

Smart Agro-Farm Using Blockchain Technology

Vishakha Khandekar, Shraddha Kumavat, Swati Malode, Dipali Shinde

ABSTRACT:

Blockchain is associate in nursing rising digital technology that allows omnipresent money transactions among distributed untrusted parties, while not the need of intermediaries, like example banks. Blockchain helps to unravel the issues related to ability, trust and transparency problems in fragmented market systems this text addresses the relevancy of Blockchain technology on farmer's Market. Market participants like suppliers, retailers and dealers are needed to travel through cumbersome method. Blockchain will build merchandise exchange for best through automation and decentralization. It helps cut back levied on customers in terms of commission whereas increasing the speed of the tactic for quick dealings settlements and therefore the use price. The technology will have a viable use in clearing and settlement, easing the work of trade and legal possession transfer of the protection. Blockchain will eliminate the need of a third-party regulator to an oversized extend, since the principles and regulation could also be constitutional inside a wise contract and enforced with every trade order to register dealings with the blockchain network acting as a regulator for all dealings. Blockchain records, transmits Associate in Nursing stores transferring activities of information price by distributed technology ensures that the knowledge isn't tempered and forget supported an uneven cryptography rule.

Keywords: Blockchain, Digital Agriculture, Hashing, Outcomes

INTRODUCTION

In several cryptocurrencies, varied organizations and alternative entities focusing at its transparency and fault tolerance the blockchain technology had gained its success and have proven its practicality to unravel issues wherever varied untrusted actors become involved within the distribution of some resource. most significant, extremely relevant areas is agriculture. Agriculture is well interlinked, because the merchandise of agriculture area unit used as inputs in distributed provide chain involving multi-actor, wherever the ultimate shopper is typically shopper. Across the world, farm sector is that the only 1 that is heavily passionate about government subsidies. what proportion of this quantity reaches the farmers is often in question? but, with blockchain the distribution and delivery of subsidizes will become a lot of clear. As new technology, the times of blockchain application have simply begun. the most aim of the blockchain application is to require the facility off from the hands of the multi-actor concerned in by dispersive info and handing it over to the individuals, democracy within the true sense.

In the normal methodology of exchange of products area unit supported advanced and paper-heavy settlement processes whereas these processes aren't a lot of clear, this includes the high risks between patrons and sellers throughout exchange important. It estimates that value the price of in operation provide chains makes up 2 thirds of the ultimate cost of products. The transactions area unit liable to fraud, with several intermediaries concerned, that will increase the general prices of the transfers. Farmers area unit

usually unaware regarding the inputs. native level retailer's area unit merchandising fraud merchandise to the purchasers to extend their profit margins. from time to time even the retailer's area unit unaware if the merchandise equipped to them by the distributors area unit fraud or real. By increasing the traceability of every product sold, blockchain application helps to unravel this drawback. This application would demolish the middleman i.e. the retailers, distributors or wholesalers by delivery entire agricultural sector and other people on common digital platform.

Improved information sharing also can facilitate cut back the \$1 trillion issues of products waste. Farmers and customers will access all the data. This makes the system a lot of democratic and economical which ends up in lesser merchandise wastage and better remuneration being paid to the farmers. Blockchain in agriculture associate to grow at an annual rate of growth of eighty-seven and increase from \$45 million in 2018 to \$3,314.6 million by 2023 (Chang, Iakovou and Shi 2019).

LITERATURE REVIEW

In Dec 2016, the corporate Agri Digital dead the world's 1st settlement of the sale of 23.46 loads of grain on a blockchain (ICT4Ag 2017). The success of Agri Digital served as a plan for the potential use of this technology within the agricultural provide chain. Agri Digital is currently planning to build sure and economical agricultural provide chains by means that of blockchain technology (Agri Digital 2017). Recently, Louis

Alfred Dreyfus Co (LDC), has teamed up for the primary agricultural artefact trade with the banks [4].

The first corporations to embrace the blockchain area unit Walmart and Kroger by victimization blockchain technology into their supply chains (CB Insights 2017), they were operating at first on case studies that focus principally on Chinese pork and Mexican mangoes (Kamath 2018). however the first results from the studies showed that, once pursuit a package of mangoes from the market to the farm wherever they were big, it took 6.5 days to spot the origin and therefore the path the fruit followed with ancient strategies, whereas with blockchain this data was accessible in barely some seconds (Wass 2017)[5].

Small cooperatives of farmers square measure the simplest way to lift fight in developing countries (Chinaka 2016). Via cooperatives, individual farmers will win an even bigger share of the worth of the crops they're cultivating (Farm Share 2017). Farm Share aims to make new kinds of possession of property, cooperation of communities and self-sustaining native economies.

