Decentralized Execution of Smart Contracts: Agent Model Perspective and Its Implications

Weidong Shi

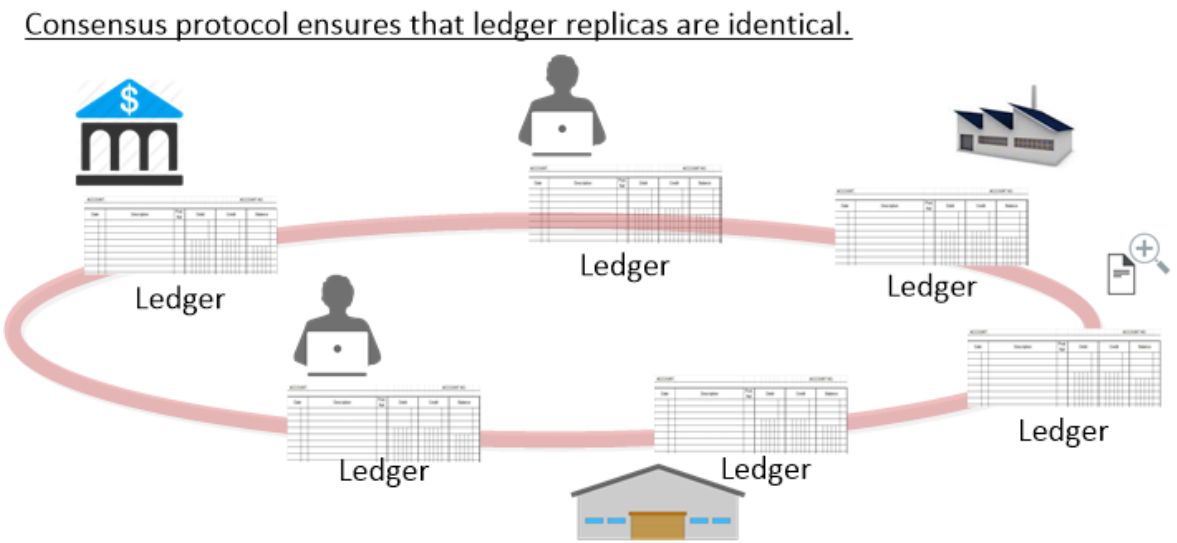
joint work with Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, and Yang Lu

University of Houston

1st Workshop on Trusted Smart Contract
Malta, April, 2017

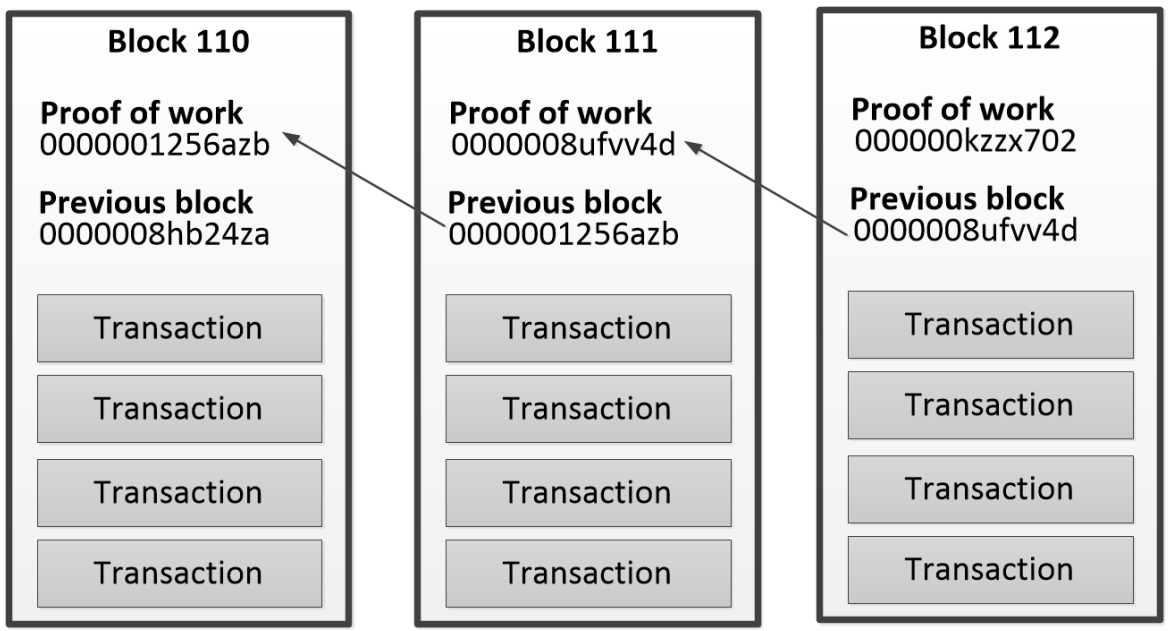
Background

- What is a blockchain?
  - Shared, replicated, ledger.



