Implementation of Block chain Technology to Maintain Halalness in the Sale of Fresh Beef

Inayatulloh
Information System Department
School of Information System
Bina Nusantara University
Jakarta, Indonesia
inay@binus.ac.id

Abstract

Indonesia as a country with a Muslim majority population is very concerned about the halal status of the food it consumes, including food in the form of fresh beef. The Indonesian Ulama Council has set the halal standard of fresh beef by collaborating with slaughterhouses that are closely monitored by the slaughtering process according to the halal standard according to Islamic law, but many illegal beef circulating does not comply with slaughter standards according to Islamic law and is difficult for Muslims to distinguish halal beef which is cut according to Islamic law and illegal beef. The purpose of this research is to help those who care about halal beef and make it easier for Muslims to find out the halalness of fresh beef using block chain technology.

Keywords
Block chain, fresh beef, halalness.

1. Introduction

Cows are a commodity in the livestock subsector. Cows have several types, namely beef cows which produce meat and dairy cows which produce milk. Beef cattle are livestock that can support the needs of meat consumption, because cows can be raised simply, easily, are liked by many people and their bodies are quite large when compared to other livestock. Beef has an advantage as a product, namely as a provider of good nutrition. Beef supply chain activities need to be carried out to meet consumer demand which is spread across several regions and is in accordance with the halal standards of the Indonesian Ulama Council or MUI.

The beef supply chain must pay attention to several aspects that can affect the smoothness of the distribution process up to the end consumers. Because in addition to meeting consumer demand, the form of regulation in the meat supply chain also aims to benefit the chain involved. So that we need an approach to the supply chain system in the form of an approach to find out product flow, financial flow, information flow besides the halal standard which is the most important thing in the beef supply chain for Muslim community.

As a country with the largest Muslim population in the world, halal products are a necessity for Indonesians. But in reality, regular people still have difficulty identifying the halalness of a food and beverage product including fresh beef sold in traditional and modern markets because there is no mechanism that can help Muslim consumers check the halalness of the beef they will consume.

1.1 Objectives

Taking into account that the majority of Indonesians are Muslim who are very concerned about the halal status of the food they consume, one of which is fresh beef and there is no mechanism that can be used for Muslims in Indonesia to check the fresh beef they will consume, a way is needed for Muslims Indonesia to know the halalness of the fresh beef it consumes. The large number of illegal beef or animal meat that is forbidden for Muslims circulating in traditional and modern markets in Indonesia is a strong reason to create a beef supply chain procedure that ensures the halal factor of beef that will be consumed by Indonesian Muslims. By considering the factors above, the aim of this research is the implementation of block chain technology to ensure the legitimacy of the beef supply chain that will be consumed by Indonesian Muslims.

2. Literature Review

2.1 Block Chain Technology

Block chain is a collection of data that is interrelated using cryptographic techniques. Block chain technology was first coined in 1991 by Stuart Haber and W. Scott Stornetta and later realized by an anonymous person named Satoshi Nakamoto who created block chain technology that became the basis for the popular cryptocurrency called Bitcoin. Along with the increasing popularity of Bitcoin and digital currency, block chain technology is also starting to be applied in various fields besides finance. Block chain technology that is decentralized and secure against manipulation or hacking of data makes it very attractive to be applied in the era of the Internet of Things (IoT). Block chain is also defined as a digital data storage system consisting of many servers (multi server). In block chain technology, data created by one server can be replicated and verified by another server (Hays, D.,2018)

Block chain is built using several existing technologies. The main technologies that build block chain are asymmetric key encryption, hash & hash chain functions, and peer-to-peer networks. (Inayatulloh, 2020)

1) Asymmetric Key Encryption is Encryption technique is a technique of changing data from one form to another by using mathematical functions without changing its content, so that only certain parties who have the key or passkey to change the encrypted data back to its original form (decryption process) are able to access the data. Encryption is the basis of securing digital data. The encryption technique used in block chain technology is asymmetric key encryption or also known as a public private key cryptosystem, where each user or user creates two keys in the form of a public key and a private key. The public key functions to identify transactions made by users on the block chain system, while the private key functions to authorize users to make transactions using the public key(Stallings, 1990),(Ferguson,2003)

   Another description explains that the public key is needed to encrypt transaction data so that it can be added to the public ledger on the block chain system, while the private key is needed to perform data decryption. The public key can be distributed to the public, while the private key must be kept private by the user, such as a password or pin. There are two types of asymmetric key encryption. The first is sending secret data, where the data sender first encrypts with a private key, then sends the encrypted data to the second party along with the public key to decrypt the data.

