Blockchain & Smart Contracts: A Use Case for Procuring Grains from Farmers by the Government

[*]Mohammedhussain Bharmal, [#]Nidhi
[*]Student, [#]Assistant Professor, [*,#]Bharati Vidyapeeth's Institute of Management and Information Technology (BVIMIT), C.B.D. Belapur, India.
[*]mohammedbharmal3695@gmail.com, [#]nidhi.poonia@bharatividyapeeth.edu

Abstract: India is an agricultural country. Farming is the main occupation of the people of India. Growing crops and maintaining them is a challenging job and so is selling the produce to the government. The current methods are very old and inefficient. Farmers usually don't get the prices fixed by the government and there are a lot of frauds. Blockchain can help to solve these problems. It is a technology which makes recording transactions much more efficient and transparent than the traditional system. It was first used in Bitcoin, a cryptocurrency to transfer coins anonymously within minutes. These coins can then be exchanged or sold for real money. Later many other cryptocurrencies were developed using blockchain. However, it has more applications than just cryptocurrencies. This paper aims to explain how blockchain and smart contracts can be used to improve the trading of agricultural goods from farmers with the government of India. It also explains how blockchain can prevent frauds and streamlines the process of paying the farmers on time.

Keywords: Agriculture, Blockchain, Ethereum, Farmers, Government of India, Smart Contracts.

I. INTRODUCTION

Agriculture contributes to around 17.4% of the Indian economy and also employs 54.6% of the population [1]. India is the second largest producer of fruits and vegetables. In 2001-02 India produced 145.8 MT and in 2014-15 it rose to 283. MT. India is also the largest producer of milk. With the advancements in technology, agricultural practices in India have changed drastically. The Green Revolution has introduced higher-yield varieties of grains and changed the old and less efficient ways of farming [1]. But most of the farmers in India are illiterate, they are not able to cope up with the rapid changes. They are being duped into buying the required things for farming. For example, many farmers can't tell the difference between a higher yield seed and a normal seed and the seller takes advantage of this and tricks the farmer. This also holds true while selling their grains to the Government.

Many farmers don't understand the current system of how the Government procures grains from them. The concept of Minimum Support Price (MSP) and how that price can change based on the quality of grains is still not clear to them. This has led to many farmers being tricked and they are forced to sell their produce for a much lower cost. To solve many solutions are being proposed. This paper introduces the use of blockchain and smart contracts to tackle this problem.

In 2009, Satoshi Nakamoto released a white paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' [2]. It states a very different approach to handling money between people without any middleman. This was done by exchanging coins on a network and all the transactions were recorded in a public ledger known as a Blockchain. The entire system is based on cryptography making it secure. It consists of blocks which are linked together to form a chain, hence, the name. Each block consists of some information like a transaction [2]. For example, in a cryptocurrency, a block contains a set of transactions, the hash of the previous block which binds it to the chain, timestamp, the hash of the current block, nonce which was used to calculate the hash of the current block. Each of these transaction consists of receiver and sender details and the amount to be transferred. Based on different cryptocurrencies these details may vary.

Blockchain is seen as a game changer in handling finances, accounting, and various other fields. Many organizations have started using blockchains because of its benefits. It currently is being used by banks, financial firms, for contesting elections, cross-border direct payments, cryptocurrencies, healthcare and many other areas. Smart contracts were first introduced by Nick Szabo. A smart contract is computer protocol to formalize and secure relations over a network [5]. In a blockchain scenario, smart contracts are simple if-then rules which means if a condition is met then take some action. These rules are

 DOI : 10.18231/2454-9150.2019.0179

agreed upon by all the parties involved when the contract is drawn.

II. BLOCKCHAIN

A blockchain consists of various nodes each having the same copy of the ledger. A record once added to this ledger is permanent and is duplicated on every node. These nodes can be located anywhere around the world. This ledger is a chain of blocks. The first block in the chain does not have any transactions or the hash of the previous block and is called the 'Genesis Block' [4]. The second block consists of the first transaction to be ever recorded on the blockchain and points to the genesis block. Figure 1 explains this process. As seen the genesis block is empty as does not have the field of 'Prev. Hash'. Block #1 points at the genesis block, Block #2 points at Block #1 and so on.

