



Designing Yield Estimation Mechanism Using Blockchain Technology

Tuncay DOĞANTUNA
Coordination Unit for Information
Systems
TKDK (ARDSI)
Ankara, Turkey

Abidin Ayberk CERAN
Department of Computer Engineering
Ankara University
Ankara, Turkey
ceran@ankara.edu.tr

Dr. Bülent TUĞRUL
Department of Computer Engineering
Ankara University
Ankara, Turkey
btugrul@eng.ankara.edu.tr

Salih DEMİR
Distance Education Center
Ankara University
Ankara, Turkey

Dr. Murat OSMANOĞLU
Department of Computer Engineering
Ankara University
Ankara, Turkey
mosmanoglu@ankara.edu.tr

Dr. Gazi Erkan BOSTANCI
Department of Computer Engineering
Ankara University
Ankara, Turkey
ebostanci@ankara.edu.tr

Abstract— Price fluctuation of agricultural products is a complicated problem influenced by many factors that can be harmful for the players of the market. One of the most important factors is uncertainty in yield estimation of the products. It is a fact that accurate yield estimation is crucial for planning and evaluating the agricultural investment. Generally, the existing yield estimation systems are designed in centralized setting. However, effective tracking may not be possible due to problems in the data flow. Recently, data can be stored in a decentralized and distributed architecture using the blockchain technology that provides a censorship-resistant, tamper-proof, and strongly immutable database. In this study, we will propose a blockchain based solution to determine the yield of agricultural products. Our solution can be considered as a platform that enables the producers to share their farming plan with the other players, and makes them to review their investments for the oncoming season.

Keywords — yield estimation; blockchain; agriculture

I. INTRODUCTION

Agricultural production can be examined under two headings as vegetable and animal production. The vegetable production consists mainly of field crops, grains, legumes, seeds and organic fruits and vegetables. Accurate estimation of vegetable production is important for both producers (farmers and investors) and consumers (human, governments and the food industry). The yield here can be defined as the amount of product produced during a production period.

Today, the predictability of the outputs of agricultural production has become increasingly important. Product prices are determined according to free market conditions. Therefore, overvaluation of the product price or selling below the actual value can be observed in many countries, including Turkey.

As a result, problems such as hunger, food price inflation and the black market may arise. Production based on data and analysis in agriculture is increasing as a result of widespread use of precision agriculture-based technologies. TARBIL, which is built on public, academia and private sector cooperation, is able to provide reports thanks to real-time observation data [1]. Through the data collected over the years, it is able to estimate the yield using machine-learning methods [2].

Precision agricultural technologies are based on communication technologies such as, satellite communication, GPS, GIS, remote sensing and supports monitoring product forecast processes [3]. In recent years, the technology has also started to be developed on the blockchain, which can produce solutions for agricultural problems other than fintech and cryptocurrency. In addition, there are also academic studies, which emphasize the future impacts of the blockchain on the agriculture and food sectors. Food and Agriculture Organization (FAO), which belongs to United Nations (UN), has highlighted the current trends in agricultural applications that can be developed with blockchain [4].

Several applications based on blockchain are available to the public. Ripe.io, which presents the origin information about the products, aims to prevent food fraud [5]. AgriLedger aims to open new markets to farmers in the developing world by using blockchain [5]. It proposes to create trust and accountability among market players. It is desired to establish mutual trust in the market without the need of any trusted broker. As seen from two applications, Projects that will enable the producer to deliver its own product directly to the consumer or food industry companies without the need for any

intermediary broker are taking interests. However, there is no decentralized and distributed blockchain application that brings producer and consumer communities together with a secure consensus mechanism on product monitoring and forecasting.

In this paper, we propose a decentralized and distributed solution to meet the needs of all parties. Our proposed solution is a platform in which the farmers share their farming plan for the oncoming harvest season. Thereby, the other parties in the platform can review their plans and make the investments accordingly. We utilize the blockchain technology to design our platform that provides a censorship-resistant, tamper-proof, and strongly immutable public ledger of time-stamped transactions. Thus, our platform establishes the optimal consensus among the producers and the other related players.

II. DEFINITIONS

In this section, we give the definitions of some structures that will be used to construct our protocol.

A. Hash Functions

Hash function is a mathematical tool that compresses an input of arbitrary length to a short fixed length string. The output of a hash function on an input message is mostly called message digest. A hash function is called collision-resistant if it is computationally infeasible to find two different inputs of any length that have same digest.

