LONTAR KOMPUTER VOL. 11, NO. 3 DECEMBER 2020 **p-ISSN 2088-1541**
DOI : 10.24843/LKJITI.2020.v11.i03.p04 **e-ISSN 2541-5832**
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017

Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification

Abdul Fadlil[1], Imam Riadi[2], Achmad Nugrahantoro[3]

[1]Department of Electrical Engineering, Ahmad Dahlan University
[2]Department of Information Systems, Ahmad Dahlan University
[3]Department of Informatics Engineering, Ahmad Dahlan University
Jl. Prof. Dr. Soepomo, S.H, Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
[1]fadlil@mti.uad.ac.id
[2]imam.riadi@is.uad.ac.id
[3]achmad1907048001@webmail.uad.ac.id (Corresponding author)

Abstract

The application of Blockchain technology has begun to be widely accommodated in industrial and business practitioner environments as a safeguard of transaction security so that now including the education sector, non-business institutions enjoy the use of this technology to support the learning process. Information on the protected Blockchain can be in the form of transactions, assets, identities, and other information packaged in digital form. Information is collected in the form of blocks that are interrelated by using the hash function as cryptographic encryption. This research uses Blockchain for online pocket money top-up transactions for students. The use of a centralized Blockchain is centralized to reduce server procurement costs, but to increase the security of transaction information, modification of each block series is carried out using the AES cryptographic approach. The results showed that the attack by inserting a Cross-Site Scripting (XSS) script if you want to know the value of the top-up transaction amount, you must be able to hack the cryptographic process. This is supported by chain validation testing to determine how many block changes have been changed.

Keywords: *Blockchain, Cryptography, AES, Transaction, Education*

1. Introduction

Blockchain is a technology that involves third parties in the process of exchanging information. Information on the Blockchain can be in the form of data entry in transactions form, assets, identities, and other information that is packaged in digital form [1]. The form of blockchain information is easy to find, tends to be transparent and permanent, allowing users to monitor the history of information that occurs [2][3]. Blockchain technology is an alternative with a centralized technology architecture to support the disruption era. Conceptually, Blockchain is a technology with a distributed database that is stored and then shared with authorized users [3][4]. This concept is to replace the role of third parties such as financial institutions or other institutions, but on the literal side, Blockchain technology is considered as a collection of interrelated blocks of information by utilizing the hash function as encryption in the field of cryptography [5][6].

Cryptography has become a science that has been widely used to maintain information security with mathematical calculation techniques [7][8]. This technique can convert plaintext using keys into random messages or ciphertext. There are several algorithms for data security, one of which is the Advanced Encryption Standard (AES), which is known as the standard crypto algorithm Data Encryption Standard (DES) [9][10]. AES is known to be resistant to differential attacks, namely conventional cryptographic cracking.

Blockchain is not a new technology this is involving old combinations with renewable means. For example, the relationship involving 3 (three) technologies such as the internet, cryptography, and protocols from software, to produce strong security but still be able to interact or transact digitally. The relationship between Blockchain technology and cryptography where the cryptography use keys as an authentication tool in terms of ownership of an authorized person. So that maintaining

the confidentiality and content of the transaction prevents hacking. Besides, the cryptographic process is required to maintain the validity of broadcasting the contents of transaction information correctly, reducing failure and the risk of fraud to remain on the Blockchain protocol path.

The application of Blockchain technology has begun to be widely accommodated in industrial and business practitioners' environments as a safeguard of transaction security so that now including the education sector as non-business institutions enjoy the use of this technology to support the learning process. In the school system in Indonesia, there are several learning contracts for students that are required to pay for school needs, such as school fees that are billed periodically every month, an obligation to save, and other transactions. Financial transactions are charged to students as the support for the sustainability of the school so that it requires the use of the internet in its digital interactions. The importance of recording risky financial transactions with costly data theft needs to present Blockchain technology as a solution. Not only that, Blockchain can reduce the involvement of many parties in online transactions because it allows building your network, thus reducing costs both administratively and operationally.

Research with Blockchain in an educational environment is used to protect many useful assets such as digital document management, such as in Nugraha's research [11]. However, the research to be carried out involves financial transactions that occur in the school environment, namely with the online top-up pocket case studies. Putra's research combines Blockchain with RSA cryptography for data security on the network, the use of the RSA method affects the number of keys, and its implementation cannot be directly applied to several devices [12]. In this research, it is implemented on mobile android, and Blockchain technology will be applied with AES, which does not affect the size of the key. In the world of education, Blockchain technology is usually in the form of block certificates, book copyrights, and e-portfolios to avoid file forgery [13], as in Winarno's research using it for case studies of e-transcript publishing. Each application of Blockchain technology makes the attacker has to challenge the system for the formation of a longer blockchain, including for e- transcript cases. So this study will modify each series of blocks by utilizing the AES cryptographic approach to better maintain the integrity of stored messages, but applied to financial transactions that occur in the school environment. Another study conducted by Perdana [14] states that if financial technology needs to be protected from cybercrime, users still have easy access to financial transactions by increasing financial literacy. If FinTech involves many servers, it requires vendor consolidation and requires a high level of system security. Then the proposed research will implement a centralized blockchain and efforts to increase its security with cryptographic techniques for each block of transactions.

