Decentralized Mechanism Design Using Blockchains

CS711 Course Project : Group 7
Abhimanyu Sethia, Atharv Singh Patlan, Rohan Baijal, V Pramodh Gopalan, Yatharth Goswami

Mentor: Ms. Garima Shakya

Contents

Motivation

Manipulating Mechanisms

1. Boston School Choice Mechanism Problem
   a. College preference order, students ranked
   b. A>B>C, IITB, IITK have 1 seat each
2. First Price Auctions
3. Second Price Auctions

1. Corruption of central authority/mechanism designer
2. Revealing of one's choice/bids to the other parties

The need for a decentralised mechanism design, that keeps the bid of all parties private

BlockChain and DAMD

- BlockChain - Distributed ledger with no central authority. Correctness on consensus and discourages tampering through Cryptographic primitives.
- Smart Contracts : Essentially code which runs on each node after verification; leads to same state throughout the network.
- Consider BlockChain as a game. PoW ensure incentive compatibility and honest computation.
- By coding rules of Mechanism into the Smart Contract, we can ensure a decentralized and distributed implementation without any central authority.
- Even if agent is a miner, he has no incentive to deviate unless she holds a monetary or computational stake in the network.

PoW : Solve computationally hard problem.

PoS : Get chance to add block by staking your worth.

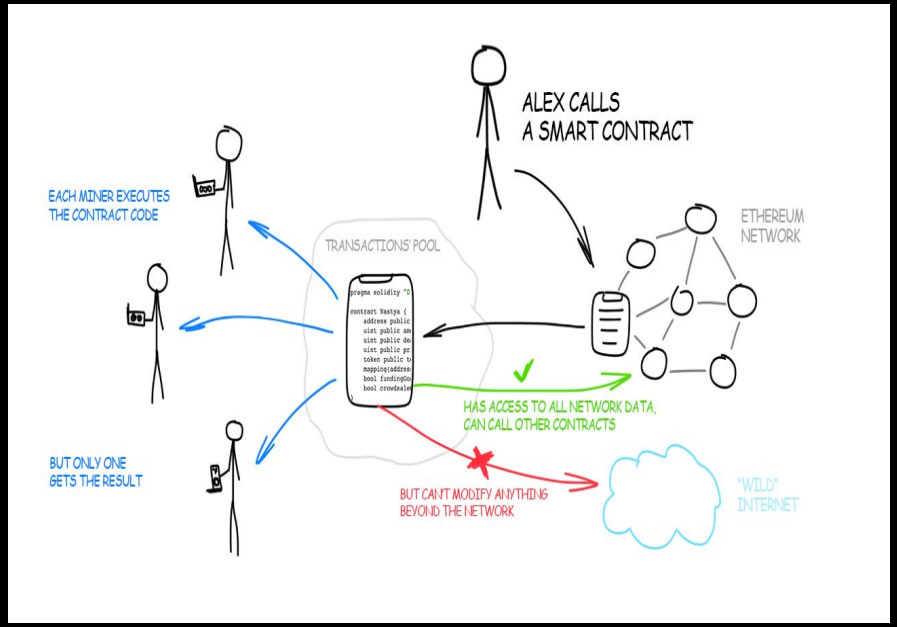
Current State of the Art

- Verifiable sealed bid auction
  - Pederson commitment scheme to store bids
  - Real bids revealed to a semi-trusted auctioneer to compute the final winner
  - Zero knowledge proof to prove correctness of winner to all parties
  - Only winning bid is revealed, others stay private

- Enigma Protocol :
  - Off-loading private computation to a different network making use of Secret Sharing and MPC
  - The other network has nodes with special hardware which ensures that the computation is secure.
  - The nodes only have parts of private data.