   The second way is to use private and public keys to sign the data. For example, there is a user who performs financial transactions. The user then encrypts the data with his private key, then publishes the unencrypted and unencrypted transaction data along with the public key it has. Other parties can decrypt the data with a public key, then compare the decrypted data with the original data, to ensure that the data is properly encrypted using the user's private key. This technique is called a digital signature, which functions to verify the validity of a transaction data.

2) Hash function and Hash chain The hash function or hash function is a mathematical function that converts data into another form of data with a fixed amount called a hash value or hash. Unlike encryption, data that is converted into a hash usually cannot be converted into its original form. An example of a hash function is modulo, where all infinite integers can be divided by an integer constant where the remainder of the division is the hash value of the module function. This hash value is a fixed number, but the converted modulo cannot be used to rebuild the original value. The nature of the hash function which is usually not possible to reconstruct the original data from the hash value makes the hash function suitable for application in cryptographic techniques. (M. Naor,1989)

   A hash function in cryptography is called a cryptographic hash function. On the block chain, hash functions are used as a technique for securing and validating data. Transaction data that will be added first are packed into a block of data before being converted using a hash function. The hash function on the block chain uses the hash value of the previous block to perform a new block hash calculation. Thus, each block is connected to each other as in a chain where changes in data in one block will affect the next blocks. Verification of the validity of a data can also be easily done by comparing the hash values between blocks. A collection of data blocks connected by a hash function is called a hash chain. Block chain is basically a hash chain in a global hash chain. In other words, the block chain is a global hash chain, where part of the data in the block is an internal hash chain.

   The hash chains are then distributed to computers owned by users of a block chain system. Asymmetric key encryption is then used to add security to the block chain. Each block in the data chain has a digital signature from the user who created the block along with its public key. This signature, generated by the user's private key, is unique and ensures that the new block is created by only one user. When a user creates a new block with his private key, the user will digitally sign the next block and leave the public key there. Then the user uses the public key left by the previous user in his block to verify the data and build the hash value of the data. In this way, each block of data is connected to each other and can be easily verified with the public key provided for each block.

3) Peer-to-peer Network Peer to peer (P2P) network is a network concept that allows a computer system to interact with one another without going through intermediaries or instructions from the main or central computer. In a P2P network all computers have the same status and they interact with each other based on mutually agreed rules, so there is no need for a central computer to regulate or give instructions. Therefore, the P2P system is decentralized.

The block chain system uses the concept of a P2P network, so that every computer can send data blocks to each other, the status of the block chain and whenever a new block is created. This makes each user a supervisor and guarantor of the validity of each block of data. The user can at any time check the validity of a block of data and any changes affect the overall structure of the block chain. Therefore, block chain does not need a central entity to manage and operate this system

.

2.2 Model

A model is a form of precise symbol, as a real procedure that permits somebody or a collection of persons to attempt to performance on the model. It is an understanding of the outcomes of explanations and capacities obtained from numerous systems". The design of the model has three foremost purposes, namely (Inayatulloh, 2016);

1) Deliver a functioning explanation of the system for a definite dated, in which near is indirectly a fixed of instructions for applying changes, how the system will function in the upcoming.
2) Deliver a explanation of definite occurrences rendering to time difference a fixed of procedures that are valued for the instruction of a system.
3) Creating models that present-day information

Around research usage models to describe research items such as new business models (Inayatulloh, 2016), DSS model for "BEKRAF" (Inayatulloh,2019), block chain models for regional head elections (Inayatulloh,2020), IT governance models for SMEs (Inayatulloh, 2020), CSF UKM models(Inayatulloh, 2020), Model for early warning system(Inayatulloh,2015) and Model for TAM SMEs (Inayatulloh, 2020).

3. Methods

Research begins by studying the process of slaughtering cows from the slaughterhouse to the market where consumers are going to buy. The second examines the parties involved in the beef supply chain or process. Figure 1 below describes the information flow and flow of beef products from the slaughterhouse to the market and the block chain implementation design:

