Designing Yield Estimation Mechanism Using Blockchain Technology

Yield Estimation

Crop Yield (récolte), the amount of agricultural production harvested per unite of land area

the total amount of harvested crop at the end of the season

Yield Estimation

Crop Yield (récolte), the amount of agricultural production harvested per unite of land area

the total amount of harvested crop at the end of the season

TCMB, Inflation Report 2018

"Driven by fresh vegetable products, the unprocessed food group stood out as the highest contributor to consumer inflation in the first half of 2018"

"The conjunctural reasons underlying the price hikes in unprocessed food products are evaluated from the perspective of structural problems"

"the inability to make an efficient and dynamic agricultural production plan is considered to be a significant structural problem. Developing a production plan requires strengthening of agricultural statistics, yield estimation and early warning system infrastructure."

"Establishing a systematic structure to facilitate a dynamic follow-up and estimation of agricultural yields will also contribute to the timely adoption of measures required to maintain sustainability of supply and price stability"

Yield Estimation

- Most countries use traditional techniques for crop monitoring and yield estimation, ground-based visit and reports.

  subjective, very costly and time consuming

Yield Estimation

- Most countries use traditional techniques for crop monitoring and yield estimation, ground-based visit and reports.

  subjective, very costly and time consuming

- Remote sensing which provides time series data and a synoptic view of the landscape

Yield Estimation

- Most countries use traditional techniques for crop monitoring and yield estimation, ground-based visit and reports.

  subjective, very costly and time consuming

- Remote sensing which provides time series data and a synoptic view of the landscape

  it can be used to warn the decision makers about potential reduction in crop yields and allow timely import and export decision

Yield Estimation

- Most countries use traditional techniques for crop monitoring and yield estimation, ground-based visit and reports.

  subjective, very costly and time consuming

- Remote sensing which provides time series data and a synoptic view of the landscape

  it can be used to warn the decision makers about potential reduction in crop yields and allow timely import and export decision

  it can be used to take action during the growing season

Yield Estimation

Years	Cultivation Area (decare)	Production (ton)
2017	80.000	523.000
2018*	60.000	150.000

Onion Production in Polatli

Yield Estimation

Years	Cultivation Area (decare)	Production (ton)
2017	80.000	523.000
2018*	60.000	150.000

Onion Production in Polatli

- Marmarabirlik applies a specific rule: the members of the union have to declare a yield commitment before the upcoming season.

  If a farmer has not declared a commitment, the union does not take his products

Yield Estimation

Years	Cultivation Area (decare)	Production (ton)
2017	80.000	523.000
2018*	60.000	150.000

Onion Production in Polatli

- Marmarabirlik applies a specific rule: the members of the union have to declare a yield commitment before the upcoming season.

  If a farmer has not declared a commitment, the union does not take his products

- 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.

Problem Formulation

There are four roles:

Problem Formulation

There are four roles:

producer (F), periodically declare yield commitments

‘I, the producer F, will plant the crop X in Y amount of the land L’

Problem Formulation

There are four roles:

producer (F), periodically declare yield commitments

‘I, the producer F, will plant the crop X in Y amount of the land L’

auditor (O), makes an observation for the commitment he was assigned and reports a rate based on his observation

Problem Formulation

There are four roles:

producer (F), periodically declare yield commitments
'I, the producer F, will plant the crop X in Y amount of the land L'

auditor (O), makes an observation for the commitment he was assigned and reports a rate based on his observation

platform, a medium that enables producers to announce their commitments and auditors to report their observations

Problem Formulation

There are four roles:

producer (F), periodically declare yield commitments
'I, the producer F, will plant the crop X in Y amount of the land L'

auditor (O), makes an observation for the commitment he was assigned and reports a rate based on his observation

platform, a medium that enables producers to announce their commitments and auditors to report their observations

registration authority (RA), manages the registration process of farmers and auditors by assigning each entity a unique credential if he satisfies the conditions.

Problem Formulation

- the platform is either maintained by a central authority or a network of players (administrators)

Problem Formulation

- the platform is either maintained by a central authority or a network of players (administrators)
- well established identities required for an effective yield commitment system
    - a malicious player may create multiple identities, may control a large fraction of the system
    - he may use this power to manipulate the market players, or even to mount a Sybil attack

Problem Formulation

- the platform is either maintained by a central authority or a network of players (administrators)
- well established identities required for an effective yield commitment system
  - a malicious player may create multiple identities, may control a large fraction of the system
  - he may use this power to manipulate the market players, or even to mount a Sybil attack
- we build the system on top of a permission blockchain network

Problem Formulation

Security Discussion

- A malicious producer may

Problem Formulation

Security Discussion

- A malicious producer may
  - declare a yield commitment of the rate different than he has planned
  - change his plan after announcing his commitment according to the others' sharing
  - prefer not to declare a commitment
  - try to change the existing commitments in the database that show him dishonest

Problem Formulation

Security Discussion

- A malicious auditor may

Problem Formulation

Security Discussion

- A malicious auditor may
  - report a rate without visiting the farmland he was assigned
  - report a 'wrong rate'
  - prefer not to provide a report

Problem Formulation

Security Discussion

- A malicious auditor may
  - report a rate without visiting the farmland he was assigned
  - report a ‘wrong rate’
  - prefer not to provide a report
- A malicious farmer may corrupt the auditor assigned to his commitment

Problem Formulation

Security Discussion

- A malicious administrator may

Problem Formulation

Security Discussion

- A malicious administrator may
  - record yield commitments or reports to the database different than the actual one
  - ignore the commitments of a particular producer, or the reports related to him
  - prefer not to do his work
  - try to change the existing commitments in the database that show him dishonest

Problem Formulation

Security Discussion

- A malicious administrator may
  - record yield commitments or reports to the database different than the actual one
  - ignore the commitments of a particular producer, or the reports related to him
  - prefer not to do his work
  - try to change the existing commitments in the database that show him dishonest
- A malicious farmer may corrupt the auditor assigned to his commitment

Problem Formulation

Challenges

Problem Formulation

Challenges

(1) Designing an efficient mechanism to enforce the auditors to report the 'correct rate'

Problem Formulation

Challenges

(1) Designing an efficient mechanism to enforce the auditors to report the 'correct rate'

- smart contracts and 'oracle problem'

Problem Formulation

Challenges

(1) Designing an efficient mechanism to enforce the auditors to report the ‘correct rate’

- smart contracts and ‘oracle problem’

  ‘the ideal oracle is hard to achieve’

Problem Formulation

Challenges

(1) Designing an efficient mechanism to enforce the auditors to report the ‘correct rate’

- smart contracts and ‘oracle problem’

  ‘the ideal oracle is hard to achieve’

(2) Designing an efficient mechanism to enforce the producers to stick to their commitments without discouraging them to declare commitments, or even to register in the system

Preliminaries

Distributed Ledger

- a database shared through a network of players
- all copies of the ledger are periodically updated when any alteration is occurred

Preliminaries

Distributed Ledger

- a database shared through a network of players
- all copies of the ledger are periodically updated when any alteration is occurred
- A robust distributed ledger has two properties :
  - safety, all non-faulty players in the network agree on a total order for the transactions recorded in the ledger
  - liveness, an honestly generated transaction is eventually accepted by all non-faulty players

Preliminaries

Blockchain

- an efficient mechanism that enables us to realize a robust distributed ledger
- considered as a set of blocks that contains an ordered records of transactions

  (each block is pointed by the next block with a reference that is a hash value of the block called parent block)

Preliminaries

Blockchain

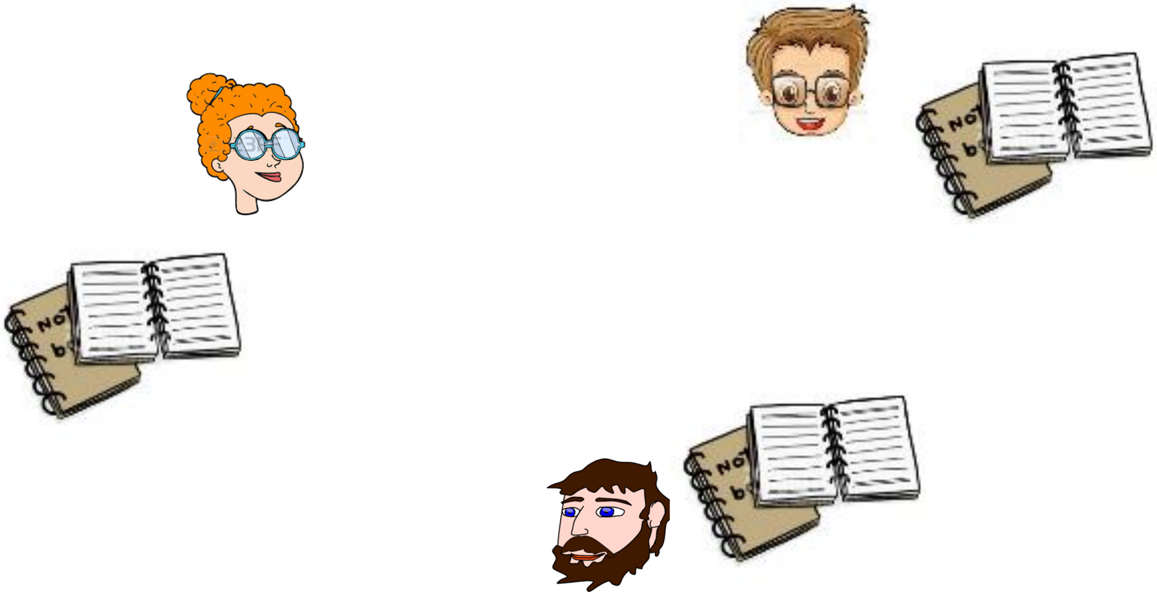
- an efficient mechanism that enables us to realize a robust distributed ledger
- considered as a set of blocks that contains an ordered records of transactions

  (each block is pointed by the next block with a reference that is a hash value of the block called parent block)

