JOIV : Int. J. Inform. Visualization, 6(2) - June 2022 364-370

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

A Blockchain-based Halal Certificate Recording and Verification Prototype

Anak Agung Gde Agung [a,*], Heru Nugroho [a], Robbi Hendriyanto [a]

[a] *School of Applied Science, Telkom University, Bandung, Indonesia*

Corresponding author: [*]agung@tass.telkomuniversity.ac.id

***Abstract*— Halal certification assures that a product or a service has been created, processed, and delivered according to Islamic laws. Currently, the certificate is printed on a security paper and includes a QR code that can be used to verify the certificate online. However, there are some problems with the ongoing certificate verification process. The verification site is centralized, creating a single point of failure. The current verification system is also unable to detect the modified printed certificate. The research aims to propose an alternative halal certificate recording and verification system. A smart contract that runs on the Ethereum blockchain is developed and deployed for that purpose. As a result, the average certificate creation cost is US$20.035, and the process requires 5.75 seconds, while verification is free, and the result can be obtained in about one second. Utilizing the blockchain to store and verify the halal certificate increases trust in the product or service since once the data is stored, it cannot be changed and accessible to the public. Nodes around the world replicate the blockchain to ensure service availability. For future consideration, the system can be extended to automate and track the halal application process and integrated as an alternative to the current system by implementing multiple signatures in the smart contract for each party. Furthermore, the system can be integrated with a peer-to-peer sharing system such as IPFS to store the digital certificate.**

***Keywords*— Ethereum; smart contract; halal certificate.**

Manuscript received 15 Jan. 2022; revised 8 Mar. 2022; accepted 25 Apr. 2022. Date of publication 30 Jun. 2022.

I. INTRODUCTION

In Indonesia, halal certificate is a document published by Halal Product Assurance Agency (*Badan Penyelenggara Jaminan Produk Halal - BPJPH*) under the decree (*fatwa*) of Indonesian Ulema Council (*Majelis Ulama Indonesia - MUI).* The Indonesian Government has appointed the BPJPHo to manage the halal certification process under Regulation 33 of 2014 [1]. The halal certificate assures that a product or service is created, processed, and distributed in any way according to Islamic laws so that the product or service can be consumed safely by Moslem [2, 3, 4].

The halal certificate is a document printed using security paper. Each certificate may contain one or more products/services a company produces. To submit for halal certification, the company should have a Business Registration Number (*Nomor Induk Berusaha – NIB)* as a unique identifier published by the Investment Coordinating Board (*Badan Koordinasi Penanaman Modal – BKPN)*. After all the required documents are submitted to BPJPH, a series of tests is conducted by the appointed Halal Audit Agency (*Lembaga Pemeriksa Halal – LPH*). The test result will be brought to the MUI assembly to determine the halal status of the proposed product/service. Should the products/services pass, MUI will publish a decree. Based on the decree, BPJPH will publish a certificate, and the products/services are eligible to bear a halal mark on the packaging.

Although the certificate is printed on a security page and contains a QR code to verify the certificate online, there are some challenging aspects regarding the ongoing certificate verification process. The verification website itself is centralized, creating a single point of failure. Companies such as restaurants and food vendors often display copies of the certificate. Somehow, the official verification website does not display any of this information. Hence, there is a chance that some of the information stated on that copy is changed, as we demonstrate later in our experiment.

Other research shows some common issues and challenges in the halal industry. Fake or forged halal certifications expired, or unauthorized halal logos, dishonest or hidden product information, or other non-compliance occur

worldwide, but these issues and challenges are not unique to the halal industry [5].

In this paper, we propose the initial stage of a blockchain-based halal certificate management system, which is a blockchain-based system to store and verify halal certificates. The use of blockchain technology to verify and validate halal certificates issued has never been carried out in previous studies.