Research by Benchoufi [15] has explored the core function of Blockchain as applied to clinical trials and the context of approval for trial protocols. The results of this study can help to check the integrity of clinical trials transparently, but if a core metadata set is defined. The proposed research will be directed to use structured metadata, namely transaction data that occurs in the school environment, namely cases of online pocket money top-up transactions that are entered as student savings data. Other studies have summarized the use of Blockchain technology in several cases, namely for cryptocurrencies, smart contracts, smart cities, and this research proves that Blockchain technology has penetrated all areas of life [16]. So the research focuses on the educational environment in schools and implements case studies of financial transactions.

Blockchain in the research of Wright and Filippi [17] proves that if this approach makes it easy for users to access an automatic transaction system and an innovative governance model based on transparency, then this research will design its implementation until the assault testing scenario and validation results are planned. Blockchain-based platforms provide solutions for distributed data governance and participatory access control in the health sector, which aims to improve Information Technology in the health sector [18], the health sector which aims to improve Information Technology in health sector [18], Shabani's research is not yet in the implementation stage. So that researchers will implement it in the field of education. Another study in the health sector revealed that Blockchain is good at structuring data types in a decentralized manner, which facilitates more transparent interactions [15]. However, the use of decentralization will cost money to procure a lot of servers. The research conducted utilizes centralization with a centralized server for financial transactions to be recorded in a transparent, centralized manner and can save costs.

The proposed method in the research uses a modified Advanced Encryption Standard (AES) cryptographic combination Blockchain technology for the protection of digital pocket money to up

transactions in a school environment. The workings of AES are in each Blockchain resulting in higher security. The use of data in research uses structured data; namely, top-up transactions carried out by students; of course, this makes it easier to centralize a centralized server so that it remains recorded transparently and, of course, saves costs. To find out the resistance of the proposed algorithm modification, the test was carried out using the attack scenario with Cross-Site Scripting (XSS) and Chain Validation.

2. Research Methods

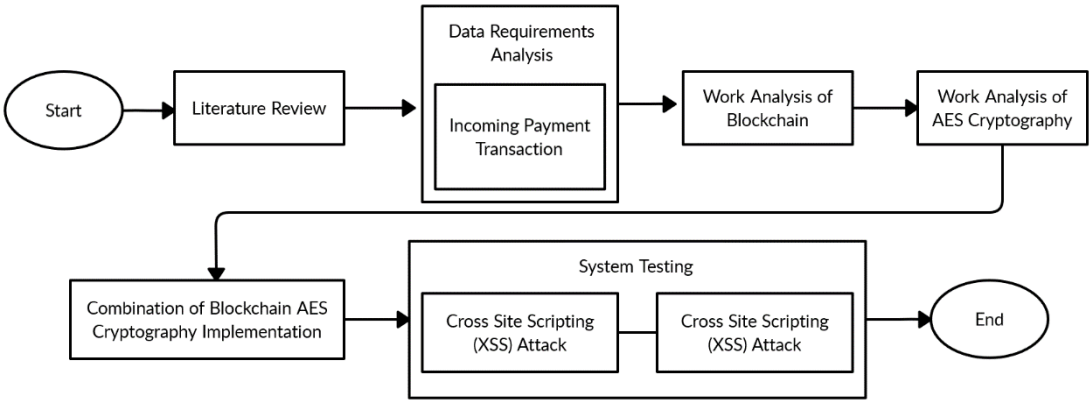

Figure 1. AES Combined Blockchain Technology Research Flowchart

The research uses Blockchain technology with AES cryptography to be utilized in the school environment, especially in pocket money top-up transactions, as shown in Figure 1. Architectural analysis of Blockchain and Cryptography with the AES method, then how the two works are combined in securing transactions. The test scenario will be carried out by injection attack with Cross-Site Scripting (XSS) and test the validity of each block with Chain Validation.

2.1. Literature Review

The literature review by studying various sources in the form of descriptions of theory and findings obtained from books, similar research journals, scientific works, and other relevant sources. Especially the discussion regarding Blockchain technology and the performance of the AES cryptographic method.