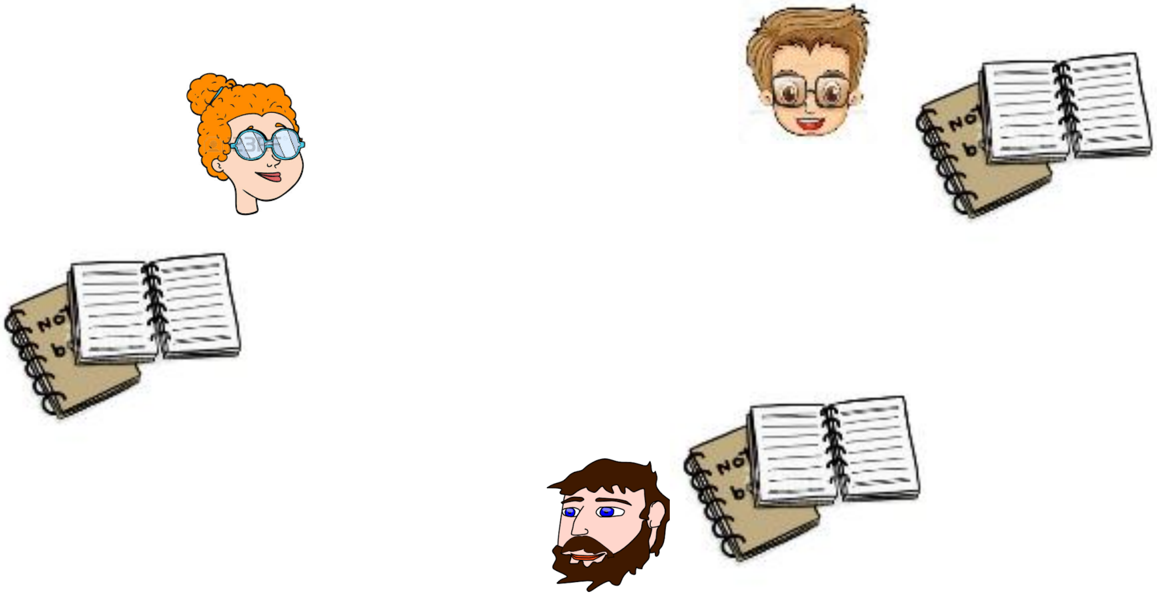
Smart Contracts

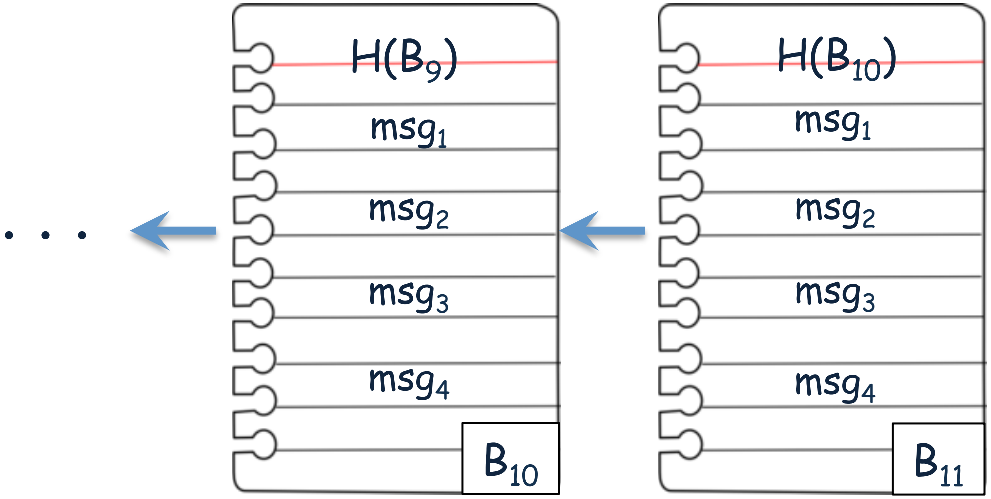
- q piece of codes that autonomously execute the terms of a contract
- they are triggered by addressing a transaction to them
- they are executed independently and automatically in a prescribed manner on every node in the network

Preliminaries



Preliminaries





. . .

$H(B_9)$

msg_1

msg_2

msg_3

msg_4

B_{10}

$H(B_{10})$

msg_1

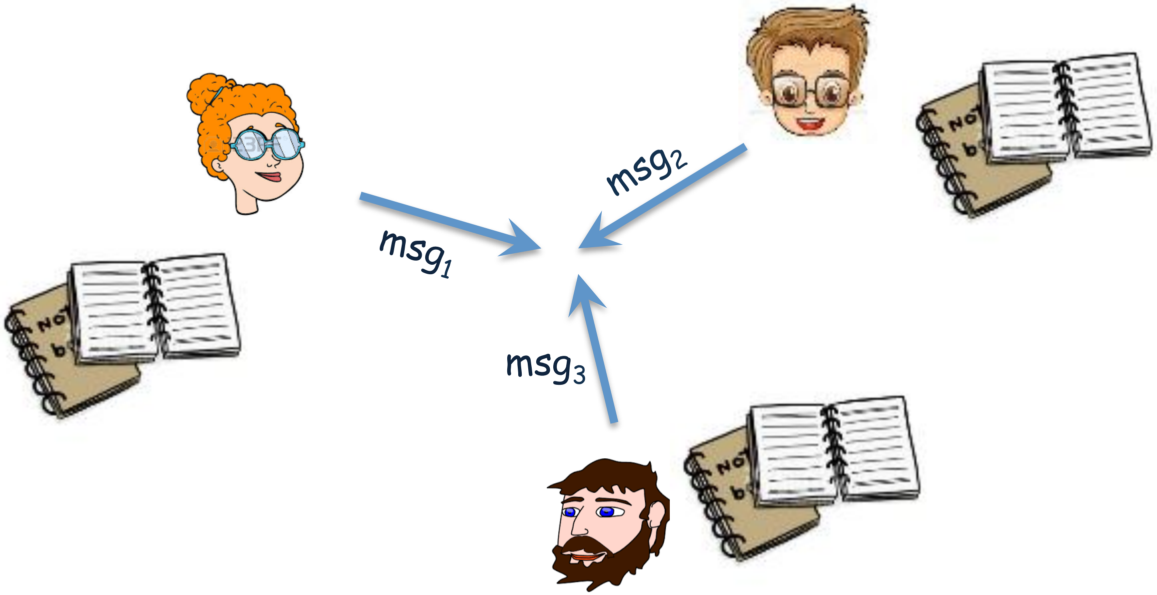
msg_2

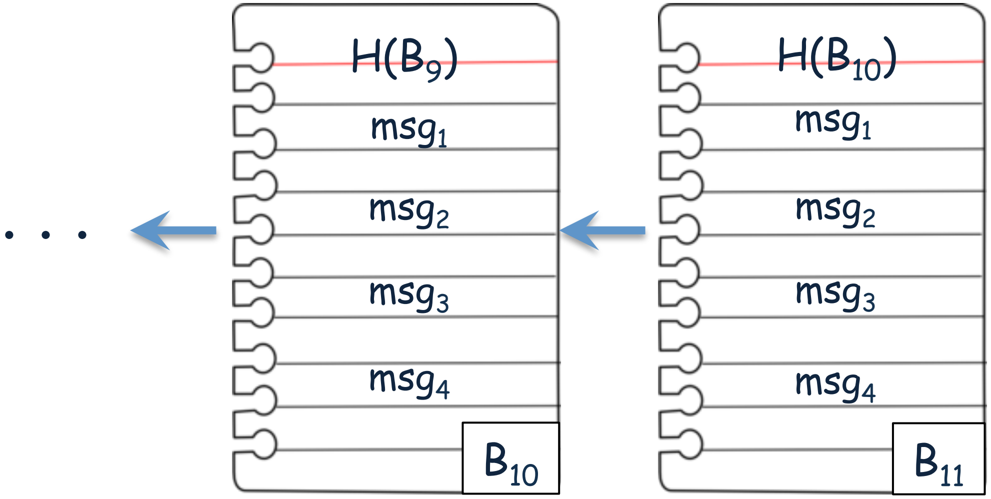
msg_3

msg_4

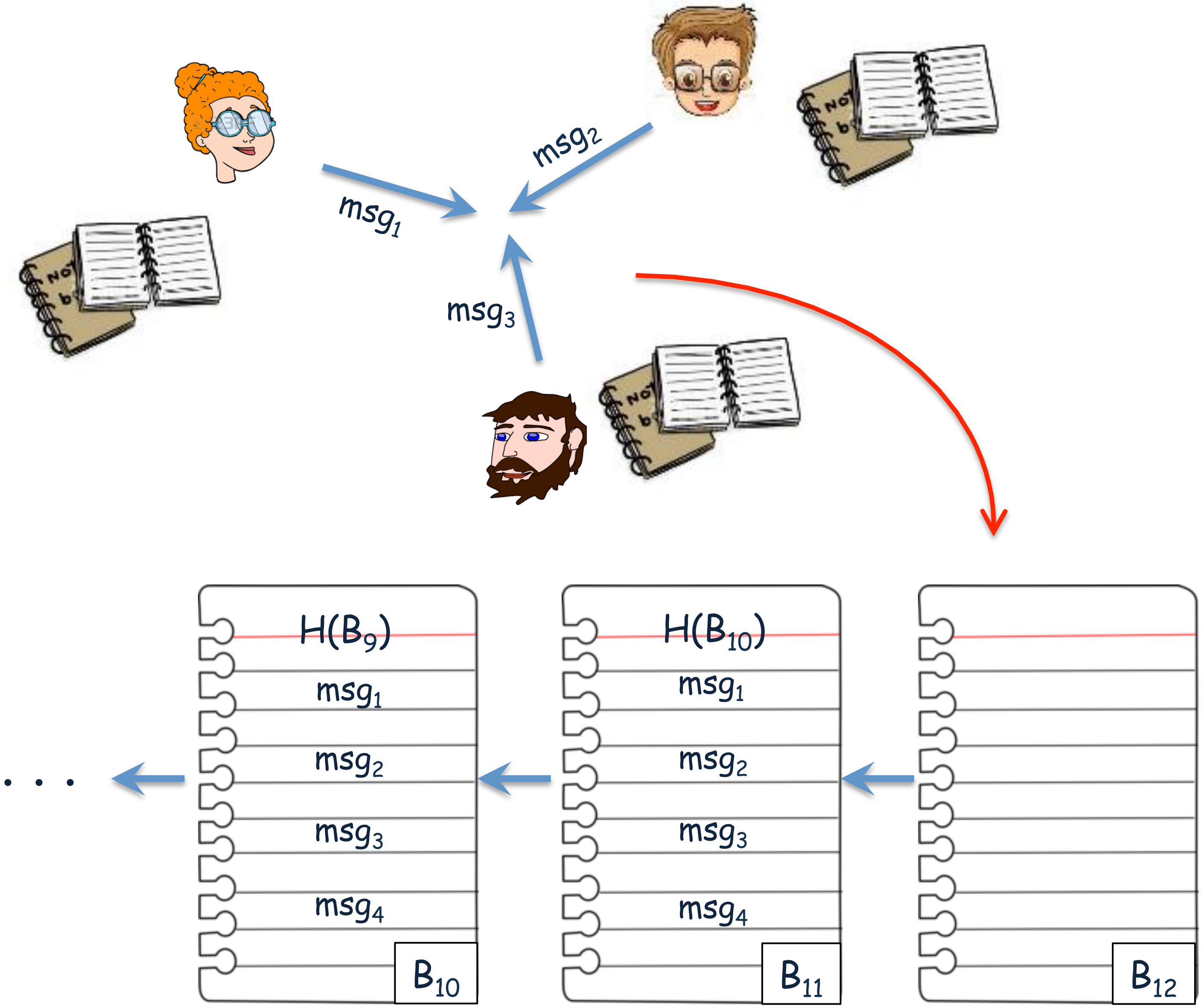
B_{11}

Preliminaries





Preliminaries



msg_1

msg_2

msg_3

. . .

