation of Blockchain Technology to Enhance Efficiency and Security in Financial Transactions in Indonesia

Adytia Wiguna Gunawan, Ngui Su Ying, Hady Pranoto, Risma Yulistiani
Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
adytia.gunawan@binus.ac.id, ngui.ying@binus.ac.id

***Abstract*— There are a lot of issues when it comes to securing transactions, especially for finance purposes. Those issues can be something like lack of transparency, lack of efficiency, and lack of security. To prevent those issues or threats, blockchain technology is made and used. Blockchain technology is a database of records of transactions that are distributed, validated, and maintained by a network of computers around the globe. It is a decentralized database system where no third party has control over it. Blockchain technology offers a more transparent and secure system, where each block is hashed by a SHA-256 hash and it's also bounded to the previous block, forming some sort of chain of blocks. The security of it increased furthermore using the Proof-of-Work (PoW) mechanism. After doing some testing, it was found that utilizing the property of blockchain technology could improve Indonesia's financial sector efficiency and security.**

Keywords— Blockchain, Transaction, Security, Block, Chain, Cryptocurrency, Decentralized, Hash, Proof-of-Work.

I. Introduction

Blockchain is a technology that is usually associated with cryptocurrencies, such as Bitcoin, Ethereum, and many more. Blockchain technology is a database of records of transactions that are distributed, validated, and maintained by a network of computers around the globe. It is a decentralized database system where no third party has control over it [38]. With that being said, no one can go back and change or erase a transaction history. Different from a normal centralized database system, blockchain technology is distributed among the users of the software. Blockchain technology enables anyone on the network to access everyone else's entries which makes it impossible for a third party or someone to take control of the whole network. Whenever someone makes a transaction, it goes through the network and computer algorithms to determine the authenticity of the transaction. Once the transaction is verified, this new transaction is stored in a "box" or a "block" and is linked with the previous transactions forming a chain of transactions. This chain of transactions is called blockchain.

In a developing and large population country like Indonesia, many transactions are performed every day and every time. Utilizing and implementing blockchain technology to secure and integrate these transactions, could potentially help Indonesia to unlock its full economic power.

By implementing blockchain technology, it will make sure every transaction in Indonesia is secured and verified. Any cyber attack to change, modify, or even interrupt any transactions will be avoided by implementing blockchain technology [39]. This could also potentially eliminate one of the biggest problems in Indonesia, which is corrupt practices. The main issue with corrupt practices is that the transactions that occur are very much a secret to anyone else besides the one involved in them and the third party or the bank that is used for those transactions. In other words, there is no transparency whatsoever. With blockchain technology, it ensures everyone will have access to the transaction records. It also ensures the security of the transactions, since no one can take control over it.

II. Literature Review

A. Introduction to Blockchain Technology

Blockchain technology is a form of peer-to-peer model architecture. It's a decentralized and distributed database system that enables the secure recording, verification, and transfer of data across a network of computers. Blockchain works by creating blocks for each transaction that occurs and linking them to the other blocks to form a chain. As an example to see how blockchain works, person A wants to send money to person B, so it requests a transaction to be performed. Then, the system makes a block to store this transaction. After the block is made, the block is broadcast to every part of the network. It ensures that the whole network knows there's a new transaction being made. After knowing that a transaction is being made, every part of the network will send their approval to make sure that the transaction is valid. With the approval of the network, the transaction is now valid and will be linked to the other blocks in the network. After going through all of that process, the transaction is now linked and valid, then the money from person A is removed and added to person B.

B. Applications of Blockchain in Finance

The application and implementation of blockchain technology in the financial sector are commonly used now. The way that blockchain is a decentralized database system, might be the greatest factor as to why it's commonly used now in the financial sector. Blockchain technology offers many different types of benefits.

The first benefit is transparency. Every transaction made in a blockchain system is broadcast throughout the whole network. This means, that every part of the network will know that a transaction is being made. Unlike banks or any other third-party entity, everyone that part of the network also has access to every transaction entry that is stored inside each block.

The second benefit of using blockchain in finance is security. Unlike banks or any other third-party entity in which a transaction is easily hacked, modified, or even deleted, every transaction entry in a blockchain technology system that is stored in each block can not be changed or modified by anyone and its records will always be there no matter what.

Lastly, the benefit of implementing blockchain technology in finance is availability. In “normal” standards, when checking some data or transaction entries, people must wait and go through all of the processes that are provided by the bank or any other third-party entity involved. Unlike that, blockchain technology always provides access to everyone that is part of the network. This means that anyone can check their transaction entries or any transaction in which they are involved, anytime and anywhere.

