Incentive Mechanism Design for Blockchain Networks: Bridging Decentralized Exchanges, Web 3.0, and the Metaverse

Presented by: Daniel Mawunyo Doe
Advisor: Dr. Zhu Han
Electrical and Computer Engineering Department
University of Houston

Committee Members: Dr. Miao Pan, Dr. David Mayerich, Dr. Yuqing Hu, Dr. Niyato Dusit, and Dr. Zhu Han

Department of Electrical and Computer Engineering
Cullen College of Engineering

Presentation Outline & Objective

1 Introduction

1. Blockchain
2. Decentralized systems (DEX, Web 3.0, and Metaverse
3. Game Theory

2 Work Examples

1. Incentive Mechanism Design For Mitigating Frontrunning and Transaction Reordering in Decentralized Exchanges
2. Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse through Diversified Incentive Mechanism Design
3. A Contract-Stackelberg Framework for Mitigating Timing Games in Proof-of-Stake Blockchain Networks

3 Conclusion

This section concludes our discussion

Works Objective

To enhance blockchain technology, each addressing unique challenges:

- **DEX integrity,**
- **Network sustainability for Web 3.0 and Metaverse**
- **Proof-of-Stake network reliability**.

Introduction: Decentralized Internet (Web 3.0)

1. Web 1.0

Drawbacks: Static (read-only), unorganized and overwhelming.

2. Web 2.0

Interact with the internet

Read, share, comment, and write

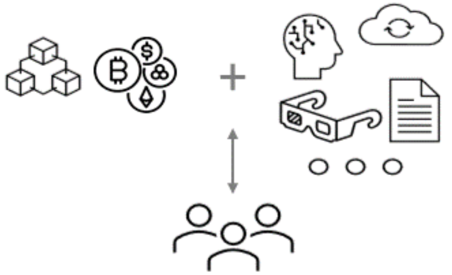
Social web: two-way communication

Computing paradigms

Drawbacks: Data privacy, exploitation, government interventions, single-point of failure, politics and censorship.

3. Web 3.0

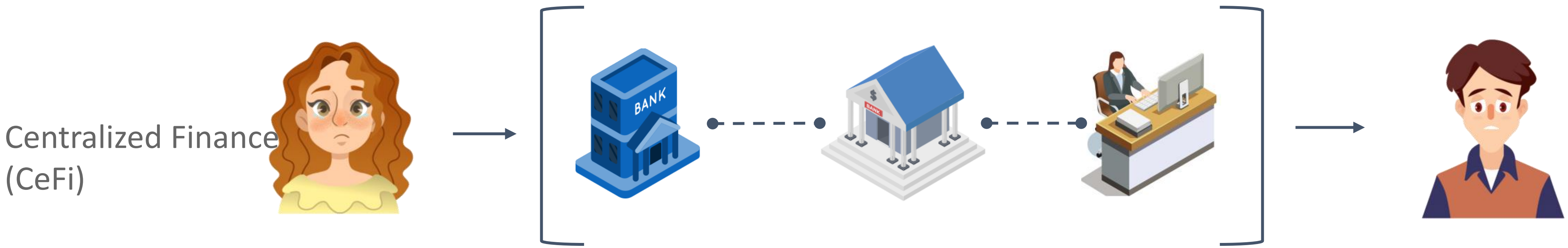
User-centric, decentralized, private, and secure (2020s and beyond)

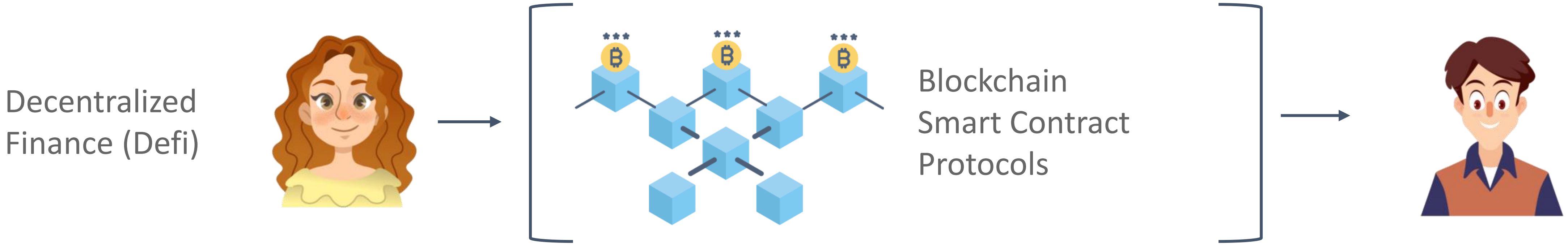


IPFS Storj Experty Essentia One Brave Steemit Akasha

Drawbacks: Relies on blockchain technologies to achieve decentralization.

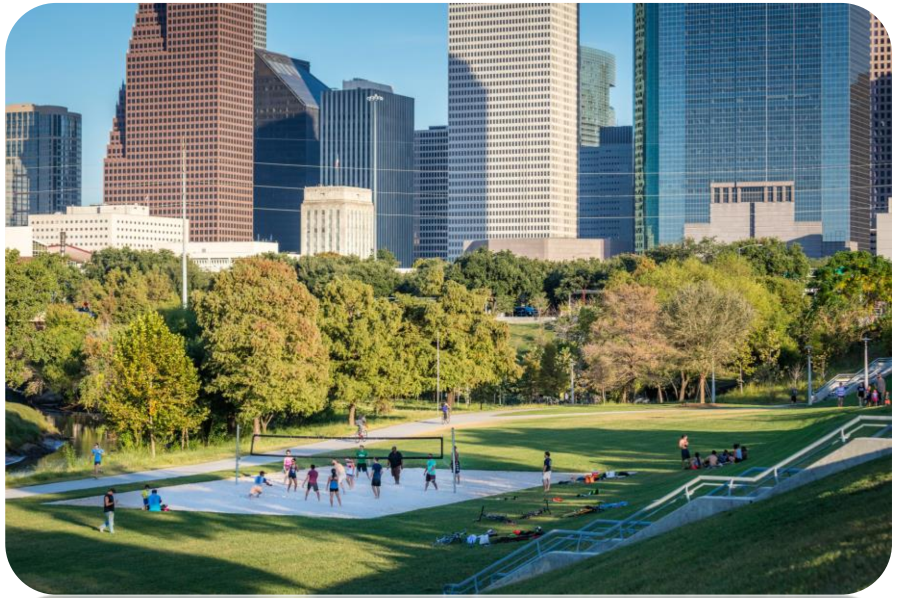
Centralized and Decentralized Finance

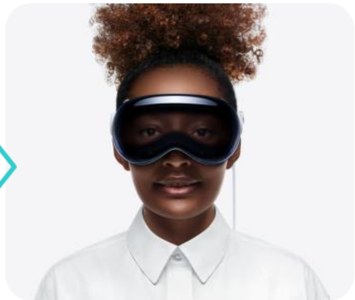




DeFi ensures **global accessibility**, offers **censorship resistance**, empowers users with **direct ownership and control**, promotes **interoperability** between platforms, thrives on **open source transparency**, and fosters **financial inclusion**.

Metaverse and The Internet





Metaverse Defined: A virtual universe of interconnected digital environments.

Merges physical reality with digital virtuality.

Revolutionizes the internet: entertainment, social interactions, commerce, education, etc.

Metaverse Research 1 (HD Map Optimization Part 1)

What is the goal for HD map data optimization?

Raw map data

Storage size:

Optimized map data

Storage size:

To reduce transmission data size to improve latency of HD map updates

Metaverse Research 1 (HD Map Optimization Part 2)

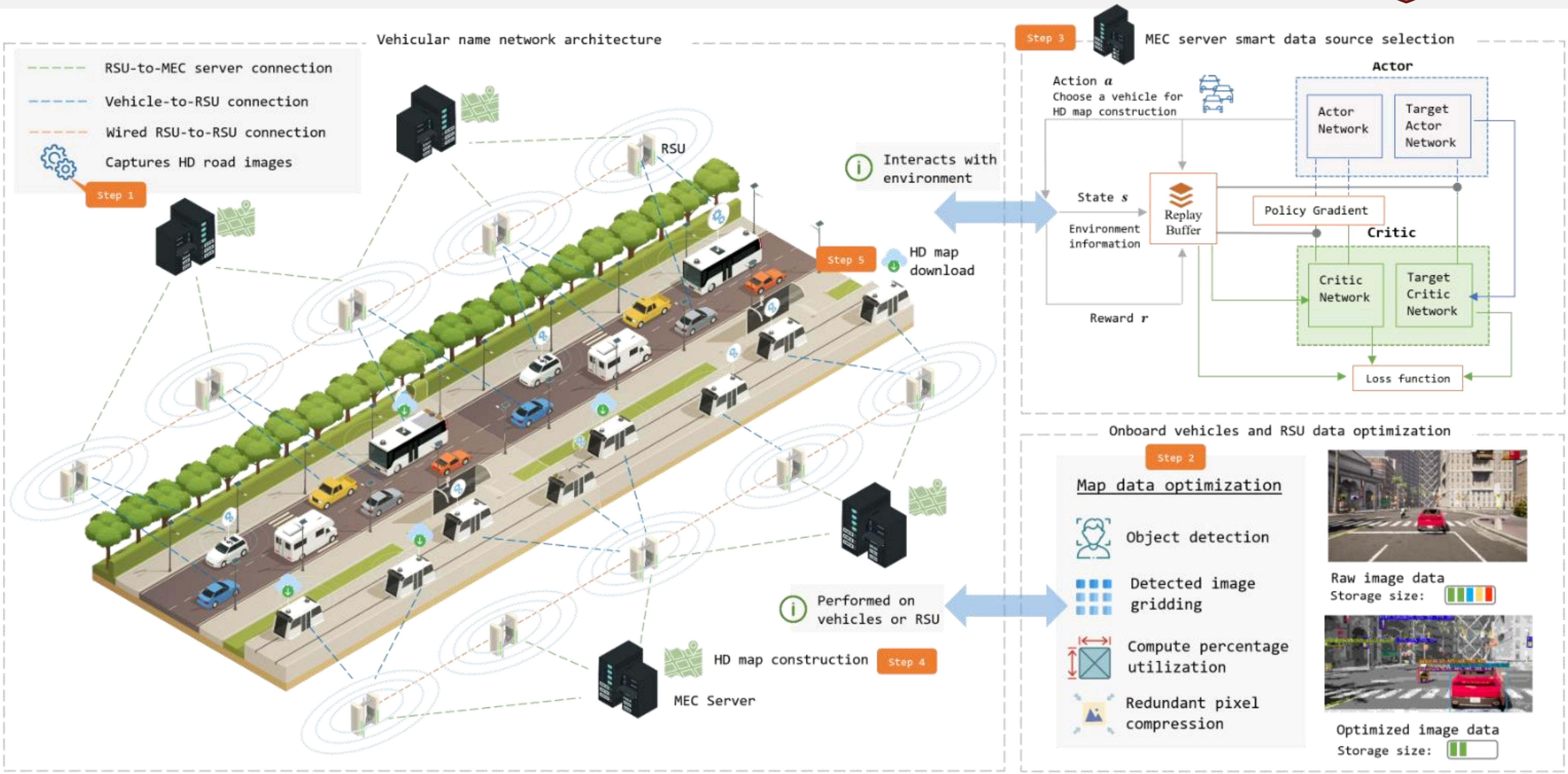
Perform object detection

Divide resulting image into grids

Compute percentage grid area used

Perform dynamic grid compression

Metaverse Research 2 (Data source Optimization)



Metaverse Research 3 (Mixed Reality in AVs)

- ❑ Leveraging edge computing for augmented reality (AR) in autonomous vehicles
- ❑ User-Centric Adaptive Object Detection for Resource-Optimized Mixed Reality in Autonomous Vehicles

