Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 237 (2024) 269–276

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry Sciences and Computer Science Innovation

Decentralize transaction records of digital payment gateway using Ethereum Blockchain and Interplanetary File System

Muhamad Agil Fachrian[1], Parman Sukarno[1], Aulia Arif Wardana[2*]

[1]*Telkom University, Bandung, Indonesia*
[2]*Wroclaw University of Science and Technology, Wroclaw, Poland*

Abstract

This research proposes a system to store transaction records from a payment gateway based on digital payments by utilizing blockchain technology and Interplanetary File System (IPFS) as distributed storage. In digital payments, the possibility of online fraud or theft of customer data is a problem that needs to be solved. Although the solution is to use a Payment Gateway with security standards to prevent these problems, the system is still centralized and vulnerable to the possibility of system failure or data changes by irresponsible people. Blockchain furnishes a secure and unalterable record for documenting payment transactions. Conversely, IPFS presents a decentralized and immune-to-censorship approach for storing and accessing data. The usage of these technologies guarantees the secure storage of payment transaction data and related documents (such as invoices and receipts) while effectively thwarting data manipulation or censorship attempts. Therefore, this research aims to build a blockchain technology system to increase security and maintain the integrity of the data generated from the Payment Gateway. This research using distributed data storage using IPFS to save transaction from the payment gateway data. Based on the evaluation and security analysis results, implementing a blockchain technology system to store transaction records from digital-based payment gateways can improve data security and integrity. In the gas fee increase analysis, the gas fee will increase according to the total number of bytes generated when the transaction is made, where each byte will cost 12 gwei to pay the gas fee.

Peer-review under responsibility of the scientific committee of the iSCSi – International Conference on Industry Sciences and Computer Science Innovation

Keywords: Blockchain; Payment Gateway; IPFS; Decentralized Transaction; Distributed Ledger

* Corresponding author.
E-mail address: auliawardan@telkomuniversity.ac.id / aulia.wardana@pwr.edu.pl

Peer-review under responsibility of the scientific committee of the iSCSi – International Conference on Industry Sciences and Computer Science Innovation
10.1016/j.procs.2024.05.105

1. Introduction

Digital payment is increasingly crucial as more people make transactions online. Making online transactions certainly makes us vulnerable to online fraud or customer data theft. The solution to this problem is using a Payment Gateway, which already provides a standardized security system to protect customer transaction data and prevent unwanted things from happening [1][2]. On the other hand, the payment gateway system still needs improvement because still centralized and less trustworthy [3]. There is potential for someone to easily change or inhibit the data stored in the database and thus misuse customer information [4]. Therefore, it is necessary to improve the security of the Payment Gateway and maintain the integrity of transaction data. This mechanism expected to prevent irresponsible parties manipulate the data.

Blockchain is a distributed, decentralized, and immutable database where data in the blockchain is stored in a block structure and verified by the consensus of participants in the system [5]. One of the main characteristics of Blockchain technology is Trust. The blockchain protocol is designed to provide an immutable record of transactions by incorporating a distributed database consisting of chronologically and cryptographically linked transaction blocks through a decentralized consensus mechanism. This structure prevents the spread of incorrect or false information and allows agents to regulate their behavior without needing a central authority [6][7].

Blockchain technology has features such as a distributed database, a consensus process that can increase trust in the blockchain network, and its immutable nature [8]. There are three significant problems in digital payments using payment gateways: systems that still need to be centralized, less trustworthy, and difficult to maintain data integrity. Therefore, to solve these problems, this paper proposes implementing a decentralized application integrated with the Payment Gateway using blockchain technology to store transaction records created by the Payment Gateway and IPFS for decentralized storage. In addition, smart contracts are also proposed to improve efficiency and security in conducting transactions. Thus, it is expected that the system integrated with the Payment Gateway can become more reliable and secure for users.