$H(B_9)$

msg_1

msg_2

msg_3

msg_4

B_{10}

$H(B_{10})$

msg_1

msg_2

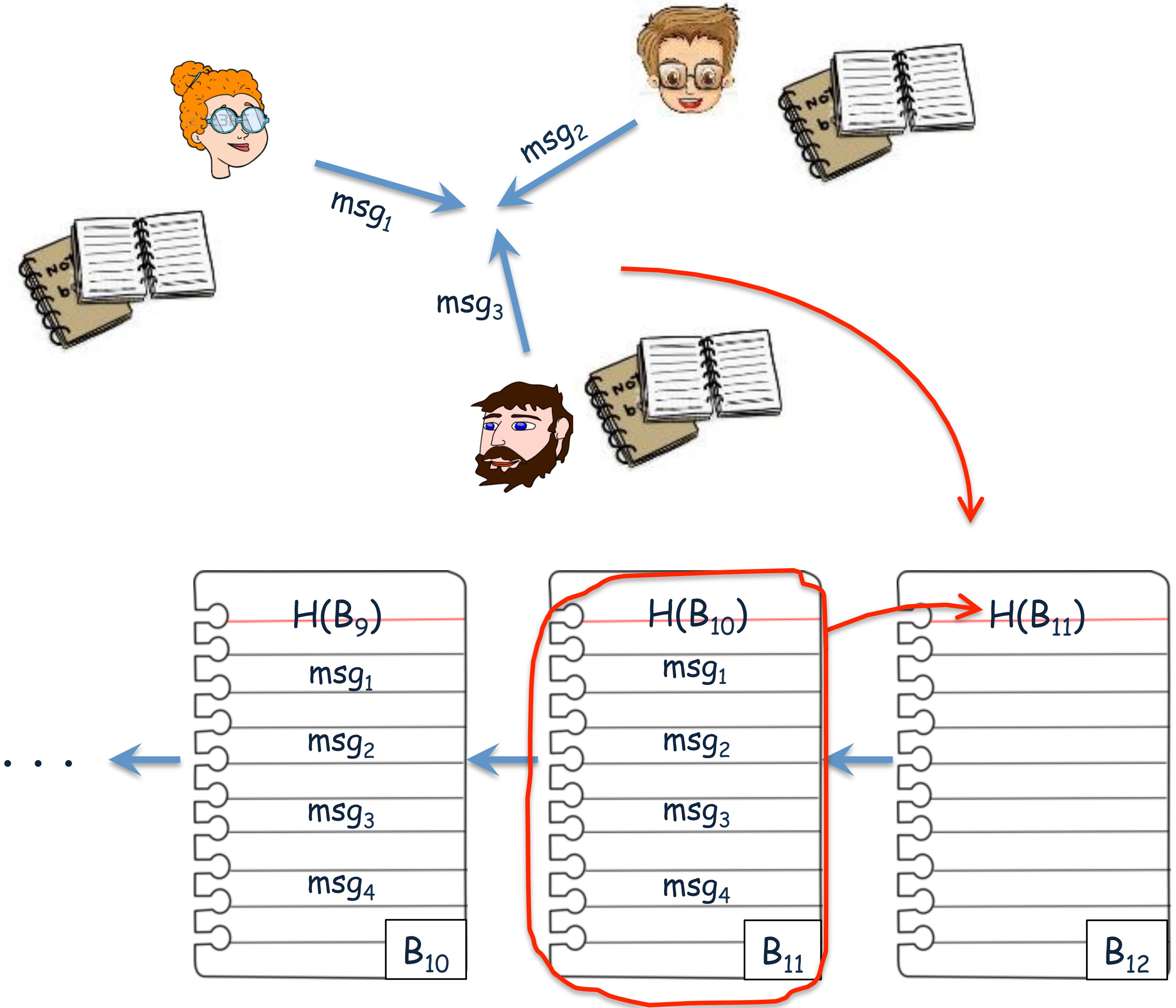
msg_3

msg_4

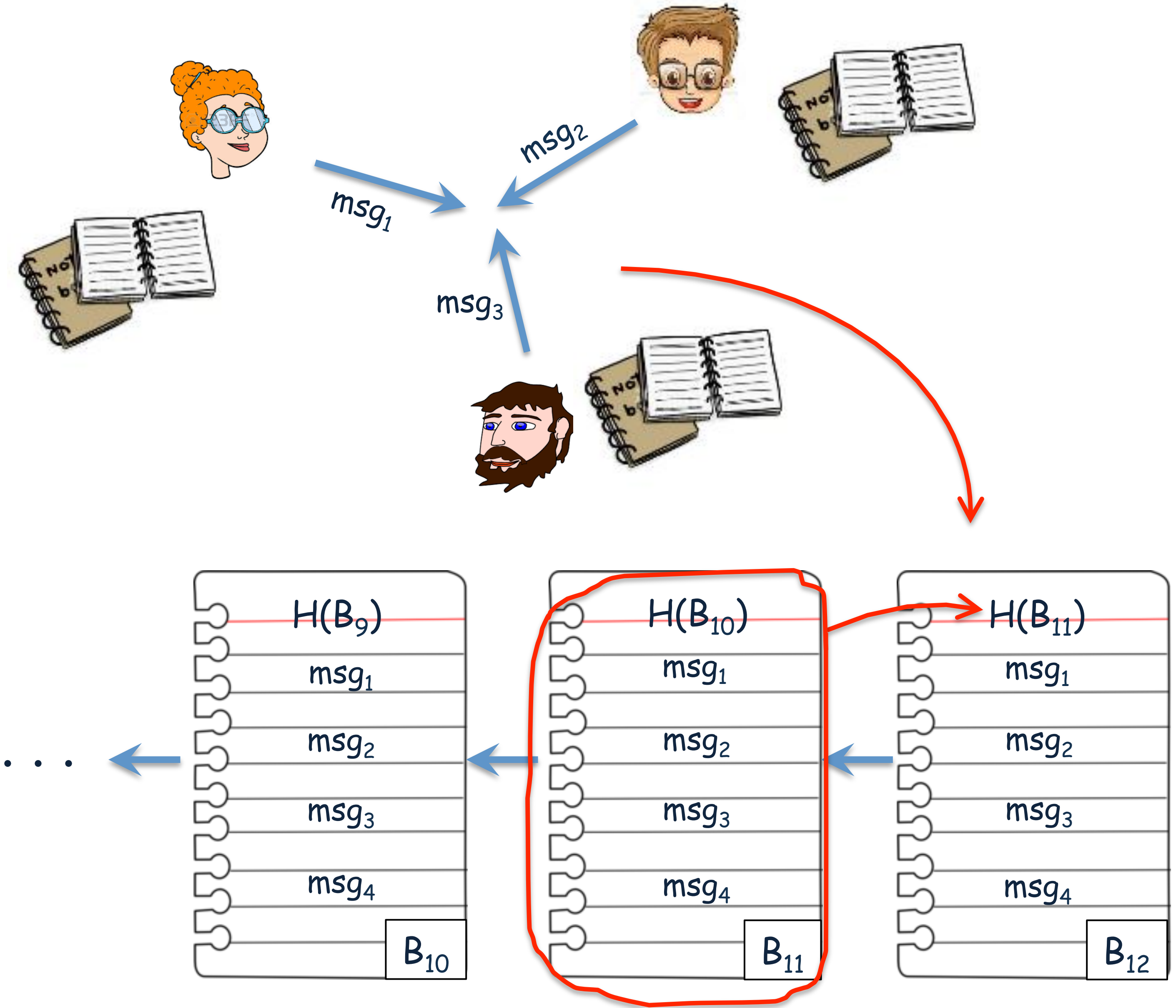
B_{11}

B_{12}

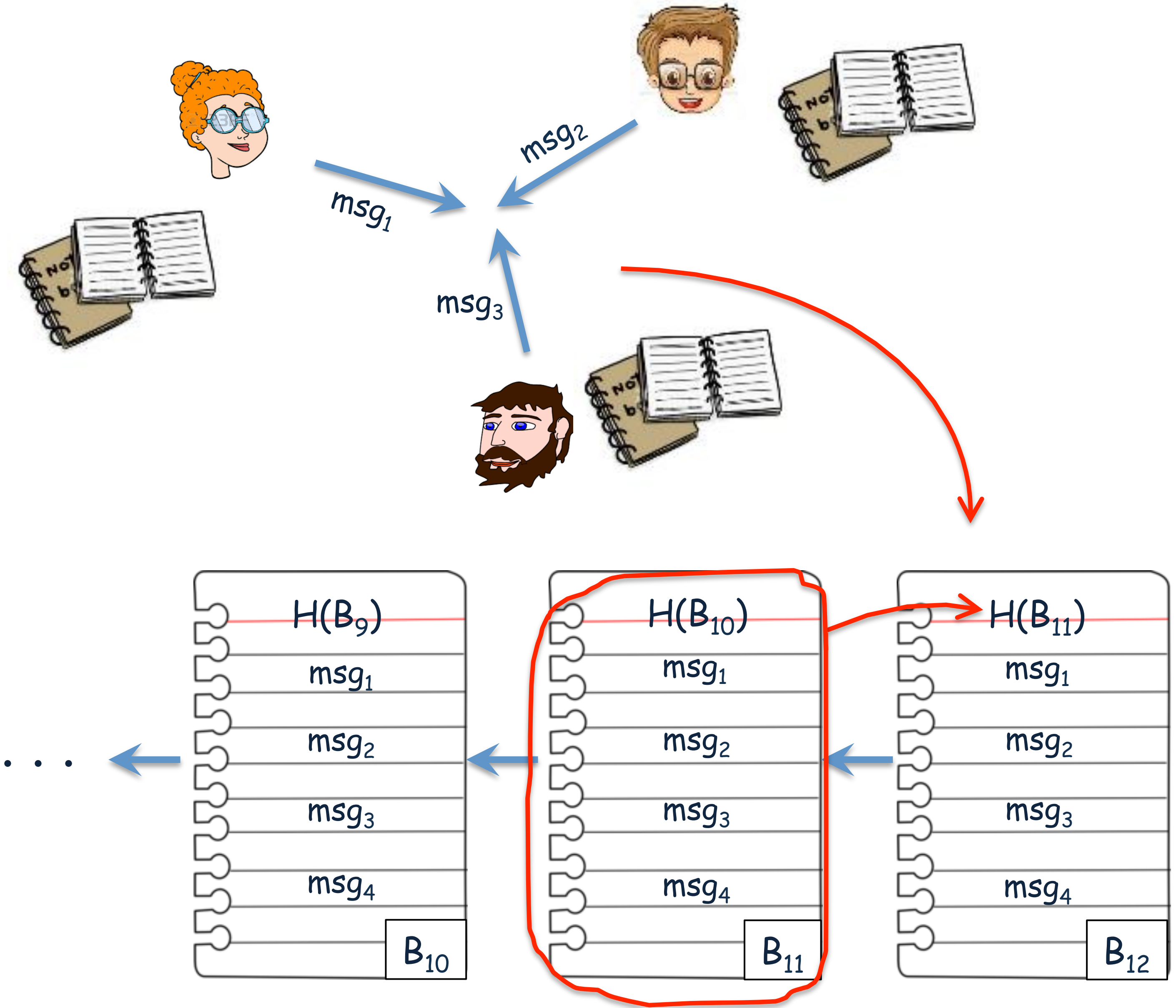
Preliminaries



Preliminaries



Preliminaries



Construction

Farmers

- the natural players who own a farmland and raise crops that correspond to the region of the land
- they support two roles: producer and auditor.
- they have to get a certificate from the agriculture authority of their region in order to register in the system

Construction

Farmers

- the natural players who own a farmland and raise crops that correspond to the region of the land
- they support two roles: producer and auditor.
- they have to get a certificate from the agriculture authority of their region in order to register in the system

Administrators