User in AV with self-driving capabilities

AV user

User data

Eye tracking

Head movements

Voice commands

AR Computations

Object detection

Eye tracking

Voice commands

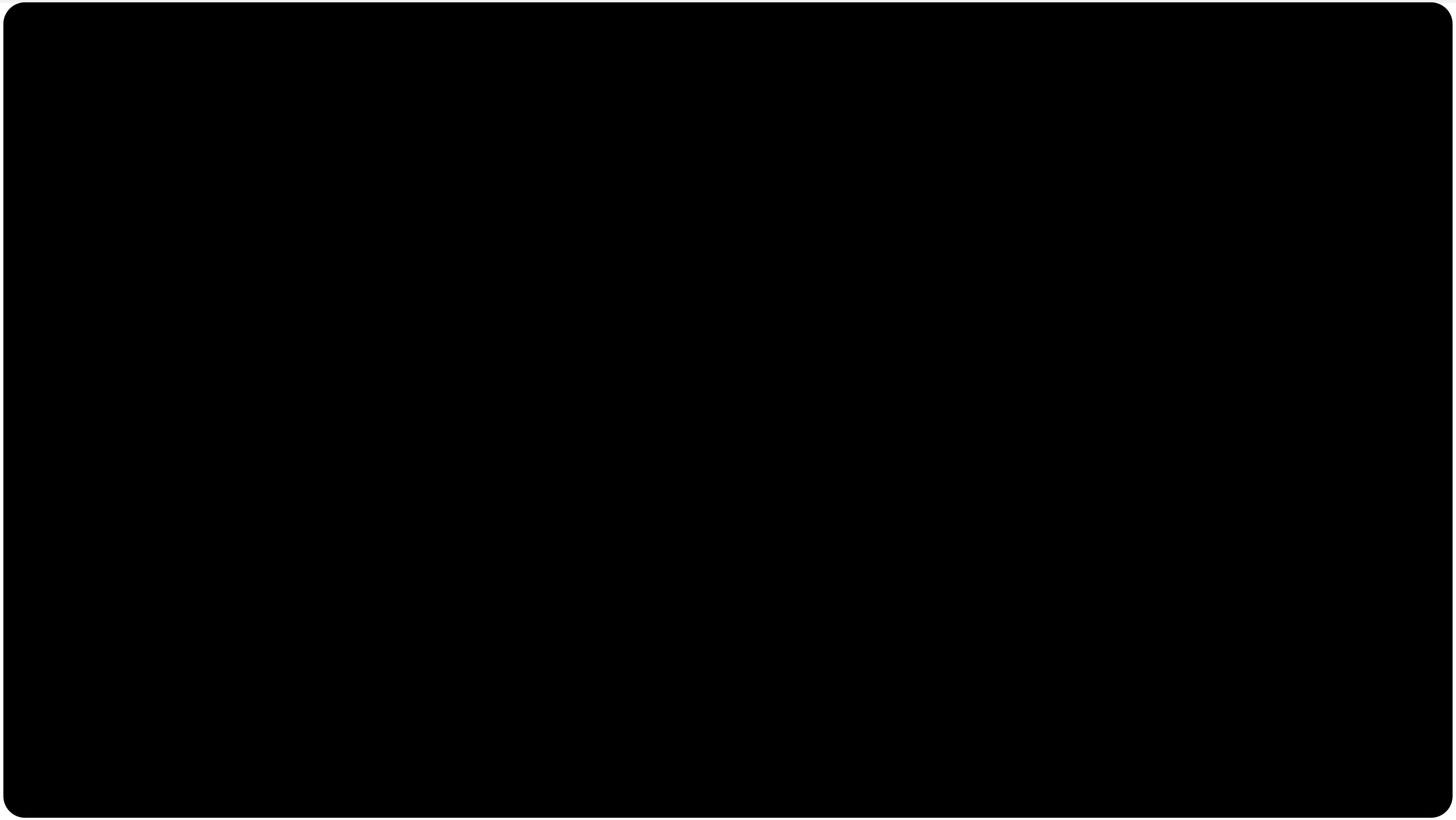
Recommendation ads

Computation Offloading

Edge server

AR headset

Metaverse Research 3 (Mixed Reality in AVs Part 2)



Web 3.0, DEXes, and Metaverse vs Blockchain

Web 3.0
Decentralization, Security and Privacy, Trustless interaction, and Data ownership and control.

DEXes
Intermediary-less, security, transparency, and Global accessibility.

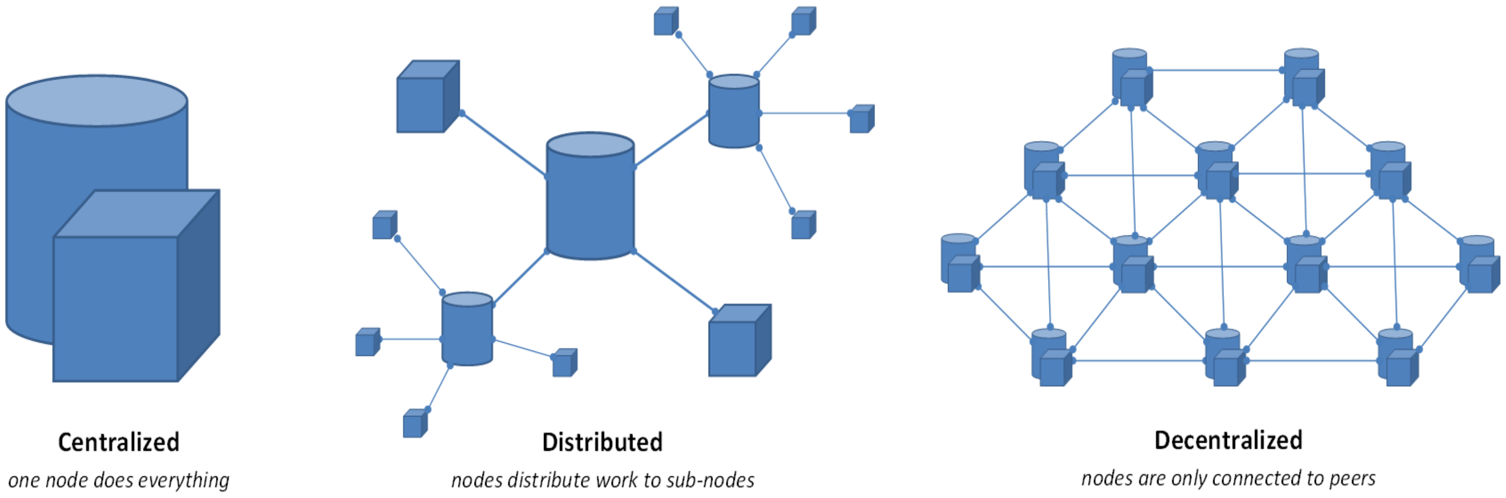
Metaverse
Ownership and Interoperability, Digital Identity, Economy and Transactions, and Governance.

Blockchains

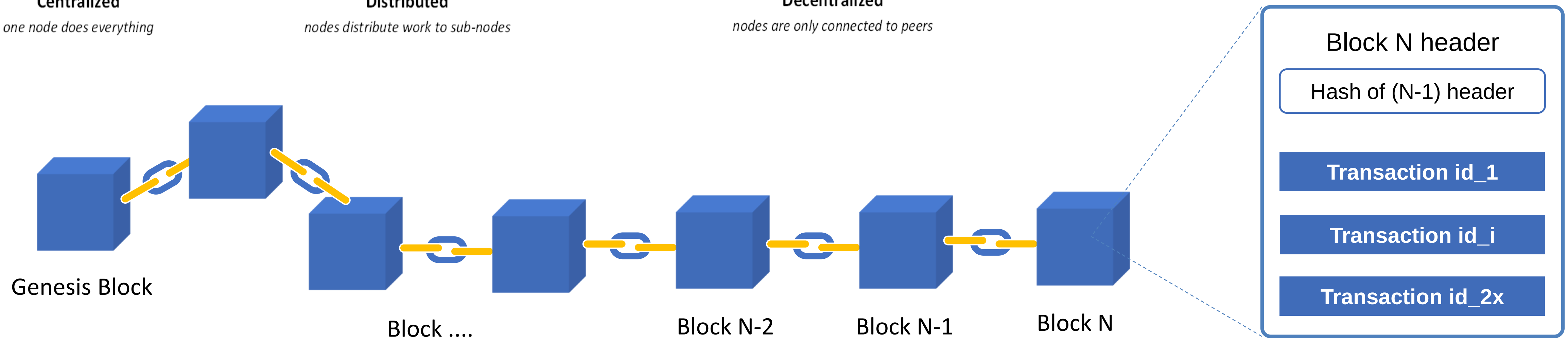
Blockchain technology underpins the infrastructure for **Web 3.0, DEXs, and the metaverse**, providing the mechanisms for **secure, transparent, and decentralized operations**.

Introduction – What is a Blockchain?

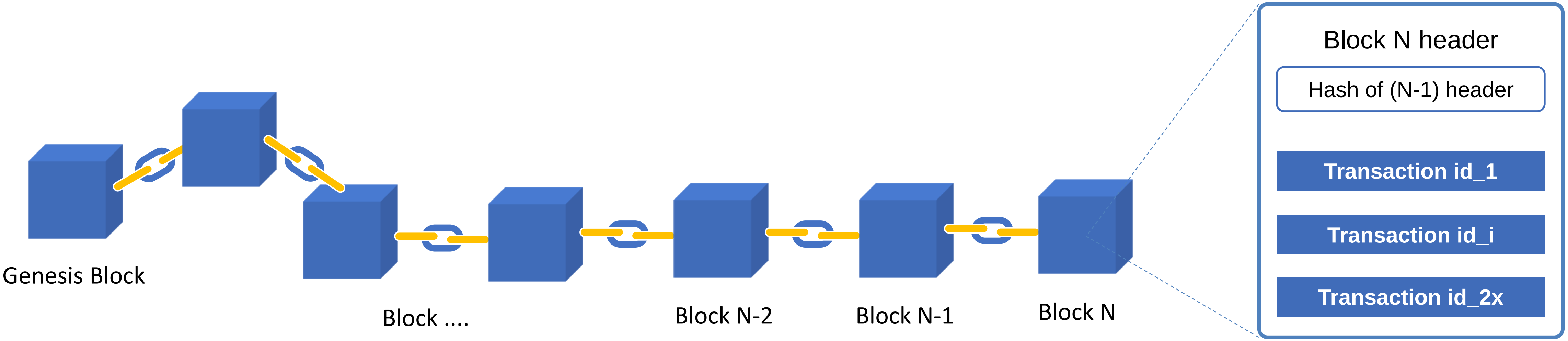
A blockchain is a ***distributed***, ***decentralized***, digital ledger that exists across a peer-to-peer network [1].



Centralized: Traditional banking systems
Distributed: BitTorrent
Decentralized: Bitcoin



Important Properties of Blockchain



Blockchain Properties

1

Decentralized Ledger

2

immutability

3

Transparency

4

Consensus Mechanisms

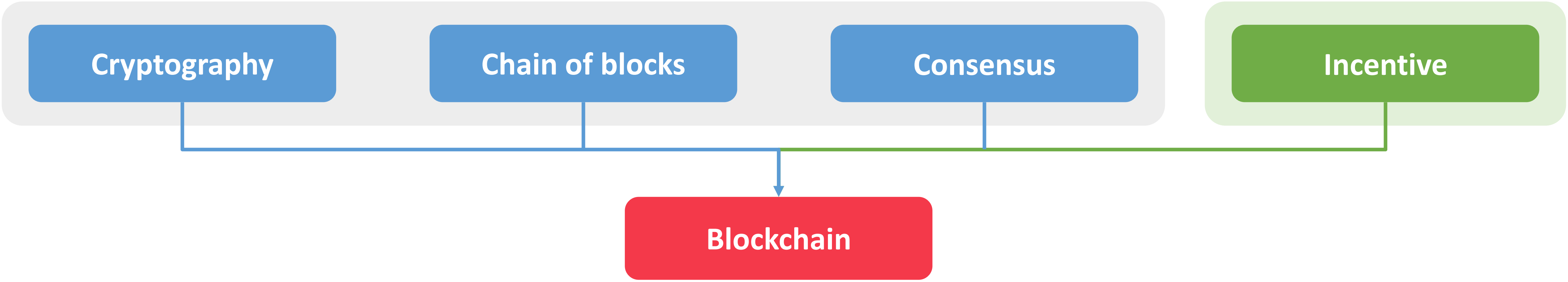
5

Cryptography

6

Smart contracts

Technology Components Of Blockchain



1

- The first camp is from implementation point of view
  - Prevent malicious users
  - Lack of relevant **incentive mechanism** design for the distributed systems

2

- The second camp formulates this issue as:
  - Provide incentive to rational users
  - **Cryptoeconomics**

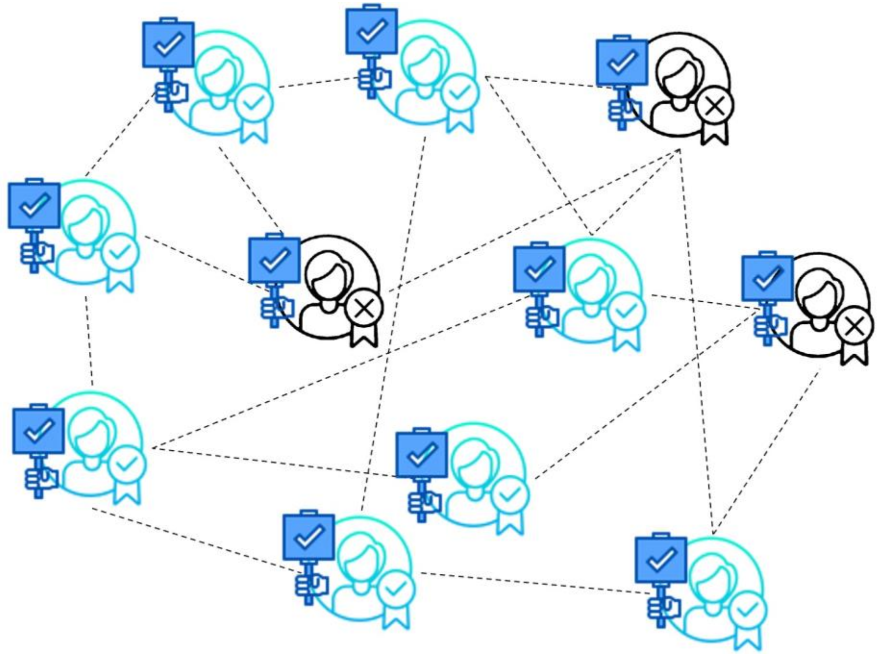
What are Incentive Mechanism Designs?

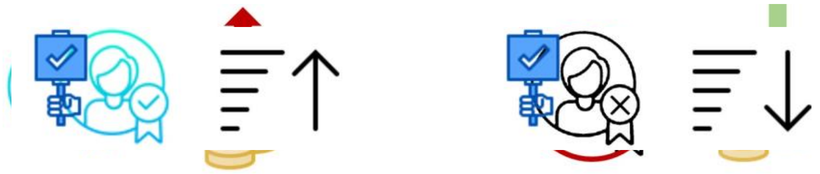
How does the incentives secure a decentralized system?