2.2. Data Requirements Analysis

Researchers used a case study of top-up pocket money transactions in educational settings, especially schools. Pocket money top-up is a digital transaction made by students as savings, which later can be useful for paying school needs such as bills, cash withdrawals, as infaq, zakat, and other transactions. The transactions that will be used and secured for the validity of the transactions are illustrated in Table 1 with the following data:

Table 1. Student Pocket Money Transaction Data

No.	ID Students	Name	Transaction	Amount	Information	Transaction Date
1.	4323	Namira Laura	Income	Rp. 3.000.000	Top Up	2020-05-23 13:03:45
2.	4112	Dwi Damayanti	Income	Rp. 250.000	Top Up	2020-05-30 13:03:45
3.	4321	Andri Reynaldi	Spending	Rp. 300.00	School costs and fees	2020-05-31 04:39:07
4.	4500	Titik Kirana Dewi	Income	Rp. 2.800.000	Top Up	2020-06-03 07:00:04
5.	4901	Habibah Rani Katrina	Spending	Rp. 300.000	School fees uniform	2020-06-04 19:42:21

In Table 1. the student pocket money transaction data consists of the student's identity number, full name, transactions that occur at that time according to the number of rupiah numbers, information about the transaction, and recording the transaction time. These data are protected,

especially in the data amount of the rupiah value top-up, the Blockchain process is carried out, and the AES cryptographic modification.

2.3. Blockchain Technology Architecture

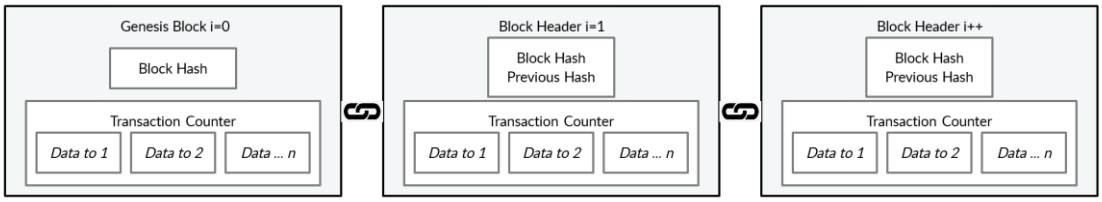

Figure 2. Blockchain Architecture Continous Sequence of Blocks

Figure 2. becomes an illustration of Blockchain architecture with a collection of transactions that occur and their history, such as conventional ledger recording [19][20]. The description is a series of blockchain architectures with one block genesis at the beginning of block formation, then followed by a block header that is strung according to the previous hash. The Genesis Block is the first block in a series of blocks.

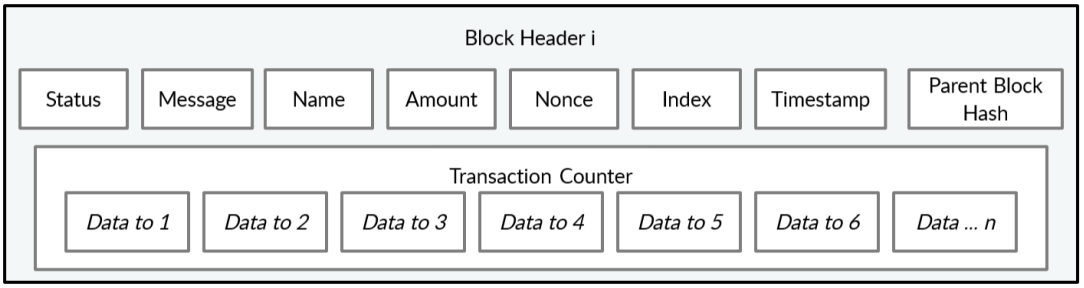

Figure 3. Single Block Structure

In Figure 3, it is explained that the contents of the block are the headers and contents of the blocks contained in online transactions on the school system that occur, namely an explanation of the transaction identity in status, message, name. In the entry, the amount is the number of transactions made in rupiah. The nonce is a 4-byte field that starts at 0 and will increase as the hash value is calculated. The index becomes the data described in each block, and the timestamp becomes the universal time in the calculation of seconds. Parents Block hash a 256-bit hash value that points to the previous block.

2.4. Advanced Encryption Standard (AES) Cryptographic Performance Analysis

Advanced Encryption Standard (AES) is one of the modern cryptographic methods as a replacement for the 56-bit block Data Encryption Standard (DES) algorithm, which is considered unsafe [21][22]. The selection criteria of this algorithm are based on the characteristics, safety, and cost if used and their implementation. This algorithm is a single key by using the same key [10][23].

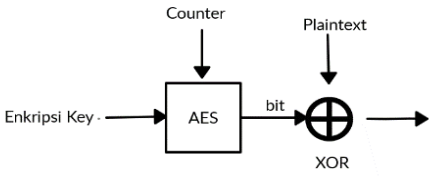

Figure 4. Single Key Cryptography AES

The description in FIgure 4. The encryption key is carried out by the AES process by previously receiving information, then processed with the selected bits. AES has assigned the bit lengths of the known keys AES-128, AES-192, and AES-256. Bit selection affects the key length, block size, and the number of rounds [24]. Plaintext or messages that will be processed in the cryptography process are XORed so that they produce meaningless messages. This study uses a 256-bit cryptographic key, with a key length of 8, block size 4, and the number of turns 14.