II. Materials and Method

A. Related Works

Blockchain is a technology first introduced in a white paper by a pseudo-anonym Nakamoto [6]. In the paper, he proposed a decentralized system for digital money, which could eliminate the double-spending problem. The double-spending problem is a weakness in the digital world, where data can be duplicated easily, so a third party is strictly needed as an intermediary or central authority. The central authority, however, can create problems for the system since it has the power to, for example, override a transaction, change transaction data, deny transactions, or charge a high fee for the services. Another example is the misuse of information for surveillance, which lowered the trust in the authorities [7]. As a result, bitcoin was launched in 2009.

Instead of trusting humans in a centralized organization, blockchain creates 'trustless' technology through cryptographic functions and decentralized computers [8]. Blockchain stores data in blocks. Each block is hashed to create a unique identifier, which also functions as the block's index. The index is then included in the next block to create a 'chain' between blocks. Adding a block to the blockchain is widely known as mining, also referring to the proof-of-work consensus mechanism used by most blockchain platforms. Data in a blockchain can only be added, so data can be traced back to its origin. A pair of private and public keys are required to identify the data owner and 'move' the data, which are mandatory for an entity to perform transactions in the blockchain.

To summarize, a blockchain platform requires computer participation to store blockchain copies, verify transactions and perform consensus mechanisms. More computer participation means more copies of blockchain available on the internet and more power to check the transactions. To compensate participants (and attract more contributors), participants are given an incentive in native cryptocurrency.

In 1994, a computerized transaction protocol to execute the terms of a contract was proposed by Szabo [9]. Later in 1996, he defined four objectives of a smart contract, (1) observability, the ability to observe each other's performance, (2) verifiability, the ability to prove that a party has fulfilled or breached a contract, (3) privity, the distribution ow power knowledge and control among parties, and (4) enforceability, to ensure predefined actions always executed once a set of conditions has been met [10].

A smart contract can be coded and stored in a blockchain. The first blockchain that utilizes a smart contract is Ethereum, proposed by Buterin [11]. Ethereum utilizes Ethereum Virtual Machine to execute codes. For every interaction with the blockchain, the initiator must pay a fee, which is meant to prevent spamming and create a stable environment because it goes to the miners. The smart contract enables people to create decentralized applications (dApps) [12]. The smart contract also provides a platform for automated, decentralized systems such as those utilized in smart cities [13], the education industry [14], health care [15], and many more.

In the case of halal certification, there are some problems identified before. The participants in the food industry appeared to regard this certification as essentially a license. Furthermore, a lack of human resources and a belief that the halal standard was costly created certain barriers to halal certification [16].

Different halal certification processes and requirements must be harmonized to allow consumers to make their own decisions based on their personal preferences. Adopting Blockchain Technology in the Halal Food Industry can help us achieve these goals. A common platform for accreditors to recognize and respect one another will be created [17].

Several studies have been carried out to develop information systems/technology related to halal certificates, like radio frequency identification establishing Halal certification for food products [18]. Another study is a mobile application that enables Muslims to verify the status of food products on the market [19]. The other study is AR technology is being used to determine the halal status of some products because there is much fake information out there these days, which is easily spread through social media [20].

B. Proposed Work

We propose a blockchain-based halal certificate recording and verification system, as shown in Fig. 1.