- ***Rewards***: increase actors' token balances if they do something good
  a) Block reward,
  b) Transaction fee.

- ***Penalties***: reduce actors' token balances if illegal behavior occurs
  a) Security deposits.

- ***Privileges***: incentivize participants by giving them decision-making right
  a) Voting weight.





Incentive Mechanism Design Methods

Auction Theory: Auction theory is a branch of economics that studies the design and behavior of auctions. It involves analyzing the properties of different types of auctions and the strategies used by bidders to acquire goods or services.

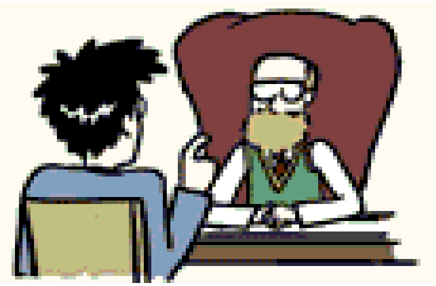
Game Theory: For e.g., coalitional game theory is a branch of game theory that studies the formation and stability of coalitions, or groups of players, in games.

Contract Theory: Contract theory is a branch of economics that studies how contracts can be designed to allocate risks and incentives between parties.

Introduction – Contract Theory

Adverse Selection of PhD Student

The plan you try to find the advisor with financial aid



"I am going to be a professor at a major research university after I graduate."

The real plan

Look for career alternatives

The secret plan

Become a photographer/baker/rock star/writer

Moral Hazard of PhD Student

What my parents think I do

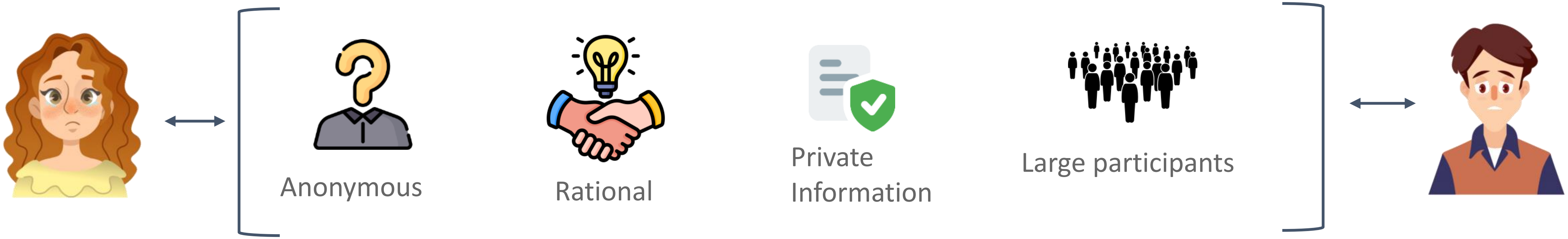
What I actually do when my advisor is present

What my advisor thinks I do

When advisor is on travel

Problem With Incentive Mechanism Designs

- There exists significant **Information Asymmetry** in incentive mechanism designs.



- Contract Theory can overcome the **Information Asymmetry** and benefit **a large number of rational participants.**

1 Incentive Mechanism Design For Mitigating Frontrunning and Transaction Reordering in Decentralized Exchanges

Department of Electrical and Computer Engineering
Cullen College of Engineering

Background

Transaction Frontrunning

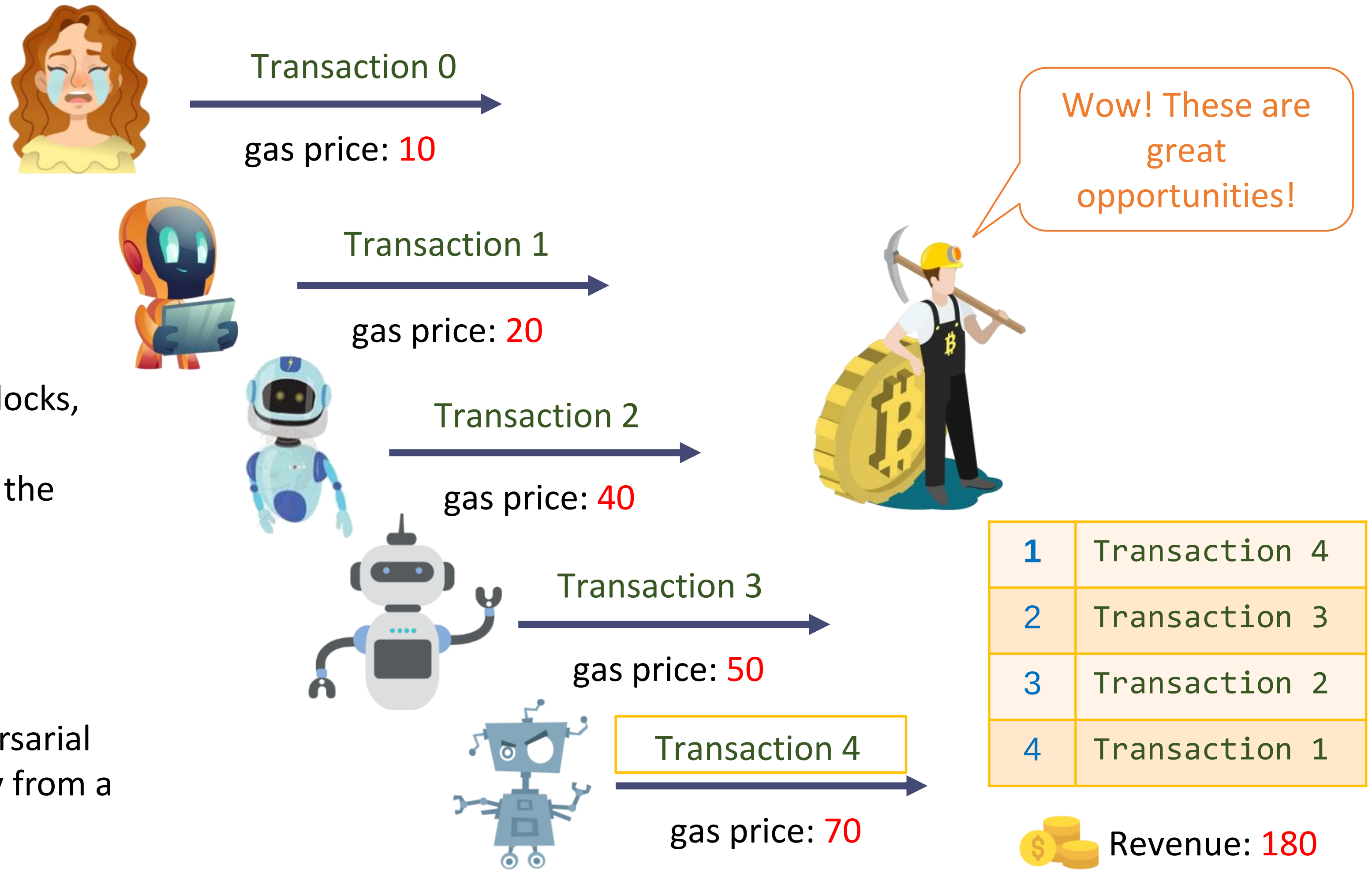
- Miner intercepts and alters a transaction to include a higher fee at the expense of the original sender.

Transaction Reordering?

- Miners selectively order transactions in the blocks, which potentially changes the order in which transactions are processed and confirmed on the blockchain.

Miner Extractable Value (MEV)

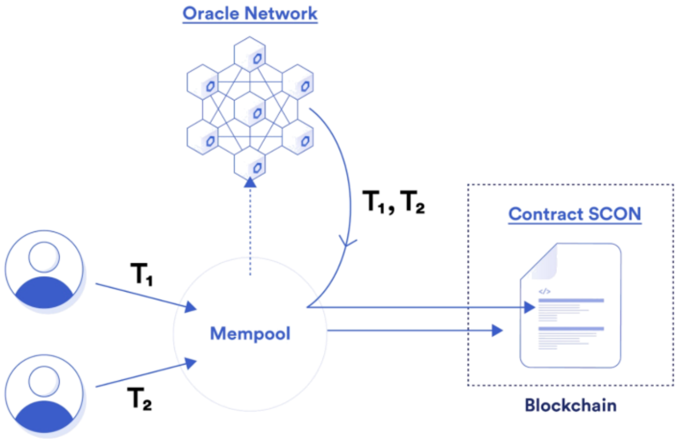
- This include various possibilities of using adversarial ordering optimization (AOO) to extract money from a blockchain smart contract system.



Existing Literature

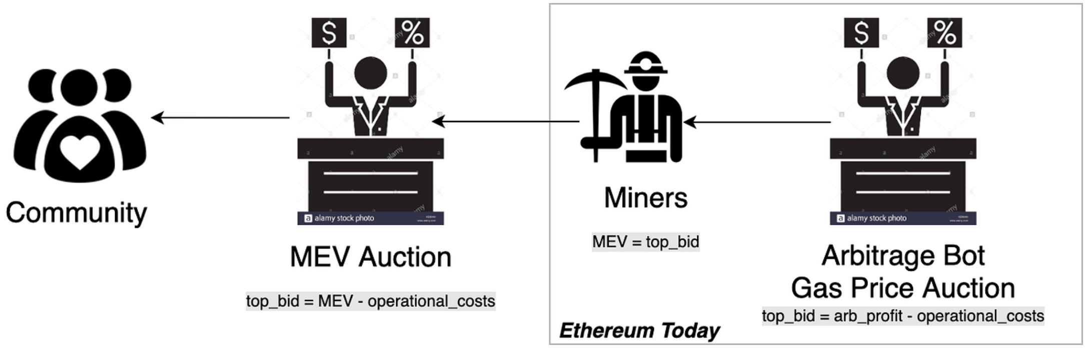
Related Works

1. Chainlink Fair Sequencing Services



Use a decentralized oracle network to fairly order transactions sent to an on-chain smart contract. Basically, **First Come First Service (FCFS)** [FSS]

2. Auction Theory



Simply **auction off the right to reorder transactions** within an N-block window to the highest bidder. [MEV Auctions]

Others

Automated market maker (AMM) to reduce users' costs by leveraging smart contracts (SCs) to alter gas fees upon incoming transaction requests autonomously [A2MM]

[1] FSS: Breidenbach L, et al, Next steps in the evolution of decentralized oracle networks. Chainlink Labs. 2021 Apr 15;1.
[2] MEV Auctions: Piet J, Fairoze J, et al, from the salt mines: Ethereum miners extracting value. arXiv preprint arXiv:2203.15930. 2022 Mar 29.
[3] A2MM: Zhou L, et. al. A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges. arXiv preprint arXiv:2106.07371. 2021 Jun 14.

Motivations and Contributions

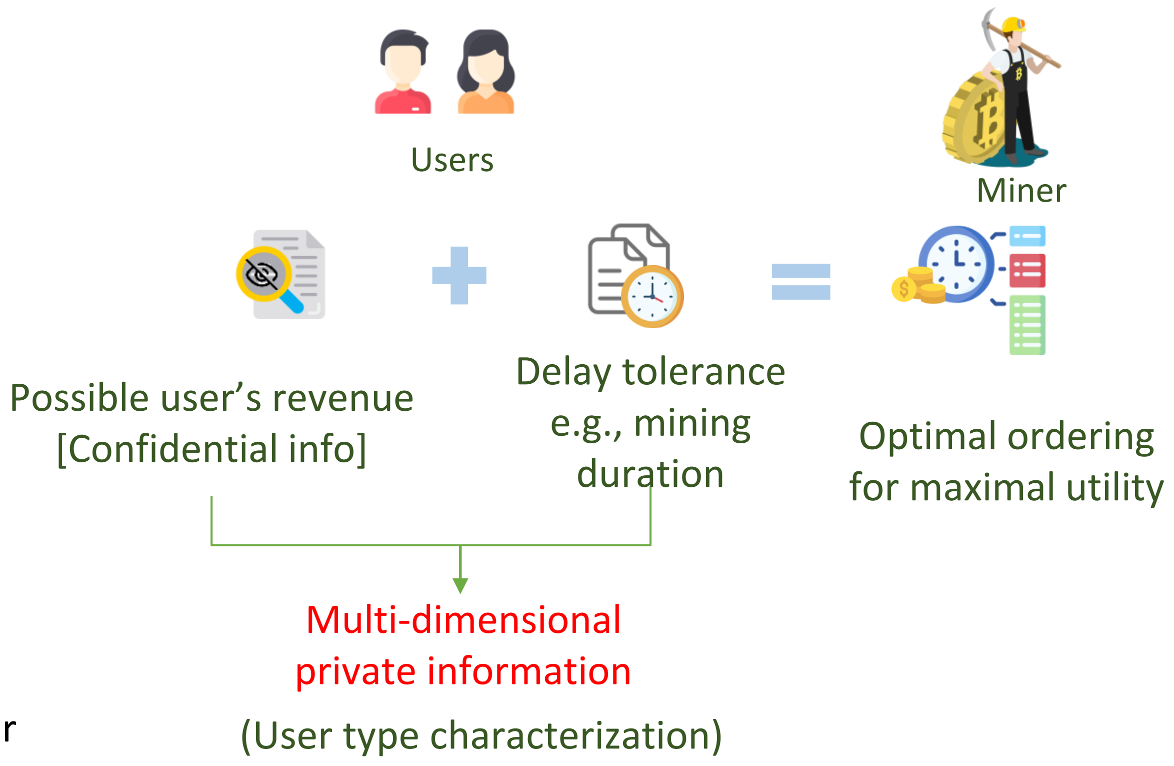
Drawbacks

- However, these existing approaches failed to consider the users **private information (e.g., transaction revenue (confidential)** and **delay tolerance**) in their design.