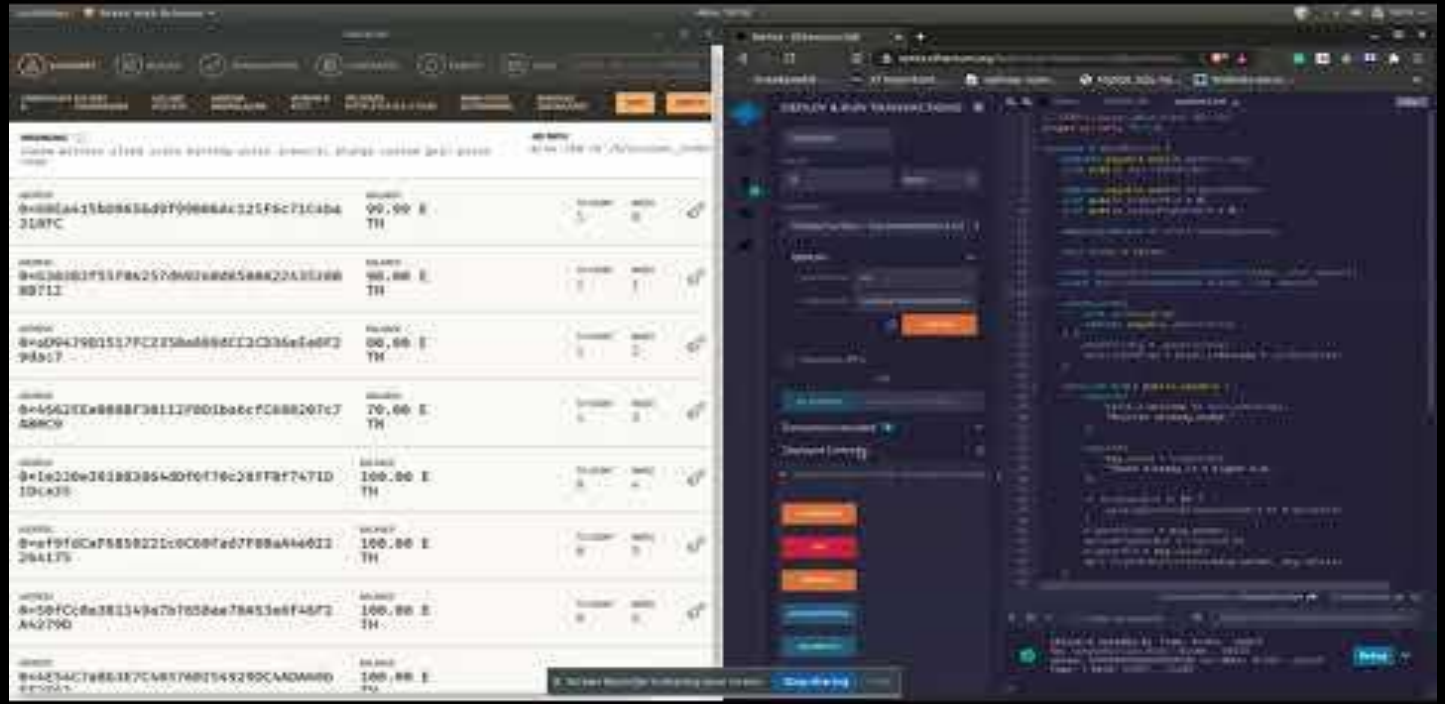
Smart Contract Based Auctions

- We simulated **Decentralised VCG Auctions** on the Ethereum blockchain.
- Made a **Smart Contract for the auction** and deployed it in a private blockchain
- While the auction was live, all the nodes in the network were **able to see the data present inside the smart contract**.
- Hence, all nodes were **aware of the current highest bid** and also the highest bidder at any time during bidding.



Smart Contract Auction simulation

Click on image to watch, or use this link: https://youtu.be/kgCkKmR4dKw



Bird's Eye view of Secret Network

- Tackling **trade-off** between decentralization and privacy
- **Evolution from Enigma**: Places trust on hardware through TEE's(Trusted Execution environments)
- **Smart contracts become secret contracts**

Secret Network : TEE + Blockchain + SC

- TEE’s and enclaves.
- How Does TEE provide confidentiality?
- Validators check correctness of output and execute Secret Contracts.
- The fee is distributed through PoS.
- The Secret Network - Private; Decentralized; No Mediator;

Auction Simulation on Secret Network (Demo)

Link to slides:
https://github.com/rohanblueboybaijal/CS711-secret-VCG/tree/main/Secret%20Contracts/Assets/simulation.pdf

Theoretical Results

- Modelled Normal Form Game between bidder and seller.
- Derived that participating in Secret Network BlockChain mechanisms is a dominant strategy, even when privacy is a significant concern for agent.

Observation:

- In the current implementation of the enigma protocol, the worker enigma nodes **lack the ability to choose** which computation task they would like to perform.
- **Necessary for them to compute the task allotted to them**, no matter how low the transaction fee offered is.

Proposal/Construction:

- Could give nodes the ability to reject allotted tasks, but this is again a waste of time and loss of revenue, due to how enigma works
- Propose: a 2nd lowest bid auction tackles this problem by allowing the participating nodes to bid the amount of transaction fee they would like to receive for each task,

Summary

- Motivated the need for a decentralised auction (mechanism in general), that preserves the privacy of bids
- Simulated auctions in a private and decentralised manner
- Modelled a game and derived that participating in a secret network auction is a dominant strategy
- Observed a shortcoming of the current enigma system
- Proposed an improvement in the enigma protocol