- **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.

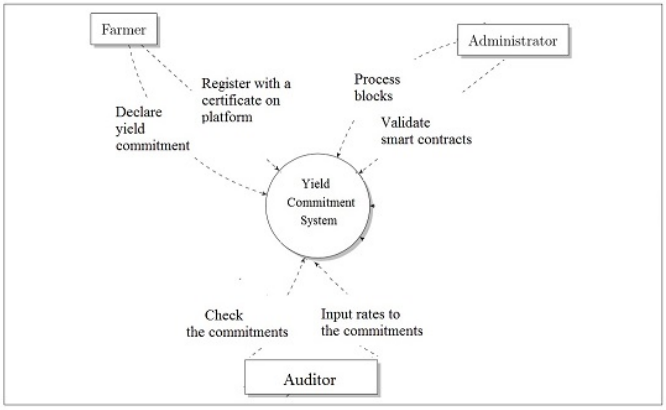

Fig. 1. Entities and their roles on yield commitment platform

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 $\left\lfloor \frac{n-1}{3} \right\rfloor$ 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