- the officers that represent the agriculture authority of different regions
- they will be the registration authority and they maintain the platform
- they have to possess a well-established identity

Construction

Registration of Administrators

- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0

Construction

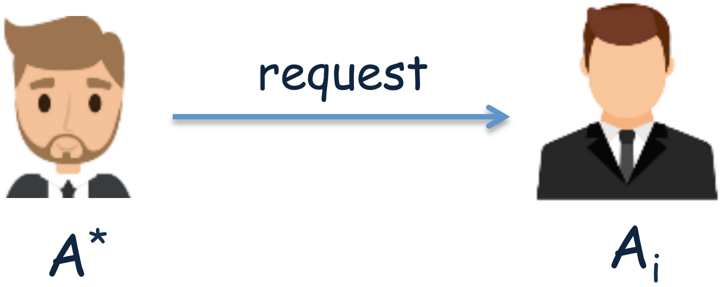
Registration of Administrators

- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0

Construction

Registration of Administrators

- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0



request

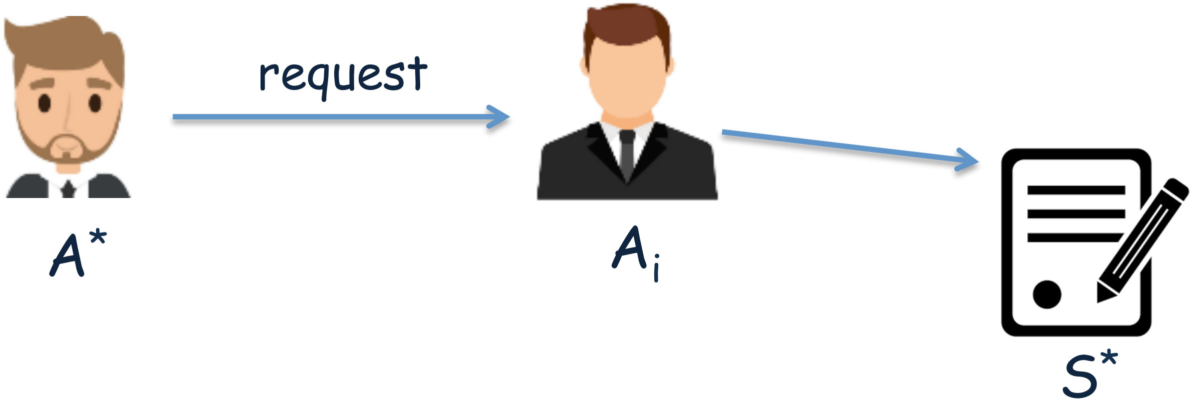
A^*

A_i

Construction

Registration of Administrators

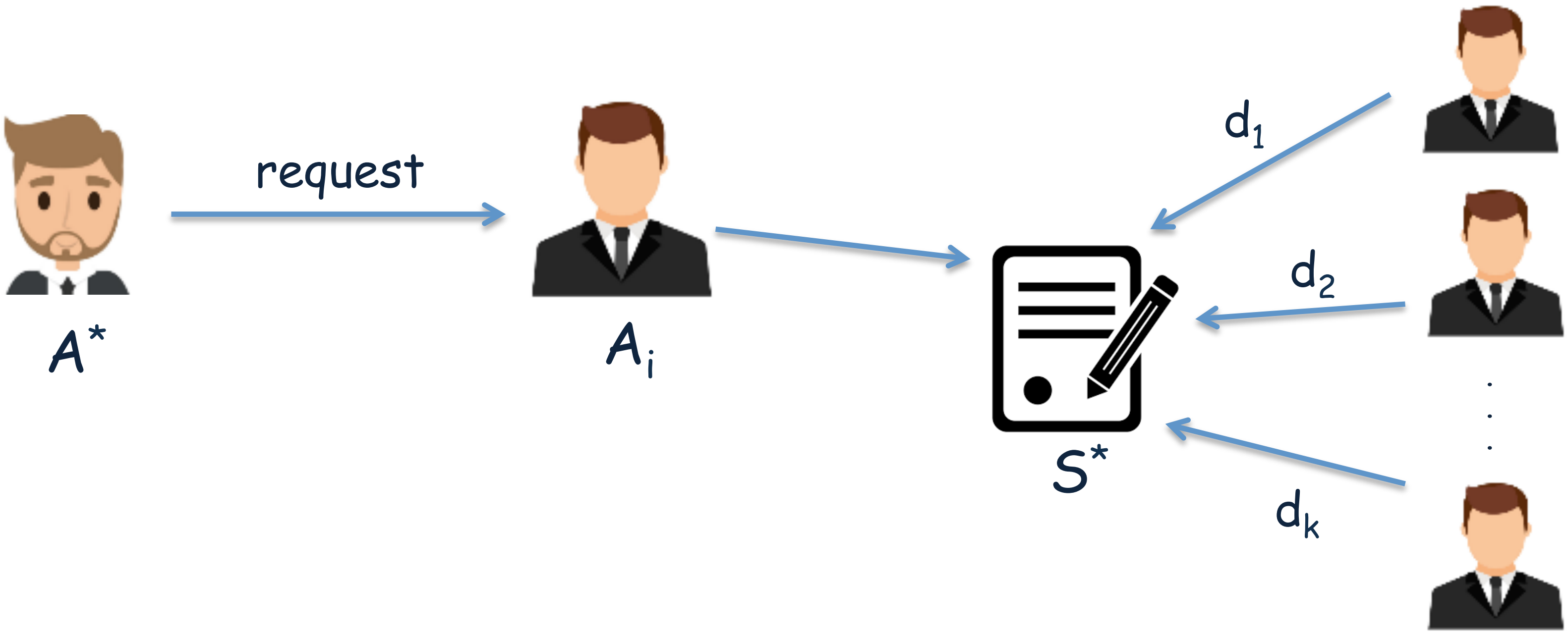
- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0



Construction

Registration of Administrators

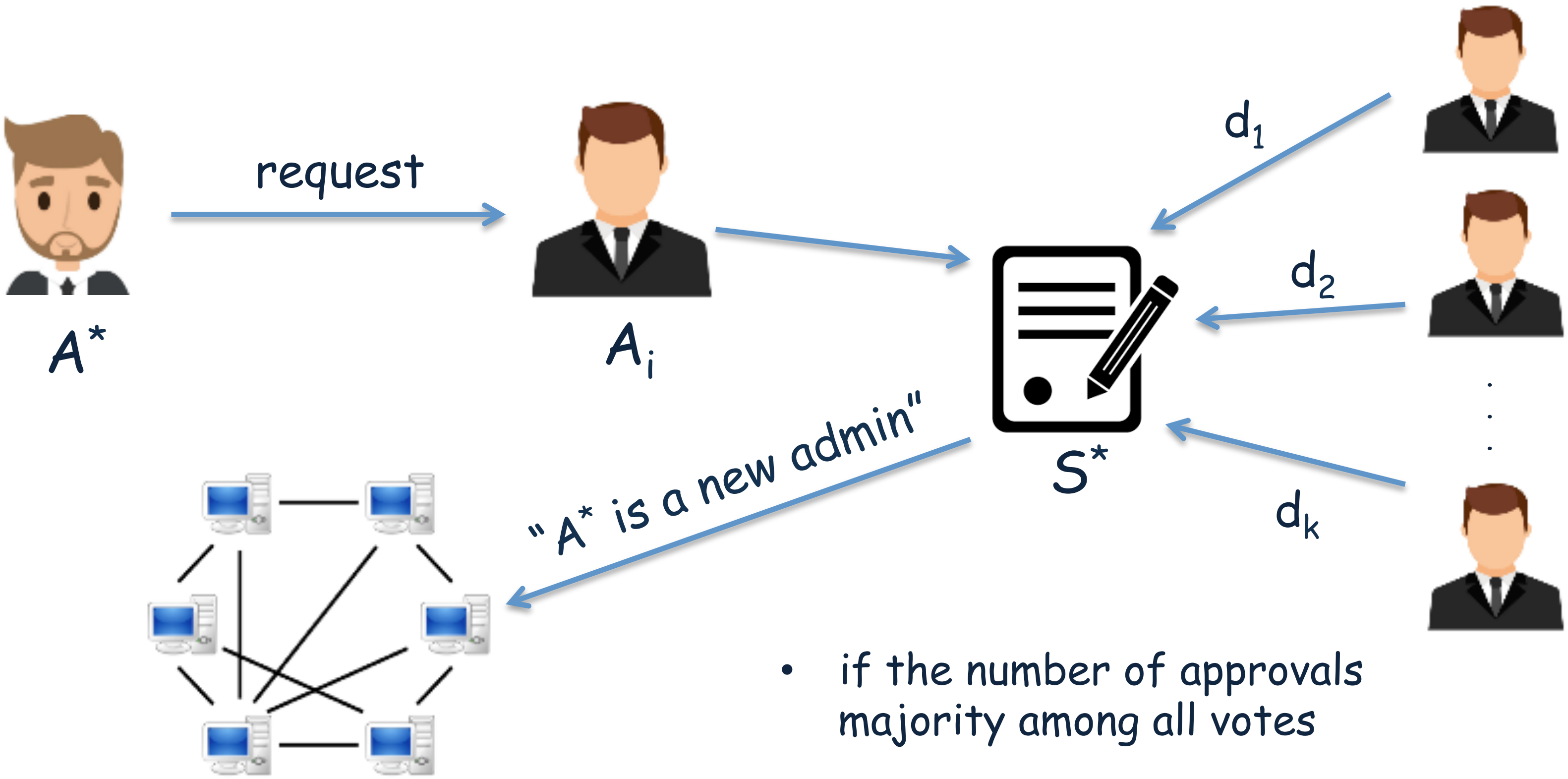
- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0