2. Related Works

Zouina et al. [9] proposed changing payment cards to tokens to improve security and confidentiality. This research uses a private blockchain consortium and an extension of EMV 3DS using blockchain technology for its payment system. Shee-Ihn Kim et al. [10] focused on creating a simple payment model using cryptocurrency features, such as public key, private key, and digital signature, to eliminate the need for transaction intermediaries such as public key certificates and payment gateways for e-commerce. The current e-commerce payment system requires a payment gateway which creates additional costs on the payment gateway. This research also implements a system comprising customers and merchants, which will be connected to the Blockchain system. Singh et al. [11] created an e-wallets system that uses Blockchain-based Digital ledger technology (DLT) architecture. This research implements the IPFS, which aims to store transactions that have been verified and will later be stored in blocks that are implemented as a file; each block must contain the SHA-256 value of the previous block along with a list of transactions. Sholeh et al. [12], one of the solutions to the problem of paying tuition at universities is to develop a decentralized payment system using an Ethereum-based blockchain. This condition is necessary because centralized payment gateway systems are naturally vulnerable to the misuse of personal data. This research uses the Truffle framework and Solidity programming language to create smart contracts, with Metamask as a transaction link using smart contract tokens and wallets. Infura Testnet is used in the intelligent contract testing procedure, and Truffle is a framework to build a dApp payment gateway interface with Ethereum as the digital currency.

This research is focusing on payment gateway and focus on the decentralize mechanism of payment gateway. The other research is focus on single payment method, while our research focus on payment gateway which can be easy integrated with many payments system. Here is the list of contribution from this research:

1. Implementing blockchain technology on a payment gateway.
2. Employ decentralize distributed storage to save the transaction using IPFS.

This study expected to prove the effectiveness of the proposed model by designing a system that combines blockchain technology and payment gateway, aiming to enhance the security of the payment gateway and ensure the integrity of transaction data even if the payment gateway server goes down.

3. Methodology

The system in this research will implement blockchain technology integrated with a payment gateway and IPFS. The Decentralized Application (dApp) created using Next.js as an interface, Truffle as a smart contract development framework, and the Solidity programming language to create smart contracts. The dApp is also connected to the Ethereum network through Go Ethereum (Geth) and Ethers.js. Geth facilitates the interaction between the application and the Ethereum network, while Web3.js helps the application interact with smart contract and perform transactions on the Ethereum network.