C. Blockchain Implementation and Challenges in Indonesia

Blockchain is the technology to store and access data because blockchain guarantees data security and transparency, the advantages of blockchain make it suitable for several fields in Indonesia especially finance. The implementation of blockchain in Indonesia is quite challenging[22]. Blockchain is a technology that has a big role in finance, it requires human resources who are capable in finance for the next few years. There are inefficiencies caused by limited human resources and the skills gap between the company's needs and worker's competencies in the workforce.

Even though technology keeps innovating, cybersecurity still can't be solved. Technological innovations have become a challenge to solve data management, especially blockchain. Blockchain operates in the finance sector which holds sensitive personal data. Human resources are involved with the personal data, and human resources with integrity are needed who maintain the privacy of the personal data. Data protection authorities and other regulators are slow in handling data problems in blockchain technology. Authorities also impose ambiguous and complex requirements on data privacy in the use of blockchain technology.

Blockchain stores a lot of data and data is added every day so it requires a large capacity. The solution to blockchain capacity by using cloud storage. The use of cloud computing on blockchain has the potential for cybersecurity attacks. If blockchain using cloud storage means that the stored data is spread as storage duplicates throughout various data centers. The implementation of blockchain in Indonesia is a solution to problems in several fields and also provides challenges to solve the problems created by blockchain technology.

D. Regulatory Framework and Policy Implications of Blockchain

The innovation of Blockchain technology brought a revolution in several fields such as finance, supply chain management, and governance. The application of blockchain provides convenience besides the benefit given on a big scale, the risk of a cyber attack on blockchain applications is very high. This is caused by Indonesian law not being strict about their legal protection to protect personal data[20]. Based on the 1945 Constitution Article 32, a citizen has the right to control their personal data.

Unlucky, some written Indonesian laws failed to protect their citizen data, thus causing a very fatal data leak. Leakage data become a concern and awareness about the security of user data. The implementation of peer-to-peer network architecture is contrary to the GDPR and CCPA regarding centralized controller-based data processing. The implementation of blockchain clashes between features, and legal protection is getting more complicated to create. This is proof of the possibility of how data can be leaked and used by the company. The weakness of legal protection becomes momentum for companies to take the authority to manage user data without restrictions so data will be unprotected and owners of the data may lose control of their belongings. Legal protection must be clear to build trust and legal certainly among users.

In Indonesia, there are at least several regulations governing digital crime, namely Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Several other rules regarding the protection of personal data are regulated in at least 32 different laws and regulations, such as Law Number 36 of 2009 concerning Health, which regulates the confidentiality of patients' conditions, while Law Number 10 of 1998 concerning Banking regulates the personal data of depositors and savings. Additionally, regulations regarding the protection of privacy and personal data are also contained in Law Number 36 of 1999 concerning Telecommunications, Law Number 39 of 1999 concerning Human Rights, Law Number 23 of 2006 concerning Population Administration (amended by Law Number 24 of 2013), and Law Number 11 of 2008 concerning Electronic Information and Transactions (amended by Law Number 19 of 2016), as well as Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. Even though Indonesia already has some legal protection to protect user data the amount of data leak cases is getting worse and worse.

E. Potential Efficiency and Security of Blockchain

The implementation of Blockchain offered a helpful solution. The implementation of Blockchain requires a high-technology solution for some problems in the industry and government especially in finance. Blockchain implementation provides transparency and immutable record-keeping capabilities. The advantages of blockchain make it easier for monitoring and auditing so the money laundering cases can be solved by this technology.

When the industry implements smart contracts, a company can increase operation efficiency without paying more. Smart contract on blockchain technology provides facilities to verify the negotiation digitally. The implementation of blockchain also enhanced security to protect the user's sensitive data from data leaks. This is an opportunity for Indonesia to enhance security by implementing blockchain. Blockchain protects user-sensitive data from data leaks. Data leak cases can also be resolved by implementing blockchain. The great security of blockchain in Indonesia is a big opportunity for some sectors that implement blockchain because blockchain enhances efficiency.

III. METHODOLOGY

This paper explores the potential implementation of blockchain technology to enhance efficiency and security in financial transactions in Indonesia. There are three stages in the financial sector's analysis and implementation process of blockchain technology: Data *Collection*, *Development*, and *Testing*.

A. *Information Gathering*

In the first phase of this study, information about blockchain technology and its potential applications in financial transactions is collected. This includes understanding the blockchain mechanism, types of blockchain platforms, and specific commands or processes used in blockchain transactions. Financial applications can vary significantly based on the blockchain technology employed.