Construction

Registration of Administrators

- we start with a set of administrators, i.e. their identifiers $(A_{i_1}, \ldots, A_{i_m})$ will be specified at the genesis block B_0



- if the number of approvals majority among all votes

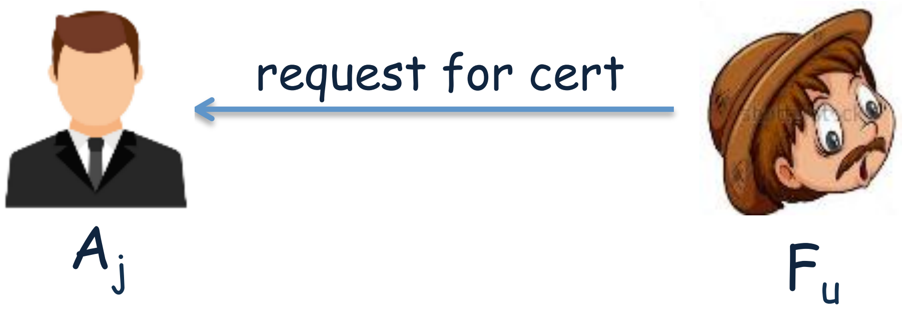
Construction

Registration of Farmer

F_u

Construction

Registration of Farmer



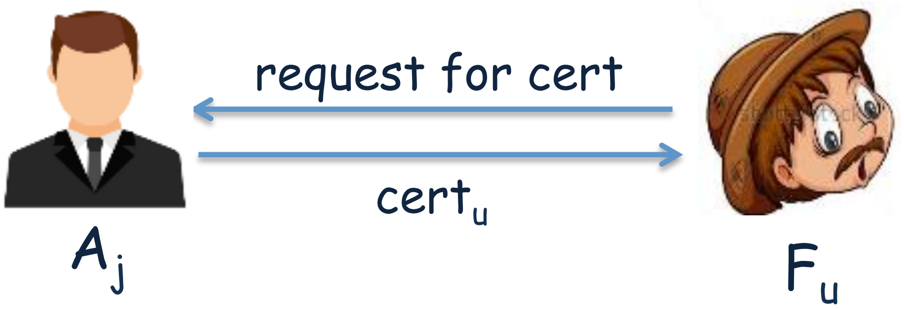
request for cert

A_j

F_u

Construction

Registration of Farmer



request for cert

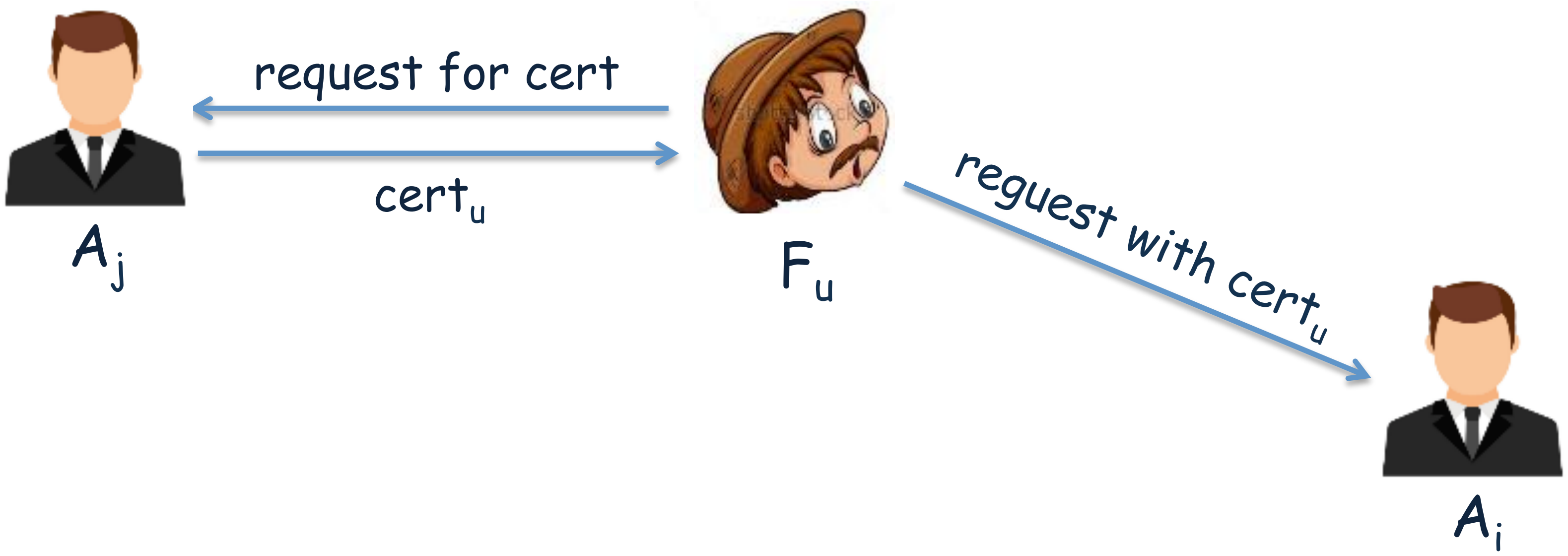
$cert_u$

A_j

F_u

Construction

Registration of Farmer



request for cert

cert$_u$

A_j

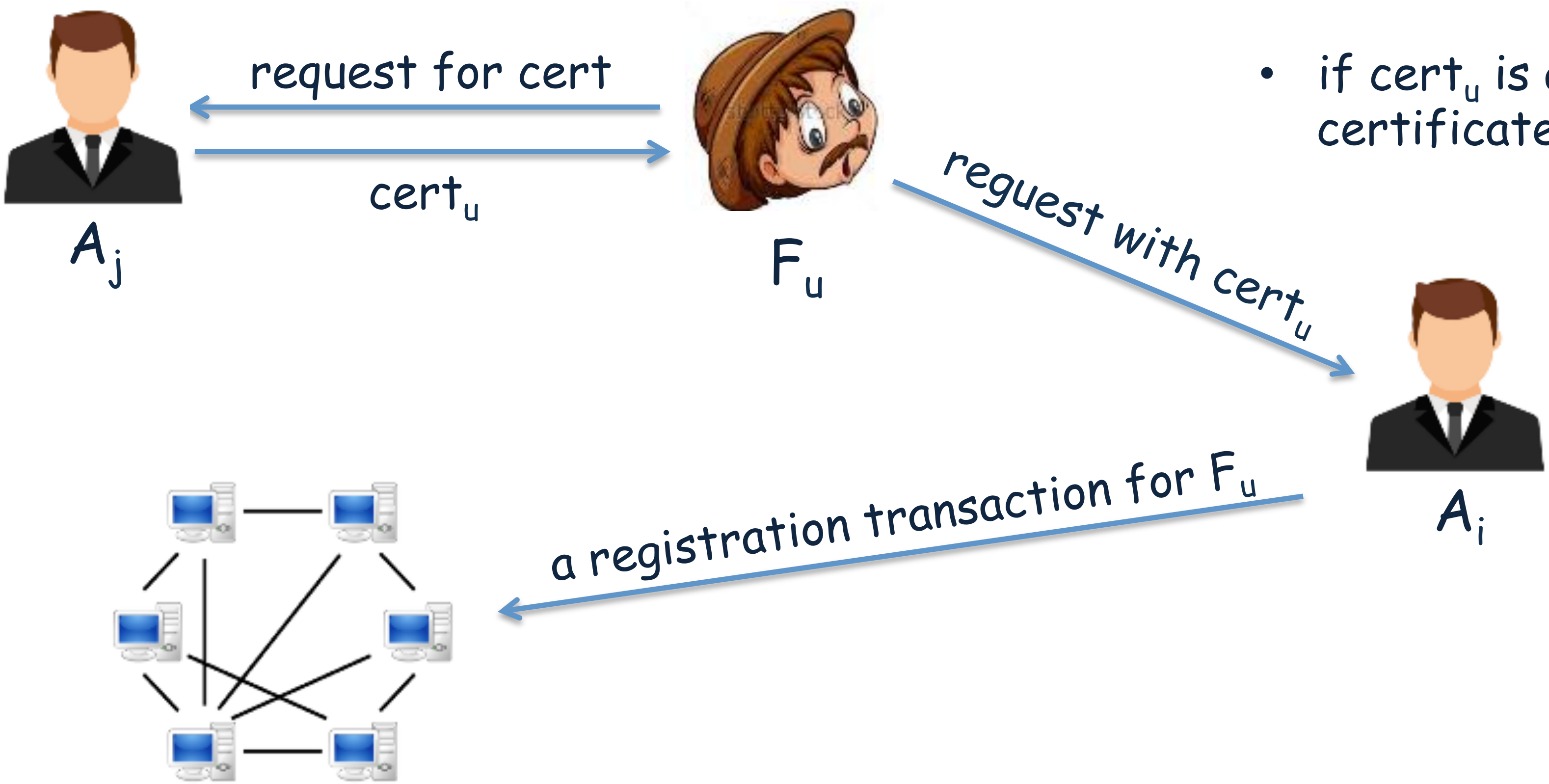
F_u

request with cert$_u$

A_i

Construction

Registration of Farmer



request for cert

$cert_u$

A_j

F_u

reguest with $cert_u$

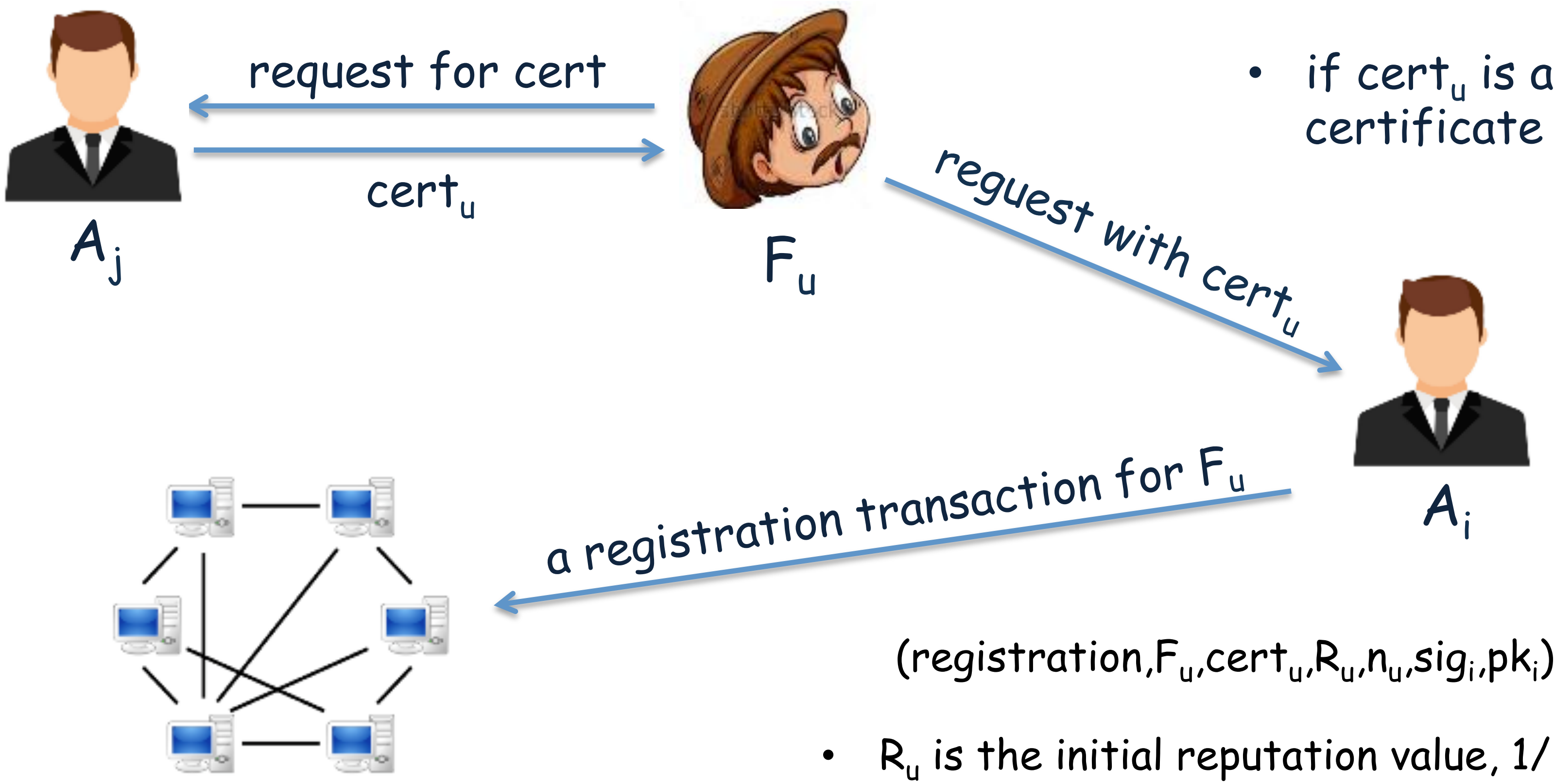
A_i

a registration transaction for F_u

- if $cert_u$ is a valid certificate

Construction

Registration of Farmer



request for cert

$cert_u$

A_j

F_u

reguest with $cert_u$

A_i

a registration transaction for F_u

- if $cert_u$ is a valid certificate

$(registration, F_u, cert_u, R_u, n_u, sig_i, pk_i)$

- R_u is the initial reputation value, 1/2
- n_u is the positive integer that helps us to count the number of farmers, and to efficiently choose random auditors

Construction

Block Format

- time divided into slots, i.e. $st_1, st_2, \ldots$

Construction

Block Format

- time divided into slots, i.e. $st_1, st_2, \ldots$
- admin A_i is responsible to create the block for the time slot st_k where i = k mod (N + 1) and N + 1 is the index of the last registered admin

Construction

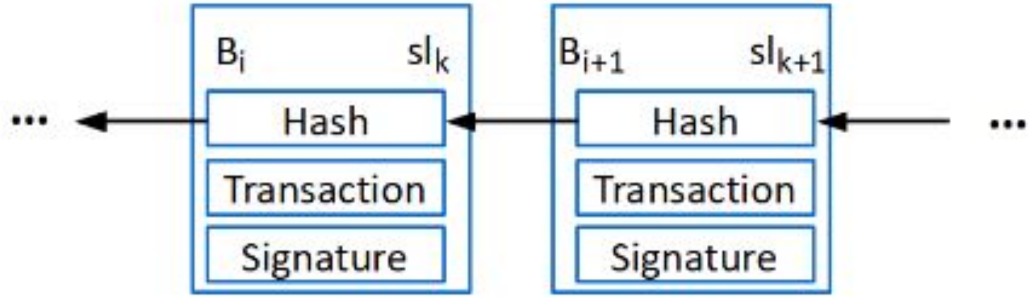
Block Format

- time divided into slots, i.e. $st_1, st_2, \ldots$
- admin A_i is responsible to create the block for the time slot st_k where i = k mod (N + 1) and N + 1 is the index of the last registered admin
- admins run PBFT to agree on a total order for the execution of smart contracts and transactions

Construction

Block Format

- time divided into slots, i.e. $st\downarrow 1$,$st\downarrow 2$,...
- admin $A\downarrow i$ is responsible to create the block for the time slot $st\downarrow k$ where i = k mod (N + 1) and N + 1 is the index of the last registered admin
- admins run PBFT to agree on a total order for the execution of smart contracts and transactions