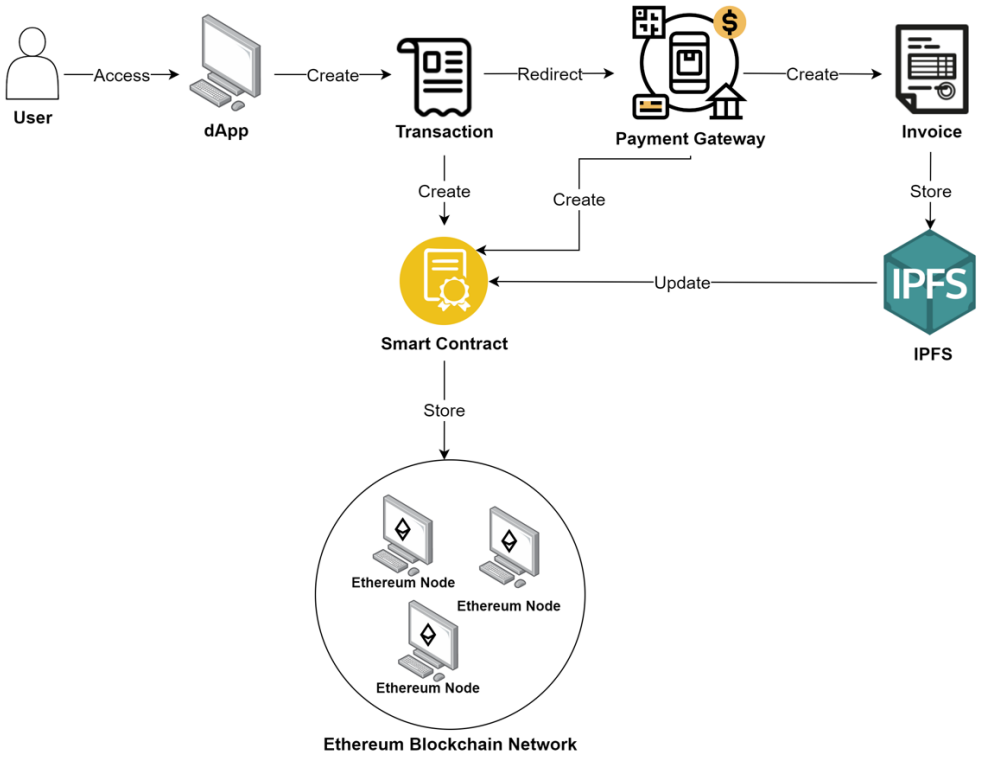

Fig. 1. Decentralize transaction record process.

Fig. 1. shows the transaction creation process, where the user will access a dApp that has been created. When accessing a dApp, the user can already create a transaction. After the transaction is completed, the transaction will be stored on the blockchain by the system. Then, the user will be redirected to the payment gateway page to make a payment. After the payment is made and validated, the system will save the transaction record from the payment gateway into the blockchain, and then the invoice will be generated by the system and stored in IPFS. After getting the hash from IPFS, the contract transaction that was first created will be updated by adding the hash from IPFS.

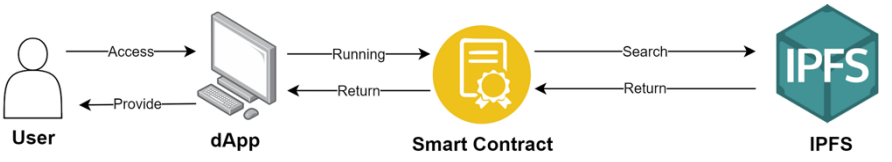

Fig. 2. Invoice file download process.

In Fig. 2. the invoice download process is done by the user accessing the dApp. Next, the dApp will run a smart contract to get the IPFS hash of the contract transaction created by the user. After the dApp gets the IPFS hash from the smart contract, the dApp will provide a link to access the invoice to the user. This section will use flowcharts to represent how the system works visually to facilitate understanding. The flowchart will show the workflow of each process and the interaction between system components.

In Fig. 3. the first process of a user creating a transaction is to fill out the form provided to create the transaction. After the transaction is completed, the system will process it and store it in the Blockchain using the smart contract that has been prepared. After being stored on the Blockchain, the user will be redirected to the Payment Gateway page to select a payment method and complete the payment. If the Payment Gateway successfully accepts the payment, the system will receive a response from the Payment Gateway indicating that the payment has been successful. The response will be stored on the Blockchain as a History Record from the Payment Gateway. The system will then create an invoice for the transaction that has been made. The invoice will be stored in IPFS, and the hash of the invoice will be used to update the first transaction smart contract on the Blockchain by adding its IPFS hash. Finally, the system will redirect to the success page in the system.

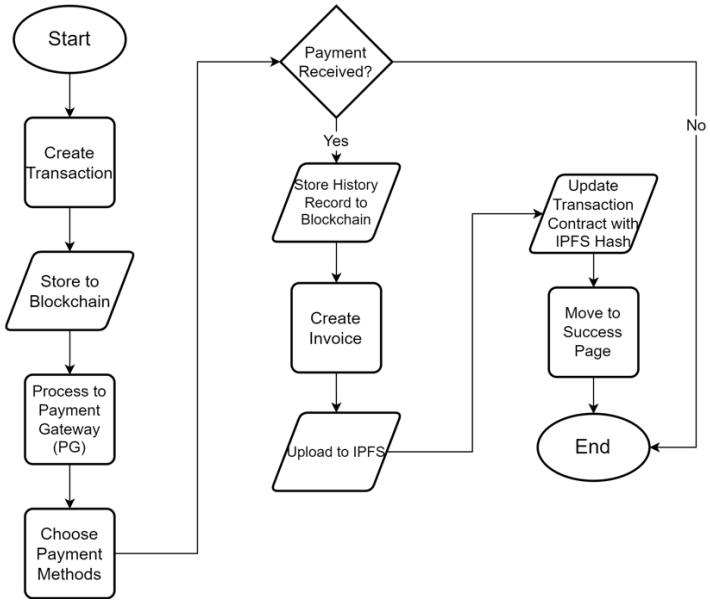

Fig. 3. Flowchart for decentralize transaction record.