1) Blockchain mechanism
   To find out the possibilities of using blockchain technology to enhance security and efficiency in financial transactions in Indonesia, a comprehensive analysis has to be done on consensus protocols and blockchain processes. Key areas have been considered which include immutability, smart contracts, decentralization, Proof-of-Work (PoW), Proof-of-Stake (PoS), Byzantine fault-tolerance (BFT) as well as security features. This information regarding the technology behind blockchains would help evaluate its suitability in securing transactions due to its ability to write agreements into code, have voting take place automatically, and secure individual transaction processing.
2) Types of blockchain platforms
   A review was conducted to explore types and platforms of blockchain whereby blockchains were categorized according to data accessibility (public, private, consortium, hybrid), authorization requirements (permissionless, permissioned, hybrid), and core functionalities (stateless, stateful). The study also looked at various blockchain platforms that included modules like blockchain runtime environment, cryptographic services; smart contract module, and blockchain secondary storage among others. This depicts the heterogeneous nature of the technology on which a firm can apply different types of blockchain to make it secure transparent and faster in many industries. Such an understanding is important for exploring the applicability of blockchain technology towards improving efficiency and security in financial transactions in Indonesia because it aids in choosing the best type of currency for specific financial industry demands as well as regulatory concerns within this region.
3) Commands or processes used in blockchain transactions
   To significantly improve the effectiveness and safety of financial transactions in Indonesia through blockchain technology, an understanding of the detailed processes involving blockchain transactions should significantly inform their potential implementation. Blockchain operations entail generating and transferring e-coins utilizing a succession of digital signatures that produce a verifiable chain of ownership and prevent double spending through public announcement of transactions followed by agreement on their order. A timestamp server hashes blocks of transactions, with each timestamp reinforcing the previous ones, forming an immutable chain. The Proof-of-Work mechanism requires substantial computational work to be performed to find specific hash values, thus protecting the network from assaults that would otherwise make it impossible to change past transactions without redoing all subsequent blocks. This system relies on incentives for nodes like new coin creation and transaction fees that promote network participation and security. Merkle Trees efficiently manage disk space; hence old transactions can be discarded without compromising the integrity of the blockchain. Simplified Payment Verification (SPV) allows users to confirm payments without having to run full network nodes but trusting that they are seeking a confirmation is in the maximum Proof-of-Work chain possible.

B. *Development*

In the second phase of this study, an attempt to implement blockchain technology is made. It is important to define the use case to identify the specific issue that blockchain can solve, in this case, to improve security in financial transactions. Then, choosing an appropriate blockchain platform is necessary where there are options like Ethereum, Hyperledger Fabric or Corda each offering different sets of features tailored to its needs. Setting up a blockchain network involves nodes and a consensus mechanism such as Proof-of-Work (PoW) or Proof-of-Stake (PoS) is needed to guarantee transaction agreement validity by all participants.

The deployment of a blockchain network is done by launching it and continuously monitoring how it performs and is secure. The working of blockchain implemented is done by securing every transaction by various methods. The transaction record is given a block and is connected to the previous block by using cryptography hashing. This way a chain is formed which cannot be altered. The digital signatures are used in the transaction initiation and can only be used by the authorized parties. The decentralized blockchain network properties avoid the single point of failure and reduce the chances of hacking and data alterations.

Lastly, the consensus mechanism of blockchain technology, be it PoW or PoS, guarantees that all transactions are verified and endorsed by most of the network participants hence enhancing further security. Simplified Payment Verification (SPV) allows users to confirm transactions without having to download the entire blockchain, thereby maintaining security and optimizing efficiency. This can widely enhance the security and efficiency of financial transactions through the implementation of these processes, which enable a strong framework against fraud as well as ensure transparency and trust in the financial system. It is imperative to understand how blockchain technology might alter financial transactions in Indonesia thus providing information on what would make an effective implementation toward attaining this objective.

In short words, in this development stage, an implementation of blockchain algorithm with a proof-of-work feature to enhance its security is made.

C. Testing

In this study's third and last phase, an algorithm for blockchain technology implementation and testing how it performs is done. In this case, the algorithm is made using the Python programming language.