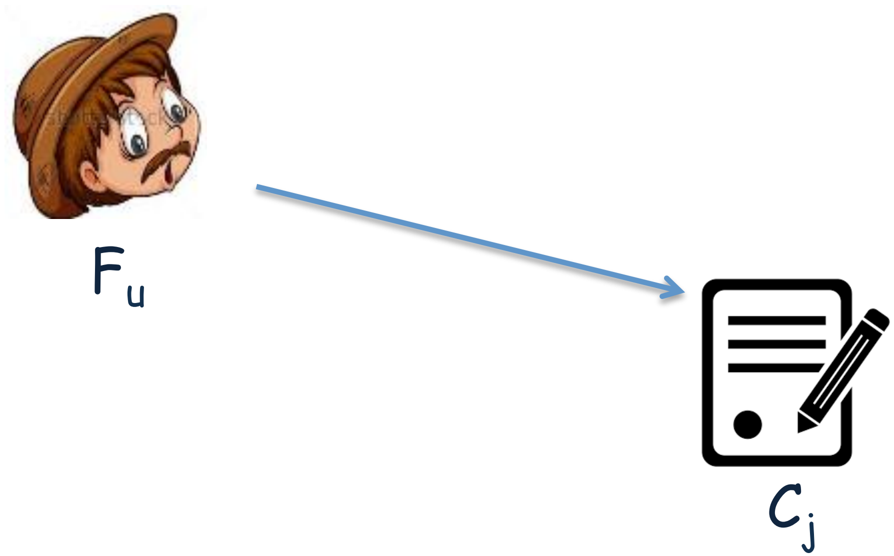
Construction

Declaring a Yield Commitment

F_u

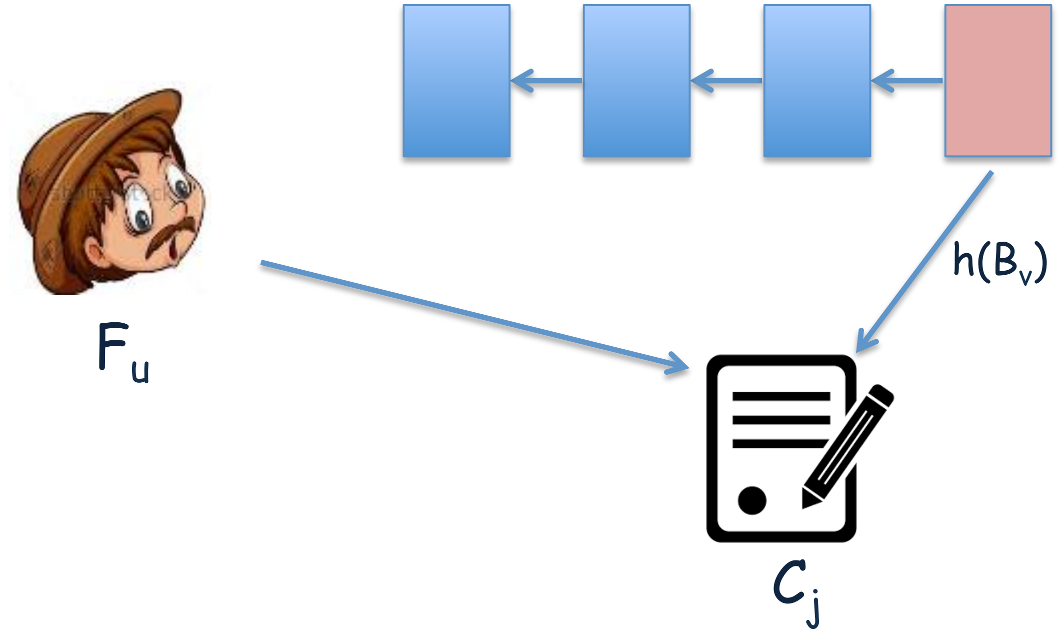
Construction

Declaring a Yield Commitment



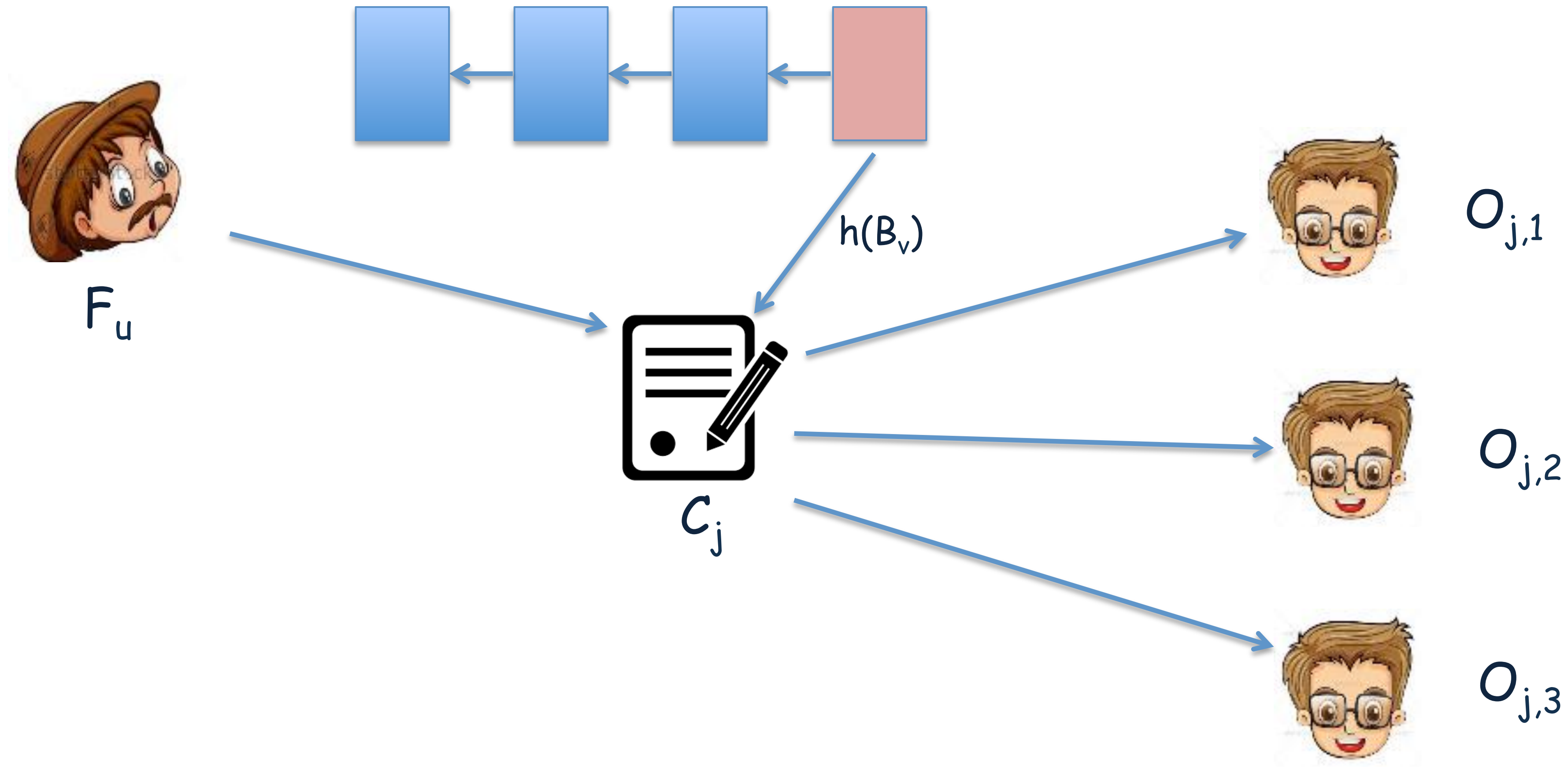
Construction

Declaring a Yield Commitment



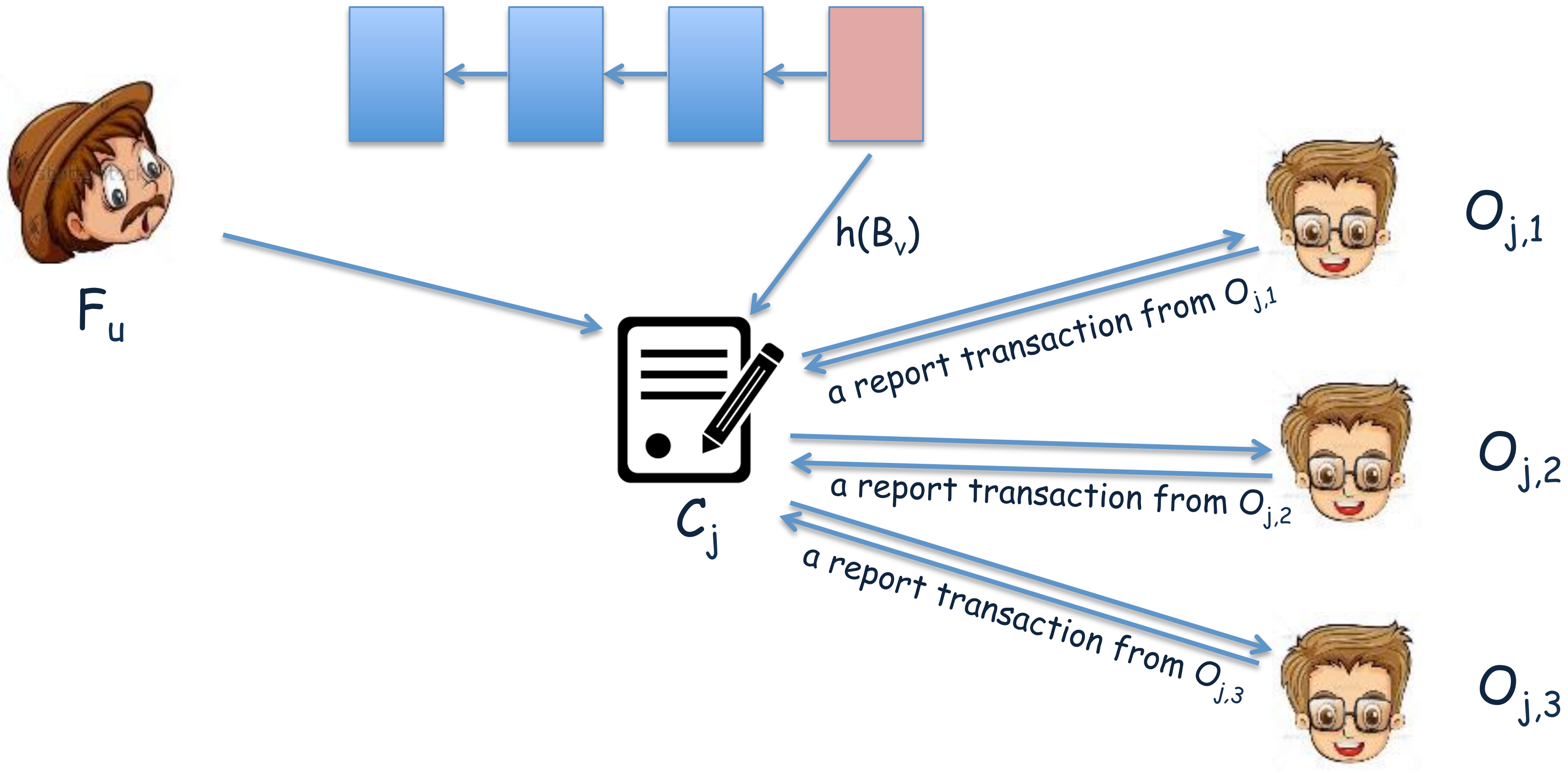