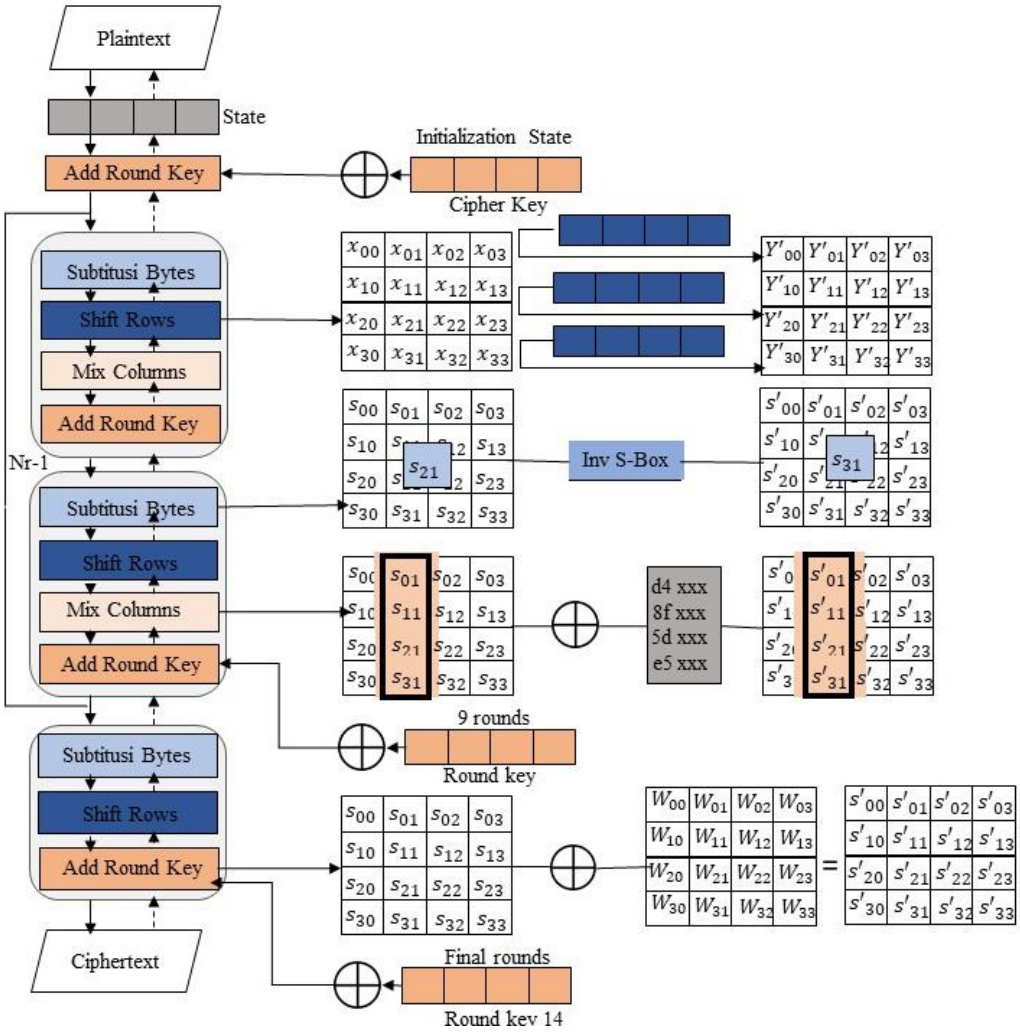

Figure 5. 256 bit AES Algorithm [25]

Figure 5 . is an outline of the AES algorithm that operates at 256 bits with the following information:

a. Add Round Key is this stage to be an initial round, namely initializing the initial state by XOR the plaintext process with a ciphertext key.
b. Round of Nr-*1* times, with 256 bits, then as many as Nr-14. Where in the process of each round includes the SubBytes process by substituting bytes with S-boxes, ShiftRows shifting on each row array, Mix Columns method randomizing data in columns, and AddRoundKey XOR process between states that occur with its round key.
c. Final round is the final round process using the SubBytes, ShiftRows, AddRoundKey methods.

2.5. Combination of Blockchain and Advanced Encryption Standard (AES) Cryptography

The modification in this study utilizes the Blockchain chain combined with the AES Cryptography method, shown in Figure 6.