The first thing to do is import all the necessary libraries that are needed. After importing all the necessary libraries, initialize the blockchain class. Next, define a new function and this new function is used to create new blocks. Following the last step, create a new function to add transactions. To provide a convenient way to access the last block in the chain, create a new function to get the last block. After that, define a method to create a SHA-256 hash of a block. To guarantee that all transactions are verified and endorsed by most of the network participants, implement the Proof-of-Work (PoW) algorithm to secure the blockchain even more. Lastly, validate the proof by checking if the hash of the combination of the last proof and the current proof contains leading zeroes. After the algorithm is made, testing is conducted to test how it performs.

```python
# Create the blockchain
blockchain = Blockchain()

# Add a transaction
block1 = blockchain.new_transaction("sender_address", "recipient_address", 5)
block2 = blockchain.new_transaction("sender_address_2", "recipient_address_2", 10)
block3 = blockchain.new_transaction("sender_address_3", "recipient_address_3", 15)

# Display the blockchain
print(json.dumps(blockchain.chain, indent=4))
```

In this example, three transactions are made, hence there will be three blocks (not including the genesis block) created in the blockchain.


```json
[
    {
        "index": 1,
        "timestamp": 1719085352.247614,
        "transactions": [],
        "proof": 100,
        "previous_hash": "1"
    },
    {
        "index": 2,
        "timestamp": 1719085352.4664538,
        "transactions": [
            {
                "sender": "sender_address",
                "recipient": "recipient_address",
                "amount": 5,
                "nonce": "1be142344c584c8992a53c0f287e3270"
            }
        ],
        "proof": 35293,
        "previous_hash": "f8e3ef0c8da9acc495347f68479ceb07f38b63683888e17d07a43ce9e4d9c137"
    },
    {
        "index": 3,
        "timestamp": 1719085352.6914978,
        "transactions": [
            {
                "sender": "sender_address_2",
                "recipient": "recipient_address_2",
                "amount": 10,
                "nonce": "a850f210c7364fd1809f485fea109b72"
            }
        ],
        "proof": 35089,
        "previous_hash": "6ca4d00bd1a0a8a7cec9ed0db927f62467318b3939d52af2b6e731327e071991"
    },
    {
        "index": 4,
        "timestamp": 1719085353.274394,
        "transactions": [
            {
                "sender": "sender_address_3",
                "recipient": "recipient_address_3",
                "amount": 15,
                "nonce": "72ea7502d4624ce186b90c19ecf82f6a"
            }
        ],
        "proof": 119678,
        "previous_hash": "9b933090c0517d38a9c3dc9956ce059a790edc28f3fb913b24db4be3104afe12"
    }
]
```


IV. Result & Discussion

In this part of the study, three all-around tests were done to find out if this blockchain algorithm is perfect in terms of finance transaction safety, optimality, and reliability. These include unit testing, integration testing, and security testing which covers diverse angles on the performance of a blockchain and its security.

A. Unit Test

Unit testing is the first step in verifying the correctness of the blockchain implementation. This involves breaking down the code into its smallest testable parts and verifying that each part functions correctly.

Unit Name	Description	Function or Method	Test Description	Expected Outcome	Successful? (Y/N)
Blockchain Init	Initialize the blockchain with the genesis block	__init__	Test if the blockchain initializes correctly with the genesis block.	Blockchain should have one block with index 1, proof 100, and previous_hash "1".	Y
New Block	Create and add a new block to the blockchain	new_block	Test creating and adding a new block.	New block should be added with correct index, proof, and previous_hash.	Y
New Transaction	Create a new transaction and add it to a block	new_transaction	Test creating a new transaction and adding it to a new block.	New block with the transaction should be added to the blockchain. Transaction should have correct sender, recipient, amount, and unique nonce.	Y
Generate Nonce	Generate a unique nonce for each transaction	generate_nonce	Test if nonce generation is unique.	Each call to generate_nonce should return a unique string.	Y
Last Block	Return the last block in the blockchain	last_block	Test retrieving the last block in the chain.	Should return the most recently added block with correct data.	Y
Hash Block	Create a SHA-256 hash of a block	hash	Test hashing a block.	Should return a consistent SHA-256 hash string for the same block data.	Y
Proof of Work	Implement a proof-of-work algorithm to find a valid proof	proof_of_work	Test finding a valid proof.	Should return a proof integer that satisfies the condition (leading 4 zeroes).	Y
Valid Proof	Validate the proof by checking if it contains leading 4 zeroes	valid_proof	Test validating proof.	Should return True if proof is valid (leading 4 zeroes), otherwise False.	Y

The result of this test shows that the algorithm is successful because all of the individual units in the algorithm run perfectly as intended. Each test confirms that the designated functions and methods are performed correctly and with high efficiency by the blockchain system. The overall dependability and functionality of a blockchain implementation are strongly grounded on the success of such unit testing.