4. Implementation and Evaluation

4.1. Experiment Setup

This section will prepare everything necessary to implement a dApp integrated with Payment Gateway, using blockchain technology to store transaction data and IPFS. Implementation is carried out using a virtual machine created in Virtual Box as an interconnected node in the blockchain network. This research will use three nodes of the virtual machine. Each machine in the Virtual Box is configured in the Network section with a Bridged Adapter and a DHCP-configured IP address. To connect each node, we took all the nodes of each node that had been created and created a static-nodes.json file on each node that contained the nodes of each node so that they could be connected. Each machine uses the Ubuntu 20.04 operating system and has the specifications in Table 1. On each machine, Go-Ethereum was installed along with the requirements when installing it. Information about the software version and environment used on each machine is described in Table 2. In addition, to create a dApp in this research using frameworks and environments with specific versions in Table 2.

Table 1. Computing Machine Specifications.

Hardware	Specification
CPU	AMD Ryzen 3 3200U
Memory	1 GB
Storage	30 GB

Table 2. Versions of the software and environment.

Go-Ethereum		dApp	
Framework & Environment Name	Version	Framework & Environment Name	Version
Geth	1.10.26-stable	Next.js	12
Go	go1.18.5	Truffle	v5.6.5
Node	v10.19.0	Node	v17.6.0
NPM	6.14.4	NPM	8.5.1

4.2. Result

The following are the results of the implementation of the use of blockchain technology in a system integrated with Payment Gateway.

a)


```
{
    "id": "63f75c95b99a2752a723555",
    "amount": 375000,
    "status": "PAID",
    "created": "2023-02-23T12:31:18.359Z",
    "is_high": false,
    "paid_at": "2023-02-23T12:31:41.846Z",
    "updated": "2023-02-23T12:31:52.380Z",
    "user_id": "63578fd0e92f3ac1265577f5",
    "currency": "IDR",
    "payment_id": "ewc_20a33ade-04aa-48ae-9bda-0d7ca5e75cf2",
    "description": "Mr.Agil",
    "external_id": "PAYMENT-8854",
    "paid_amount": 375000,
    "payer_email": "agilfachrian@gmail.com",
    "ewallet_type": "LINKAJA",
    "merchant_name": "Buat Project",
    "payment_method": "EWALLET",
    "payment_channel": "LINKAJA",
    "payment_method_id": "pm-2ca16c55-476b-4e3c-b905-494f788a08da",
    "success_redirect_url": "http://localhost:3000/success",
}
```


b)


```
{
    "id": "63f75c95b99a2752a723555",
    "amount": 375000,
    "status": "PAID",
    "paid_at": "2023-02-23T12:31:41.846Z",
    "currency": "IDR",
    "description": "Mr.Agil",
    "external_id": "PAYMENT-8854",
    "paid_amount": 375000,
    "payer_email": "agilfachrian@gmail.com",
    "payment_method": "EWALLET",
    "payment_channel": "LINKAJA"
}
```


Fig. 4. (a) Original payment gateway response; (b) Reprocessed payment gateway response.


```
(3) [Array(11), Array(11), Array(11)]
  0: (11) ['63f75bf6f7f24373cc04733e', 'PAYMENT-2584', 'EWALLET', true, BigNumber,
  1: (11) ['63f75c5ea47685805a43b888', 'PAYMENT-2731', 'EWALLET', true, BigNumber,
  2: (11) ['63f75c95b995a2752a723555', 'PAYMENT-8854', 'EWALLET', true, BigNumber,
  length: 3
  [[Prototype]]: Array(0)
```


Fig. 5. Transaction Record.