Background

- A chain of blocks of transactions - examples including:
  - Bitcoin
  - NXT
  - Ethereum
  - ...



Background

- Crypto ledgers (e.g., Ethereum, Hyperledger) aim at supporting "smart contracts".

Definition

A smart contract is a set of promises, specified in a digital form, including protocols within which the parties perform on these promises.

Background

- Another definition:

Definition

A smart contract is an event driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger [Swanson2015].

Background

- Abstract smart contract model:
  - Shared public ledger
  - Replicated states (smart contracts)
  - Using crypto-currency rewarding contract execution
  - Contracts involving financial gains or losses
  - Event driven
  - Consensus based (smart contract execution)
  - Participants are not trusted
  - Inter-dependent contracts

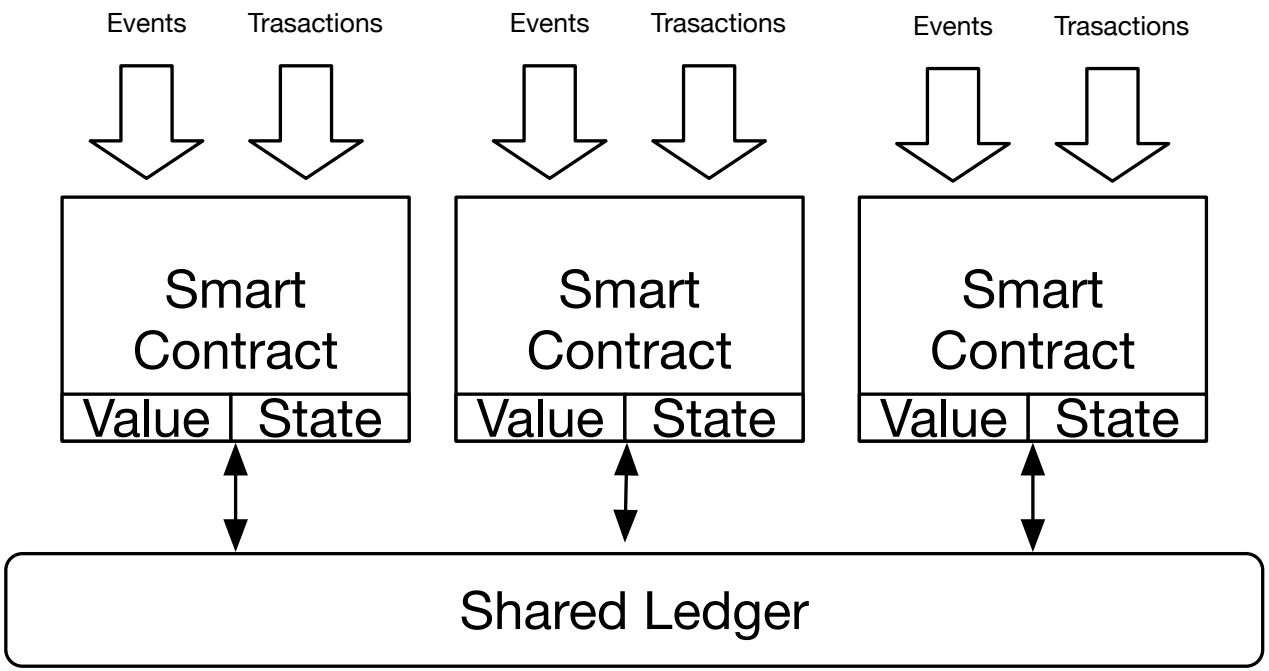
Background

- A simple example of a smart contract.

Background

- A simple example of a smart contract.