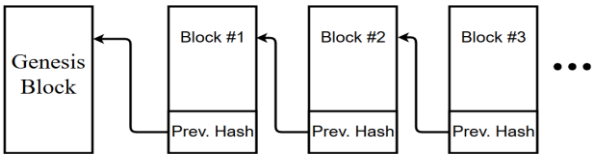

Figure 1: Architecture of a blockchain

The transactions are public which means that anyone can see what is being done. As the number of nodes increases, it becomes more and more difficult to alter the chain as the alteration has to be done on every single node connected, but it also makes it difficult to maintain a single version of the chain on all the nodes. It is possible that there can be two versions of the blockchain on the same network as seen in Figure 2. This happens when one set of nodes have a different set of blocks and other set of nodes have a different set of blocks [3]. For example, there are multiple blocks being mined in the network and the last block mined what block-19. Now node-A receives and appends block-20 after block-19 but node-B receives and appends node-21 after block-19 creating two different versions of a blockchain. This is known as a fork and block-19 is known as divergence block.

When this happens the majority rule is followed. The majority rule states that the version of blockchain which is present on the majority of the nodes is taken forward and the other versions should be discarded.

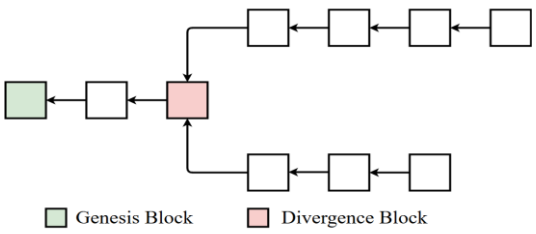

Figure 2: Blockchain Fork

Forks can also be when there is a change at the protocol level in the blockchain [3]. For example, a blockchain has a block size of four transactions, but as the network grows and the traffic increases the block size also needs to be changed. Suppose the protocol is changed and now the block contains eight transactions. An update is released and all miners are required to update the mining software, but suppose some miners are not aware of this update and are still mining on the older version, this will create lots of confusion and errors. This is known as a hard fork. A soft fork is when the mining does not create major errors and the changes are reversible [3]. So if a particular node does not adhere to the changed protocol and is still using the old protocol to mine than the blocks added by that node could be removed and the correct chain is continued.

This makes it very difficult for anyone to change the details of a transaction. If someone wishes to alter the blockchain than it has to be done on 51% of the nodes to get the majority. This becomes more and more difficult as the number of nodes grow. Hence, it is very difficult to commit frauds on a blockchain system. There are two types of blockchains:

1. Public Blockchain
2. Private Blockchain

Public blockchains are where the people are in control of the network and it is open to anyone who wants to join like a cryptocurrency. The above is the description of a public blockchain like Bitcoin, Litecoin, etc. Here many nodes spend a large amount of time, money and energy to reach a consensus. For example, Bitcoin, since it is a public blockchain trust is absent, hence the concept of 'proof-of-work' is used. Here miners who are the ones who verify and append the transactions solve complex mathematical problems to append a block. Once the problem is solved, it is announced on the network and the node is awarded specified amount of bitcoins, as the number of nodes increases the difficulty of this mathematical problems also increase and it becomes harder and harder to mine bitcoins [4]. This results in a large amount of energy and money being spent even though the time remains more or less the same.

Private Blockchains, on the other hand, are a bit different. Here a single organization or a collaboration of multiple organizations are responsible for running and maintaining the blockchain internally and only authorized people are allowed to append to the chain. If there are multiple organizations than an informal agreement is done between them as to who and how much access does one party have over the blockchain[4]. Due to this forks are unlikely to happen in a private blockchain. Also, they secured by cryptography just like in a public blockchain and does not require for everyone to reach a consensus thus saving a lot of time and energy.

 DOI : 10.18231/2454-9150.2019.0179

III. SMART CONTRACTS

When a normal contract is drawn between two or more entities, the terms and conditions are legally binding, clearly stated and agreed upon by everyone, but there is no guarantee that all the parties will follow them as stated. It is possible that one of the parties can violate these terms and conditions for their own good. A legal action taken against the violation can take days, months or even years to resolve and there is no guarantee that the party who violated the agreement will pay in full. In contrast to this, a smart contract is programmatically implemented.