Motivations-**How should we :**

Prevent MEV centralization, **incentivize honest behaviors** for users with **complex private data**, and **implement multi-dimensional contracts** on the blockchain.

Proposed Mechanism

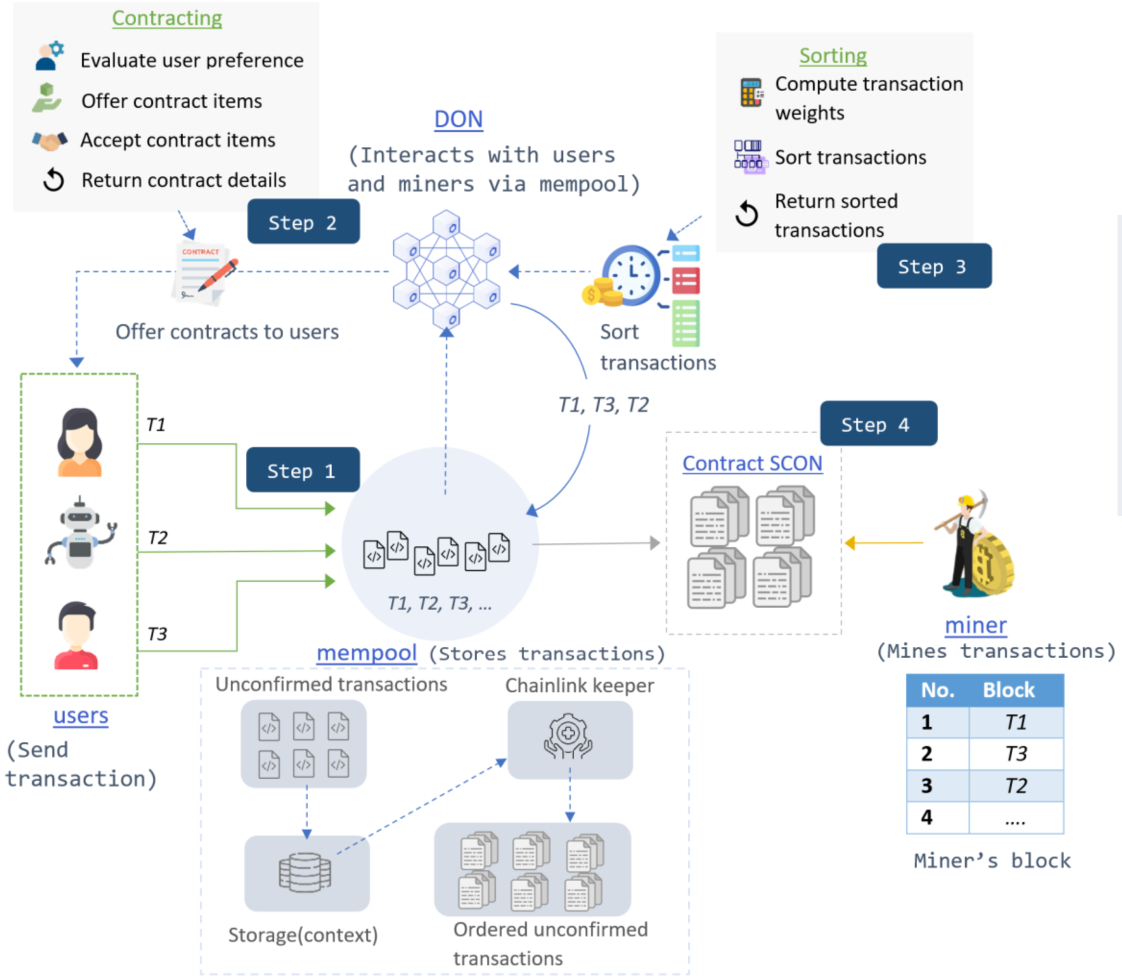


Contributions

1. We design a **weighted transaction ordering mechanism** based on users' multi-dimensional private data.
2. We propose a **multi-dimensional contract design** to extract user private information.

System Model and Utility Model

System Model



Utility Model

- Miner's utility:

$$U_{\varphi_i} = \boxed{\mathbb{1}_{t_i \le t_{max}}}\boxed{r(s_i)} - \boxed{\theta_i}\boxed{\omega(s_i)}$$

Transaction revenue

Transaction workload

Ensures miners process transaction on time.

$$\mathbb{1}_{t_i \le t_{max}} = \begin{cases} 1, & \text{if } t_i \le t_{max}, \\ 0, & \text{if } t_i > t_{max}, \end{cases}$$

Reward paid by users for mining a block

- User's payoff:

$$W_{\varphi_i} = \boxed{V(\theta_i, t_i)} - \boxed{c_i r(s_i)}$$

User's evaluation for transaction based on ***revenue*** and ***delay***

Reward paid to miners for mining with a cost coefficient

Problem Formulation (Contract Design)

Contract Design For Users

- **Complete Information Scenario:** The miner is aware of each user's type, which provides an upper bound of its reward compared with the incomplete information scenario.

- **Incomplete Information Scenario:** The miner does not know the user type but only knows the distribution of user types (e.g., the probability that a user belongs to a particular type).

Complete Information Scenario

$$\max_{t_{max},\varphi} \quad U_{\varphi_i}$$
$$\text{s.t.} \quad \boxed{W_{\varphi_i} \geq 0,} \quad \forall i \in \mathcal{I},$$

Individual Rationality: A contract is individually rational if it provides a non-negative payoff to each type that accepts the contract item designed for its type

Incomplete Information Scenario

$$\max_{t_{max},\varphi} \quad \mathbb{E}\left\{U_{\varphi_i}\right\} = \sum_{i=1}^{N} \mathbb{P}_i(U_{\varphi_i})$$
$$\text{s.t.} \quad \boxed{W_{\varphi_i} \geq 0,} \quad \forall i \in \mathcal{I},$$
$$\boxed{W_{\varphi_i} \geq W_{\varphi_j}},$$
$$\boxed{\begin{array}{l} \varphi_i > \mathbf{0}, \varphi_j > \mathbf{0}, \quad \forall i,j \in \chi; \\ \varphi_k = \mathbf{0}, \quad \forall k \in \mathcal{I} \backslash \chi. \end{array}}$$

Individual Rationality: A contract is individually rational if it provides a non-negative payoff to each type that accepts the contract item designed for its type

Incentive Compatibility: A contract is incentive compatible if it provides the maximal payoff for each type user when he chooses the contract item designed for its type.

Simplified user group sets.

Problem Formulation (Overall System Architecture)

Contract one

$$\max_{t_{max},\varphi} \quad U_{\varphi_i}$$
$$\text{s.t.} \quad W_{\varphi_i} \geq 0, \quad \forall i \in \mathcal{I},$$

Contract two

$$\max_{t_{max},\varphi} \quad \mathbb{E}\{U_{\varphi_i}\}$$
$$= \sum_{i=1}^{N} \mathbb{P}_i(U_{\varphi_i})$$
$$\begin{aligned} \text{s.t.} \quad & W_{\varphi_i} \geq 0, \quad \forall i \in \mathcal{I}, \\ & W_{\varphi_i} \geq W_{\varphi_j}, \\ & \varphi_i > \mathbf{0}, \varphi_j > \mathbf{0}, \quad \forall i, j \in \chi; \\ & \varphi_k = \mathbf{0}, \quad \forall k \in \mathcal{I} \backslash \chi. \end{aligned}$$

Sorting algorithm

Employ counting sort to order transactions for miners

→ Extract user private information

→ Compute the transaction weights to determine their ordering

$$\sigma_i = \frac{t_i \times \theta_i \times \omega(s_i)}{N}$$

Transaction Delay Tolerance

Transaction revenue

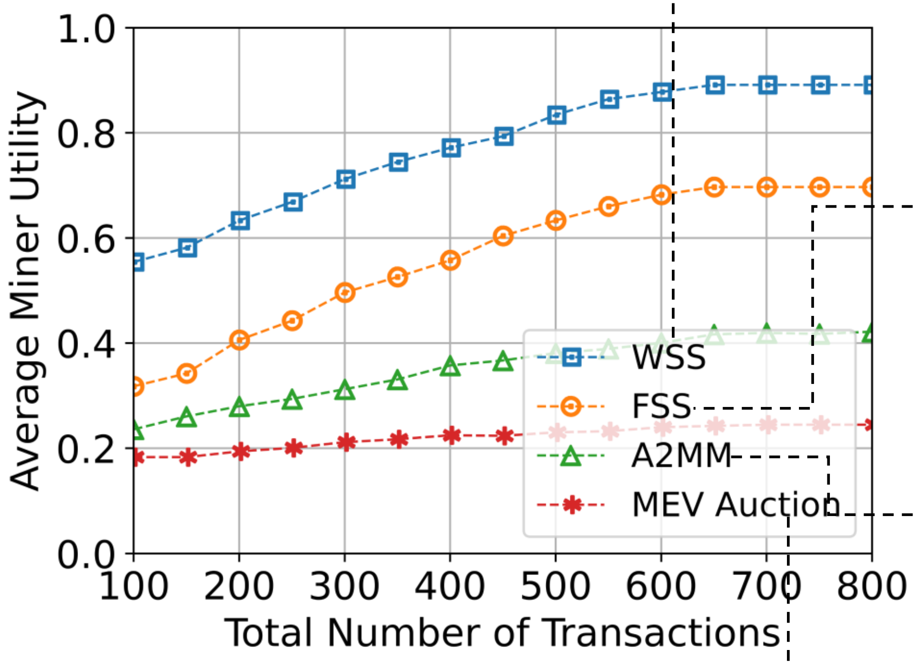
$$\mathcal{P}_1 = (t_i < 0.5 \times \tfrac{1}{4} t_{max}) \cap (\theta_i > \tfrac{1}{N} \textstyle\sum_{i=1}^{N} \theta_i),$$
$$\mathcal{P}_2 = (t_i > 0.5 \times \tfrac{2}{4} t_{max}) \cap (\theta_i > \tfrac{1}{N} \textstyle\sum_{i=1}^{N} \theta_i),$$
$$\mathcal{P}_3 = (t_i < 0.5 \times \tfrac{3}{4} t_{max}) \cap (\theta_i < \tfrac{1}{N} \textstyle\sum_{i=1}^{N} \theta_i),$$
$$\mathcal{P}_4 = (t_i > 0.5 \times t_{max}) \cap (\theta_i < \tfrac{1}{N} \textstyle\sum_{i=1}^{N} \theta_i),$$

→ Integrating the transaction ordering and contracts into one problem set.

$$\max_{t_{max},\varphi} \quad \mathbb{E}\{U_{\varphi_i}\}$$
$$\begin{aligned} \text{s.t.} \quad & W_{\varphi_i} \geq 0, \quad \forall i \in \mathcal{I}, \\ & W_{\varphi_i} \geq W_{\varphi_j}, \quad \forall i, j \in \mathcal{I}, \\ & \varphi_i \geq \mathbf{0}, \varphi_j \geq \mathbf{0}, \quad \forall i, j \in \chi, \\ & \varphi_k = \mathbf{0}, \quad \forall k \in \mathcal{I} \backslash \chi \\ & \sum_{z=1}^{Z} Q_z = \mathcal{Q}, \quad \sum_{z=1}^{Z} \sum_{m=1}^{M} Q_{z,m} = \mathcal{Q}^*. \end{aligned}$$

→ Classifies user's private information based on very high (**VHP**), high (**HP**), medium (**MP**), and low (**LP**) priorities

Average Miner Utility Analysis



Proposed Scheme (WSS):
- Average Utility: 0.7958
- Highest Utility: 0.8913
- Lowest Utility: 0.5815

Fair sequencing services (FSS):
- Average Utility: 0.5891
- Highest Utility: 0.6970
- Lowest Utility: 0.3424

Automated arbitrage market maker (A2MM):
- Average Utility: 0.3647
- Highest Utility: 0.4217
- Lowest Utility: 0.2607

MEV Auctions:
- Average Utility: 0.2252
- Highest Utility: 0.2448
- Lowest Utility: 0.1831

Average Miner Utility Analysis

Average Miner Utility Remarks:

- Increased utility with WSS is due to the contract design, which **tailors** to various **user types** and **delay tolerance**.
- Transaction weighting based on user evaluations post-contract enhances utility in WSS.

Insights and Conclusions:

- WSS improves miner's utility by **78.42%-84.57%** over FSS, A2MM, and MEV Auction.
- WSS advantages come from **multi-dimensional** contracts and optimal strategy deployment.