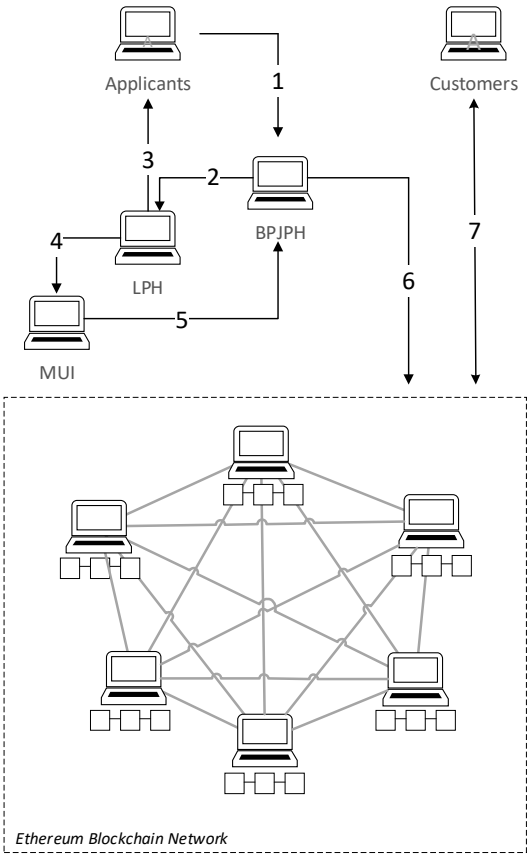

Fig. 1 Proposed System

For the first phase, the system is proposed to follow the current halal registration business process. Applicants apply for the certificate through BPJPH (1). BPJPH then appoints LPH (2) to assess the proposed products/services (3). The assessment result is used in the MUI assembly to determine the halal status of the products/services (4). If the proposed products/services pass, MUI will issue a decree. Based on the recommendation, BPJPH issues a halal certificate (6). Besides the printed certificate, the proposed system also records the certificate information on the blockchain. A unique ID is generated for each certificate, which the customers can use to verify a certificate (7).

The smart contract is a small program deployed on the blockchain network; it is accessible by the public. The smart contract has a built-in function to check and limit the user accessing the functions and data to manage the access right. The logical steps of recording the certificate, also known as the certificate mining process, can be found in Fig. 2. First, the company producing the products/services must be registered on the smart contract. This process is similar to the NIB registration process compared to the current halal registration process.

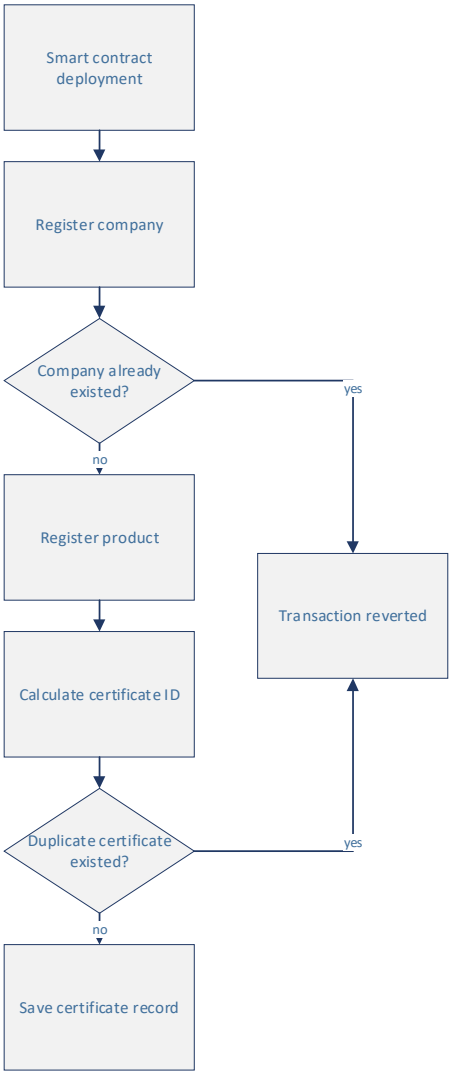

Fig. 2 Certificate Mining Process

In this proposed system, the company ID is an Ethereum address generated specifically for the company. A company should have a single ID. Should the duplicate ID be found, the process is stopped, and the transaction is reverted. The company record format can be found in Fig. 3 (A).

The next step is creating a halal certificate. The certificate contains all data in the printed certificate and records the hash of the official digital certificate published by BPJPH and the decree published by MUI. The file themselves are not stored in the blockchain to maintain lower fees. The documents can be shared publicly by recording the digital certificate and decree. Any changes made to the documents can be detected easily by comparing the hash. Before the certificate is stored in the blockchain, the data is hashed once again. The process provides a unique ID for the current certificate and can also be used for security measures if any data in the certificate is changed by comparing the hash value to the hash of all data. The system checks the blockchain for the ID. Should the ID exist, the transaction will be reverted. The record is saved in the blockchain if the certificate is unique, and no further modification is allowed. The certificate record format can be found in Fig. 3 (B).