B. Integration Test

After testing all of the key units in the blockchain system individually, a test to see how they work together must also be conducted, to see how it works as a single system.

Test Case No.	Test Description	Pre-conditions	Steps to Execute	Expected Outcome	Successful? (Y/N)
1	Initialize Blockchain	None	1. Create a new instance of Blockchain.	Blockchain should initialize with the genesis block having index 1, proof 100, and previous_hash "1".	Y
2	Add First Transaction and Block	Blockchain initialized	1. Call new_transaction with sender, recipient, and amount. 2. Verify the transaction is included in the new block.	Blockchain should have 2 blocks, with the new block containing the transaction and a valid proof of work.	Y
3	Add Multiple Transactions and Blocks	Blockchain initialized	1. Call new_transaction multiple times with different sender, recipient, and amount. 2. Verify each transaction is included in new blocks.	Blockchain should have multiple blocks, each containing a transaction with correct sender, recipient, amount, and unique nonce.	Y
4	Validate Proof of Work for Multiple Blocks	Blockchain initialized with multiple transactions	1. Retrieve the proof of work for each block. 2. Verify proof of work for each block using valid_proof method.	Each block should have a valid proof of work that satisfies the condition (leading 4 zeroes).	Y
5	Validate Previous Hash Linking	Blockchain initialized with multiple transactions	1. Retrieve the previous hash for each block. 2. Verify the previous hash matches the hash of the previous block.	Each block should correctly reference the hash of the previous block, ensuring the chain integrity.	Y
6	Verify Blockchain Integrity	Blockchain initialized with multiple transactions	1. Traverse the blockchain. 2. Verify integrity of each block by checking index, previous_hash, and proof.	The blockchain should maintain integrity, with correct indices, previous hashes, and valid proofs for all blocks.	Y
7	Generate Unique Nonce for Transactions	Blockchain initialized	1. Call generate_nonce multiple times. 2. Verify each nonce is unique.	Each call to generate_nonce should return a unique string.	Y
8	Hashing Blocks	Blockchain initialized	1. Call hash method on each block. 2. Verify the hash is a valid SHA-256 hash.	The hash for each block should be a valid SHA-256 hash string.	Y

From the results of integration testing, it is clear that this algorithm is functioning correctly and efficiently. The test findings show that all elements in the blockchain system work well together, affirming the soundness and efficient implementation of the algorithm. For, the approach ensures that new transactions are made, new blocks mined and the integrity of the blockchain verified through this algorithm thus ensuring each component interacts as expected within a wider system.

C. Security Test

To make sure blockchain is resistant to attacks and tampering, it is important to conduct security tests. This involves replication of various possible attack scenarios to evaluate the ability of the blockchain network to identify and repel such activities. For this research, a tamper detection test and a replay attack prevention test are being used.

To ensure that every block in the chain has not been altered, the "previous_hash" attribute in each block correctly points to the hash of the previous block. Therefore, any tampering with a single block will definitely cause mismatching in all other subsequent blocks leading to the detection of tampering.

The presence of “nonce” which is generated using “uuid.uuid4().hex” per transaction ensures that every transaction generated is unique hence preventing attackers from reusing transactions as they try manipulating the blockchain system.

Test Case No.	Test Description	Pre-conditions	Steps to Execute	Expected Outcome	Successful? (Y/N)
1	Prevent Double Spending	Blockchain initialized	1. Create a transaction from a sender. 2. Attempt to create another transaction from the same sender before the first is confirmed.	The second transaction should be rejected or create a new block with proof of work, ensuring no double spending.	Y
2	Validate Proof of Work	Blockchain initialized	1. Add multiple transactions. 2. Verify the proof of work for each block.	Each block should have a valid proof of work that satisfies the condition (leading 4 zeroes).	Y
3	Verify Blockchain Integrity Against Tampering	Blockchain initialized with multiple transactions	1. Manually alter a block's data. 2. Verify the integrity of the blockchain.	The altered block should invalidate the blockchain, failing integrity checks.	Y
4	Ensure Previous Hash Consistency	Blockchain initialized with multiple transactions	1. Traverse the blockchain. 2. Verify each block's previous_hash matches the hash of the previous block.	Each block's previous_hash should correctly reference the previous block's hash, ensuring chain integrity.	Y
5	Nonce Uniqueness for Transactions	Blockchain initialized	1. Generate multiple transactions. 2. Verify each transaction's nonce is unique.	Each transaction should have a unique nonce.	Y
6	SHA-256 Hash Validation	Blockchain initialized	1. Call the hash method on each block. 2. Verify the hash is a valid SHA-256 hash.	The hash for each block should be a valid SHA-256 hash string.	Y
7	Prevent Replay Attacks	Blockchain initialized	1. Record a transaction. 2. Attempt to add the same transaction again.	The blockchain should detect and prevent the replayed transaction.	Y
8	Confirm Valid Proof of Work for New Transactions	Blockchain initialized with multiple transactions	1. Add a transaction. 2. Verify the proof of work for the block containing the transaction.	The proof of work should be valid for the new block.	Y
9	Validate Genesis Block Properties	None	1. Initialize the blockchain. 2. Verify properties of the genesis block (index, proof, previous_hash).	The genesis block should have index 1, proof 100, and previous_hash "1".	Y
10	Test against Malicious Node Adding Invalid Transactions	Blockchain initialized	1. Add an invalid transaction manually (e.g., negative amount). 2. Verify the blockchain's reaction.	The blockchain should reject the invalid transaction.	Y