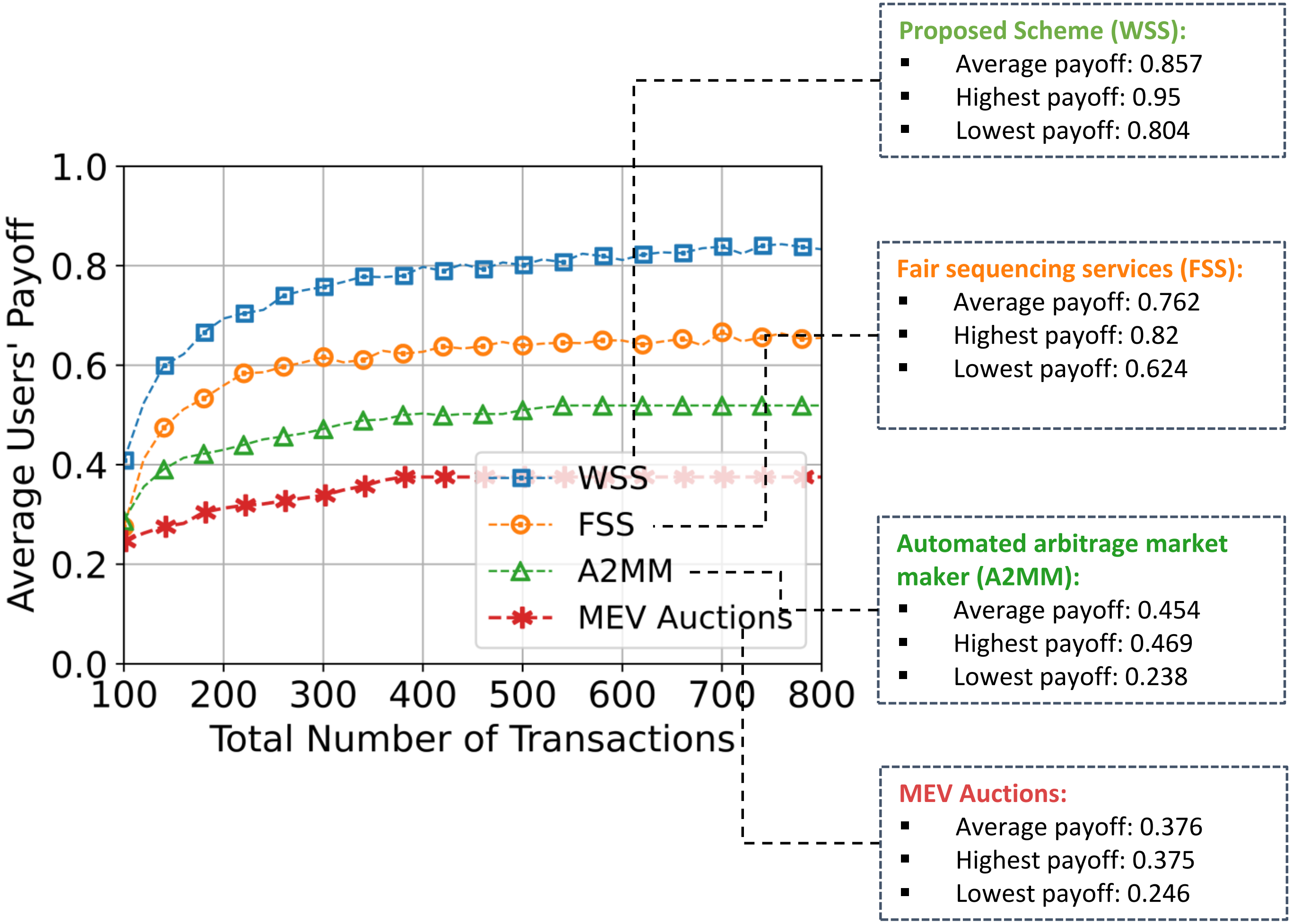
Average User Payoff Analysis

Average User Payoff Remarks:

- WSS scheme achieves up to **64.47% cost reduction** compared to other schemes.
- Users' payoff is influenced by **workload evaluation** and transaction **cost**.
- WSS ensures efficient **profit extraction** for miners without increasing transaction fees.

Insights and Conclusions:

- WSS provides **higher user payoffs** through efficient pricing and **transaction ordering**.
- Users benefit from guaranteed transaction inclusion and reduced fees.



Average User Payoff Analysis

Summary of work I

Core Summary

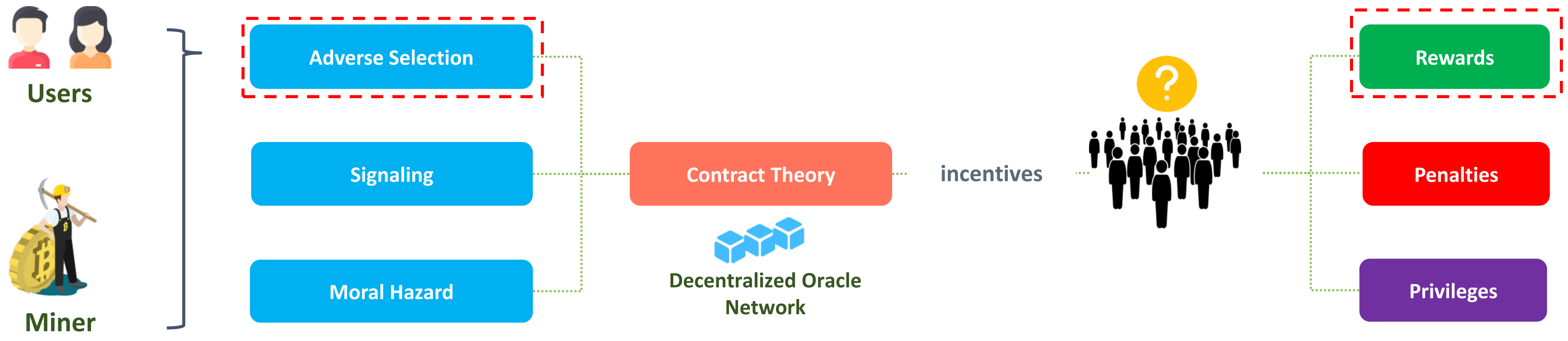
- Use contract theory to elicit users' private information
- Utilize users' private information to compute the weights of transactions for ordering by the miner
- Employ weighted counting sort algorithm to sort transactions for miners to process

Focus:

Entities: Users, Miner, and Decentralized Oracle Network (DON)

Contract Design: Adverse selection

Incentive: Rewards



2 Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse through Diversified Incentive Mechanism Design

Department of Electrical and Computer Engineering
Cullen College of Engineering

Background (Types of Blockchain Nodes)

Full nodes:

- The most standard type of node is a full node.
- Full nodes store all blockchain data on disk and verify the network's rules, including block validation, transaction verification, and data service.

Req: 120GB+ of storage and 8GB+ of memory.

Price: aveg $20/mo [1]

~~$153,000/annual [2].~~

$300/mo [3].

$49.25/mo [4]

$35.00/mo [5]

AWS pricing: $0.15/hr | $999.00 /mo [6]

Archival nodes

- An archival node could be described as a full node with a massive amount of cached historical data but does not provide any more validation or security than a full node.

Light nodes:

- light clients provide high security and low computing power for resource-constrained devices, making blockchain networks more accessible.

Req: 100MB+ of storage and 128–512MB of memory [7].

Motivations and Contributions

Effects of decreasing number of full nodes

Scalability: smaller number of full nodes leads to scalability problems as there are not enough nodes available.

Poor QoS: poor quality of service to users as the limited nodes control the mining.

Centralization: centralization of nodes due to very few nodes available.

Sub-optimal prioritization: platform may have to make sub-optimal decisions.

Research Questions

1. How should **users with information asymmetry levels be incentivized** to share resources for the long-term sustainability of the blockchain?

2. How can the blockchain network **balance the need to incentivize users** with the limited resources available for funding incentives?

Contributions

1. We propose a novel **incentive mechanism addressing** “adverse selection" and “moral hazard" problems.

2. We propose a **diversified reward scheme** for funding user incentives.

System Architecture & Utility Model

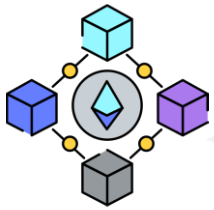
System Architecture

Adverse selection

Does not know the blockchain node implementation of users.

Adverse selection

Does not know the capability of users, e.g., making profit, etc.



Ethereum network

Does not know how much effort users exert in node types.

Moral hazard

Utility Model

Probability of user generating significant revenue

$$U_{EN} = \sum_{i=1}^{I} \lambda_i [q_i + \theta_i \xi_i r(\xi_i)] - r(\xi_i),$$
$$= \lambda[q_H + \theta_H \xi_H r(\xi_H)] - r(\xi_H)$$
$$+ (1-\lambda)[q_L + \theta_L \xi_L r(\xi_L)] - r(\xi_L),$$

Platform payment to EN

Reward paid users

Revenue generated

$$U_{EU} = \sum_{i=1}^{I} \theta_i \xi_i [\gamma_i + r(\xi_i)] - q_i - \xi_i.$$

User’s cost as payments and efforts

$\theta \in \{\theta_L, \theta_H\}$ revenue-generating capabilities of users e.g., low and high

Problem Formulation (Contract Design)

Problem 1 (EN's utility maximization problem):

$$
\begin{aligned}
\max_{q_i, r(\xi_i)} \quad & \lambda[q_H + \theta_H \xi_H r(\xi_H)] - r(\xi_H) \\
& + (1-\lambda)[q_L + \theta_L \xi_L r(\xi_L)] - r(\xi_L), \\
& \theta_i \xi_i [\gamma_i + r(\xi_i)] - q_i - \xi_i \geq \theta_i \xi_j [\gamma_j + r(\xi_j)] - q_j - \xi_j, \\
& \theta_i \xi_i [\gamma_i + r(\xi_i)] - q_i - \xi_i \geq 0, \\
& 0 \leq r(\xi_1) < \cdots < r(\xi_i) < \cdots < r(\xi_I), \\
& \forall j \neq i.
\end{aligned}
$$

EN utility function

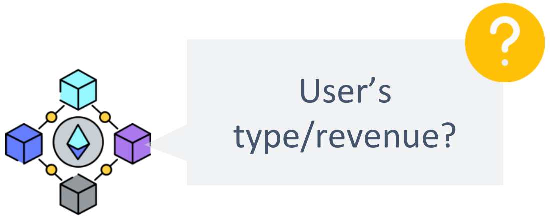
Incentive Compatibility

Individual Rationality

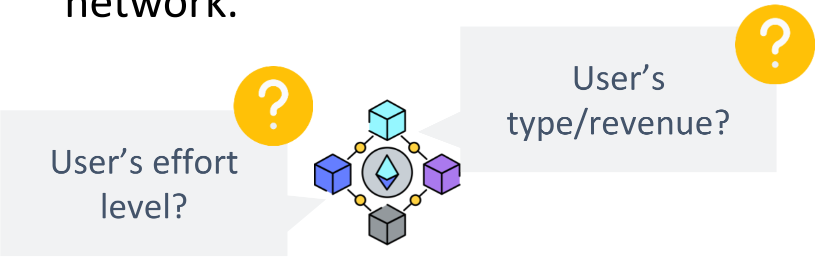
Monotonicity constraints

1. **Moral Hazard Scenario:** EN is unaware of user effort, equating it to operating cost.

2. **Adverse Selection Scenario:** Users generate revenue on the EN platform, but EN is unaware of their profitability likelihood.



3. **Both Scenarios:** We tackle a combined scenario of both adverse selection and moral hazard, reflecting the current blockchain network.



Problem Formulation (Contract Design) Contd.

1 **Moral Hazard Only**

$$\max_{q_i, r(\xi_i)} \quad q_i - r(\xi_i) + \frac{1}{2}\theta_i^2[\gamma_i - r(\xi_i)],$$
$$\frac{1}{2}[\theta_i(\gamma_i - r(\xi_i))]^2 - q_i - \xi_i \geq 0,$$
$$0 \leq r(\xi_1) < \cdots < r(\xi_i) < \cdots < r(\xi_I),$$
$$\forall j \neq i.$$

2 **Adverse Selection Only**

$$\max_{q_i, r(\xi)} \quad \lambda[q_H + \theta_H \xi r(\xi)] - r(\xi_H)$$
$$+ (1-\lambda)[q_L + \theta_L \xi r(\xi)] - r(\xi_L),$$
$$\theta_i \xi[\gamma_i + r(\xi)] - q_i - \xi_i \geq \theta_i \xi[\gamma_j + r(\xi)] - q_j - \xi_j,$$
$$\theta_i \xi[\gamma_i + r(\xi)] - q_i - \xi_i \geq 0,$$
$$0 \leq r(\xi_1) < \cdots < r(\xi_i) < \cdots < r(\xi_I),$$
$$\forall j \neq i.$$

3 **Both Adverse Selection and Moral Hazard**

$$\max_{q_i, r(\xi_i)} \quad \lambda[q_H - r(\xi_H) + \frac{1}{2}\theta_H^2(\gamma_H - r(\xi_H))]$$
$$+ (1-\lambda)[q_L - r(\xi_L) + \frac{1}{2}\theta_L^2(\gamma_L - r(\xi_L))],$$
$$\frac{1}{2}[\theta_i(\gamma_i - r(\xi_i))]^2 - q_i \geq \frac{1}{2}[\theta_j(\gamma_j - r(\xi_j))]^2 - q_j,$$
$$\frac{1}{2}[\theta_i(\gamma_i - r(\xi_i))]^2 - q_i \geq 0,$$
$$0 \leq r(\xi_1) < \cdots < r(\xi_i) < \cdots < r(\xi_I),$$
$$\forall j \neq i.$$

Moral Hazard Scenario Only:

1. Rewards based on outcomes to motivate effort.
2. Risk of overpaying due to unknown user potential.

Adverse Selection Scenario Only:

1. Pays users based on inherent abilities.
2. Ensures only high-capability users participate.

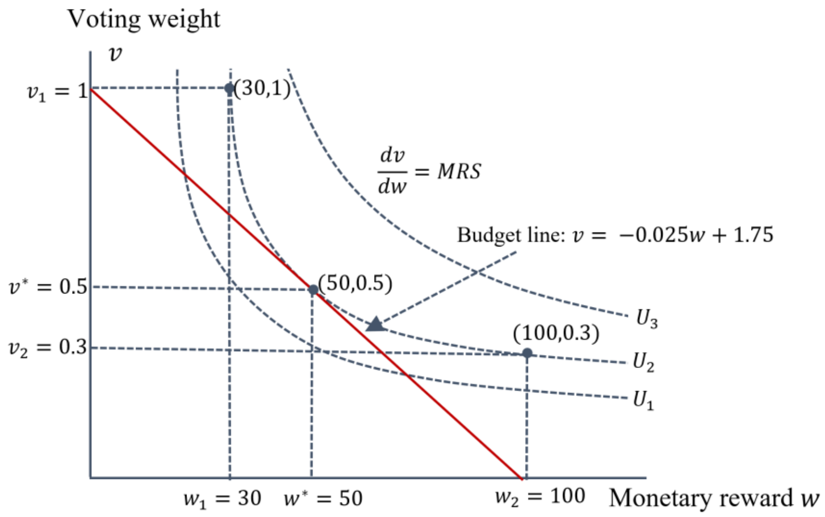
Both Scenarios:

1. Rewards balance both effort and capability.
2. Payment system prevents over-/under-compensation.
3. Aligns user potential with actual outcomes.

