ISSN 2614-0047

Data retrieval service on poverty blockchain-based on regional government

Moh. Hidayat Koniyo [a, 1, *], Made Sudarma [b, 2]

[a] Departement of Informatics Engineering, Universitas Negeri Gorontalo, Gorontalo, Indonesia
[b] Departement of Electrical Engineering, Universitas Udayana, Bali, Indonesia
[1] hidayat_koniyo@ung.ac.id; [2] imasudarma@gmail.com;
* corresponding author

ARTICLE INFO

Article history
Received December 23, 2019
Revised January 20, 2020
Accepted February 3, 2020

Keywords
Service
Poverty data
Integrity
Non-repudiation
Blockchain

ABSTRACT

The distribution of assistance to disadvantaged people in an area is always synonymous with problems especially, in the duplication of assistance and manipulation of family data that actually has no right to obtain assistance data for underprivileged families. To ensure the integrity of the data taken is not duplicated and non-repudiation, the blockchain-based poverty data collection plan is one solution. The purpose of this research is to ensure that the data retrieved cannot be modified after data retrieval, and the database cannot validly deny that the data has been provided as a result of a particular request. The feasibility of the proposed service using the blockchain method is a request from the poverty database in the form of low-income family data and assistance type data that are placed in the blockchain series and tested with hash values that have been created from the blockchain.

1. Introduction

Aid funds provided by the Government of Gorontalo city are currently classified in various types of assistance, with the hope that every family who is less fortunate after obtaining assistance can improve their standard of living so that the poor can be reduced each year. The distribution of aid to disadvantaged communities to Regional Governments has used a particular application for distributing assistance to disadvantaged people. In principle, these types of assistance are the same and distributed to low-income families can only get one type of assistance, the process of determining and providing assistance so far has used an application that selects the data of low-income families and assistance, but in its implementation, it is still found assistance which is duplicated, or there is a change in the type of assistance to a family that falls into the category of receiving assistance.

The poverty database changes every time the status of a low-income family is processed every year if the family has received assistance; it is expected to improve its standard of living so that in subsequent years it is not included in the low-income family. Thus, it is important to ensure that data cannot be manipulated and the user can have evidence of what data was taken from the database of poverty families at certain times as a result of the request.

Good data collection services must meet at least two requirements, namely integrity and non-repudiation [1]. Integrity is a query and the data retrieved cannot be modified (intentionally or unintentionally), when the retrieval operation is complete. Non-repudiation means that in view of past retrieval operations, poverty data retrieval services cannot validly reject data that has been provided by the service in response to requests given at a certain time [1].

This is what underlies the need for a block chain-based poverty data collection service that can seal each other's requests and results in every time a certain party requests distribution of assistance

to families who get help from a poverty database, so matters relating to duplication of low-income family data and low-income family status can be avoided. Nowadays, there is a great belief that Blockchain technology will revolutionize the health care industry [2], and reviews about the advantages and challenges of using Blockchain technology [3], [4].

2. Method

2.1. Integrity and Non-repudiation

Data integrity and repudiation are important things in application development. In article [5] mentions a list that compares various methods to achieve integrity, authenticity, non-repudiation, and evidence of existence. Furthermore, to provide a completed and structured overview of security requirements in the field of cloud computing solution [6], in addition to large-scale data processing that is distributed on MapReduce [7] and ad hoc vehicle networks (Vanet) [8], are aspects of security and privacy on this technology.

Common methods that used to ensure data integrity are backing up data, checksum techniques or using hash cryptographic [9]. This method has input length data and outputs a fixed-sized bit sequence. It has a one-way function, for example, internationally it is not feasible to calculate input from output, and it is deterministically, that is, a specific input that provides the same output. A slight change of input will produce a different output. So that, to ensure message integrity, a hash cryptographic functions can be used to calculate the message of hash values. On the other hand, the message integrity can be checked by comparing the initial hash value, which is stored with the hash value provided by the same hash cryptographic function in that message.

The technique often used on handling non-repudiation is a digital signature [9], an analogy from handwriting or manuals. For instance, the sender signed a message generated by a hash function which cryptographically secured. Then, the digital signal is implemented using asymmetric cryptography, by a pair of public keys to ensure there is no rejection, where the sender signed the message with the private key and the recipient uses the sender's public key to validate the signature.

2.2. Blockchain technology

The application of Blockchain technology has been applied to the demanding of biomedical data consumers (human or similar programs) who can get accurate data from biomedical database references [1]. Blockchain is a distributed transaction management technology that cannot be updated by certain parties. The first blockchain technology was proposed and implemented in bitcoin [10], with whom users can make transactions without regulators need (for example in banks). Besides, there is Ethereum [11], whom everyone can participate, and Hyperledger Fabric [12], that only approved parties can post to the blockchain.

