



OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SUPPLY CHAIN MANAGEMENT FOR AGRICULTURAL PRODUCTS USING BLOCKCHAIN TECHNOLOGY

Prof. P. S. Nawghare¹, Chinmay Ramdasi², Saras Sangle³, Vikas Yadav⁴, Radhika Yeware⁵

Zeal College of Engineering and Research, Narhe Pune Maharashtra, India ^{1,2,3,4,5}

Abstract: Nowadays the agricultural production in market is in centralized system. But by this approach, the transparency among different stakeholders (i.e. farmers, middle agents/ distributor, sellers) doesn't exist. In this paper transparency is maintained by using Blockchain technology. Supplying the products among stakeholders are tracked by the system to avoid misunderstanding between the suppliers. The main reason of using Blockchain technology for tracking the agricultural products is to maintain transparency, decentralized system (where there is no centralized system) and the most important asset is to maintain security. These are some key features of implementing Blockchain technology.

Keywords—MD5, AES, Blockchain

I INTRODUCTION

The traceability management system deals with supervising the quality of food products that are manufactured as well as supplied to different stakeholders involved in the supply chain. As the paper suggests that this system uses blockchain technology, the transactions for each block has been monitored by the admin. So even if there is some misleading information the admin will track and notify to the middle agent. If the problem is serious with respect to supplying false product the system will remove the distributor out of the system.

Blockchain consist of the several number of blocks(i.e. Transactions) which are linked together by providing the information of previous block to the current block to maintain transparency this even if the certain transaction gets an error in maintaining information it will not the whole system flow and also it will create more backups .Each block in the system creates a hash code which is referred by the next block. If there is some insertion of transactions(block) then that is done by at the tail so that the linked blocks are not disturbed.

For the tracing agricultural products is much more complex

thing because it require a large amount of data.For this some models are created for each transactions and they are referred in the next block.

For the security purpose various security mechanism are implemented such as for encryption algorithm AES algorithm is used and for creating hash code for the transactions MD5 algorithm is used.

II ALGORITHMS:

Algorithms used by the supply chain traceability system are for the security purpose so that the stranger should not be able to monitored or read the information during the entire process. For encryption of the data AES (Advanced Encryption Standard) algorithm is used and for creating hash code from the hash function MD5(Message digest 5) Algorithm is used. These two algorithms will to maintain security of the data.

AES Algorithm:

AES is used to encrypt the database. The encryption process uses a set of derived keys called as round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call as a state array.

Specification:

Blocksize: 128 bits.

Keysize: Depends upon number of rounds(10 rounds-128 bits 12 rounds-192 bits 14 rounds-256 bits)

STEPS:

- 1) Derive the set of round keys from cipher key.
- 2) Initialize the state array with the block data (information of the product).
- 3) Add the initial round key to the starting state array.
- 4) Perform nine rounds of state manipulation.
- 5) Perform the tenth and final round of state manipulation.
- 6) Copy the final state array.

MD5 Algorithm:

One of the key features of the blockchain in terms of security is visual cryptography.

In cryptography, MD5 is widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. The 512-bit input is of variable size.

An MD5 hash is typically expressed as a 32-digit hexadecimal number.

STEPS:

- 1) Append Padding Bits.
- 2) Append Length
- 3) Initialize MD Buffer
- 4) Process Message in 16-Word Block.
- 5) Output.