B. Digital Signature Schemes

Digital Signature is an authentication mechanism that verifies to the receiver the origin of the message which is actually received from the user. There is a pair of keys in digital signature system, that are called a secret key and a public key. A user creates a signature on a message using his secret key. Anyone who has the user's public key can easily verify that the signature was generated by the user. Similar to hand-written signatures, digital signatures present two properties; authenticity (a signature convinces a verifier that it was indeed generated by the owner of the public key) and integrity (the signature wasn't modified during transition). A digital signature scheme is called unforgeable if no one can create a valid signature without the secret key.

C. Distributed Ledgers

Distributed ledger is a database shared through a network of multiple sites, corporation or region. In the corresponding network, all shareholders have privilege to take a copy of the ledger on its own. All copies of the ledger are periodically updated when any alteration is occurred. The security and accuracy of the assets stored in the ledger are maintained through the cryptographic tools such as cryptographic hash functions and digital signature schemes. Entries of the ledger can also be updated by one, some or all of the participants, according to rules agreed by the network. A robust distributed ledger has two properties: safety and liveness. The former one

ensures that all non-faulty players in the network agree on a total order for the transactions recorded in the ledger, and the latter one ensures that an honestly generated transaction is eventually accepted by all non-faulty players.

D. Blockchains

Blockchain is an efficient mechanism that enables the realization of a distributed ledger. It can be considered as a set of blocks which contains an ordered records of transactions. Every block is pointed by the next block with a reference which is a hash value of the block called parent block. There is a special block, named as Genesis block, which is the first block of blockchain. Transaction counter and transactions constitute the body of the block. Note that the number of transactions in a block and the size of each transaction determine the maximum number of transactions that can be placed in a block.

E. Smart Contracts

Smart contracts are computer programs that autonomously execute the terms of a contract. They are triggered by addressing a transaction to them. Then, they are executed independently and automatically in a prescribed manner on every node in the network, according to the data that were included in the triggering transaction.

III. CONSTRUCTION

In this section, we explain our protocol that enables the producers to share their farming plan with the other players of the market, and makes them to have positions based on the information the producers share for the oncoming harvest season. In other words, the platform establishes the optimal consensus among the producers and the other related players.

A. Entities in Our Protocol

There will be three entities that are involved in our protocol as shown in figure below:

- **Farmers:** are the natural players or the legal entities who own a farmed land and raise field crops corresponding to the region of the land. Farmers periodically declare a yield commitment for crops that can be raised in their lands. Note that farmers have to get a certificate from the agricultural authority of their region in order to register the platform and to declare a yield commitment.
- **Auditors:** are the ones that verify the commitments of the farmers. They are randomly chosen among farmers depending on the proximity of region. Regarding to the observation, they rate the farmers' commitments.

- **Administrators:** are the officers that represent the agriculture authorities of different regions. They are responsible for providing certificates to the farmers and maintaining the platform. Besides, they have the ability to deploy and validate smart contracts.

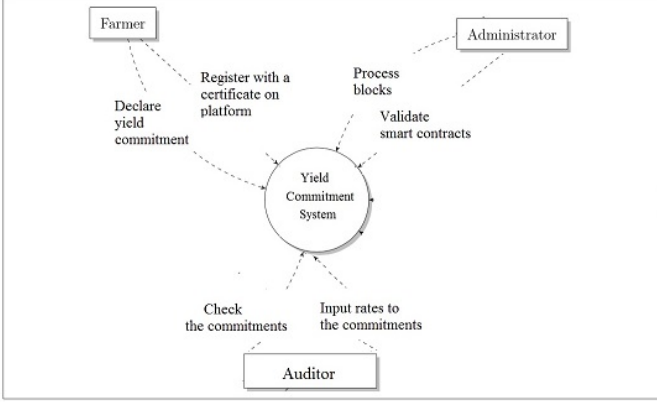


Fig. 1. Entities and their roles on yield commitment platform

B. Design of The Protocol

First, a farmer gets a certificate from the agriculture authority of his region. This certificate proves that the farmer owns the farmed land he claims in the corresponding region. The farmer then provides this certificate to the platform as a request for the registration. After the validation of the certificate, the platform leads the farmer to create a yield commitment about his land. This commitment will be a declaration that determines the farmer's intention, i.e. 'X crop will be planted in Y amount of the land for the coming season'.

In the platform, the farmer initiates a smart contract to declare a commitment. He also attaches the signature of his commitment to the contract to ensure the authenticity of the data. The smart contract randomly assigns a farmer to the commitment as the auditor. When the specified period of time passes, the contract triggers the auditor to input a rate value $p \in [0,1]$ based on his observation regarding the farmer's commitment. The rate value here is determined depending on what percentage of the commitment is fulfilled. Finally, the administrators validate the smart contract according to the inputs provided by the farmer and the auditor.