According to [10], smart contract is "code that is stored, verified and executed on a blockchain." This means the code is stored on blockchain and, therefore, can't be tampered with once it is deployed. The main purpose of a smart contract is that it can contain details which can automatically do things when a certain condition is met. But its capabilities are limited to the programming language that has been used and the features of the blockchain.

One of the ways a smart contract is implemented is in Ethereum using Solidity, a programming language designed specifically for this job. After all the parties agree upon the terms and conditions they are coded in solidity. A binary file is generated after compiling this code and deployed on the Ethereum blockchain network. Once deployed, this contract is irreversible which means none of the parties involved can change or violate the agreement. For example, a person-A wants to purchase a car from person-B but is not sure if person-B can be trusted. So he draws a smart contract with rules specified and person-B agrees to it. One rule can state the date at which the contract is to be triggered, another rule can state the price of the car, another rule can contain the ownership transfer details, etc. As soon as the date of the contract arrives, the amount agreed upon is automatically deducted from person-A's account and transferred to person-B's account and the ownership is then transferred from person-B to person-A. If person-A does not sufficient funds in his/her bank account than the ownership is never transferred and the transaction never happens. Based on the terms of the contract either the contract can get canceled or an extension can be given to the buyer to gather funds and again execute the same contract at a later date. In either case, there is no chance of fraud.

From the above example, it can also be concluded that one smart contract can handle other smart contracts, it can also handle the transfer of money and digital assets. This eliminates the need for a middleman and also prevents frauds.

IV. PROCUREMENT OF GRAINS FROM FARMERS

There are two ways in which grains are procured from farmers. One way is directly by the Central Government. This is done by the Food Corporation of India (FCI). A second way is Decentralized Procurement Scheme (DCP). In DCP instead of the Central Government, grains are procured by the State Governments. In both the cases procurement centres are open where the farmer can go to sell his produce. The State Government and their agencies together decide where and when to open a procurement centre. The State Government then procures, stores and distributes the grains according to the National Food Security Act (NFSA), 2013 and Other Welfare Schemes (OWS) [6].

The State Government then conducts an annual meeting in which issues like opening of new centres, storage space for the acquired produce, arrangement of packaging, etc. are discussed in detail. The expenses incurred by the State Government are covered by the Central Government. The Central Government also monitors the quality of the grains being procured [6]. The State Government then procure the grains and distribute across the state based on demand. If excess grains are left with them then it is handed over to the Central Government. The Central Government maintains a pool where all the excess grains from all the states and union territories are gathered. Also, if a state is not able to meet its demand from the grains procured by the State Government then it requests the Central Government to send the balance from the central pool.

Many procurement centres are then set up across the country during the Rabi and Kharif seasons. The Rabi season starts from 1st October and lasts till 31st September of the next year and is known as Rabi Marketing Season (RMS). The Kharif season starts from 1st April and lasts till 31st March of the next year and is known as Kharif Marketing Season (KMS) [6].

Food grains are procured on the basis of Minimum Support Price (MSP) fixed by the government. MSP is decided based on various factors like demand and supply, cost of production, price trends in the market, inter-crop price parity, etc [7]. A farmer who wishes to sell has to go to one of these centres and sell his grains for the MSP decided by the government.

India is a vast country with millions of farmers looking to sell their grains every year. Many of these farmers are illiterate and don't know much about the system and how it works. Each procurement centre is handled by one person who is in charge of buying the grains and paying the farmers according to the MSP. Since many of the farmers in India are illiterate they are easily being misled by the people in charge of the centres.