The output of the security testing indicates correctly and efficiently operating blockchain algorithm. The test results also show that the system is strong against tampering detection and replay attack prevention, both of which are integral aspects of blockchain security.

D. Test Result

Test Type	Running Time	Succesful? (Y/N)
Unit Test	0.001 second(s)	Y
Integration Test	0.001 second(s)	Y
Security Test	0.001 second(s)	Y

After testing the algorithm with those three testing methods, it is proven that the blockchain algorithm that is made runs efficiently and is secure.

V. CONCLUSION

The success of testing the basic implementation of a blockchain algorithm in this study shows promise, Indonesia's financial sector has a great chance to be completely transformed by blockchain technology. Blockchain can improve transaction efficiency significantly, as indicated in findings of this study. The study also mentions that these improvements are caused by reduction in processing times and optimization of conventional banking systems. Furthermore, trust, transparency, and immutability provided by decentralized verification make it possible to prevent fraud and interference with transactions thus enhancing the belief in financial operations. This research highlights on blockchain’s role of promoting financial inclusion, particularly for the unbanked population through easily accessible and secure digital finance services. By integrating blockchain technology into its financial system, Indonesia can increase operational efficiency, harmonize regulatory compliance, and create an inclusive economic environment that is resilient too. The paper concludes that strategic adoption and implementation of blockchain technology could bring about major advances in Indonesia's financial infrastructure thereby supporting sustainable economic development as well as creations of novelty.

REFERENCES

[1] U. Rahardja, Q. Aini, M. Yusup, & A. Edliyanti. (2020). "Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce," CESS (Journal of Computer Engineering, System and Science), vol. 5, hal. 28, doi: 10.24114/cess.v5i1.14893.

[2] E. P. Harahap, Q. Aini, & R. K. Anam.(2019). "Pemanfaatan Teknologi Blockchain pada Platform Crowdfunding," Technomedia Journal, vol. 4, pp. 199-210, doi: 10.33050/tmj.v4i2.1108.

[3] F. W. Delli, S. Nurdiati, A. Buono, dan E. Santosa.(2021). "Blockchain dan Kecerdasan Buatan dalam Pertanian: Studi Literatur," J. Teknol. Inf. Ilmu Komputer, vol. 8, hal. 177, doi: 10.25126/jtiik.0814059.

[4] Loso Judijanto, Wildoms Sahusilawane, dan Eva Yuniarti Utami.(2024)."Sanskara Akuntansi dan Keuangan," vol. 2, no. 2, PT. Sanskara Karya Internasional. https://sj.eastasouth-institute.com/index.php/sak/article/view/321/146

[5] Luthfiyyah, Z. (2023). "IMPLIKASI BLOCKCHAIN PADA KECURANGAN AKUNTANSI: TELAAH LITERATUR SISTEMATIS (SLR)". Fakultas Ilmu Ekonomika dan Bisnis,12. https://eprints2.undip.ac.id/id/eprint/19487/

[6] Argani, Abimanyu & Taraka, Wahyatma. (2020). "Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi". ADI Bisnis Digital Interdisiplin Jurnal. 1. 10-21. doi: 10.34306/abdi.v1i1.121.

[7] Warijo, Inka. (2024). "PENERAPAN BLOCKCHAIN PADA LINGKUNGAN PENDIDIKAN".doi: 10.13140/RG.2.2.23691.30246.

[8] Khaerunisa, T. F., & Enjat Munajat, M. D. (2022). "SOLUSI PEMANFAATAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI PERMASALAHAN PENYALURAN DANA BANTUAN SOSIAL COVID-19". JANE - Jurnal Administrasi Negara, 13(2), 264. doi: 10.24198/jane.v13i2.35133

[9] Rahardja, Untung. (2022). "Skema Catatan Kesehatan menggunakan Teknologi Blockchain dalam Pendidikan". Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi. 1. 29-37. 10.34306/mentari.v1i1.134.