Agri Ledger to extend trust among little cooperatives in Africa uses distributed crypto ledger (Agri Ledger 2017). The authors in (Davcev, et al. 2018) planned a brand new approach that ends up in trustworthy cooperative applications and services at intervals the agro-food chain, among farmers and different entities of the chain to a different example is that the OlivaCoin that is the B2B platform used for trade of vegetable oil, supporting the market of vegetable oil, that helps to reduce the money prices, increase transparency and find the better access to international markets (OlivaCoin 2016)[4].

ARCHITECTURE

In this, we present the theory on online small-scale market for farmers and customers. The overall diagram of the proposed method is explained. For benefits of middle class and farmers we are going to develop application which is decentralized and secure way. Every seller and person who wants to rent product, make their profile with gov. identity and personal contacts, email, etc. attributes. Customers who are interested will search for a product, set the near buy location and go for delivery servants. If they are available, then sign the smart contract and price between or its by personalservice or according to owners rules one can deliver it to each other. Then one can pay online or cash on deliver.

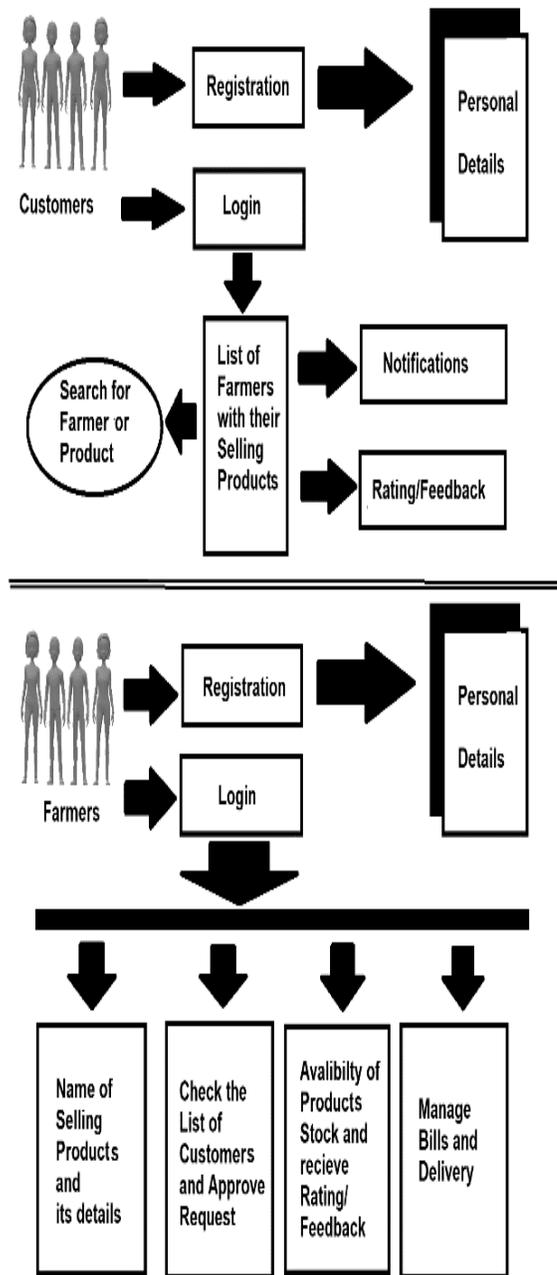


fig. Login Architectural Diagram

Fig 1. Login Architectural Diagram

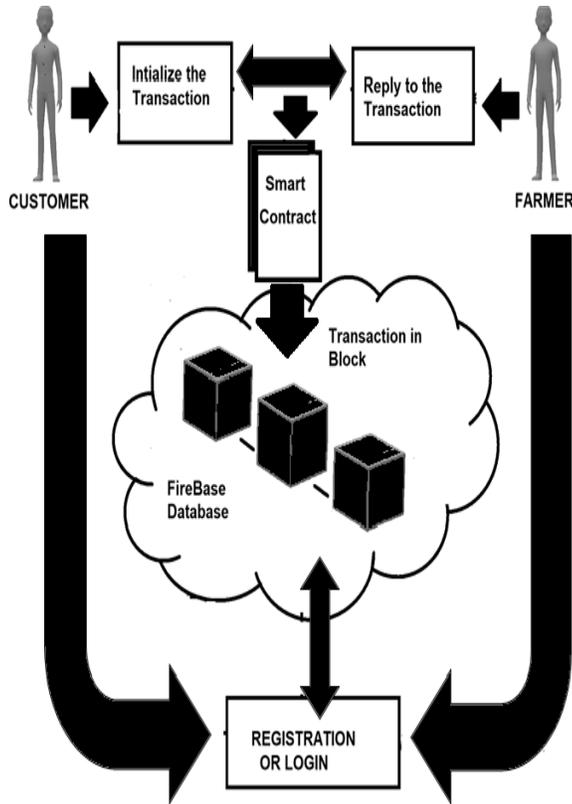


fig. Transactional Architecture Diagram

Fig 2. Transactional architecture diagram

Later, every farmer and deliver servant is involved in process will get the feedback and rating from customer and that will decide their ranking of product as well as sincere work of deliver servant. For rating we are going to use Average or Mean Algorithm.