Background


Events
Trasactions
Events
Trasactions
Events
Trasactions
Smart Contract
Value
State
Smart Contract
Value
State
Smart Contract
Value
State
Shared Ledger

Background

- Execution of a smart contract can be tricky:
  - The amount of crypto-currency involved in a contract may be many times and significantly higher than the cost of running the contract itself.

Background

- Execution of a smart contract can be tricky:
  - The amount of crypto-currency involved in a contract may be many times and significantly higher than the cost of running the contract itself.

Background

- Execution of a smart contract can be tricky:
  - The amount of crypto-currency involved in a contract may be many times and significantly higher than the cost of running the contract itself.

- If the random dice returns 1, Alice has the incentive of lying.

Background

- Execution of a smart contract can be tricky:
  - The amount of crypto-currency involved in a contract may be many times and significantly higher than the cost of running the contract itself.
  - If a significant portion of users in system are directly or indirectly involved in a smart contract, then this smart contract might not get executed correctly.

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)
  - Weight w_j for user j (indicating the potential of manipulating the result)

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)
  - Weight w_j for user j (indicating the potential of manipulating the result)
    - The computation power in a proof-of-work system
    - The number of stakes in a proof-of-stake system
    - ...

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)
  - Weight w_j for user j (indicating the potential of manipulating the result)
    - The computation power in a proof-of-work system
    - The number of stakes in a proof-of-stake system
    - ...
  - Possible states S_i
    - If S_i occurs, the payoff of user j is z_j^i

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)
  - Weight w_j for user j (indicating the potential of manipulating the result)
    - The computation power in a proof-of-work system
    - The number of stakes in a proof-of-stake system
    - ...
  - Possible states S_i
    - If S_i occurs, the payoff of user j is z_j^i
  - Users "vote" to reach a consensus on the correct state
    - Byzantine: broadcast a certain state
    - Longest chain: adding blocks after a specific chain
    - ...

The problem

- A game theoretical model (smart contract participants and execution nodes are agents):
  - N players (users in the system)
  - Weight w_j for user j (indicating the potential of manipulating the result)
    - The computation power in a proof-of-work system
    - The number of stakes in a proof-of-stake system
    - ...
  - Possible states S_i
    - If S_i occurs, the payoff of user j is z_j^i
  - Users "vote" to reach a consensus on the correct state
    - Byzantine: broadcast a certain state
    - Longest chain: adding blocks after a specific chain
    - ...
  - A state receiving αW votes in weight wins

The problem

Q: Can we prevent users from lying when they vote?

Our contribution

- In general, lying can not be prevented.

Lemma

Voting for the state that a user prefers the most is his/her dominant strategy.

Our contribution

- In general, lying can not be prevented.

Lemma

Voting for the state that a user prefers the most is his/her dominant strategy.

- Can we discourage users from lying by adding punishment?

Our contribution

- The system can impose a penalty on a user if his/her vote is different from the accepted state.

Theorem

In the agent model with penalty, if j is superrational and knows that $\sum_{k \in U} w_k \geq \alpha W$, then no matter how high the penalty is, j will always lie.

Our contribution

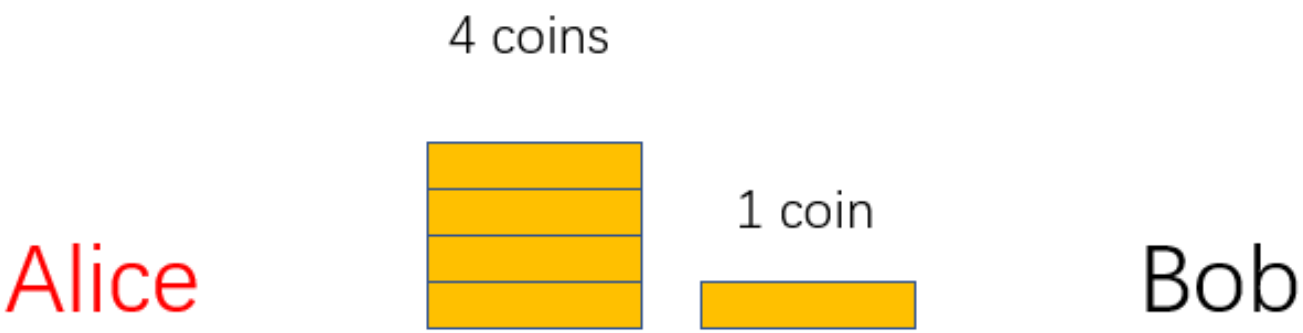
- The classical game theory seems to lead us nowhere...