III SYSTEM DESIGN

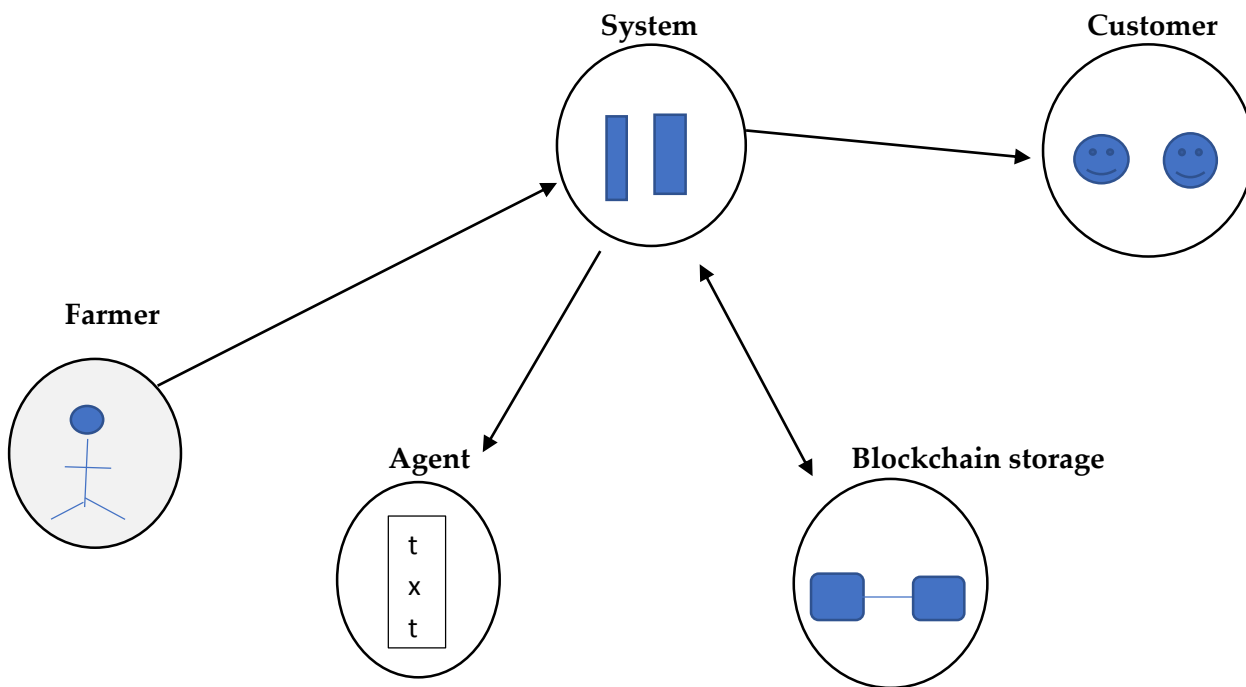


Figure 1: System Architecture of The Agricultural Products

From the figure the overall system architecture is explained and the tracking of the product is monitored by the system. Various Stakeholders (i.e. farmers, agents, customer) are actively participated in the system. Firstly, the farmer will register on the blockchain portal i.e. system. The details of the famers are stored in the portal and acknowledgement is given to the farmer using the portal app. Then the agent will register all his details in the portal so that the admin will monitor the agent. Then the farmer will give the product details to the

system and the information of the product which is in the system is transferred to the middle agent. The agents will further send the goods to the other suppliers. Meanwhile the admin will monitor the suppliers. If the system found any errors while delivering the products the system will give alerts to the admin and the admin will block the supplier.

The storing of the information of the famers and the goods are in blocks and the data is transfer to agent by using hash code.

IV UML Diagrams:

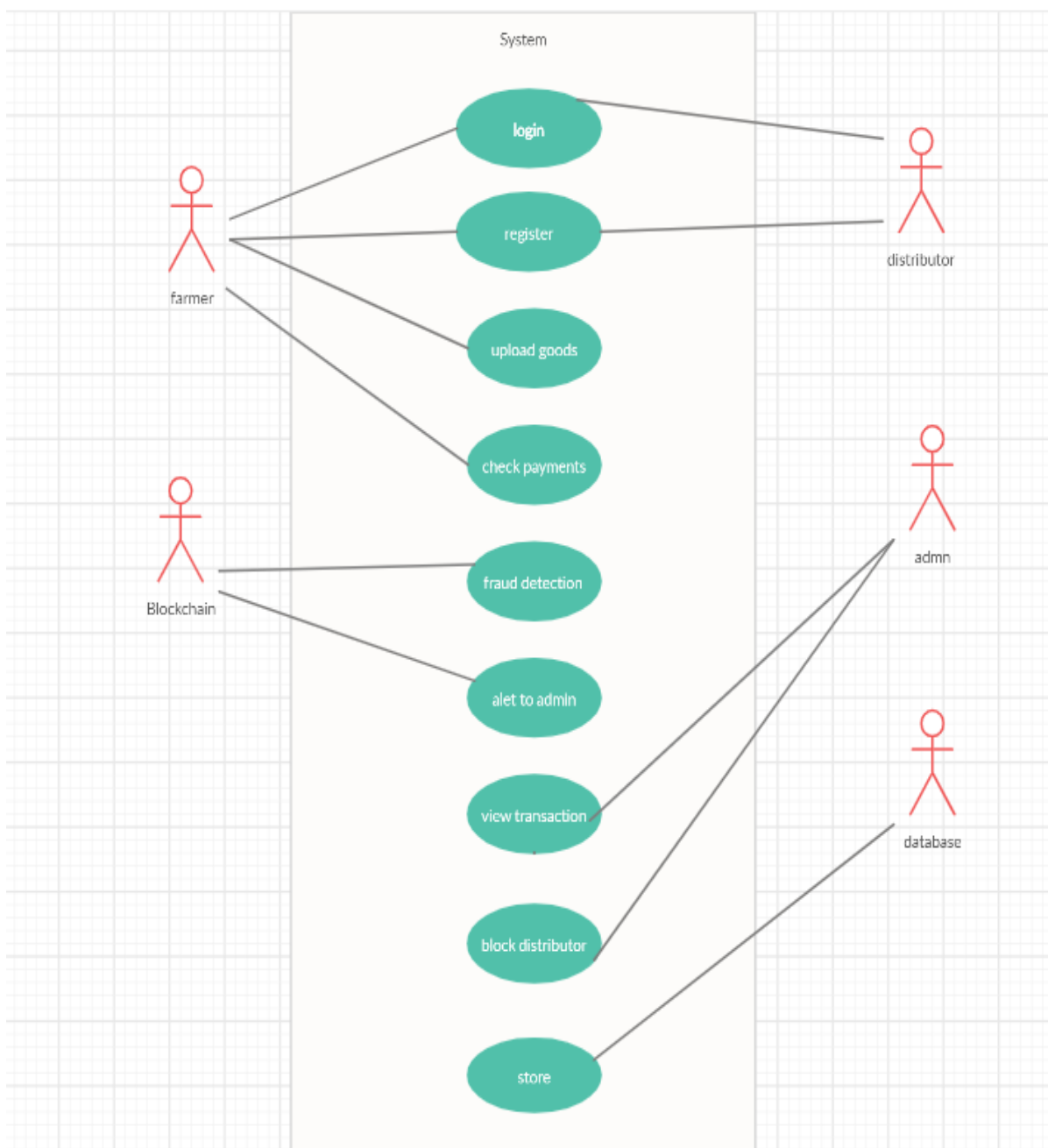


Figure 2: Use Case Diagram

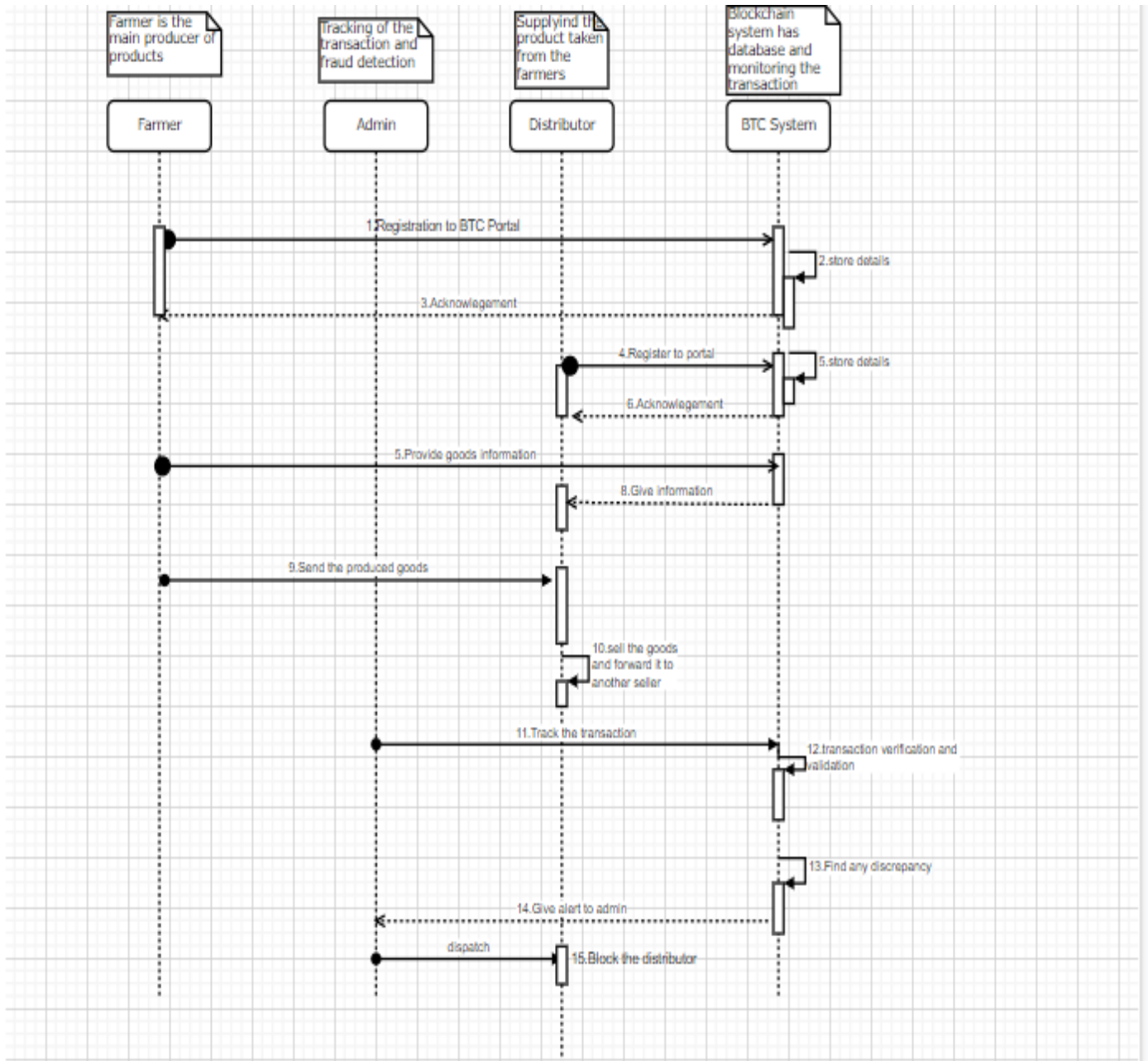


Figure 3: Sequence Diagram

V CONCLUSION:

As the paper explains about the tracking of agricultural products that is helpful for the farmers as well as the customer. Corruption in the market will be reduced by the system. Supply chain management will be well in control and well managed. Security is maintained.

REFERENCES:

[1] F. Lv and S. Chen, "Research on Establishing a Traceability System of Quality and Safety of Agricultural Products Based on Blockchain Technology," Rural Finance Research, vol. 12, pp. 22-26, 2016.

[2] Y. Yang and Z. Jia, "Application and Challenge of Blockchain Technology in the Field of Agricultural Internet of Things," Information Technology, vol. 258, pp. 24-26, 2017.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2008.

[4] Y. Yuan and F. Y. Wang, "Blockchain: The State of the Art and Future Trends," Acta Automatica Sinica, 2016.