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 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. DEFINITONS

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 occured. 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 schemeus. 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.