Construction

Declaring a Yield Commitment



Construction

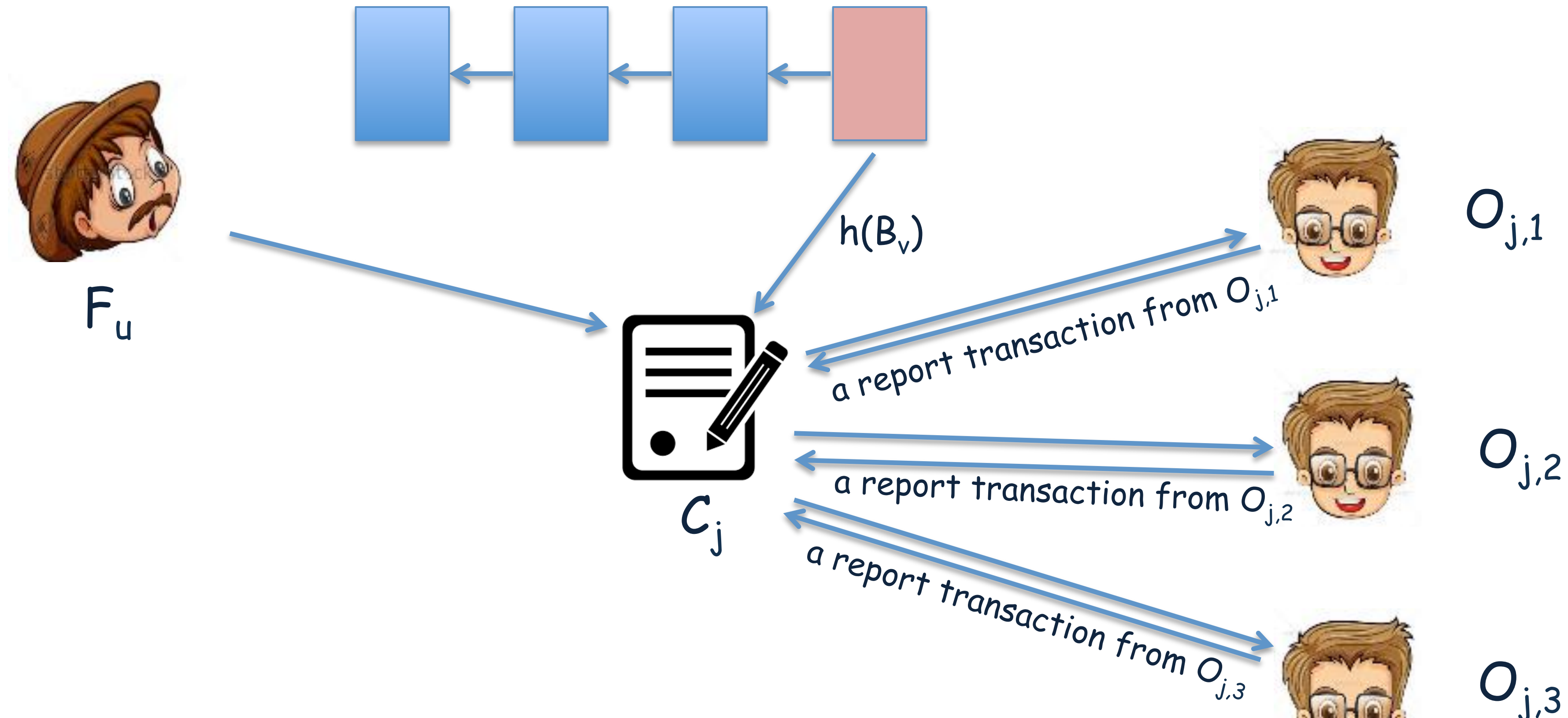
Declaring a Yield Commitment



h(B_v)
F_u
C_j
$O_{j,1}$
$O_{j,2}$
$O_{j,3}$
a report transaction from $O_{j,1}$
a report transaction from $O_{j,2}$
a report transaction from $O_{j,3}$