A

CompanyID	*CompanyName*
	CompanyAddress

B

CertificateID	*CertificateNo*	*ProductType*	*ProductName*	*CompanyID*
	IssuedDate	*ExpiredDate*	*CertificateHash*	*DecreeHash*

Fig. 3 Certificate Record (A) and Company Record (B)

The company record contains the following information.

- CompanyID contains the Ethereum address of the company. This field is
- CompanyName contains the name of the company which produces the product or services. The company should have been registered and had a NIB.
- CompanyAddress, address of the company registered in NIB.
- The certificate record contains the following information.
- CertificateID contains the hash of the remaining field of the certificate.
- CertificateNo. contains the number of the physical certificate issued by BPJPH
- ProductType explains the type of business.
- ProductName contains the name of the product that bears the certificate.
- CompanyID contains the Ethereum address of the company. This should be linked to the corresponding field in the company record.
- IssuedDate contains the issue date of the physical certificate.
- ExpiredDate contains the expiration date of the physical certificate.
- CertificateHash contains the hash of the official version of the digitalized physical certificate issued by the BPJPH.
- DecreeHash contains the hash of the official version of the digitalized physical decree issued by the MUI.

We provide the fields to store certification and decree hash so the respective issuer can create a digital version of the physical certificate. Later, this file can be distributed freely or hosted on the internet. In our design, we do not design nor recommend using IPFS to store the certificate file since they still can be inaccessible if certain requirements are not fulfilled [21].

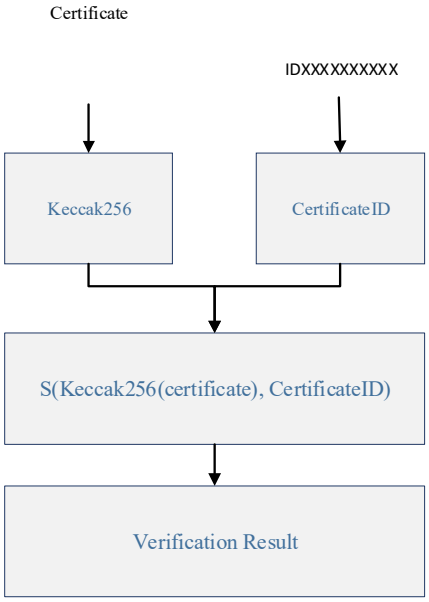

Fig. 4 Verification Process

Fig. 4 shows the verification logic process. Verifying a certificate involves a certificate ID or a pair of Certificate IDs and a digital certificate. The digital certificate is then processed through the Keccak256 [22] hash function, which is later compared to the hash stored in the blockchain. The result is then displayed to the operator.

C. *Testing Environment*

The smart contract is written in Solidity and deployed on Ethereum Ripstein Network. Ethereum network is selected for its ability to support smart contracts and large communities that support the platform. To test the functionality of the smart contract, we register five companies, each one registering one halal certificate. Each certificate contains unique values, including a set of hash values of the digital version of the halal certificate and halal decree. The costs and time needed for each operation are recorded.

III. Results and Discussion

A. *Results*

Fig. 5 shows the smart contract deployed. This contract can be accessed publicly using the contract address. However, only the contract owner (BPJPH) can add a company and add a certificate.