Recall that permissionless blockchain allows anyone to participate in the network and to create blocks. On the other hand, in a permissioned blockchain, only an authorized set of entities is allowed to create blocks and to maintain the ledger. Permissioned blockchains possess a lot of advantages over permissionless blockchain due to its ability to allow the use of parallel computing and better scaling. Since the entities are appeared with their original identities in our system, permissioned blockchain protocols [6,7,8] will be sufficient to effectively build our platform.

In our case, the agricultural authorities from different regions (administrators) will be responsible to create the blocks and to maintain the ledger. The authorities run the Byzantine consensus algorithm PBFT [9] that enables them to agree on a total order for the execution of the smart contracts in presence of failures of some authorities. PBFT [9] provides both safety and liveness as explained in Section 2, at most $\lfloor \frac{n-1}{3} \rfloor$ faulties out of a total of n authorities.

Note that the authorities are identified with their public keys, and need to be specified at the genesis block. However, the authorities may accept a new administrator as the agricultural authority of a new agricultural division.

C. Reputation

It is a fact that farmers may declare an incorrect commitment, or may not fulfill the commitment they have declared in order to maximize their profit. However, this act ruins the market, and causes the other players, which have made investments based on the commitments, to loose their investments. To avoid such cases, we introduce a key concept, 'reputation', that forces the farmers to stick to their commitments.

Reputation is a real value from $[0,1]$ that is assigned to each farmer at the registration process, and is renewed at each commitment based on the performance of the farmer. For instance, a simple process to renew the reputation can be designed as follows: let $rep \in [0,1]$ be a reputation value of a farmer and $p \in [0,1]$ be the rate value of the last commitment of the farmer given by the auditor assigned to the commitment. Then the new reputation value can be computed as

$$(rep + p)/2 \quad (1)$$

Note that in our platform farmers are expected to declare commitments periodically. Reputation can also be used to enforce that, i.e. if a farmer does not declare a commitment, his reputation value may be decreased. Besides, to ensure the farmers to behave honestly, the authorities may establish a specific rule such that if the reputation value of a farmer is less than a determined threshold value for more than a number of blocks, then the farmer will be expelled from the system. Thus, adding this concept to the system preserves the continuity and correctness of market.

IV. SECURITY ANALYSIS

In this section, we discuss the security issues related to the protocol we proposed. As we stated before, the farmers attach a signature of the commitment when they initiate a smart contract for it. The unforgeability of the signature scheme ensures that a farmer cannot create a commitment on behalf of another farmer, and no entity in the system can change the content of the commitment after it is deployed to the system.

On the other hand, the authorities add a new valid block to the chain by embedding the hash of the previously created block

to the new one. Due to the collision resistant property of the underlying hash function, it is computationally infeasible to change the content of the block. Moreover, since every entity has a copy of the ledger and the authorities communicate with each other, the replacement of one block in the ledger with another one can easily be detected.

Besides these facts, a malicious farmer may still try to replace a commitment placed in the ledger with the another one, or to remove a deployed commitment from the ledger by creating an alternate chain. As we explained in Section 3, our system tolerates at most $\left\lfloor \frac{n-1}{3} \right\rfloor$ faulty authorities where n is the total number of authorities. Thanks to the safety property of the consensus algorithm, a malicious entity cannot create an alternate chain if he controls less than $\left\lfloor \frac{n-1}{3} \right\rfloor$ authorities.

REFERENCES

- [1] ÇEKER, Ali. "SÜRDÜRÜLEBİLİR TARIM VE TÜRKİYE AÇISINDAN BİR DEĞERLENDİRME." *Electronic Turkish Studies* 11.2, 2016, p.3-8
- [2] Kogan, Felix, et al. "Winter wheat yield forecasting in Ukraine based on Earth observation, meteorological data and biophysical models." *International Journal of Applied Earth Observation and Geoinformation* 23, 2013, pp.192-203.
- [3] Fernandez-Ordoñez, Yolanda M., and Jesus Soria-Ruiz. "Maize crop yield estimation with remote sensing and empirical models." *2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*. IEEE, 2017.
- [4] Tripoli, M. & Schmidhuber, J. 2018. *Emerging Opportunities for the Application of Blockchain in the Agri-food Industry*. FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA 3.0 IGO
- [5] Kamilaris, A., Fonts, A., & Prenafeta-Boldó, F. X. The Rise of the Blockchain Technology in Agriculture and Food Supply Chain
- [6] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. Vol. 310. 2016.
- [7] Vukolić, M. (2017, April). Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 3-7). ACM
- [8] Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017, September). Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric). In *Reliable Distributed Systems (SRDS), 2017 IEEE 36th Symposium on* (pp. 253-255). IEEE.
- [9] Castro, M. and Liskov, B. Practical Byzantine Fault Tolerance. *Proc. Usenix OSDI*, Berkeley, California. 1999