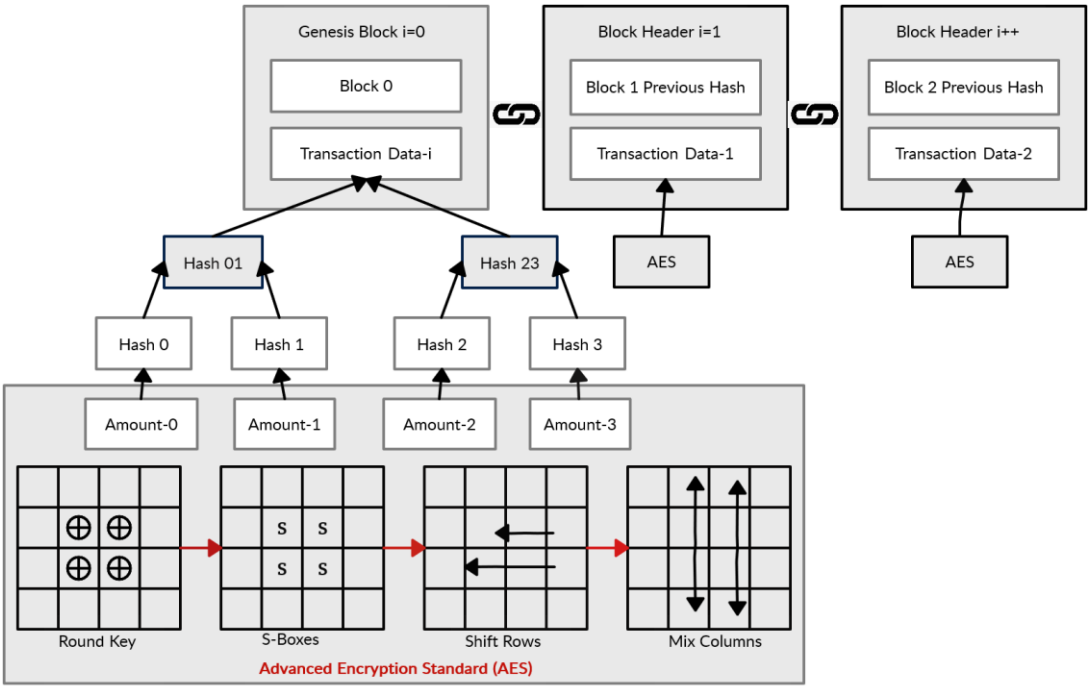

Figure 6. AES Blockchain Modification

Explanation in Figure 6. The Blockchain in each block contains information from each student who makes top-up transactions and other transactions. Of course, the transaction is changed in the form of a hash, but in this study using the parameter amount (top-up value in rupiah) to perform the cryptographic process with AES. Applies to each chain in the transaction because the amount is prone to attacks to avoid a difference in the value of both the initial transaction and the total.

2.6. Testing

2.6.1. Cross-Site Scripting (XSS)

Cross-Site Scripting is also known as an injection attack from Cross Scripting, where the attack inserts the attack command code script on a website [26]. The attacker will change the data by hijacking the session, attacking cookies to cause data consistency [27]. So that this research will utilize the XSS scenario in attacking transactions, then perform a validation test on the Blockchain.

2.6.2. Chain Validation

This test validates the chain on each Blockchain to detect changes in each block by verifying the hash associated with the previous and next block [28][29]. Valid chains will produce true output that is true without any changes, and invalid chains will give false output indicating an attack from unauthorized parties. In checking the validation, the researcher utilizes a script from Proof of Work, which is a computational method commonly used for Blockchain technology [30].

p-ISSN 2088-1541
e-ISSN 2541-5832

3. Result and Discussion

3.1. School Transaction with Top Up

a. Use Case Diagram

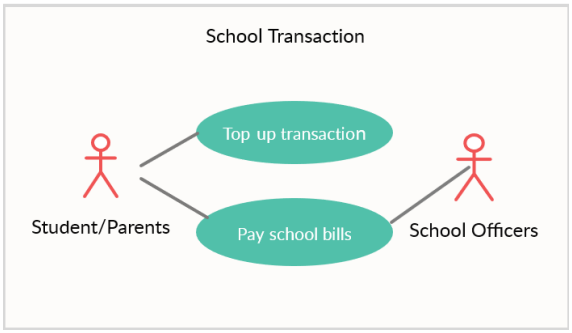

Figure 7. Use Case School Transaction Diagram

Use Case diagram illustrates the relationship between the parties of students, both parents or guardians and the school and the school transaction system according to Figure 7. The interaction made by the students is a digital pocket money top-up transaction that can be used to pay school bills. Then the payment will be followed up by the school. This transaction requires protection.