The user fills a form to create a transaction, where the user is asked to fill in revenue, title, name, email, and phone number. After the form is filled in, the user can click the “PAY” button which will redirect to the Payment Gateway page to pay for the transaction they made. The purpose of making this dApp is to make transaction payments by multiplying the income by a percentage of 2.5%. After that, the page on the Payment Gateway that is directed from the dApp. The Payment Gateway used is Xendit (https://www.xendit.co/en/). Here, users are asked to choose the payment method they want to use, ranging from bank transfers, credit cards, e-wallets, and so on. We reprocessed the transaction record from the Payment Gateway response, and as can be seen in Fig 4, part (a) is the transaction record derived from the original Payment Gateway response, while part (b) is the data that has been processed and will be

stored in the Blockchain. Fig. 5. shows the list of transaction success from dApp and the Payment Gateway. After the transaction has been successfully paid then the invoice has been created. In addition, the transaction data that has been created has been stored on the blockchain, including the transaction record from the payment gateway. Fig. 6. shows that all transactions made by the user will be displayed in the table on the "All Transactions" page. The table includes information such as transaction id, name, nominal, date, and a link to the invoice created in IPFS. The proposed system program can open in here https://github.com/agilfchx/zakatchains/tree/main/zakatchains-app.

Fig. 6. All Transactions.

4.3. Evaluation

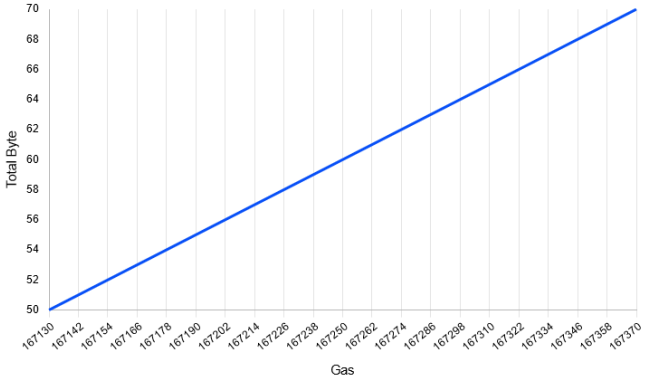

Fig. 7. Total Byte and Gas.

We conducted an evaluation by analyzing the factors that affect gas fees when making transactions on the Ethereum network. Gas is a mechanism used to determine the fee that will be charged to a program that will be executed on the Blockchain network. The gas price is basically a measure of how much Ether the user will invest in each unit of gas [13][14][15]. Wei is the smallest unit of Ether and the most common unit used to measure gas price is gwei [13][16]. 1 wei is equal to 10^{-18} and 1 gwei is equal to 10^{-9} Ether. Based on the results of our analysis, we can see in Fig 7 that the gas cost of a transaction depends on the total bytes sent. For example, in Fig 7, when sending a transaction with 50 bytes, the gas fee is 167130 gwei, while when sending a transaction with 51 bytes, the gas fee is 167142 gwei. It can also be seen in Fig 11 that every additional 1 byte in the transaction will increase the gas cost by 12 gwei, indicating that the total bytes in the transaction are a significant factor in increasing the gas cost.

4.4. Security Analysis

This section analyzes the security protection of decentralize transaction record from payment gateway from cybersecurity threat. There are two major protections for the system, here is the list:

A. Protects against Data Tampering

Blockchain technology offers robust protection against data tampering thanks to its inherent attributes of immutability, decentralization, and cryptographic hashing. Once data is incorporated into a blockchain, modifying or erasing it becomes an exceptionally arduous task. Within a blockchain, each block contains a cryptographic hash of the preceding block, forming an interconnected chain of blocks. Any attempt to tamper with data within a block would necessitate altering that block's hash, subsequently triggering modifications in the hashes of all ensuing blocks. Blockchain's decentralized nature further heightens security, as no single entity possesses the capability to manipulate data unilaterally; instead, a consensus mechanism is employed to validate transactions [17][18]. This security feature is very useful when implemented on payment gateway. Each payment transaction can be recorded as a block on the blockchain. Once recorded, this data is virtually immutable, making it extremely difficult for malicious actors to tamper with payment records.