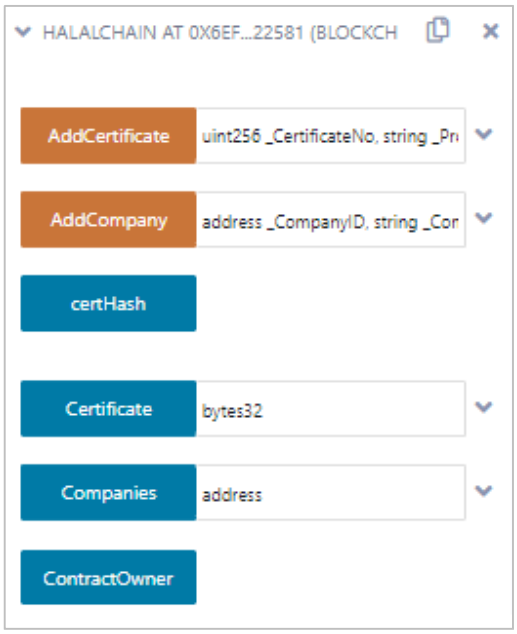

Fig. 5 Smart Contract

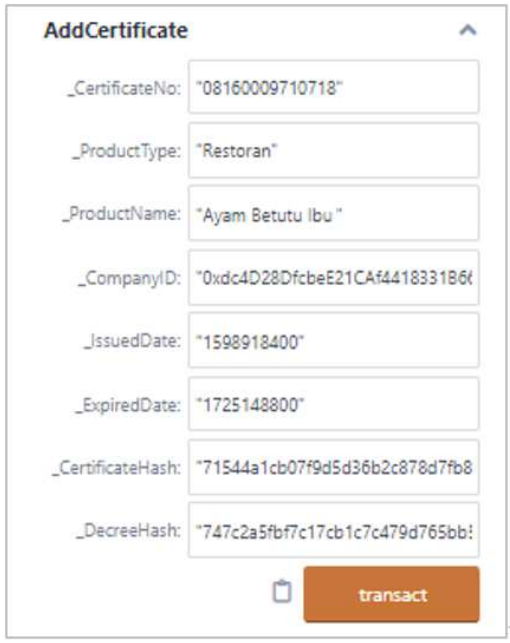

Fig. 6 Add A New Halal Certificate

Fig. 6 shows the interface where the operator can insert data to create a new certificate. Fig. 7 shows an error message when a duplicate certificate is found during the certificate creation process. Fig. 8 shows the system response when a certificate ID provided by the operator found a match during the verifying process.

```
The transaction has been reverted to the initial state.
Reason provided by the contract: "Certificate already existed".
```

Fig. 7 Example of Error Message (Duplicate Certificate Found)

Fig. 8 Verifying A Certificate

The smart contract has certification verification features. The first one is verifying the certificate's digital version, which checks if the digital certificate has been modified. In this test, we modify various modifications to the digital certificate, such as changing the certificate's issued date and expired date (Fig. 9). The digital certificate was detected as fake by calculating and comparing the hash with the stored hash, as shown in Fig. 10.

Fig. 9 Original Certificate (top) vs Fake Certificate (bottom)

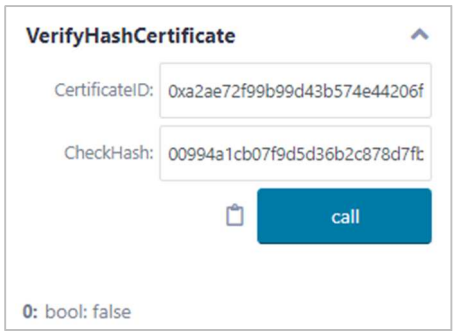

Fig. 10 Verification Feature by Hash

The other one checks if a certificate is still valid or has expired. Fig. 11 shows the validity check result of an expired certificate.

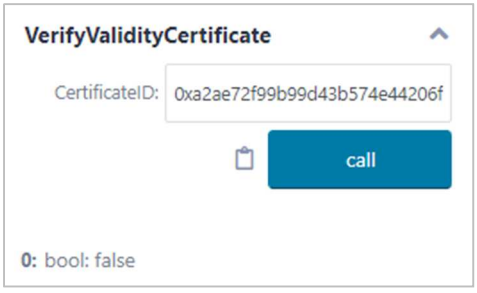

Fig. 11 Verification Feature by Date

Fig. 12 shows the time needed for each type of transaction. We observe that transaction times may fluctuate significantly, and the transaction times may vary even for the same transaction. The fastest time for company registration, for example, was eight seconds, while the longest was 18 seconds (125%).