[10] Julianto. (2023). "ANALISIS SISTEM PADA NFT (NON-FUNGIBLE TOKEN) DAN PERKEMBANGANNYA DALAM DUNIA BISNIS". 3. 50-75. doi: 10.46306/sm.v3i1.36.

[11] Grahal, Ega Rudy & Wardhani, Ire Puspa.(2022).Kajian Literatur Penerapan Teknologi Blockchain pada Human Computer Interaction. Jurnal Ilmiah Komputasi, 21(1). doi: 10.32409/jikstik.21.1.2932

[12] Ruslan, Z. (2022). "Blockchain Letter of Credit: Apakah Sekarang Saatnya?". Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 5(1), 493–508. doi: 10.32670/fairvalue.v5i1.2189

[13] Atmomintarso, B. E., & Wirawan, W. (2021). "Sistem Pelaporan Pajak Pertambahan Nilai pada Web dengan Menggunakan Teknik Blockchain". Jurnal Teknik ITS, 10(2). doi: 10.12962/j23373539.v10i2.65827

[14] Apriani, D., Nur Azizah, N., Ramadhona, N., & Kusumawardhani, D. A. R. (2023). "Optimasi Transparansi Data dalam Rantai Pasokan melalui Integrasi Teknologi Blockchain". Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi, 2(1), 1–10. doi:10.33050/mentari.v2i1.326

[15] Xu, Min & Chen, Xingtong & Kou, Gang. (2019). "A systematic review of blockchain". Financial Innovation. 5. doi: 10.1186/s40854-019-0147-z.

[16] Saha, Satarupa & Jana, Bappaditya and Poray, Jayanta. (2019)." A Study on Blockchain Technology". SSRN Electronic Journal,6. doi: 10.2139/ssrn.3477373

[17] "Kogon, Jeffrey. (2017)." Blockchain Technology: An Analysis of Potential Applications and Uses"". Honors College Theses. 157.

[18] https://digitalcommons.pace.edu/honorscollege_theses/157"

[19] Saputra, Upayana Wiguna Eka, & Gede Sri Darma. (2022). "The Intention to Use Blockchain in Indonesia Using Extended Approach Technology Acceptance Model (TAM)". CommIT (Communication and Information Technology) Journal, 16, 27-35. doi: 10.21512/commit.v16i1.7609

[20] "Pujiyono, P., Imanullah, M. N., Hadi, H., & Waskita, S. (2023). "The role of blockchain in strengthening Indonesia's economic stability." In Proceedings of the International Conference for Democracy and National Resilience 2022 (ICDNR 2022), pp. 198–207. Atlantis Press SARL. doi: 10.2991/978-2-494069-75-6_25

[21] Putra, M. R. S., Yapputro, P. A., Najmi, M. S., & Dianova, E. R. (2022). "Protection of personal data of BPJS health users against data leakage". International Journal of Law and Politics Studies, 4(2), 98–108. doi: 10.32996/ijlps.2022.4.2.11

[22] Tedjakusuma, Adi & Yahya, Bernardo Nugroho. (2020). "A Study into Opportunities and Challenges of Blockchain Adoption for Sustainable Nonfinancial Sector Micro, Small, Medium Enterprises—Case Studies in Indonesia". doi: Advances in Economics, Business and Management Research,15. doi: 10.2991/aebmr.k.200127.007.

[23] P. A. Sunarya, "Penerapan Sertifikat Pada Sistem Keamanan Menggunakan teknologi blockchain," Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, vol. 1, no. 1, pp. 58–67, Sep. 2022. doi:10.33050/mentari.v1i1.139

[24] I. Elan Maulani, T. . Herdianto, D. . Febri Syawaludin, and M. . Oga Laksana, "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi", Jurnal sostech, vol. 3, no. 2, pp. 99–102, Feb. 2023.