B. Protects against Data Loss

Blockchains constitute decentralized networks comprising nodes, which are essentially computers holding a complete copy of the entire blockchain. Consequently, there exists no central authority or singular point of control within blockchain networks. The validation and addition of new blocks to the chain rely on consensus mechanisms. Network participants must reach a consensus on transaction validity and the chronological order of their inclusion in the blockchain. This consensus mechanism serves as a safeguard, promptly identifying and rejecting any attempts at tampering made within the network. Additionally, blockchain can harness smart contracts, which are self-executing agreements governed by predetermined rules and conditions. Smart contracts introduce automation to various processes and ensure data integrity by executing actions solely when specific criteria are met [19][20]. This security feature is also very useful when implemented on payment gateway. A blockchain-based payment gateway can operate on a decentralized network of nodes. This eliminates the need for a central authority or intermediary, reducing the risk of single points of failure that caused data loss, and lowering transaction fees.

5. Discussion

This section discusses the results that have been done such as implementation, evaluation, and security analysis. In this research, the use of cryptocurrency does not always have to be applied to users to pay gas fees for each transaction, because there are still some countries that still prohibit it [21]. In the system that has been created, gas fees are handled by the system, so users can pay for their transactions with their currency through a payment gateway. This makes us more efficient when we want to use blockchain technology but are limited by issues such as the use of cryptocurrency in the country. In addition, we can also see from the evaluation side that one of the factors that gas fees increase is the total bytes created when making transactions. Therefore, the estimated amount of ether required to make a transaction must be calculated properly. In terms of Security Analysis, because this uses blockchain technology so the integrity and security of the data are very well maintained, so it can protect against data manipulation and data loss.

Blockchain has the potential to streamline and accelerate cross-border payment processes by offering a unified, transparent ledger for global transactions. Such a system can alleviate the intricacies and expenses typically linked with conventional cross-border payment systems. Blockchain introduces a level of transparency that benefits both customers and merchants. It grants them the ability to autonomously verify transaction details and historical records stored on the blockchain, assuring the accuracy and timeliness of payment processing. Moreover, the cryptographic attributes and decentralized structure of blockchain heighten the difficulty for malicious actors to tamper with payment information or pose as authentic users.

6. Conclusion

This research proposes a system to store transaction records from a payment gateway based on digital payments by utilizing blockchain technology and IPFS as a distributed storage. Implementation and analysis show that the use of blockchain technology can maintain data integrity and security when storing transaction records on the blockchain. In addition, to perform transactions, gas is required to execute on the blockchain network, and the cost of gas is affected by the total bytes sent, where each increase of 1 byte will increase the cost of gas by 12 gwei. This research also

provides suggestions for payment gateway around the world to adopt decentralized payment gateways and can also be a suggestion for companies that want to build a system using payment gateway but are worried about data loss and data manipulation. For future research, it can be considered to explore new ways to reduce gas costs in transactions using blockchain technology, such as by improving the efficiency of the consensus algorithm used or by improving the blockchain network technology itself.

References

[1] M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Efficient Secure Electronic Payment System for E-Commerce," *Computers*, vol. 9, no. 3, 2020, doi: 10.3390/computers9030066.

[2] S. Bojjagani, V. N. Sastry, C.-M. Chen, S. Kumari, and M. K. Khan, "Systematic survey of mobile payments, protocols, and security infrastructure," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 1, pp. 609–654, 2023, doi: 10.1007/s12652-021-03316-4.

[3] R. Hossain, D. Sarker, K. Sumya Sultana Meem, and M. Shahrina, "Analysis of Centralized Payment Eco-System: A Systematic Review on E-Payments," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 3, pp. 14139–14159, 2020, [Online]. Available: http://sersc.org/journals/index.php/IJAST/article/view/31855.

[4] S. Sekar *et al.*, "Autonomous transaction model for e-commerce management using blockchain technology," *Int. J. Inf. Technol. Web Eng.*, vol. 17, no. 1, pp. 1–14, 2022.