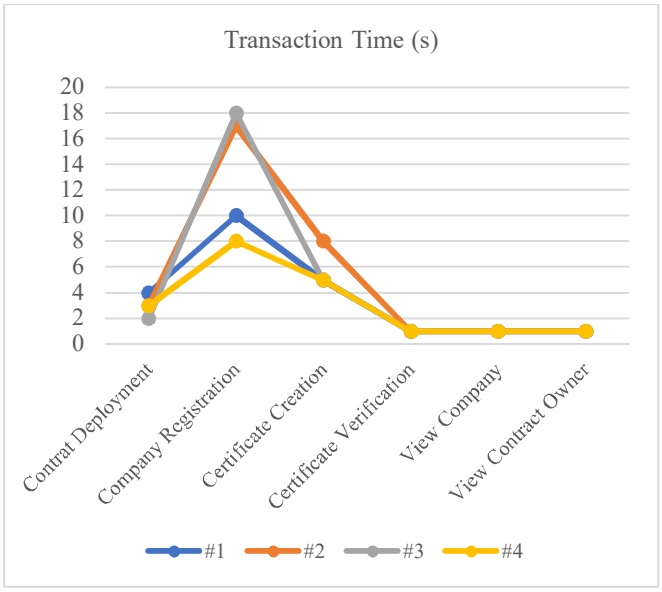

Fig. 12 Transaction Time

Fig. 13 shows the transaction fee for each type of transaction. The result shows that transaction fees are always changing over time. We notice that the highest contract deployment fee is 63.90% compared to the lowest fee. Although Ethereum implements a protocol to prevent a sudden spike in transaction fees, price change is inevitable and almost impossible to predict, as demonstrated in our previous research [23].

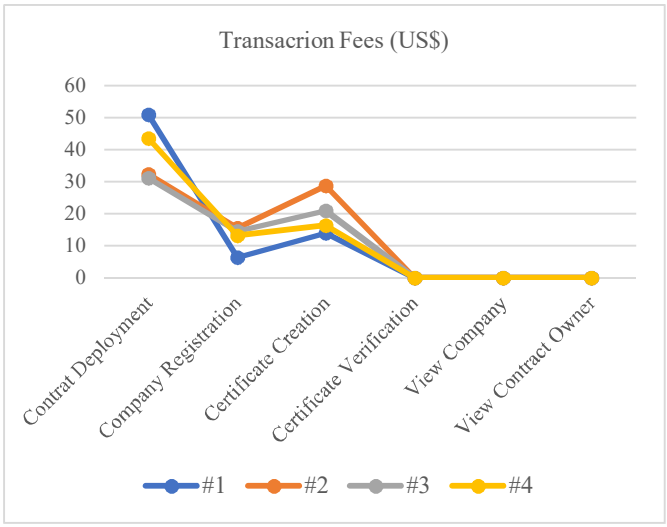

Fig. 13 Transaction Fee

TABLE shows the smart contract performance in summary, in terms of average time needed for execution and average transaction fee consumed for each action. Due to the fluctuation of the Ethereum price to the fiat currency, shortly

after the network confirms a transaction, the cost is converted to US$ to capture the equivalent value in US$.