This is mobile android application, so for it we are going to use firebase database so it can keep in sync easily. Most of the data is going to update like rating, location record, products, etc. attributes and to store whole data and update time to time firebase cloud database is used which is supported by android, iOS and web applications.

ALGORITHM

Secure Hashing Algorithm (SHA-1)

The foremost adopted secure hashing algorithms related to the blockchain technology are SHA-1, SHA2, and SHA-256 etc., encoding as a result of their quality of hash operate that make distinctive outputs once given completely different inputs [1,2]. In the secure hash function unique key created to identify a transaction at the same time it identifies an individual in the petroleum supply chain. SHA was originally designed by the United States National Security Agency (NSA) and United States Federal Information

Processing Standard. This algorithm is very efficient to verifying file and message integrity during transaction, data identification, and password verification. SHA-1 contains message size of $<2^{64}$ bits 512-bit block size, 32-bit word size, and 160 message digests [3].

Step 1: Append Padding Bits

Padding means addition of bits to original message. To make length of original message to a value of 64 bits less than multiple of 512. The padding message consists of single 1-bit, followed by 0 bits as required.

Step 2: Append Length

A block of 64-bits is appended to a message. 64 bits of original message is appended to the result of above step 1 (Original message + padding). It is appended such that least significant bytes to most significant byte.

Step 3: Initialize MD5 Buffer

A 160-bit buffer is used to store the intermediate as well as the result. It uses a big-endian method. The buffer is represented as five 32-registers as P, Q, R, S, T as

P = 67 45 23 01
 Q = EF CD AB 89
 R = 98 BA DC FE
 S = 10 32 54 76
 T = C3 D2 E1 F0

Step 4: Process Message in 512-bits Block

It consists of four rounds of 20-step each. They are referred as F1, F2, F3, F4 have similar structure but these rounds use different primitive logical function. Each round takes input 512-bits block processed it and produced 160-bit output. Each round also uses an additive constant k where $0 < k < 79$.

Step 5: Output

After processing all L 512-bit blocks, the 160-bit message digest is produced as the output.

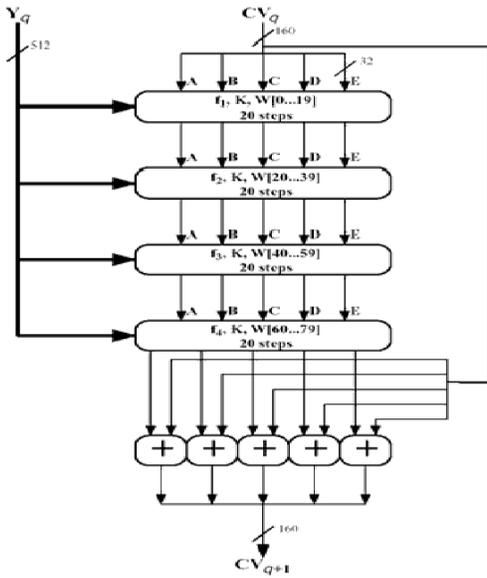


Fig 3. SHA-1

Blockchain technology is a combination of blocks in its design. Every block is created from information and the hash of the previous block, apart from the origin block that contains hash value of previous block as shown in Figure.

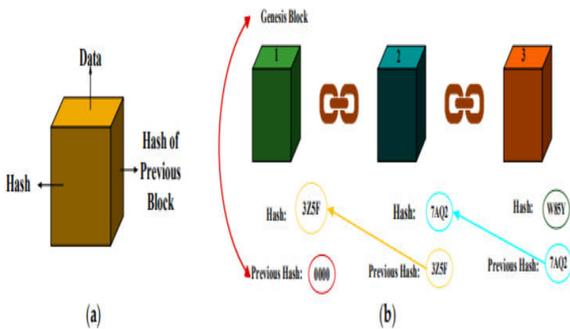


Fig4. Hash Block algorithm

Blockchain technology functions are reliable to be used during a hashing crypto technique, that helps produce an adequate and powerful hashing code and convert it from a small amount of fastened size knowledge to strings of character. every dealing projected during a blockchain are hashed along before shoving during a block, and therefore the hash pointers connect every block to successive block for holding of previous hash knowledge because it is incontestable. Therefore, any changes within the blockchain dealings of hashing perform can lead to completely different hash string of character and influence all the concerned blocks.