[5] M. D. Muis, M. R. Fauzan, P. Sukarno, and A. A. Wardana, "Access Control and File Distribution Management for Electronic Diploma and Transcript using Ethereum Smart Contract and InterPlanetary File System," *J. Sist. Inf.*, vol. 17, no. 2, pp. 48–61, 2021, doi: https://doi.org/10.21609/jsi.v17i2.1093.

[6] M. J. M. Chowdhury *et al.*, "A comparative analysis of distributed ledger technology platforms," *IEEE Access*, vol. 7, pp. 167930–167943, 2019, doi: 10.1109/ACCESS.2019.2953729.

[7] M. C. I. Putri, P. Sukarno, and A. A. Wardana, "Two factor authentication framework based on ethereum blockchain with dapp as token generation system instead of third-party on web application," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 6, no. 2, pp. 74–85, 2020, doi: 10.26594/register.v6i2.1932.

[8] N. El Ioini and C. Pahl, "A review of distributed ledger technologies," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11230 LNCS, no. November, pp. 277–288, 2018, doi: 10.1007/978-3-030-02671-4_16.

[9] M. Zouina and B. Outtai, "Towards a distributed token based payment system using blockchain technology," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1–10, doi: 10.1109/COMMNET.2019.8742380.

[10] S.-I. Kim and S.-H. Kim, "E-commerce payment model using blockchain," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 3, pp. 1673–1685, 2022, doi: 10.1007/s12652-020-02519-5.

[11] K. Singh, N. Singh, and D. Singh Kushwaha, "An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain," in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 2018, pp. 165–169, doi: 10.1109/GUCON.2018.8674919.

[12] M. Sholeh, E. Y. Talahaturuson, M. Rizqi, and A. B. Gumelar, "Designing an Ethereum-based blockchain for tuition payment system using smart contract service," *J. RESTI (Rekayasa Sist. Dan Teknol. Inf.)*, vol. 6, no. 2, pp. 275–280, Apr. 2022.

[13] S. Bhatia and S. S. Tyagi, "Ethereum," in *Blockchain for Business*, John Wiley & Sons, Ltd, 2021, pp. 77–96.

[14] L. Marchesi, M. Marchesi, G. Destefanis, G. Barabino, and D. Tigano, "Design Patterns for Gas Optimization in Ethereum," in *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2020, pp. 9–15, doi: 10.1109/IWBOSE50093.2020.9050163.

[15] N. Chaniago, P. Sukarno, and A. A. Wardana, "Electronic document authenticity verification of diploma and transcript using smart contract on ethereum blockchain," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 7, no. 2, pp. 149–163, 2021, doi: 10.26594/REGISTER.V7I2.1959.

[16] A. A. Zarir, G. A. Oliva, Z. M. (Jack) Jiang, and A. E. Hassan, "Developing Cost-Effective Blockchain-Powered Applications: A Case Study of the Gas Usage of Smart Contract Transactions in the Ethereum Blockchain Platform," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 3, Mar. 2021, doi: 10.1145/3431726.

[17] M. Iqbal and R. Matulevičius, "Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, 2019, pp. 13–28.

[18] C. Pop *et al.*, "Blockchain-Based Scalable and Tamper-Evident Solution for Registering Energy Data," *Sensors*, vol. 19, no. 14, 2019, doi: 10.3390/s19143033.

[19] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham, "Blockchain Technology: What is It Good For?," *Commun. ACM*, vol. 63, no. 1, pp. 46–53, Dec. 2019, doi: 10.1145/3369752.

[20] R. K. Raman and L. R. Varshney, "Distributed Storage Meets Secret Sharing on the Blockchain," in *2018 Information Theory and Applications Workshop (ITA)*, 2018, pp. 1–6, doi: 10.1109/ITA.2018.8503089.

[21] S. P. Yadav, K. K. Agrawal, B. S. Bhati, F. Al-Turjman, and L. Mostarda, "Blockchain-Based Cryptocurrency Regulation: An Overview," *Comput. Econ.*, vol. 59, no. 4, pp. 1659–1675, 2022, doi: 10.1007/s10614-020-10050-0.