In a blockchain, each new transaction is placed on a network of distributed nodes, after all nodes have agreed that the transaction is valid, the transaction is added to the block. Each block contains a timestamp, hash from the previous block, and transaction data so that a chain is created which doesn't change and adds up only. A copy of the entire blockchain is managed by each participating node. Within each block, transaction data is encoded in a hash tree [13].

Many applications use blockchain technology including the HER integration [14], sharing and access control [15], [16], preservation [17] and overall management [18], [19], so that, the distribution of assistance to poverty families in local governments needs to be developed using this Blockchain technology.

2.3. Poverty Data Request Service Architecture

Fig. 1 shows the architecture of poverty data collection services, where the main components are users, nodes/programs, databases, and blockchain. The service process mechanism starts from all users making requests (queries) to the blockchain system through the node, the node will retrieve its blockchain data, and if needed, the node will request DB Poverty data through the DB API Client. Furthermore, the results of requests are placed in each block, which continues to grow according to family data requests and types of assistance. Then the blocks are sent in the Blockchain with the hash value of each block. Retrieval results and information are then validated in the blockchain to avoid manipulation of aid distribution data to low-income families, and it is almost certain that there is no duplication of beneficiary data.

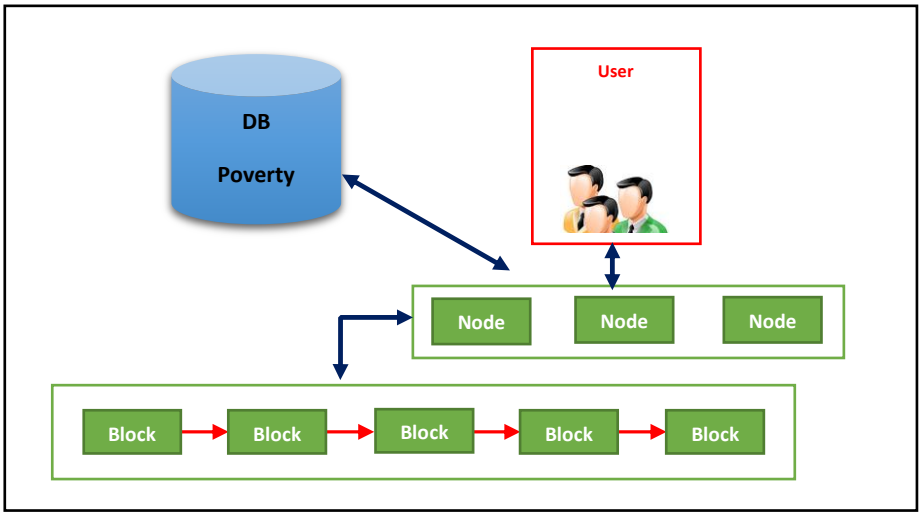

Fig. 1. Poverty Data Request Service Architecture

3. Results and Discussion

The results obtained from the application of blockchain technology in the distribution of assistance to Regional Governments are carried out in two scenarios, namely querying the data and testing the validity of the data channeling the assistance as shown in Fig. 2 the data query algorithm and Fig. 3 the testing algorithm.

In Fig. 2, shows a request service workflow to determine which families get this type of assistance using blockchain technology, where the flow starts from requests on client applications (nodes), the results of these requests are in the form of querying low-income family data and the type of assistance that has already received assistance. Furthermore, checking the query results of the data query, if the query does not exist, then it will form a new data block which will then be added to the blockchain. Results both from the old block and from the new block are displayed to the user.

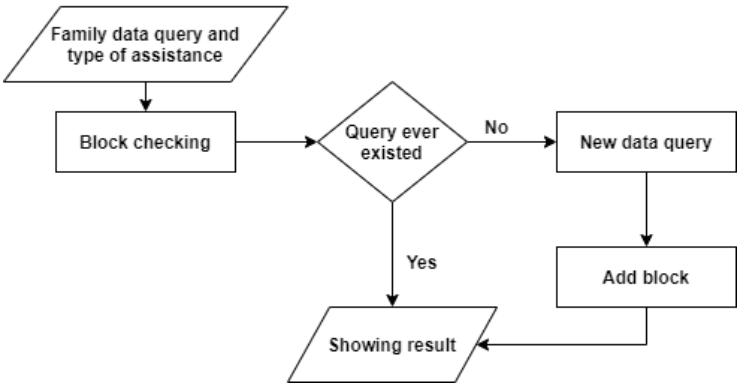

Fig. 2. Data Request Algorithm

To find out whether the hash of the query results is fitting with the previous user's request, then it is done by checking the hash, as shown in Fig. 3 of the hash proof algorithm. The principle of proof of hash with four conditions, namely:

- The hash is invalid or unproven
- The hash is valid with the condition that there are already new results in the blockchain
- The hash is valid with the condition that there is no new result yet from the transaction database.
- The valid hash with the condition that there is no new result from the blockchain, but there is already a new result from the transaction database.