b. Database Design

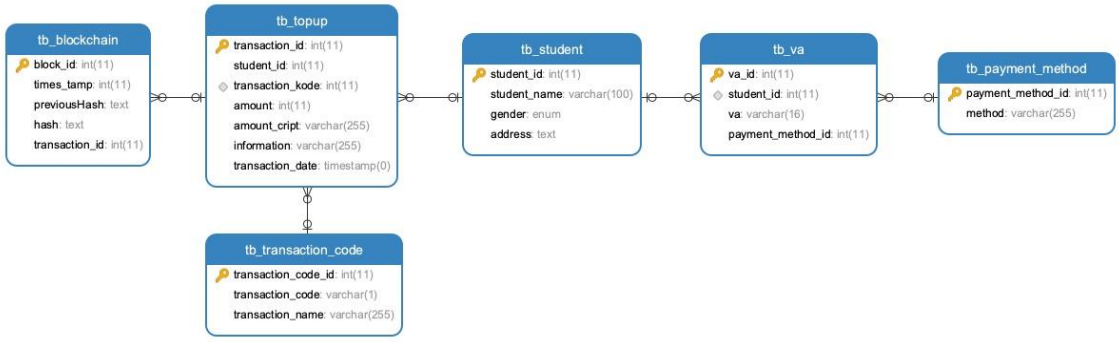

Figure 8. Database Design Top Up with Blockchain-AES

In the blockchain table is a combination Blockchain approach process with AES that is related to the top-up table, where one top-up transaction made by the student is related to each block so that the process that occurs when witness transactions are always recorded and processed by Blockchain-AES. The students can conduct transactions top up many times. Payment methods can only be done with a Virtual Account (VA) because it is easier, faster, and more practical. VA is given to students in a unique form and nominal according to the desired top-up. Each top-up transaction has a record indicating the addition and reduction of the balance in the allowance where the information will be monitored and followed up by the school.

c. User Interface Design

Figure 9. Payment Simulator Top-Up Transaction

Each student has a unique code in the form of VA, which is used in transactions according to Figure 9. If you are going to make a transaction, it will appear in Figure 10.

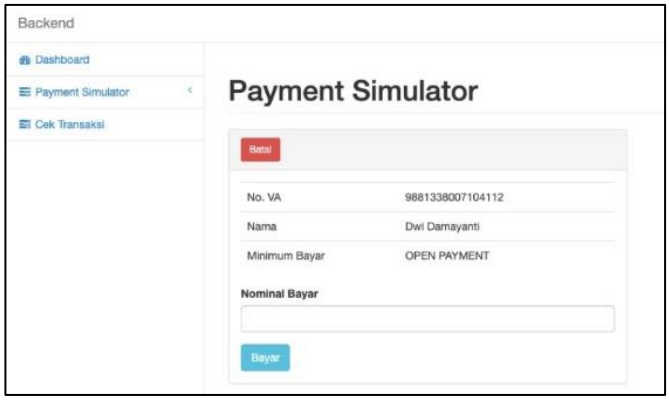

Figure 10. Interface Simulator Top Up by Students

The display on the student side is like Figure 10. The student who will do the top-up is provided with an open payment field and adjusts the nominal top-up that will be done.

3.2. Transaction Top-Up System Design

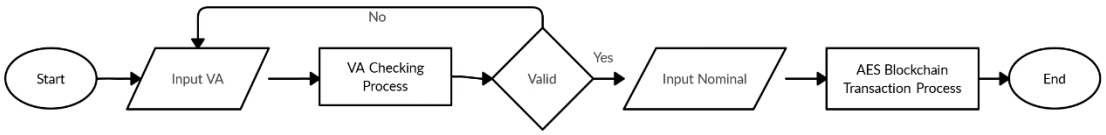

Figure 11. Alur Kerja Transaksi Top

It is shown in Figure 11. In the design of the procedure for a top-up of pocket money transactions, the students do top up with the VA listed, then the system checks if the VA is valid, then it will continue to be able to enter the top-up nominal. In the transaction process that occurs, the Blockchain-AES approach process is carried out.

3.3. Implementation of Modified Blockchain Technology with Cryptography Advanced Encryption Standard (AES)

```
{
    "status": "00",
    "message": "success",
```

```
    "name": "Dwi Damayanti",
    "amount_total": "Rp. 650,000",
    "result": {
        "chain": [
            {
                "nonce": 0,
                "index": 0,
                "timestamp": 1587747600,
                "data": "Genesis Block",
                "previousHash": null,
                "hash":
"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300"
            },
            {
                "nonce": 29,
                "index": 1,
                "timestamp": "1602598649",
                "data": "SeiiBlLqNXokldSU7mMGVw==",
                "previousHash":
"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300",
                "hash":
"0c612d1f67db6234bb26c6cf1c418e17658b027c4cd994dd914f5f4b542c27eb"
            },
            . . .
        ],
        "difficulty": 1
    }

}
```


Figure 12. API Response Top Up

Figure 12. is the result of response API when successful conduct transactions top up money pocket. Status 00 in the source code in Fig. 8 indicates the success of the transaction, on behalf of "Dwi Damayanti," top up with a total transaction balance of 650,000 IDR. In the first chain, it is initiated with the Genesis Block, then the value in the "data" chain represents the amount or value of the top-up transaction that has undergone the AES cryptography process then continues to the next chain, which is connected to the previous hash before which is chained with the next hash. The implementation of this proposed method uses the PHP programming language CodeIgniter, which generates an API response.