Problem Formulation 2 (Diversifying Incentives)

Voting points reward system for **high-capacity users** and **monetary rewards** for **low-capacity users**.

For example:



Runs node implementations — Voting points rewards

$$v_i = \frac{r(\xi_i)}{\sum_{i=1}^{I_v} r(\xi_i)} \times \bar{v},$$

Only uses full node or blockchain — Monetary rewards

$$w_i = \frac{r(\xi_i)}{\sum_{i=1}^{I_w} r(\xi_i)} \times \bar{w},$$

Indifference Curve

An indifference curve (or, in several dimensions, an indifference surface) represents a **collection of consumption bundles** towards which a person is **indifferent**. In other words, all bundles offer the **same amount** of benefit.

Marginal Rate of Substitution (MRS)

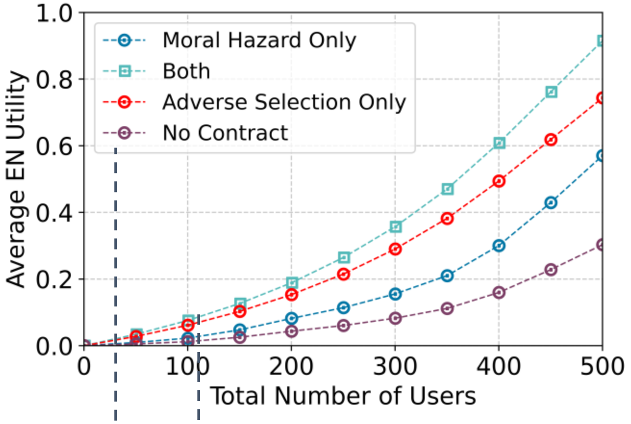
At a given position, the marginal rate of substitution (MRS) is defined as the *U1* indifference curve's negative slope. That is,

$$MRS = -\frac{dv}{dw}\Big|_{U=U_1}$$

where the notation specifies that the slope should be determined along the U1 indifference curve.

Ethereum network Utility & User Payoff Analysis

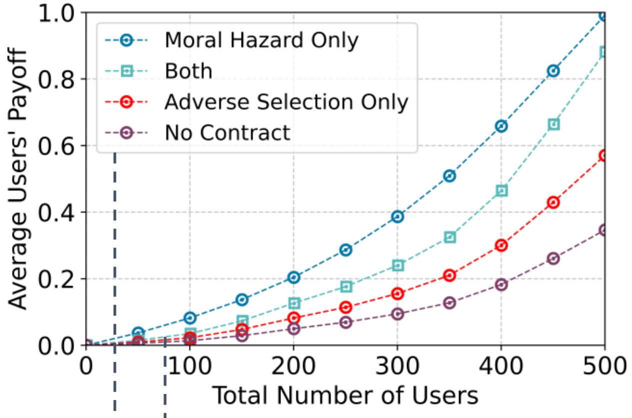
Ethereum Network



- Highest: 0.7437
- Both-> Adverse Selection -> Moral Hazard -> No Contract

- Moral Hazard: 0.3245
- Both: 0.5155
- Adverse Selection: 0.3866
- No Contract: 0.1863

Users' Payoff



- Highest: 0.7437
- Moral Hazard -> Both -> Adverse Selection -> No Contract

- Moral Hazard: 0.4158
- Both: 0.4502
- Adverse Selection: 0.4198
- No Contract: 0.3419

EN Utility & User payoff Remarks:

- Both moral hazard and adverse selection yields a **33.33%-58.33%** increase in EN's utility.
- Users' payoff is enhanced by **7.25%-31.71%** but Moral hazard outperforms proposed scheme.

Analysis Insights and Conclusions:

- Both moral hazard and adverse selection significantly enhances the EN utility and users' payoff.
- Reward diversification enhances EN utility and users' payoff.

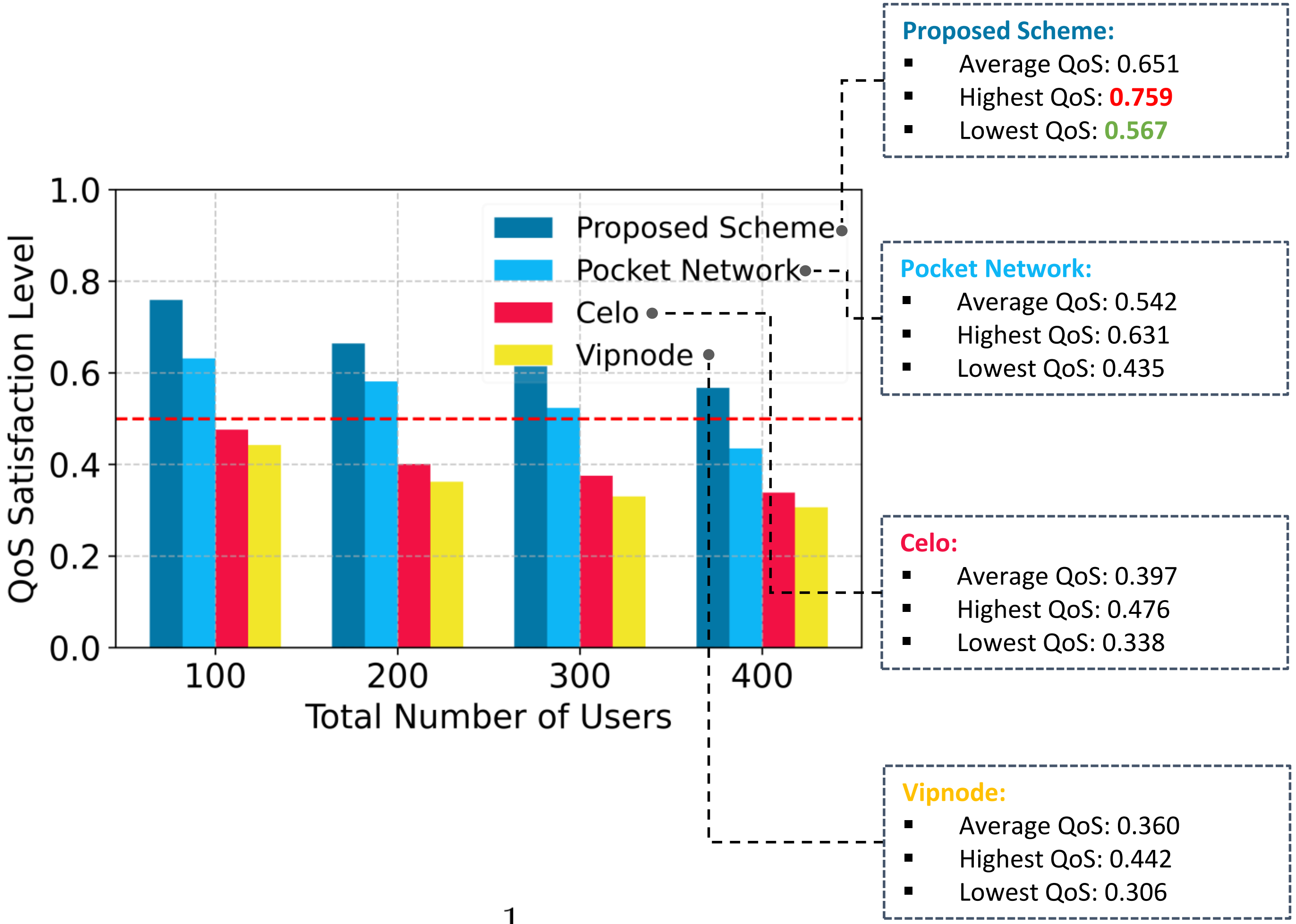
QoS Satisfaction Analysis

Average QoS Remarks:

- QoS satisfaction in our proposed scheme exhibits approximately **19.87%**, **63.72%**, and **80.62%** increases compared to Pocket Network, Celo, and Vipnode.

Insights and Conclusions:

- Our mechanism significantly **enhances QoS satisfaction** by considering **user characterizations** and offering **diversified incentives**.
- In contrast, other schemes lack such **user-centric designs**, resulting in lower QoS satisfaction levels.



$$\beta_i = \frac{1}{1 + e^{-\mu} \times U_{EU}(i)},$$

QoS Satisfaction Analysis

Summary of work II

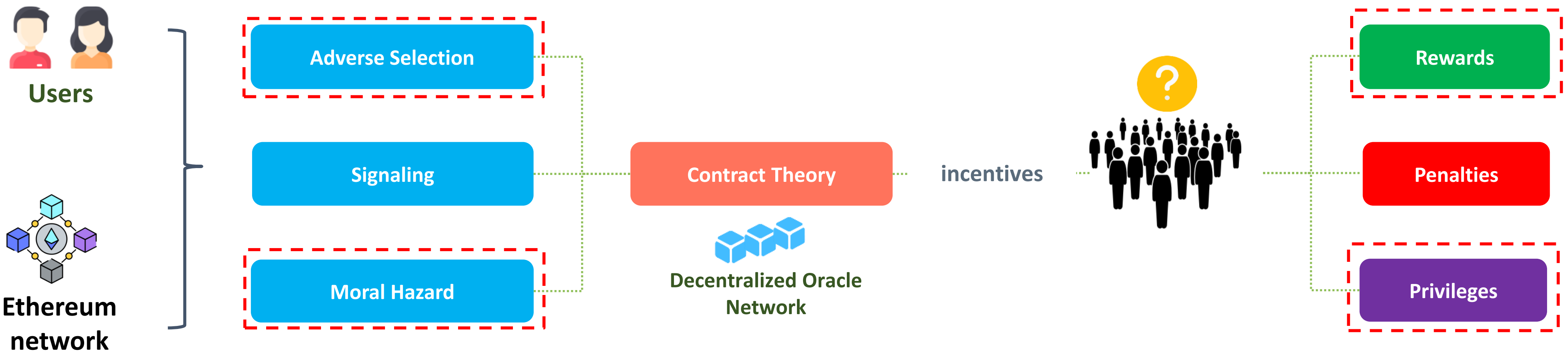
- Proposed **incentive mechanism** addresses **high expenses** in developing **full nodes** for **blockchain sustainability**.
- Utilized adverse selection and moral hazard in analysis.
- Diversified incentives with **voting points** for **high-capability** users and **monetary rewards** for **low-capability users**.