The procurement of grains is done based on the quality of the produce. For example, paddy is procured by the government based on the moisture content in the grain. Higher the moisture, lower the price the farmer will get. The rural farmer is forced to sell his produce at a lower cost than what he is supposed to get. In the state of Haryana,

 DOI : 10.18231/2454-9150.2019.0179

farmers have to fill J-form to sell their paddy which contains all the details including the price which was given to the farmer. According to a report by Hindustan Times [8], the person in charge of the centre gives the farmer less amount than what is mentioned in the form. All of this is done by hand and on paper, so once the paper is lost everything is lost. Many people take advantage of this system. This is where technology comes in. Blockchain can be used to overcome the above problems of scamming the farmers and maintaining records.

V. BLOCKCHAIN APPROACH TO PROCUREMENT

The above sections mention three major problems in the Government system of procuring grains from farmers.

First is maintaining records. All transactions that take place are recorded in books or on paper, this is unreliable as once the paper is lost or destroyed the record is completely gone. Many people take advantage of this and destroy the paper deliberately to their advantage, and since the paper was the only record of the transaction, it can no longer be recovered. Hence, if somebody wants to get away with a scam it is very easy. Also, paper is degradable, which means that after a certain amount of time, it starts to go bad and the information is lost. Blockchain solves this problem as every transaction is stored electronically and securely over a network of nodes making it very hard to tamper with.

Secondly, many farmers are tricked to sell their produce at a low cost. As mentioned in the article by Hindustan Times [9], farmers are scammed for their grains. They are given a certain price for their crops but in the official records the price is completely different. This is solved by smart contracts where everything is fixed and cannot be changed. So if a farmer sells his crops for a certain amount, he is guaranteed to receive that money. The person handling the procurement at that centre has no benefit as the money will directly be transferred to the farmer's bank account.

Thirdly, the problem of retrieving historical records for any purpose is a cumbersome process. It requires a lot of man power to go through all the records for a particular area for a particular time period. If large number of records are to be retrieved than this would take a lot of time and also reduces the accuracy as many of the records may have gotten lost. Blockchain solves this problem, as any authorized person can retrieve records for any period or any region almost instantly.

There are a total twenty-nine states and seven union territories in India. In all, there constitute a total of 725 districts. According to Food Corporation of India (FCI), for Wheat procurement 19,280 procurement centers were operated during RMS 2018-19 & for Rice procurement, more than 45,000 procurement centers are operating in KMS 2018-19 [9]. To set up so many nodes is a very expensive and time-consuming task. Even if so many nodes are set up then adding another node incurs more cost. To solve this problem Decentralized Applications (DApps) can be used. Each district can have a primary node which is connected to all the procurement centres within that district.

A DApps is a user-friendly application directly connected to the blockchain network. A DApp provides a friendly user interface for the user to interact with and also a backend which connects to a node on the blockchain network. The front-end is created in HTML and CSS and is accessible by a browser and the back-end is coded using simple languages like JavaScript. However, more complex languages can be used to create better performing DApps. Also, if native apps are required for a smartphone than that can be done as well. There are pros and cons to native apps. Pros being that since it is a native app, compatibility issues are solved, direct access to memory is gained for faster speed, etc. The cons being that the cost of building the system goes up as separate apps are to be developed for each platform and also if there is a fork in the blockchain than, unlike the browser version which refreshes at every transaction to see if there are any changes, native apps need to be updated at each centre causing delays. And if the app is not updated and continues to add to the blockchain than it may create serious problems and errors.

Since DApps use plain HTML and CSS for front-end, the training for the people at the procurement centre is very easy. The front-end can be designed with simple textboxes, checkboxes and buttons. Labels can be provided where necessary. Also, with the growing use of smartphones, people nowadays have a fair understanding of what a front-end is and how it works just by looking at it and spending a few minutes using it. This reduces the training cost and time significantly.

Once the methodology is decided, the DApp should now be able to communicate with their respective district nodes. This is accomplished by a simple Remote Procedure Call (RPC). The DApp interacts with the node by giving an RPC as shown in Figure 3. This DApp can then be deployed to every procurement centre. A DApp only requires only an internet connection and a browser to run, so this can easily be used on a smartphone as well. To set up a blockchain network, each district in a state can have a node running which will manage all the instance of DApp within the district, then all the nodes in the state can form a blockchain network within the state. So if a new procurement centre is to open or an existing one is relocated only the DApp needs to be set up with the device that the user will use.