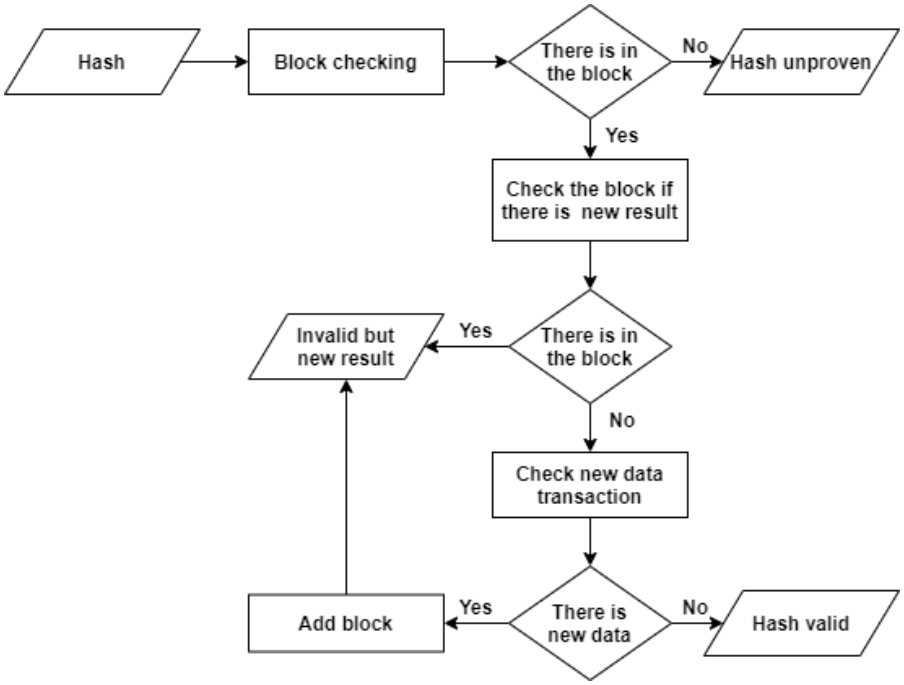

Fig. 3. Hash Proof Algorithm

Interfaces of family data requests and types of assistance for cases (a) that have been received, (b) that have not been received (data are in the blockchain) and (c) have never received assistance (Data is not in the blockchain, so it is requested from the database and added to the new blockchain). As shown in Fig. 4.

Query results by entering the family code in a blockchain for cases (a) that have not and (b) that have received aid in the blockchain obtained query results in the form of family data with the status of receiving and not receiving and the hash of the result of the query block in the blockchain. For case (c), which has never received aid (not in the blockchain), the query is sent to the database and entered in the new blockchain.

Interface testing (validation) hash data receiver and type of help for the case (a) invalid hash, (b) valid hash, with the condition that there is already a new result on the blockchain, (c) valid hash, with the condition, that there is no new result from the DB (d) valid hash, with the condition that there is no new result from the blockchain but there is already a new result from the DB.