TABLE I
SMART CONTRACT PERFORMANCE

Actions	Average Time (s)	Average Trx Fee (ETH)	Average Trx Fee (US$) *
Contract Deployment	3	0.012556001	39.525
Company Registration	13.25	0.003953133	12.43
Certificate Creation	5.75	0.006363784	20.035
Certificate Verification	1	0	0
View Company Data	1	0	0
View Contract Owner	1	0	0

* Average transaction fee in US$ is converted shortly after the transaction is confirmed

B. Discussions

A new transaction is pooled on the network memory, picked up by miners, and validated before being mined into the blockchain cause the process may need different times. It depends on many factors, such as the transaction fee offered by the contract executor and network traffic. This is due to the Ethereum protocol, which automatically adjusts fees depending on the network load. Contract deployment is a one-time cost paid by the contract owner (BPJPH). Company registration is a one-time cost that can be charged to each company, while certificate creation is paid for every certificate. However, due to the nature of the contract, a certificate cannot be changed once it is saved.

The verification process is accessible to everyone connected to the network, and the verification process needs about one second and can be performed without any cost. Although blockchain technology is novel to halal certification, other industries have taken advantage of blockchain utilization for recording and verifying valuable documents. This is due to the nature of the blockchain, (1) once the smart contract is deployed, predefined action must be executed when certain predefined requirements are met; (2) the blockchain provides immutability, so the action cannot be reversed; since nodes around the world maintain the blockchain in a peer-to-peer mode, it (3) the blockchain provides 'neutral' platform to the stakeholders, and (4) it eliminates the single point of failure, thus provides reliability and availability. Several studies, including the proposed method, are detailed in TABLE II below.

TABLE II
COMPARISON OF SIMILAR PROPOSALS

Ref.	Year	Proposed Method
[24]	2016	An application for patient record management system using blockchain.
[25]	2019	Blockchain and cloud storage utilization to store medical records.
[26]	2021	A blockchain-based system to store and verify the graduates' credentials.
Proposed method	2022	The use of blockchain through a smart contract to record and verify the halal certificate.

The blockchain, however, has some things that must be considered, (1) the pricing mechanism is based on the network traffic, so it is very hard to determine the exact fee for publishing a certificate; (2) users must keep the private keys secret all the time. In most cases, the breach in the blockchain account is because the user failed to do so; (3) the certificate cannot be edited once created. To minimize error, it is recommended to integrate the whole process into the smart contract. This way, user interaction can be limited to a minimum avoiding human errors. A further transition scenario is required to ensure the readiness of the current system.

IV. CONCLUSION

In this paper, we have proposed a blockchain-based system to store and verify the halal certificate. The smart contract stores information based on the printed certificate for this research. The contract also stores the hashes of the printed certificate and decree to accommodate the previously published certificates. The system has two verification processes, one showing current validity status and one verifying the digital document, to ensure the digital document has not been modified. For future works, the proposed system can be integrated more to replace the system used by the current business process. However, changing from the current system to a blockchain-based platform will take considerable effort and time. It requires at least modification to the current web system, building and deploying the smart contract, and training the users.

For this research, we propose the initial stage of the change, a smart contract to record and verify the halal certificate. The most challenging issue probably will be the current lack of regulation of blockchain technology. In the future, the halal decree and halal certificate can be made digital, eliminating the need for printed certificates. Document signing can be carried out with digital keys, and actions can be initiated automatically after a set of requirements have been fulfilled. A multi-signature mechanism can be initiated for processes involving multiple parties. A similar mechanism can also be used for international halal certification and simplify the current system. With a multi-signature mechanism, halal accreditors in a country only need to sign to recognize halal products/services already certified by other countries, based on the application record and testing history. In this proposed method, the smart contract is owned by BPJPH as the contract owner. This way, although the data is decentralized and miners will conduct the verification process, BPJPH still retains control of the process.

ACKNOWLEDGMENT

We thank Telkom University for funding this research.

REFERENCES

[1] Presiden Republik Indonesia, *Undang-Undang No. 33 Tahun 2014 tentang Jaminan Produk Halal*, 2014.

[2] Kementerian Perencanaan Pembangunan Nasional/ Badan Perencanaan Pembangunan Nasional, "Masterplan Ekonomi Syariah Indonesia 2019-2024: Hasil Kajian Analisis Ekonomi Syariah di Indonesia," Kementerian Perencanaan Pembangunan Nasional/ Badan Perencanaan Pembangunan Nasional, Jakarta, 2018.