 DOI : 10.18231/2454-9150.2019.0179

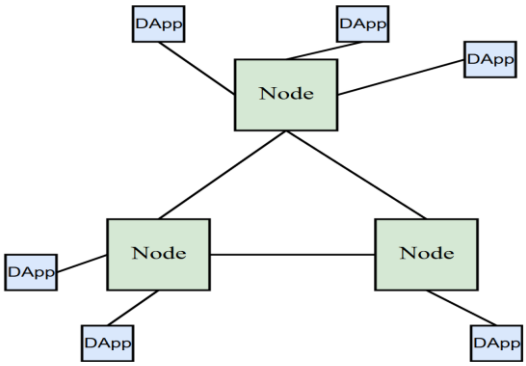

Figure 4: DApps and Nodes

Figure 4 gives a detailed explanation of the architecture of how a DApp is connected to a node. Each node here identifies a district in a state.

In order to give its better performance, there are some desirable features of a DApp [11], they are:

- Low Latency: The DApp should be able to respond within seconds after the transaction is being initiated. In our case the DApp directly communicates with its node and sends the data there. All the required processing is done at the node.\
- High Throughput: The DApp should be able to handle hundreds of users at a time. Since, during the harvest season many farmers are looking to sell their grains to the Government and hence, the Government experiences a sudden influx of crops. The DApps should be able to handle this throughput.
- Fast Sequential Performance: The DApp should be able to process sequential operations at high speed. The sequence of operations can be retrieving farmer details, entry of the purchase, etc. The DApp should be able to handle all the sequential steps while maintaining performance.

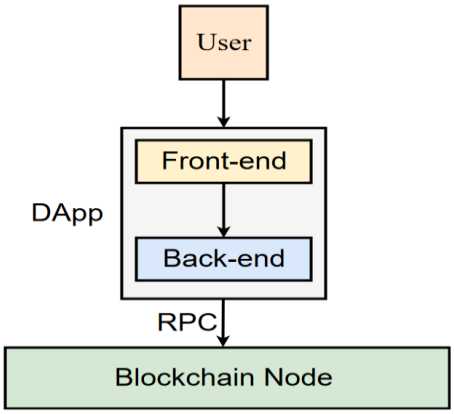

Figure 3: Working of a DApp

The following steps show how blockchain can be integrated into the current system:

1. A Decentralized Application (DApp) can be created with which the user will interact. Each centre will have this DApp installed.
2. A farmer wishing to sell his grains will then go to the centre and provide his/her aadhar card number.
3. The person will then check the quality of the grains.
4. According to the quality the relevant MSP will be selected from the user interface provided by the DApp.
5. The farmer verifies these details and proceeds with the transaction if he/she sees that everything is correct.
6. Money is directly transferred to the farmer's bank account that is linked with his/her aadhar card.
7. A batch number is generated for the grain just purchased by the procurement center.
8. Transaction completed and sent to the node to append to the chain.

Since most of the farmers have an aadhar card and bank account with them, the current system can easily integrate with the provided infrastructure. Also due to the boom in the internet sector, with the internet being available at affordable prices and the availability of affordable smartphones in India, more and more people are getting connected. Hence, the major two requirements are met to set up the system in rural areas as well.

There are various advantages to this system. Firstly, the person in charge of the procurement centre cannot embezzle any money as the entire process is online and the Government directly send money to every farmer's bank accounts. The farmers get the worth of their produce. Secondly, the network can be scaled or existing procurement centre can be easily relocated with minimum resources. Also relocation and setting up a new centre requires minimum amount of time. Thirdly, the government can get details of any transaction that took place at any time almost instantly. This speeds up report generation which can be used to further improve the process. Since, accurate data is present, the Government can create its financial records accordingly and reporting to the public about the current status of procurement becomes more trustworthy and reliable.

Another main advantage is traceability. The grains purchased by the Government of one state are then further distributed to other states or are given to the central pool. Hence, it becomes very important to know where a particular batch of produce came from. This can be done by tracing the batch number that was created while purchasing the grains.