Focus:

Entities: Users and Ethereum Network

Contract Design: Adverse selection and Moral Hazard

Incentive: Rewards and Privileges



A Contract-Stackelberg Framework for Mitigating Timing Games in Proof-of-Stake Blockchain Networks

Background of Timing Games 1

1. Validators staking some of their coins to get selected for adding a new block of transactions

Dan

Alice

Bob

2. Coins at "STAKE" in as guaranteed account

3. Function that randomly picks a validator

4. Bob got selected to add a block to the blockchain network

Bob

5. New block is validated by validators

Valid

Bob adds new block and receives network fee as a reward

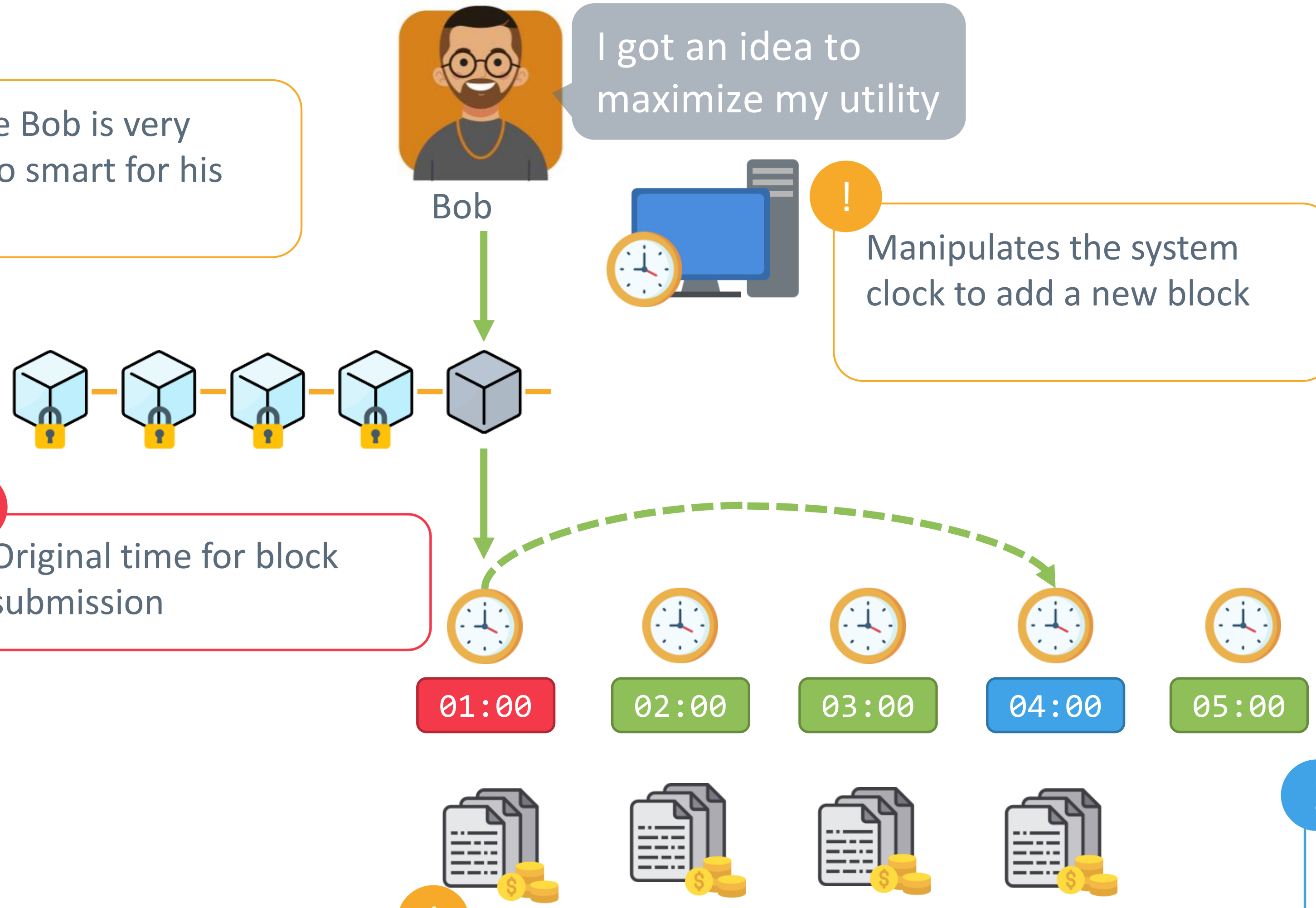
Invalid

Bob loses his staked coins to the network

Background of Timing Games 2

Now

Now, assume Bob is very greedy or too smart for his own good



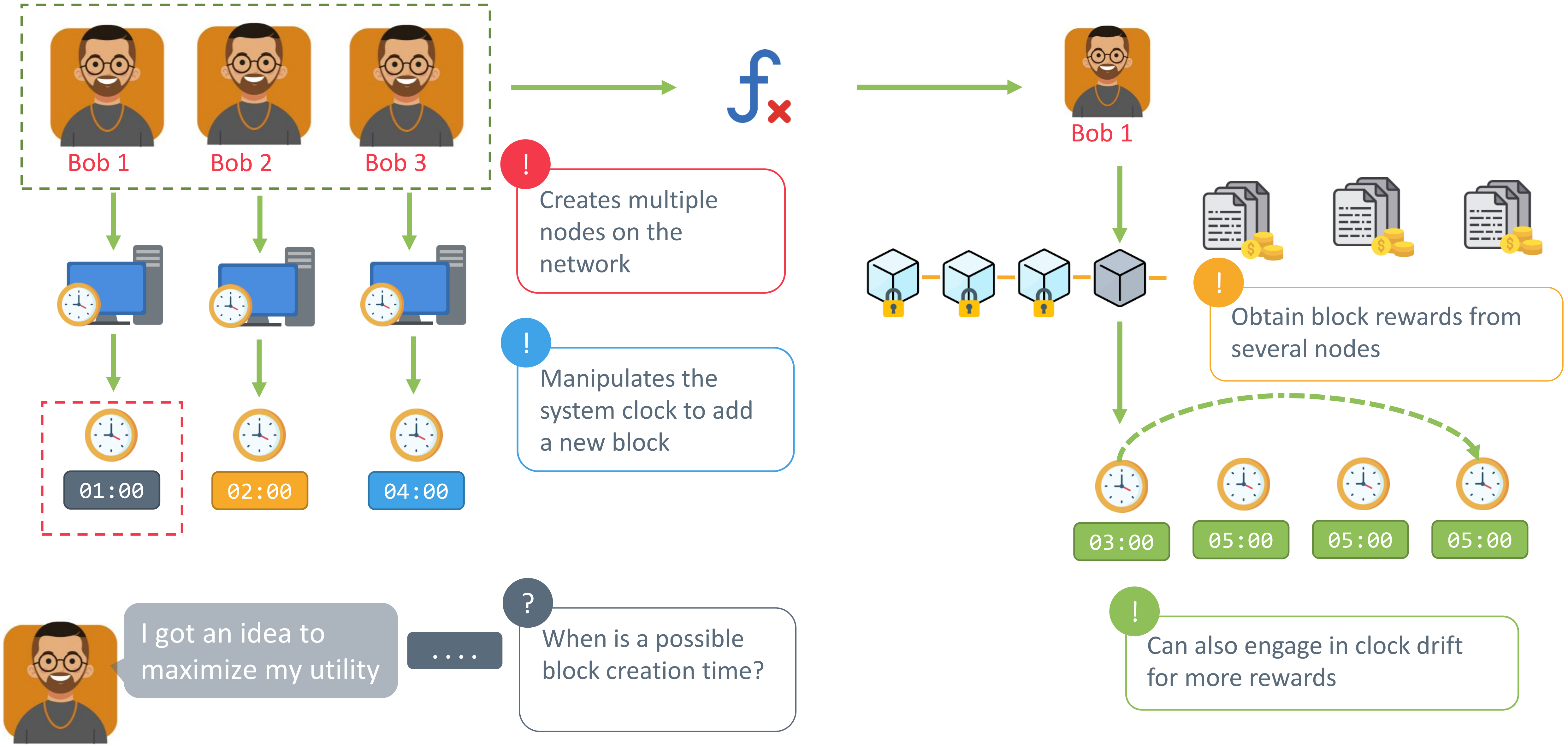
Manipulates the system clock to add a new block

Original time for block submission

New adjusted time for block submission

Accumulates transactions from the various timestamps

Background of Timing Games 3



Motivation and Problem Statement

Motivations

1. How can validators' strategic behaviors in timing games be effectively modeled?

2. How can the blockchain network effectively discourage timing manipulations without compromising network operations?

Challenges

1. Conflicting interests between validators and the blockchain network.

2. The dynamic nature of blockchain operations makes a one-size-fits-all difficult.

Proposed Solution

- We propose a Contract-Stackelberg Framework for holistic mitigation of timing games in PoS network.

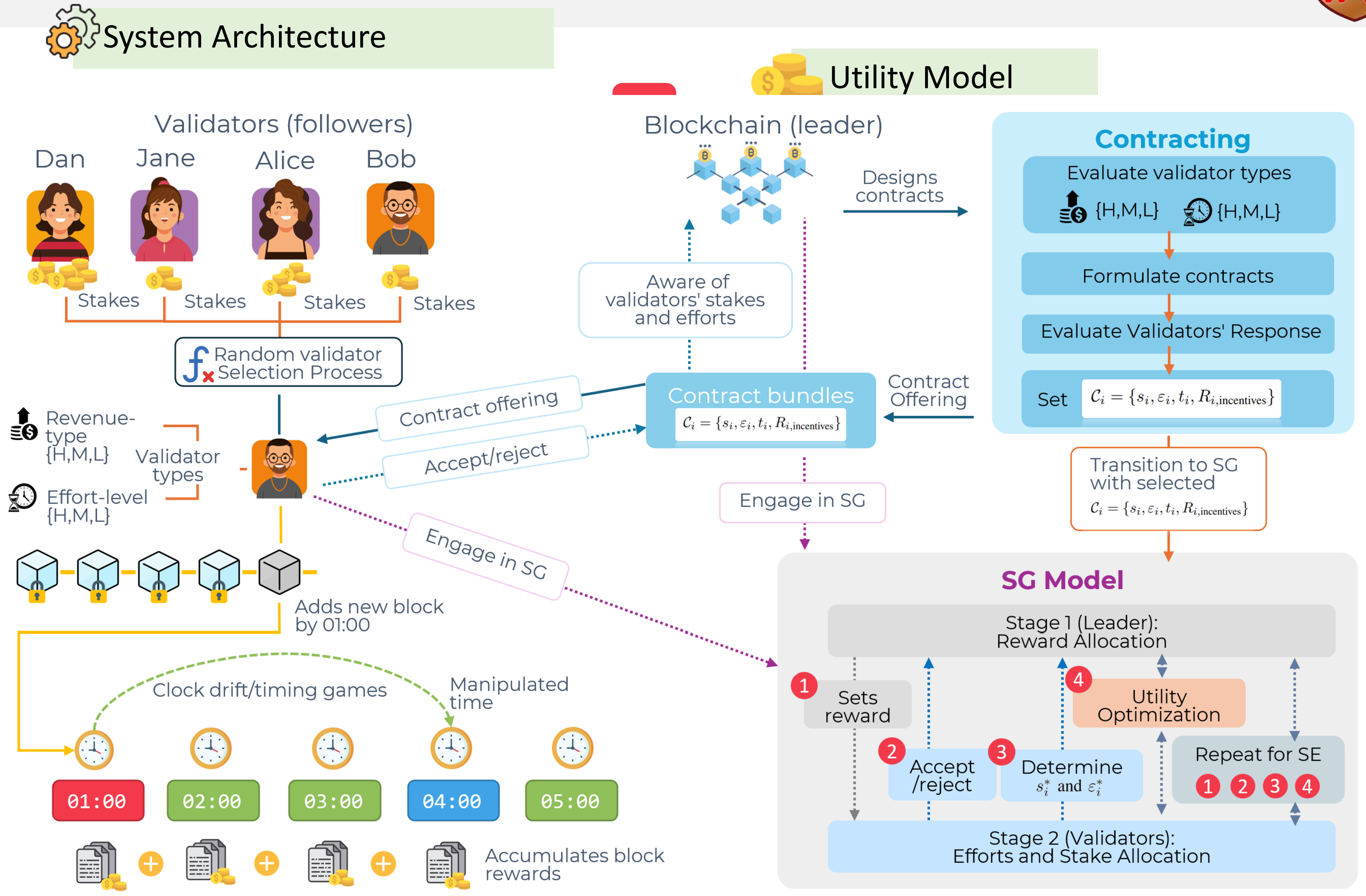
Contributions

1. **Validator Categorization**: Mitigates adverse selection and moral hazard by categorizing validators based on revenue potential.

2. **Asymmetric Contract Design**: Enhances incentives by accounting for information asymmetries between the network and validators.

3. **Stackelberg Game Alignment**: Aligns validators' incentives with network goals to minimize timing game tactics.

System Architecture & Utility Model



Problem Formulation (Contract Design)

$$
\begin{aligned}
\max_{\mathcal{C}_i} \quad & U_{SW} = W + \sum_{i=1}^{I} U_i \\
\text{subject to} \quad & U_i(s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq 0, \\
& U_i(s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq U_j(s_i, \varepsilon_i, t_i, R_{j,\text{incentives}}), \\
& 0 \leq R_{1,\text{incentives}} < \cdots < R_{i,\text{incentives}} < \cdots < R_{I,\text{incentives}}
\end{aligned}
$$

Social Welfare

Individual Rationality

Incentive Compatibility

Monotonicity constraints

1. **Optimal s_i^* and ε_i^* :** validators should align their stakes and efforts for maximal SW as follows:

$$\boxed{s_i^* = \frac{\theta_i \varepsilon_i}{1 + \lambda_i \varepsilon_i^{\sigma}} \qquad \varepsilon_i^* = \frac{c + 2\theta_i s_i}{\lambda_i \theta_i - \mu_{ij} \theta_i}}$$

2. **Optimal incentive:** time-constraint, rely on the user type, effort level, and stakes.

$$\boxed{R^*_{i,\text{incentives}} = \frac{\mu_{ij} \mathbb{1}_{t_i \leq t_{\max}} \theta_i s_i - \gamma}{p_i + \mathbb{1}_{t_i \leq t_{\max}} \lambda_i \varepsilon_i}}$$

3. **Time allocation:** blockchain should set time for block validation based on validators' type.

$$\boxed{t_i^* = \frac{\sum_{i,j} \mu_{ij} \theta_i}{\sum_i \lambda_i \theta_i}}$$

Problem Formulation (Stackelberg Game)

1 **Stage 1: Leader's problem (Reward Imposition)**

$$\begin{aligned} \underset{R_{i,\text{incentives}}}{\text{maximize}} \quad & W(R_{i,\text{incentives}}), \\ \text{subject to} \quad & U_i(s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq 0, \\ & U_i(s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq U_j(s_i, \varepsilon_i, t_i, R_{j,\text{incentives}}), \\ & 0 \leq R_{1,\text{incentives}} < \cdots < R_{i,\text{incentives}} < \cdots < R_{i,\text{incentives}} \end{aligned}$$

2 **Stage 2: Followers' Problem (Stake and Effort allocation)**

$$U_i = \begin{cases} \mathbb{1}_{t_i \leq t_{\max}} \theta_i \varepsilon_i R_{i,\text{incentives}} - \frac{c}{2}\varepsilon_i^2 \\ - \alpha s_i \times \frac{1}{1+\varepsilon_i^{\sigma}}, \quad \text{if } A_i = 1 \text{ (contract accepted)}, \\ 0, \quad \text{if } A_i = 0 \text{ (contract rejected)}. \end{cases}$$

$$\begin{aligned} \underset{A_i, s_i, \varepsilon_i}{\text{maximize}} \quad & U_i(A_i, s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \\ \text{subject to} \quad & U_i(A_i, s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq 0, \\ & U_i(A_i, s_i, \varepsilon_i, t_i, R_{i,\text{incentives}}) \geq U_j(A_i, s_i, \varepsilon_i, t_i, R_{j,\text{incentives}}), \\ & 0 \leq R_{1,\text{incentives}} < \cdots < R_{i,\text{incentives}} < \cdots < R_{I,\text{incentives}}, \\ & s_{i,\min} \leq s_i \leq s_{i,\max}, \quad \varepsilon_{i,\min} \leq \varepsilon_i \leq \varepsilon_{i,\max}, \\ & |\varepsilon_i - \bar{\varepsilon}_i| \leq \delta_\varepsilon, \quad t_i \leq t_{\max}, \quad \sum_{i=1}^{I} s_i \leq S_{\max}, \end{aligned}$$

Strategic Equilibrium:

1. SG converges to SE where leader optimizes utility, followers adjust strategies.
2. Ensures stability, robustness in contract design.