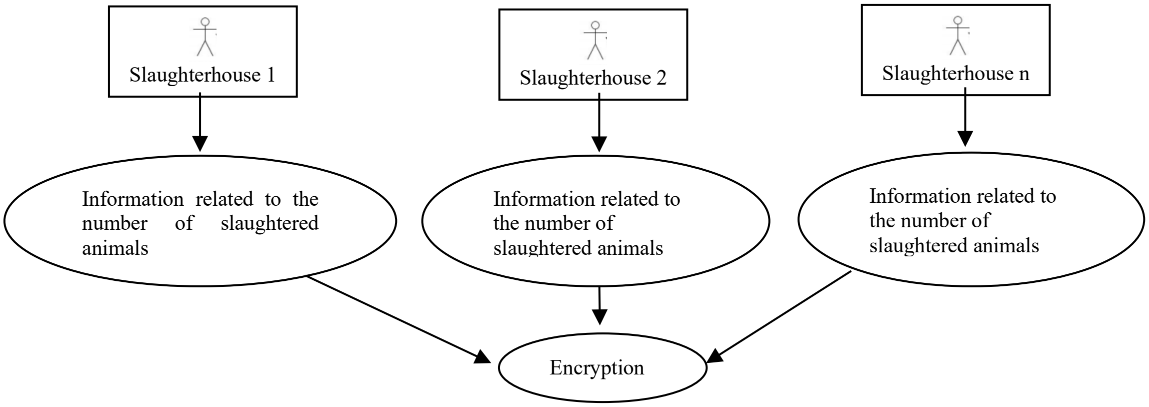
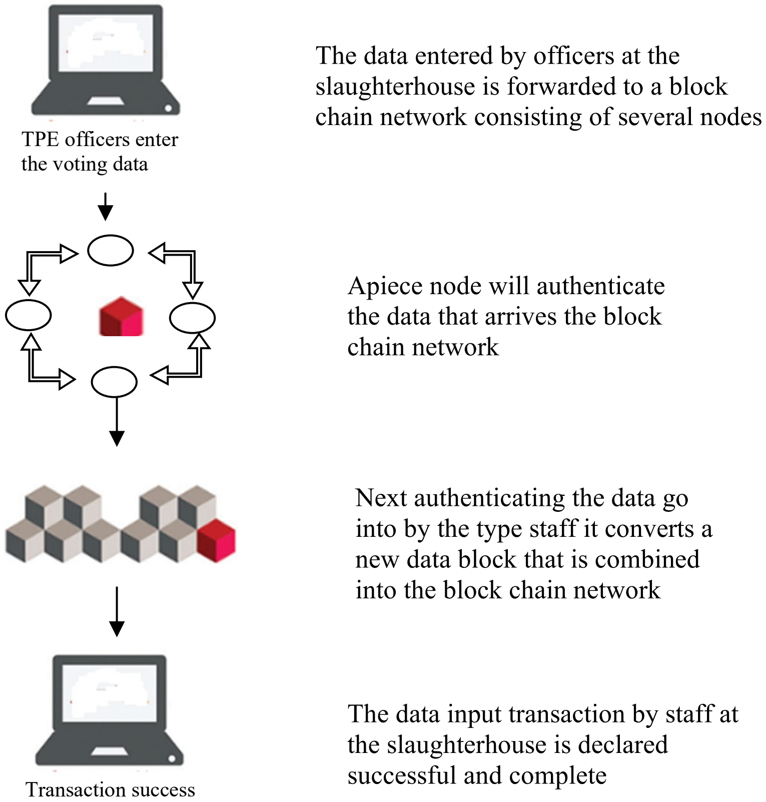

Slaughterhouse 1
Slaughterhouse 2
Slaughterhouse n
Information related to the number of slaughtered animals
Information related to the number of slaughtered animals
Information related to the number of slaughtered animals
Encryption

Figure 1 information encryption from slaughtered animals

The process of slaughtering animals is carried out at the slaughterhouse then the information about the slaughterhouse is encrypted..



The data entered by officers at the slaughterhouse is forwarded to a block chain network consisting of several nodes

Apiece node will authenticate the data that arrives the block chain network

Next authenticating the data go into by the type staff it converts a new data block that is combined into the block chain network

.

The data input transaction by staff at the slaughterhouse is declared successful and complete

Figure 2 the process of inputting data into the block chain

Figure 2 describes the validation process in a block chain network. Officers at the slaughterhouse input information based on the practice of slaughtering animals in that place. Then the information will go through a validation process before entering the block chain network. After the information is validated correctly, the information will become part of all existing block chain chains and block chain transactions are successful