FUNCTIONAL REQUIREMENTS

Registration

The system will allow to farmer and customer to add their data to the system.

Upload Image

The system will allow the farmer to upload/add images of his goods to the system.

Product order via app

Customer can order product with the help of app.

Take order

The farmer will take order and if it is available then farmer will confirm the order.

Available goods

Farmer will check the what goods are available.

Serve order

When order is ready, farmer will serve order.

Payment

Customer will make payment through Paytm or by cash on delivery and Farmer will receive the payment.

Required goods

Farmer can add the required goods.

Customer feedback

Customer will give feedback about product and services.

A. Database

Customer Dataset

This dataset can store all data related to customer (customer name, mobile number, and address).

Farmer Dataset

This dataset can store all data related to farmer (farmer name, mobile number address, product information).

Product Dataset

This dataset can store all data related to product (ProductName, available quantity, prize, farmer name).

Feedback Dataset

This dataset can store all feedbacks given by customer related to the product and services.

B. Design Constraints

Database

The system will use fire base database, which is open source and free.

Operating-system

The development environment will be windows 10.

Framework

The system will be developing under .net framework 2.0.

Android-application

The system will be android base application.

Multi-use

The multiple user can use this system at a time.

NON-FUNCTIONAL REQUIREMENTS

A. Security

Login ID

Any user who uses the system will have login ID and password.

Modification

Any modification (insert, delete, update) of the product for database will be synchronized and will be done by farmer.

B. Performance Requirements

Response Time

The system will give responses in 1 sec after checking the products.

Capacity

The system must support near about 1000 people at a time.

User-interface

User-interface screen will respond within 5 seconds.

C. Maintainability

Errors

The system will keep a log of all the errors.

Reliability

The system will be reliable i.e. in any malicious attack the data can't be change or approved at next level due to use of hash function.

Availability

The system will be available all the time whenever you login to the system.

SYSTEM REQUIREMENTS

A. Hardware Requirement

- 2GB Ram and above.
- Dual Processor.
- Hard Disk 320gb and above.

B. Software Requirement

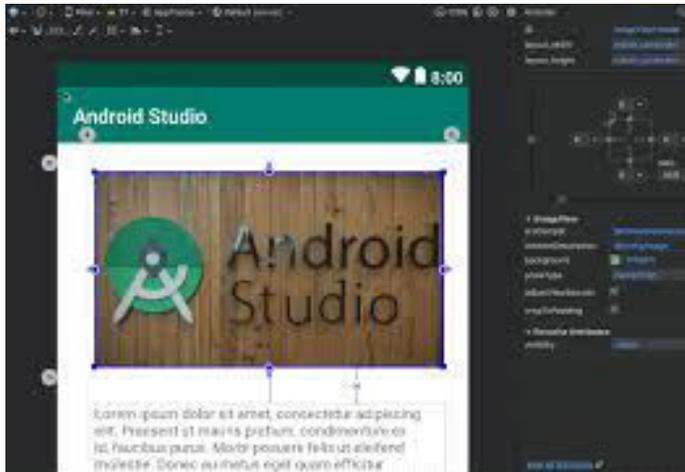
- Firebase Database.



- Windows 10.

C. Test Environmental Tools

- Android Studio.



OUTCOMES

- I. Individual customers, organizations, hotels, restaurants etc., can directly get connected with sellers.
- II. Easy information accepts for local level markets.
- III. Direct connection between buyers and sellers.
- IV. Empowering farmers by providing latest technology.

CONCLUSION

This article demonstrates that blockchain technology is already being employed by several projects and initiatives, planning to establish verified and trustworthy environment to make a clear and additional sustainable decentralized marketplace which might connect the farmers and customers on the one platform, which might facilitate to cut back the fraud, and third party get eliminated also, this would additionally help to decrease the wastage of farmers product.

REFERENCES

- I. Kumar, S.; Gupta, P. A comparative analysis of sha and MD5 algorithm. *Int. J. Comput. Sci. Inf. Technol.* 2014,5, 4492–4495.
- II. Gligoroski, D.; Markovski, S.; Knapskog, S.J. A secure hash algorithm with only 8 folded sha-1 steps. *Int. J.194 Comput. Sci. Netw. Secur.* 2006, 6, 194–205.
- III. Manuel, S. Classification and generation of disturbance vectors for collision attacks against SHA-1. *Des.Codes Cryptogr.* 2011, 59, 247–263. [CrossRef]
- IV. <https://arxiv.org/ftp/arxiv/papers/1908/1908.07391.pdf>
- V. Tian, F.: An agri-food supply chain traceability system for china based on RFID and blockchain technology. In 2016 13th International Conference on service systems and service management (ICSSSM),pp. 1-6. IEEE (2016)