[3] A. Nurcahyo and H. Hudrasyah, "The Influence of Halal Awareness, Halal Certification, and Personal Societal Perception Toward Purchase Intention: a Study of Instant Noodle Consumption of College Student in Bandung.," *Journal of Business and Management*, vol. 6, no. 1, 2017.

[4] H. M. Putri, M. Dachyar and R. Nurcahyo, "Measuring Service Quality of Halal Certification in Indonesia Food Industry using Fuzzy-

SERVQUAL Method for Service Quality Improvement," in *11th Annual International Conference on Industrial Engineering and Operations Management*, Singapore, 2021.
[5] N. A. Wahab, F. Shahwahid and N. Ab Hamid, "Issues, Challenges and Strength of The Halal Industry In Singapore: Muis's Experience," in *2nd International Conference on Economics & Banking*.
[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[7] P. D. Filippia, M. Mannan and W. Reijers, "Blockchain as a confidence machine: The problem of trust & challenges of governance," *Technology in Society*, vol. 62, 2020.
[8] F. Hawlitschek, B. Notheisen and T. Teubner, "The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy," *Electronic Commerce Research and Applications*, vol. 29, 2018.
[9] N. Szabo, "Smart Contract," 1994.
[10] N. Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996.
[11] V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*.
[12] W. Cai, Z. Wang, J. B. Ernst and Z. Hong, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access*, vol. 6, 2018.
[13] A. A. G. Agung and R. Handayani, "Blockchain for smart grid," *Journal of King Saud University - Computer and Information Sciences*, 2020.
[14] G. Chen, B. Xu, M. Lu and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, 2018.
[15] M. Gaynor, J. Tuttle-Newhall, J. Parker, A. Patel and C. Tang, "Adoption of Blockchain in Health Care," *Journal of Medical Internet Research*, vol. 22, no. 9, 2020.
[16] M. K. Anwar, A. Fahrullah and A. A. Ridlwan, "The Problems of Halal Certification for Food Industry In Indonesia," *International Journal of Civil Engineering and Technology (IJCIET)*, vol. 9, no. 8, pp. 1625-1632, 2018.
[17] G. R. Chandra, I. Ali and B. K. Sharma, "Blockchain Redefining: The Halal Food Sector," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Dubai, 2019.
[18] M. Nasir, A. Norman, S. Fauzi and M. Azmi, "An RFID-Based Validation System for Halal Food," *The International Arab Journal of Information Technology*, vol. 8, no. 2, 2011.
[19] M. S. b. Hashim, "Mobile Application on Halal Status Checking," Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 2013.
[20] H. Arshad, W. K. Obeidy, S. A. b. A. Shukri and R. Z. Abidin, "An Interactive Application for Halal Products Identification based on Augmented Reality," *International Journal on Advanced Science Engineering and Information Technology*, vol. 7, no. 1, 2017.
[21] IPFS Documentation, "Persistence, permanence, and pinning," [Online]. Available: https://docs.ipfs.io/concepts/persistence/#garbage-collection. [Accessed 12 12 2021].
[22] G. Bertoni, J. Daemen, M. Peeters and G. V. Assche, *The Keccak SHA-3 Submission*, 2011.
[23] A. A. G. Agung, R. G. Dillak, D. R. Suchendra and R. H., "Proof of Work: Energy Inefficiency and Profitability," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 5, pp. 1623-1633, 2019.
[24] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence," *Journal of Medical System*, vol. 40, no. 218, 2016.
[25] Y. Chen, S. Ding, Z. Xu, H. Zheng and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical," *Journal of Medical Systems*, vol. 43, no. 5, 2019.
[26] T. R. Reddy, P. V. G. D. P. Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha and B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," *EURASIP Journal on Information Security*, vol. 7, 2021.