3. Results and Discussion

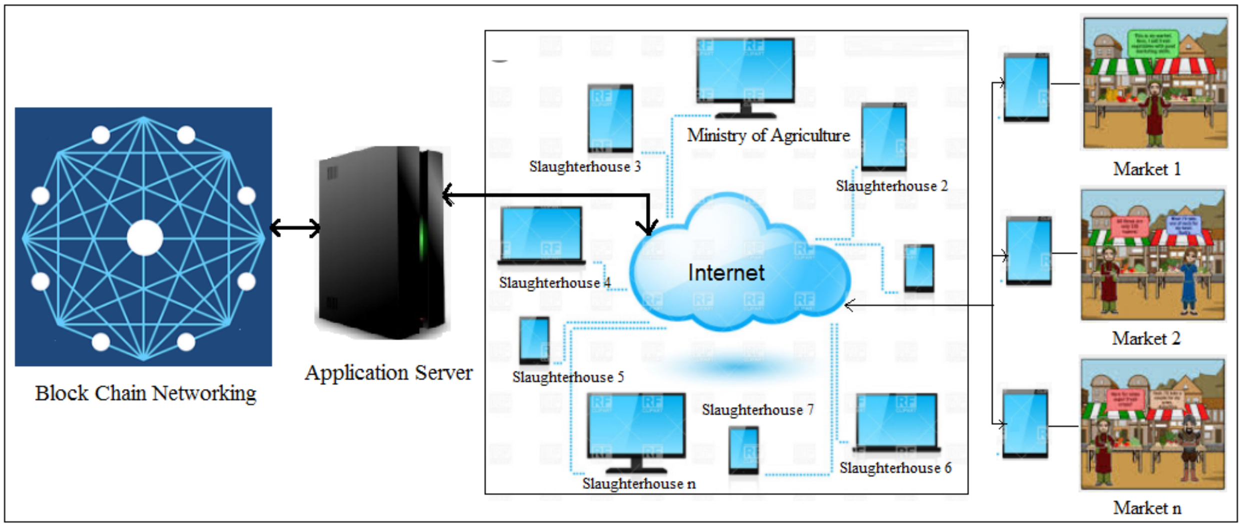


Figure 3. Block chain model for halal beef fresh

Figure 3 describes the overall interaction between all parties involved in the halal beef supply chain using the block chain network. As explained in the previous figure, the information that comes from the slaughterhouse is connected in a block chain network, which means that any changes or additions to existing fresh beef information are protected from illegal beef. Information on halal fresh beef that has been rigorously validated and is continuously updated can be used by consumers from the market via the internet using a smartphone or computer. The government can also use the information available for government purposes.

References

Ferguson, Niels; Schneier, Bruce (2003). *Practical Cryptography*. Wiley. ISBN 0-4712-2357-3

Hartono, I. K., & Alianto, H. (2020, August). Improving SMEs Knowledge and Performance With Cloud Computing CSF Approach: Systematic Literature Review. In 2020 International Conference on Information Management and Technology (ICIMTech) (pp. 664-668). IEEE

Hays, D. (2018). Blockchain: an overview. *LSE Business Review*.

Inayatulloh, Hartono, I. K., & Alianto, H. (2019, August). Decision Support System Model for Badan Ekonomi Kreatif Indonesia. In 2019 International Conference on Information Management and Technology (ICIMTech) (Vol. 1, pp. 498-502). IEEE

Inayatulloh, " IT governance training for small medium enterprises" Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020, 2020, pp. 876-880, 9211276

Inayatulloh . Technology acceptance model (TAM) for the implementation of knowledge acquired model for SME. Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020, 2020, pp. 767–770, 9211279

Inayatulloh , Early Warning System for infectious diseases, Proceeding of the 2015 9th International Conference on Telecommunication Systems Services and Applications, TSSA 2015, 2016, 7440435

Inayatulloh, Information system supporting partial transport, a new business model, Proceedings of 2016 International Conference on Information Management and Technology, ICIMTech 2016, 2017, pp. 286–290, 7930346

Inayatulloh, Cahya, S. P. . Block Chain Model for Regional Elections in Indonesia. In 2020 International Conference on Information Management and Technology (ICIMTech) (pp. 61-66). IEEE.

Inayatulloh (2015), Early Warning System for infectious diseases, Proceeding of the 2015 9th International Conference on Telecommunication Systems Services and Applications, TSSA 2015, 2016, 7440435

M. Naor, and M. Yung, "Universal One-Way Hash Functions and their Cryptographic Applications", in STOC, 1989, pp.33-43

Stallings, William (3 Mei 1990). *Cryptography and Network Security: Principles and Practice* . Prentice Hall. p. 165. ISBN 978-0-1386-9017-5

Biography

Inayatulloh is a candidate doctor at Bina Nusanatara University's Doctor of Computer Science. Since 2000, Inayatulloh has been a lecturer at several universities and colleges in Indonesia such as Bina Nusnantara University, Indonusa University, State Islamic University, Archipelago Economics College and is currently a lecturer at Bina Nusantara University in the school of information system. Scopus indexed publications have been produced with topics related to information systems such as e-learning, e-SCM, e-CRM. E-government and others