Our contribution

- The classical game theory seems to lead us nowhere...
- But rationality or superrationality is questionable.

Irrational behaviors

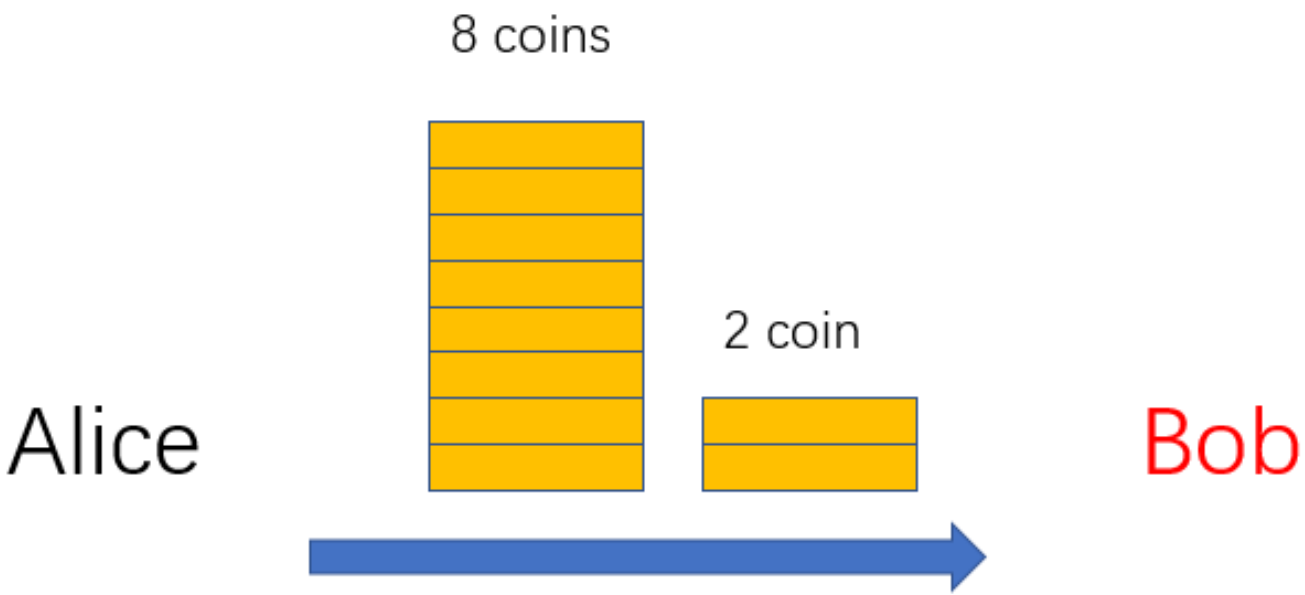
- Centipede game:



Alice can: Take the pile of 4 coins, or pass both piles to Bob

Irrational behaviors

- Centipede game:



The coins double if Alice chooses to pass them to Bob, but then it becomes Bob's turn to decide.

Irrational behaviors

- Centipede game
  - The game lasts for a fixed number of rounds, which is known to both players.
  - A rational player chooses to take the larger pile and the game ends immediately. Only 15% players choose to do so in experiments.

Our contribution

- In our problem, the situation changes when irrationality is taken into consideration.

Our contribution

- In our problem, the situation changes when irrationality is taken into consideration.

Theorem

In the agent model with penalty, if users do not fully believe in the rationality of others, then a mechanism with penalty can be designed such that users do not lie in voting.

Conclusion

- We consider smart contract execution in a blockchain based system and propose an agent model.

Conclusion

- We consider smart contract execution in a blockchain based system and propose an agent model.
- Truthfulness of users can not be achieved if rationality or superrationality is assumed, even if penalty is introduced.

Conclusion

- We consider smart contract execution in a blockchain based system and propose an agent model.
- Truthfulness of users can not be achieved if rationality or superrationality is assumed, even if penalty is introduced.
- Truthfulness of users can be achieved with a carefully designed penalty, if irrationality is assumed.