3.4. Testing Scenario

a. Cross-Site Scripting (XSS) Attack
   Scenario testing an attack on the system is using XSS is to deliberately insert a script that can change the data of transactions specific to the system when it is executed. The scenario for which the attack is performed on the 'amount' data. In this scenario, the attacker has succeeded in changing the security of his transaction data without knowing the actual amount because it is encrypted.

Table 2. Transaction Data Conducted by Students (Top-up)

Transaction ID	ID Students	Name	Transaction	Amount	Info	Transaction Date
1.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:17:29
2.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:22:19
3.	4112	Dwi Damayanti	Income	Rp. 250.000	Top Up	2020-10-13 21:32:35
4.	4112	Dwi Damayanti	Income	Rp. 150.000	Top Up	2020-10-13 21:49:43
5.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:54:26
6.	4112	Dwi Damayanti	Income	Rp. 100.000	Top Up	2020-10-13 22:05:26

Table 2 shown the transaction data conducted by students on behalf of Dwi Damayanti, where the top-up of the transaction has been recorded in the database server according to the

transaction date and according to the top-up value. The scenario (see table 3) was performed by the attacker, and the data was changed in the third transaction.

Table 3. Modified Attacker Data Scenarios

Test Parameters							
Transac-tion ID	Amount	Status	Message	ID Students	Name	Transac tion	Amount Total
3	300.000	00	Success	4112	Dwi Damayanti	Income	700.000
4	5.000.000	00	Success	4112	Dwi Damayanti	Income	5.550.000
5	300.000	00	Success	4112	Dwi Damayanti	Income	5.800.000
6	100.000	00	Success	4112	Dwi Damayanti	Income	5.800.000

Table 3. is the attack scenario on transaction id 3, where the attacker changes the transaction to 300,000 IDR. The total amount was obtained to be 700,000 IDR because previously in the user database, under the name "Dwi Damayanti," 650,000 IDR were stored according to the actual data. The calculation is that on transaction ID 3, the actual data value (according to table 2) is 250,000 IDR, then the attacker (see table 3) fills in the amount of 300,000 IDR, then the difference is 50,000 IDR. The difference is added to the total amount of the actual data. Then the attacker data will add the total amount to 700,000 IDR so that the amount of data affects the next chain.

b. Chain Validation

This test needs to be done to determine the successful performance of Blockchain technology modification with cryptography. Scenario testing on the system is using a chain validation that will correct the blocks one by one to match the previous hash of the block before. Chain valid will produce output true, and the chain is not valid will provide output false.

Table 4. Chain Validation Test Results

Index	Timestamp	Data			Amount	Previous Hash	Hash	Valid
		Transac tion ID	Transac tion Code	Infor mation				
0	1587747600	Null	Null	Null	Genesis Block	Null	558fdb1144...	true
1	1602598649	1	1	Top Up	SeiiBll...	558fdb1144...	Oc612d1f6...	true
2	1602598939	2	1	Top Up	SeiiBll...	Oc612d1f6...	007ce0918...	true
3	1602599555	3	1	Top Up	aX/+0kf...	007ce0918...	0355789ac...	false
4	1602600583	4	1	Top Up	6/9CLU...	0355789ac...	0b59b0b2d...	false
5	1602601462	5	1	Top Up	aX/+0kf...	0b59b0b2d...	030d2e016...	false
6	1602601526	6	1	Top Up	hTx63b...	030d2e016...	0047e66bd...	false

The results of the p chain validation test are shown in Table 4. The performance of this cryptographic modification of Blockchain technology is working properly on this system. This evidenced in the success of the chain validation to detect whether there is the immutability data or not that shown on the valid column valuable true or false.

4. Conclusion

The performance of blockchain technology with a combination of AES cryptography can be applied to online transactions to top up pocket money in schools. The use of a centralized blockchain can save costs in using servers, but double security can be provided, namely by involving AES cryptography. The test scenario involves the insertion of the script with Cross-Site Scripting (XSS) attacks, and an attacker must first perform a cryptographic process to find out the

actual top-up value of the transaction. In chain validation testing, it can be seen that chain has been attacked and the changes can be identified.

References

[1] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, "Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks," *CoRR*, vol. abs/1612.0, pp. 1–14, 2016, [Online]. Available: http://arxiv.org/abs/1612.05491.

[2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *CoRR*, vol. abs/1906.1, pp. 1–57, 2019, [Online]. Available: http://arxiv.org/abs/1906.11078.