Construction

Declaring a Yield Commitment

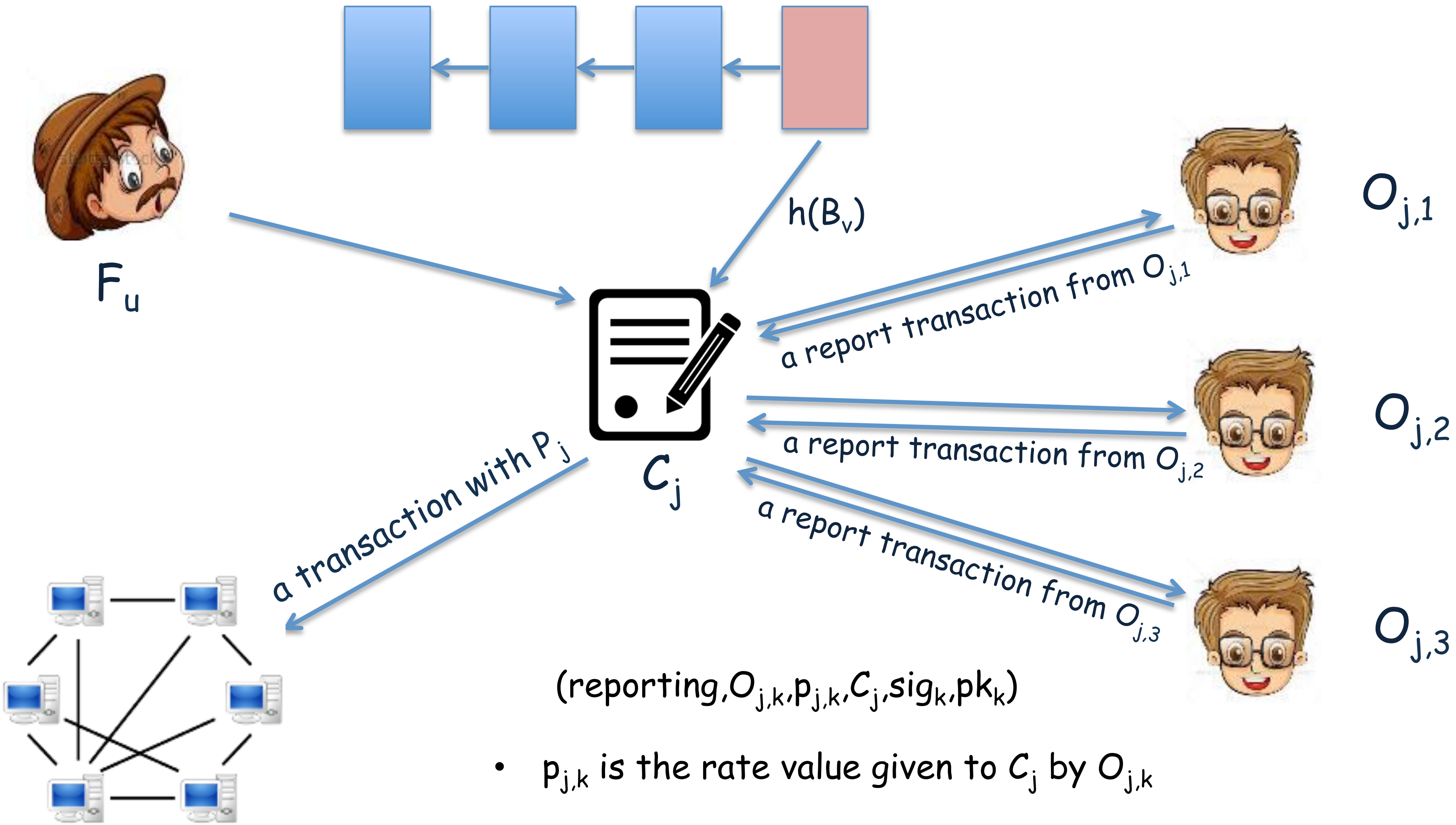

F_u
$h(B_v)$
C_j
$O_{j,1}$
$O_{j,2}$
$O_{j,3}$
a report transaction from $O_{j,1}$
a report transaction from $O_{j,2}$
a report transaction from $O_{j,3}$

$(reporting, O_{j,k}, p_{j,k}, C_j, sig_k, pk_k)$

- $p_{j,k}$ is the rate value given to C_j by $O_{j,k}$

Construction

Declaring a Yield Commitment


$h(B_v)$
F_u
C_j
$O_{j,1}$
$O_{j,2}$
$O_{j,3}$
a report transaction from $O_{j,1}$
a report transaction from $O_{j,2}$
a report transaction from $O_{j,3}$
a transaction with P_j

$(\text{reporting}, O_{j,k}, p_{j,k}, C_j, sig_k, pk_k)$

- $p_{j,k}$ is the rate value given to C_j by $O_{j,k}$

Construction

Updating Reputation

- P_j is the final score of C_j

Construction

Updating Reputation

- P_j is the final score of C_j
- it will be either a real number from [0,1] or Φ if no auditor reports a rate for the contract

Construction

Updating Reputation

- P_j is the final score of C_j
- it will be either a real number from [0,1] or Φ if no auditor reports a rate for the contract
- if P_j is Φ, then administrator A_i will not consider this commitment

Construction

Updating Reputation

- P_j is the final score of C_j
- it will be either a real number from [0,1] or Φ if no auditor reports a rate for the contract
- if P_j is Φ, then administrator A_i will not consider this commitment
- Otherwise, A_i will create an updating-reputation transaction (update, F_u, c, R^*, sig_i, pk_i)

Construction

Updating Reputation

- P_j is the final score of C_j
- it will be either a real number from [0,1] or Φ if no auditor reports a rate for the contract
- if P_j is Φ, then administrator A_i will not consider this commitment
- Otherwise, A_i will create an updating-reputation transaction (update, F_u, c, R^*, sig_i, pk_i)
- R^* is computed as $(R_u + P_j) / 2$, where R_u is the reputation value of the last updating-transaction created for F_u

Construction

Updating Reputation

- P_j is the final score of C_j
- it will be either a real number from [0,1] or Φ if no auditor reports a rate for the contract
- if P_j is Φ, then administrator A_i will not consider this commitment
- Otherwise, A_i will create an updating-reputation transaction (update, F_u, c, R^*, sig_i, pk_i)
- R^* is computed as $(R_u + P_j) / 2$, where R_u is the reputation value of the last updating-transaction created for F_u
- c is the counter indicating the number of consecutive commitments in which the reputation of F_u stays below a certain threshold

Construction

Updating Reputation

- if an administrator A_i detects a farmer F_u that has not declared a yield commitment in a certain time period, he creates an upgrading reputation transaction

$$(\text{update}, F_u, c, R_u/2, \text{sig}_i, \text{pk}_i)$$

Construction

Updating Reputation

- if an administrator A_i detects a farmer F_u that has not declared a yield commitment in a certain time period, he creates an upgrading reputation transaction

$$(update, F_u, c, R_u/2, sig_i, pk_i)$$

- if an administrator A_i detects an auditor $O_{j,k}$ that has not reported a rate for the corresponding commitment in a certain time period, he creates an upgrading-reputation transaction

$$(update, O_{j,k}, c, R_u/2, sig_i, pk_i)$$

Construction

Revocation

- administrators revoke farmers that have not performed well in their recent commitments by creating a revocation transaction. It has the following form:

$$(\text{revocation}, F_u, sig_i, pk_i)$$

Construction

Revocation

- administrators revoke farmers that have not performed well in their recent commitments by creating a revocation transaction. It has the following form:

$$(\text{revocation}, F_u, sig_i, pk_i)$$

- this transaction is only created if the counter in the last upgrading reputation transaction of F_u is equal to the threshold t and F_u fails on the last commitment

Instantiation

- used Solidity to write smart contracts that run on the Ethereum Virtual Machine (EVM)

Instantiation

- used Solidity to write smart contracts that run on the Ethereum Virtual Machine (EVM)
- planning to use Hyperledger Burrow that is a blockchain platform.

  it executes EVM smart contract on a permission virtual machine

  it uses Tendermint consensus engine

Instantiation

- used Solidity to write smart contracts that run on the Ethereum Virtual Machine (EVM)

- planning to use Hyperledger Burrow that is a blockchain platform.

  it executes EVM smart contract on a permission virtual machine

  it uses Tendermint consensus engine

- Tendermint BFT consensus engine (Tendermint core)

  it is a BFT consensus mechanism, i.e. it assumes that no more than 1/3 of the administrators in the network can be byzantine

  BFT assumption is predicated on the weight (stake) of each validator rather than 1/3 of the total nodes participating

Future Works

- The system may require auditors to prove that they have indeed visited the corresponding farmland and made enough observations.

auditors may attach a location proof to their reports

Future Works

- The system may require auditors to prove that they have indeed visited the corresponding farmland and made enough observations.

  auditors may attach a location proof to their reports

- Reputation can be used outside of the platform in order to incentivize farmers to act honestly in the platform

Future Works

- The system may require auditors to prove that they have indeed visited the corresponding farmland and made enough observations.

  auditors may attach a location proof to their reports

- Reputation can be used outside of the platform in order to incentivize farmers to act honestly in the platform

- Reputation can also be used to even enforce the administrators to follow the protocol

Future Works

- The system may require auditors to prove that they have indeed visited the corresponding farmland and made enough observations.

  auditors may attach a location proof to their reports

- Reputation can be used outside of the platform in order to incentivize farmers to act honestly in the platform

- Reputation can also be used to even enforce the administrators to follow the protocol

- Yield commitment can be extended in a way that it also determines the amount of crop the farmers planning to harvest

Thanks!