[25] C. Lukita, "Penerapan Sistem Pendataan Hak cipta content menggunakan blockchain," ADI Bisnis Digital Interdisiplin Jurnal, vol. 1, no. 2, pp. 40–45, Dec. 2020. doi:10.34306/abdi.v1i2.120

[26] T. Imelda Bandaso, F. Randa, and F. F. Arwinda Mongan, "Blockchain technology: Bagaimana Menghadapinya? – Dalam Perspektif akuntansi," Accounting Profession Journal, vol. 4, no. 2, pp. 97–115, Jul. 2022. doi:10.35593/apaji.v4i2.55

[27] K. Septianzah, G. R. Fernandes, and I. M. Lina, "Blockchain Techonology for Payless Transactions and Investment Activities in the Digital Era With a SWOT Approach," Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi), vol. 5, no. 1, pp. 12–17, 2021. doi:https://doi.org/10.29407/inotek.v5i1.895

[28] Hadiana, A. I., Permana, Y. S., & Putra, E. K., "Pemanfaatan Blockchain pada Pembangunan Sistem Informasi Pembiayaan Usaha Mikro Kecil Menengah", Prosiding SISFOTEK, Vol. 3, no. 2, pp. 12 - 17, 2019. http://seminar.iaii.or.id/index.php/SISFOTEK/article/view/97

[29] G. Witjaksono, V. Virginia, A. Z. Amanda, P. Pandri, and L. Judijanto, "Teknologi Blockchain dalam Supply Chain Management: Meningkatkan Transparansi dan Keamanan", jcm, vol. 3, no. 2, pp. 2146-2152, Dec. 2023.

[30] A. I. Santoso, M. Zarlis, and H. Mawengkang, "Analysis of the role of Blockchain technology in Recording Motor Vehicle Ownership Data," JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING, vol. 7, no. 2, pp. 397–408, Jan. 2024. doi:10.31289/jite.v7i2.10938

[31] Y. W. Pratama and D. Kurniadi, "IMPLEMENTASI BLOCKCHAIN DALAM APLIKASI PEMILU," INCARE (International Journal of Educational Resources), vol. 2, no. 2, Aug. 2021.

[32] Q. Aini, U. Rahardja, M. R. Tangkaw, N. P. Santoso, and A. Khoirunisa, "Embedding a blockchain technology pattern into the QR code for an authentication certificate," Jurnal Online Informatika, vol. 5, no. 2, pp. 239–244, Dec. 2020. doi:10.15575/join.v5i2.583

[33] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia", J. Stud. Keb. Publ., vol. 2, no. 1, pp. 55–68, May 2023.

[34] A. Williams and E. Dolan, "Application of Blockchain Technology in e-LoA Technopreneurship Journal", ATT, vol. 2, no. 1, pp. 98–103, Mar. 2020.

[35] S. Sihombing, M. R. . Nasution, and I. Sadalia, "Analisis Fundamental Cryptocurrency terhadap Fluktuasi Harga: Studi Kasus Tahun 2019-2020", j. akunt. keuang. manaj., vol. 2, no. 3, pp. 213–224, Jun. 2021.

[36] S. Sutandi, "Pengaruh big data Dan Teknologi Blockchain TERHADAP model Bisnis Sektor Logistik Dengan Pendekatan business model canvas," Jurnal Logistik Indonesia, vol. 2, no. 1, pp. 9–20, Oct. 2018. doi:10.31334/jli.v2i1.214

[37] W. Swastika, H. Wirasantosa, and O. H. Kelana, "Rancang Bangun website Akademik Dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi blockchain," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 9, no. 1, pp. 33–40, Feb. 2022. doi:10.25126/jtiik.2021863645

[38] Simanta Shekhar Sarmah, "Understanding Blockchain Technology", Computer Science and Engineering, Vol. 8 No. 2, 2018, pp. 23-29. doi: 10.5923/j.computer.20180802.02.

[39] S. Trivedi, K. Mehta, and R. Sharma, "Systematic literature review on application of blockchain technology in E-finance and Financial Services," Journal of technology management & innovation, vol. 16, no. 3, pp. 89–102, Dec. 2021. doi:10.4067/s0718-27242021000300089

[40] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, https://bitcoin.org/bitcoin.pdf (accessed Jun. 18, 2024).

[41] M. K. Shrivas and T. Dr. Yeboah, "The Disruptive Blockchain: Types, Platforms and Applications," Texila International Journal of Academic Research (TIJAR), vol. Special Edition, no. 2019, pp. 17-39, 2019. doi:10.21522/TIJAR.2014.SE.19.02.Art003

[42] B. Lashkari and P. Musilek, "A comprehensive review of Blockchain Consensus Mechanisms," IEEE Access, vol. 9, pp. 43620–43652, 2021. doi:10.1109/access.2021.3065880

[43] L. Pietrewicz, "Blockchain: A coordination mechanism," SSRN Electronic Journal, vol. 5, no. 1, pp. 105–111, Sep. 2019. doi:10.2139/ssrn.3490168