Fig. 4. The query data interface from the Blockchain

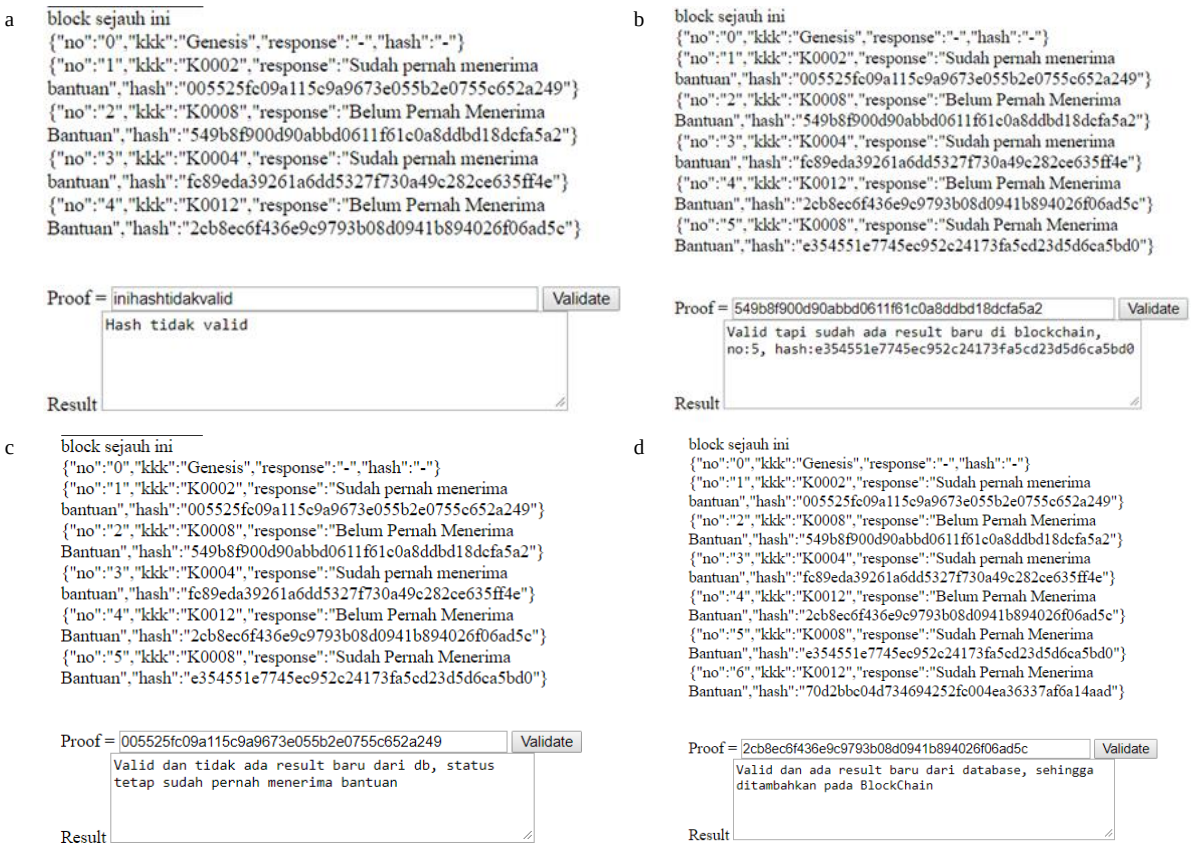

Fig. 5. The hash testing interface

The results of hash testing by entering hash values in the blockchain are two possibilities, namely valid and invalid. For case (a), the hash value is tested if it is not appropriate, then the result is a hash value that is invalid or not appropriate. For case (b), the hash value is tested if it is suitable, then the result is a valid hash value with the condition that there is a recent result on the blockchain. For case (c) the hash value is tested, the result is a valid hash value, with the condition that there is no new result from the DB, and for case (d) the hash value is tested, the result is a valid hash value, with the condition that there is no new result in the blockchain but has already a new result from DB.

4. Conclusion

This paper is one of the solutions for collecting poverty data in Regional Governments with the hope of minimizing data manipulation on the distribution of aid to low-income families. The service developed in taking data uses the blockchain method, where the process is carried out in a poverty database to request family data and types of assistance by checking on the blockchain for the status of receiving assistance and not receiving assistance. For the condition of the data contained in the blockchain, there are two statuses, they have received assistance and have not yet received assistance. As for data that is not in the blockchain, it is requested in the database and added to the new blockchain. For testing hash values, there are two possibilities, namely invalid hash value or not appropriate and valid hash value. For valid conditions, there are three states, namely valid hash values with new result conditions on the blockchain, with conditions, there are no new results from the database, and with conditions, there are no new results from the blockchain but there are new results from the database. Thus data retrieval using the blockchain method can be an effective solution to prevent manipulation of beneficiary data in the case of aid distribution in a Regional Government.

References

[1] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, “A blockchain-based notarization service for biomedical knowledge retrieval,” *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 288–297, 2018.

[2] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, 2016, pp. 1–3.

[3] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[4] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare." BioMed Central, 2018.

[5] M. Vigil, J. Buchmann, D. Cabarcas, C. Weinert, and A. Wiesmaier, "Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey," *Comput. Secur.*, vol. 50, pp. 16–32, 2015.

[6] I. Iankoulova and M. Daneva, "Cloud computing security requirements: A systematic review," in *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*, 2012, pp. 1–7.

[7] P. Derbeko, S. Dolev, E. Gudes, and S. Sharma, "Security and privacy aspects in MapReduce on clouds: A survey," *Comput. Sci. Rev.*, vol. 20, pp. 1–28, 2016.

[8] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, 2015.

[9] A. J. Menezes, J. Katz, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System.—2008.—9 p.[Electronic resource]," *URL http//bitcoin. org/bitcoin. pdf (date access 25.05. 2019)*.

[11] V. Buterin, "A next-generation smart contract and decentralized application platform," *white Pap.*, vol. 3, no. 37, 2014.

[12] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, 2016, vol. 310, p. 4.

[13] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Proj. yellow Pap.*, vol. 151, no. 2014, pp. 1–32, 2014.

[14] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.

[15] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[16] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. cities Soc.*, vol. 39, pp. 283–297, 2018.

[17] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, p. 141, 2018.

[18] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[19] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 136, 2018.