[3] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains," *CoRR*, vol. abs/1809.0, pp. 103–113, 2018, [Online]. Available: http://arxiv.org/abs/1809.02702.

[4] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," *CoRR*, vol. abs/1608.0, pp. 1–13, 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.

[5] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/j.procs.2018.05.140.

[6] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," *2017 International Smart Cities Conference ISC2 2017*, vol. 00, no. c, pp. 1–4, 2017, doi: 10.1109/ISC2.2017.8090839.

[7] T. G. N. R. Alamelu and R. Soundararajan, "Cryptography Using Neural Network," *Proc. INDICON 2005 An International Conference of the IEEE India Council*, vol. 2005, no. I, pp. 258–261, 2005, doi: 10.1109/INDCON.2005.1590168.

[8] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. S. Ahmad, "Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control*,, vol. 17, no. 3, p. 1282, 2019, doi: 10.12928/telkomnika.v17i3.9384.

[9] S. Man and S. Shrestha, "C ++ Implementation of Neural Cryptography for Public Key Exchange and Secure Message Encryption with Rijndael Cipher," *Academia.Edu*, pp. 1–8, 2013, [Online]. Available: http://www.academia.edu/4055547/NeuroCrypto_C_Implementation_of_Neural_Cryptography_for_Public_Key_Exchange_and_Secure_Message_Encryption_with_Rijndael_Cipher.

[10] R. M. Awangga, "Peuyeum: A Geospatial {URL} Encrypted Web Framework Using Advance Encryption Standard-Cipher Block Chaining Mode," *{IOP} Conf. Ser. Earth Environ. Sci.*, vol. 145, p. 12055, Apr. 2018, doi: 10.1088/1755-1315/145/1/012055.

[11] A. C. Nugraha, “Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan,” *Jurnal PRODUKTIF*, vol. 4, no. 1, pp. 15–20, 2020.

[12] H. F. Putra and O. Penangsang, “Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid,” *J. Tek. ITS*, vol. 8, no. 1, pp. 11–16, 2019.

[13] A. Winarno, “Desain e-Transkip dengan Teknologi Blockchain,” *Seminar Nasional Pakar ke 2*, pp. 1–6, 2019.

[14] M. D. K. Perdani, Widyawan, and P. I. Santosa, “Blockchain Untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus Pada PT XYZ),” *Seminar Nasional Teknologi Informasi dan Multimedia*, pp. 7–12, 2018.

[15] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, pp. 1–5, 2017, doi: 10.1186/s13063-017-2035-z.

[16] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia computer science*, vol. 123, pp. 116–121, 2018, doi: 10.1016/j.procs.2018.01.019.

[17] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," *British Poultry Science*, vol. 14, no. 2, pp. 149–152, 2015, doi: 10.1080/00071667308416007.

[18] M. Shabani, "Blockchain-based platforms for genomic data sharing: a decentralized approach in response to the governance problems?," *Journal of the American Medical Informatics Association.*, vol. 26, no. 1, pp. 76–80, 2019, doi: 10.1093/jamia/ocy149.

[19] D. L. K. Chuen, *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press, 2015.

[20] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 38–45, 2018, doi: 10.1109/MSP.2018.3111245.
[21] P. Mahajan and A. Sachdeva, "A Study of Encrytion Algorithms AES, DES and RSA for Security," *Exp. Mech.*, vol. 13, no. 15, p. 9, 2013, doi: 10.1007/BF02322384.
[22] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *Jurnal Teknologi Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.
[23] G. W. Bhaudhayana and I. M. Widiartha, "Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap," *Jurnal ilmu Komputer. Univ. Udayana*, vol. 8, no. 2, pp. 15–25, 2015.
[24] R. K. Meenakshi and A. Arivazhagan, "RTL Modelling for the Cipher Block Chaining Mode (CBC) for Data Security," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 8, no. 3, pp. 709–711, 2017, doi: 10.11591/ijeecs.v8.i3.pp709-711.
[25] A. Nugrahantoro *et al.*, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," vol. XII, no. 1, pp. 12–21, 2020.
[26] R. Firmansyah and W. S. Prasetya, "Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery," *Jurnal ENTER*, vol. 1, no. Agustus, pp. 294–306, 2018.
[27] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," *Computer Networks*, vol. 166, p. 106960, 2020, doi: https://doi.org/10.1016/j.comnet.2019.106960.
[28] D. Deuber, B. Magri, and S. A. K. Thyagarajan, "Redactable blockchain in the permissionless setting," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp. 124–138, 2019, doi: 10.1109/SP.2019.00039.
[29] N. Alzahrani and N. Bulusu, "Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 30–35, doi: 10.1145/3211933.3211939.
[30] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T. H. Kim, "Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, 2019, doi: 10.1109/JIOT.2019.2911969.