This ensures food safety and food security. For example, if there are reports of a certain area population being affected by a food-related illness then the records can be obtained from the blockchain which will give the batch number of

 DOI : 10.18231/2454-9150.2019.0179

the grains that were dispatched in that regions. This batch number can then be traced back to the particular procurement centre and even to the particular farmer from where the grains came from and see what went wrong. The reports can be analyzed as to what is causing the problem. This process can be completed within 2-3 days. A pattern can then be created to see whether the problem originated from a single source or not. Proper actions can then be taken to avoid such a problem in the future. It also helps the government to keep track of how much grain was procured and from where, directly from the blockchain network and does not have to rely on the individual centres to report their purchases.

Each district within a state will have a separate node. Each procurement centre will have a DApp installed which will be connected to a node present in that district. All of these nodes together will form a private blockchain. The district node can be placed at a fixed location whereas the DApp is fairly easy to deploy at a new or existing centre.

VI. Conclusion And Future Work

Each year thousands of metric tons of grains are procured from farmers all over the country. This paper has presented an overview of how blockchain can be used to help streamline the procurement process. This study was also done to determine whether smart contracts are efficient than the current system and how it can be implemented. The Government of India should now decide whether and when blockchain can be integrated into the current system. A cost/benefit analysis should be prepared as there may be some aspects that were not covered in this paper and if blockchain is suitable for those aspects.

This paper also highlights how blockchain can be used to reduce frauds and scam that happen with innocent farmers, maintain records permanently without the risk of losing them again, get accurate details of the transactions that take place every day, retrieve records instantly, provide traceability for the grains procured, increase food safety and security and also ensure that farmers get what they are promised. This paper also highlights how authority from the middleman, i.e., the man at the procurement centre can be reduced and the process is automated.

The future work can be to scale this application from the state level to the national level where the states and union territories altogether form and national level blockchain. Also, the application of HyperLedger and Ethereum can be studied instead of building an entire blockchain from scratch.

References

[1] Krisih Annual Report, Department of Agriculture, Cooperation & Farmers Welfare, Ministry of Agriculture & Farmers Welfare, Government of India, 2017-2018.

http://agricoop.nic.in/sites/default/files/Krishi%20AR%202017-18-1%20for%20web.pdf

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

https://bitcoin.org/bitcoin.pdf

[3] Andrew LR, Douglas AO, Bitcoin Investigations: Evolving Methodologies and Case Studies, Journal of Forensic Research, 2018.

https://www.omicsonline.org/open-access/bitcoin-investigations-evolving-methodologies-and-case-studies-2157-7145-1000420.pdf

[4]Deloitte, “What Is Blockchain?”, 2016 https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf

[5] N. Szabo, Formalizing and Securing Relationships on Public Networks, FirstMonday, vol. 2, no. 9, Sept. 1997.

https://firstmonday.org/ojs/index.php/fm/article/view/548/469

[6] Annual Report 2017-2018, Department of Food & Public Distribution, Ministry of Consumer Affairs, Food & Public Distribution, Government of India.

https://dfpd.gov.in/LwB3AHIAaQB0AGUAcgBlAGEAZABkAGEAdABhAC8AUABvAHIAdABhAGwALwBNAGEAZwBhAHoAaQBuAGUALwBEAG8AYwB1AG0AZQBuAHQALwA=1_141_1_annualreportenglish.pdf

[7] Determinants of MSP, Commission for Agricultural Costs & Prices, Ministry of Agriculture & Farmers Welfare, Government of India.

http://cacp.dacnet.nic.in/content.aspx?pid=62

[8] Haryana farmers allege scam in procurement, say paddy being bought below MSP, Hindustan Times.

https://www.hindustantimes.com/india-news/haryana-farmers-allege-scam-in-procurement-say-paddy-being-bought-below-msp/story-HeZGCGwSyGZj7HAQjeoalO.html

[9] Procurement, Food Corporation of India,

http://fci.gov.in/procurements.php

[10] J. Stark, Making Sense of Blockchain Smart Contracts.

https://www.coindesk.com/making-sense-smart-contracts

[11] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," in IEEE Access, vol. 6, pp. 53019-53033, 2018.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8466786&isnumber=8274985

 DOI : 10.18231/2454-9150.2019.0179