Leader-Follower Dynamics:

1. Leader sets contracts, followers respond strategically.
2. Reflects rational behavior, hierarchical interactions.

Emergent Patterns:

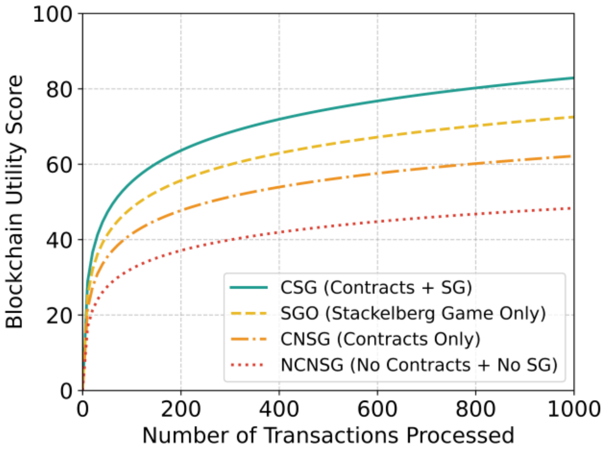
1. Validators exhibit cooperative, competitive strategies.

Takeaways:

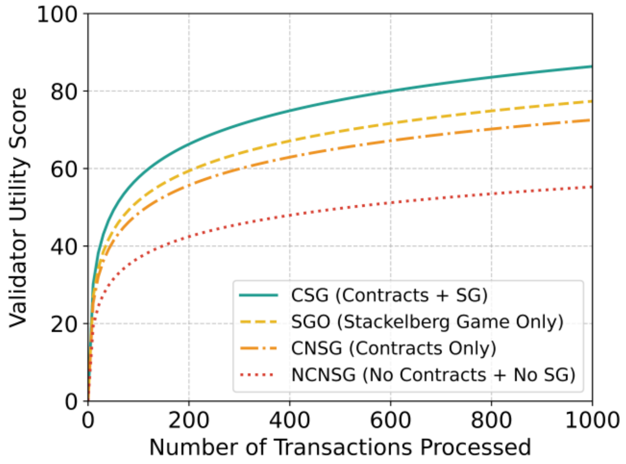
1. SE analysis guides stable, strategic contract design.
2. Critical for sustainable growth in blockchain networks.

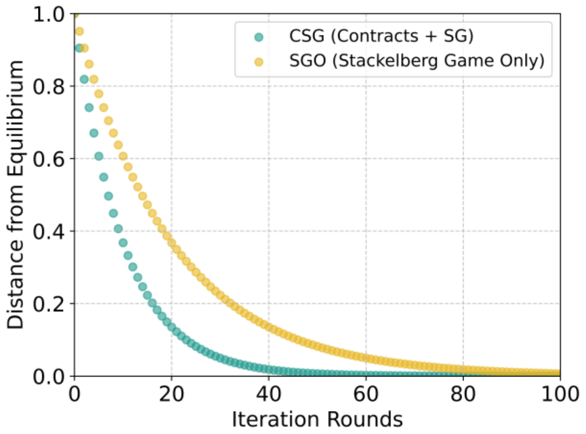
Experiment Results And Analysis

1. Blockchain Utility

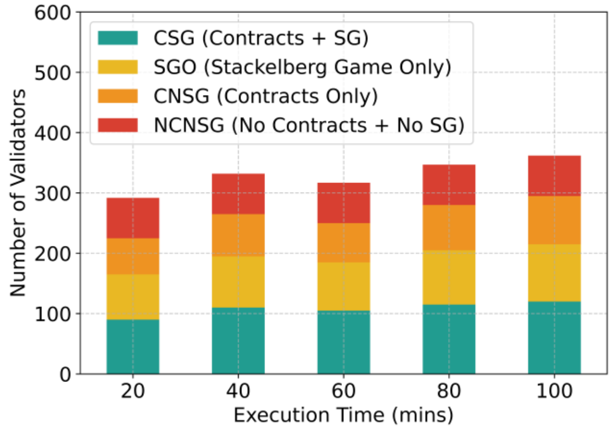


2. Validator Utility





3. Equilibrium Analysis



4. Participation rate

EN Utility & User payoff Remarks:

- Average Blockchain Utility Score of CSG compared to other schemes:
  - CSG vs. SGO: 14.29%
  - CSG vs. CNSG: 33.33%
  - CSG vs. NCNSG: 71.43%
- Average Validator Utility Score of CSG compared to other schemes:
  - CSG vs. SGO: 11.61%
  - CSG vs. CNSG: 19.05%
  - CSG vs. NCNSG: 56.25%
- CSG **converges** rapidly to **equilibrium**, showing the effectiveness of combining contracts with the Stackelberg game.
- CSG yields **higher validator participation rates**, indicating a preference for integrating contracts with the Stackelberg game.

Summary of Work 3

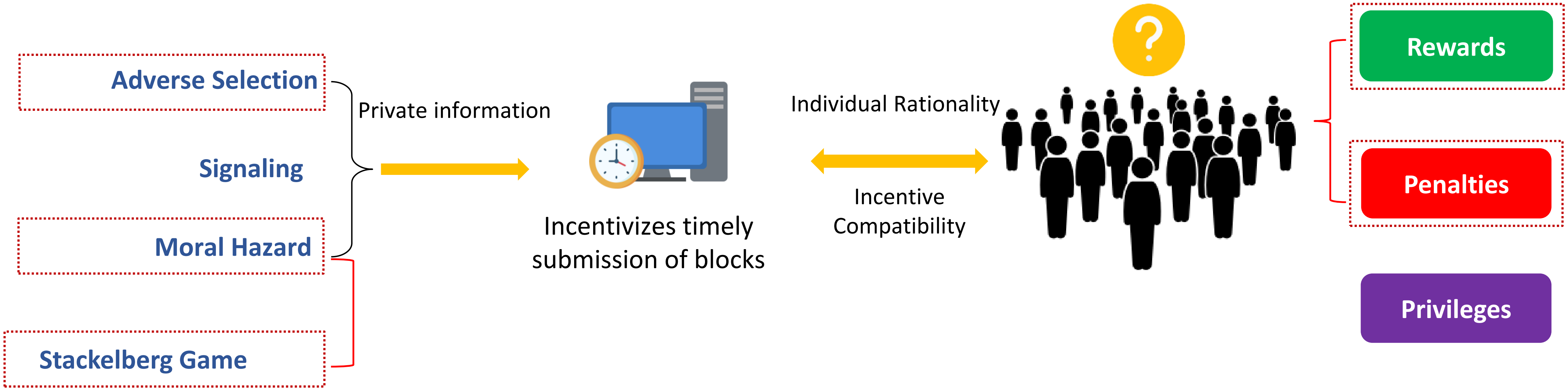
- We proposed Contract-Stackelberg Game (CSG) framework that integrates contracts and strategic game theory for timely block submissions.
- Studied two categories of **economic incentives** in **blockchain networks** by using **Contract Theory and Stackelberg Games**: Reward and Penalties.

Focus:

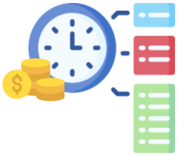
Entities: Validators, Blockchain Network, and Decentralized Oracle Network (DON)

Contract Design: Adverse selection, Moral hazard + Stackelberg Games

Incentive: Rewards and Penalties



Collusion in Contract Theory Designs



Order transactions based on user information

Incentivizes node implementations

Incentivizes timely submission of blocks

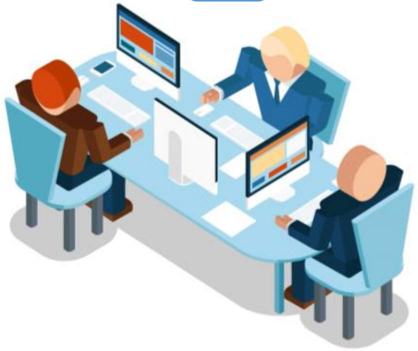
1

Validators **agree** to **share** their **rewards** regardless who validates a block.

2

Validators **increase** their **expected earnings** and **reduce** their **variance** in rewards.

3

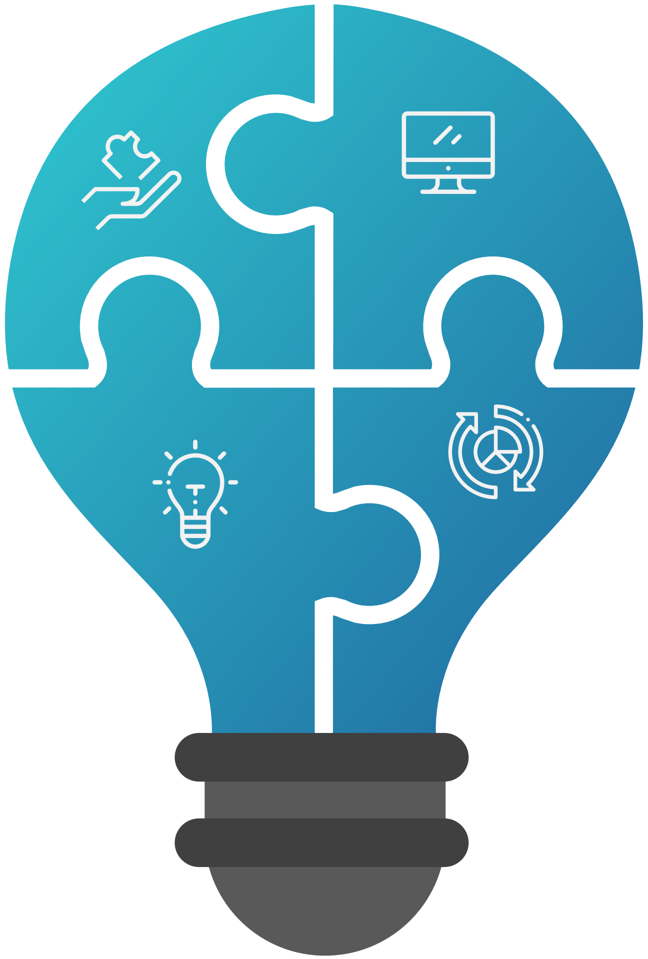


Validators consistently **vote** for each other's blocks, **ignoring** more deserving blocks.

Future Works: Addressing Collusion in Our Designs

Robust Contract Design

To create contracts that automatically make collusion unattractive and easily detectable.



Deep Reinforcement Learning Application

To apply Deep Reinforcement Learning to adaptively identify and mitigate collusion tactics in real-time.

Zero-Knowledge Proof Integration

To integrate Zero-Knowledge Proofs to ensure actions are verifiable without risking collusion.

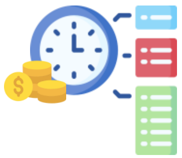
Reputation-Driven Ecosystem

To establish a dynamic reputation-based system that discourages collusion through continuous monitoring and incentivizes honest behavior across the blockchain ecosystem.

Summary of Works

Work 1

- Studied two categories of **economic incentives** in **decentralized exchanges** by using **Contract Theory**: Reward and Penalty.
- Work I: **Reward** – Knowledge of user types can incentivize miners to order transactions fairly.



Order transactions based on user information

Work 2

- Studied two categories of **economic incentives** in **Web 3.0 and Metaverse stability** by using **Contract Theory**: Reward and Privilege.
- Work II: **Reward and Privilege** – Can incentivize users to contribute resources towards blockchain networks.

Incentivizes node implementations

Work 3

- Studied two categories of **economic incentives** in **blockchain networks** by using **Contract Theory and Stackelberg Games**: Reward and Penalties.
- Work III: **Reward, Penalties, and Privileges** – Knowledge of user types can incentivize miners to order transactions fairly.

Incentivizes timely submission of blocks

JOURNALS:

1. D. M. Doe, J. Li, N. Dusit, L. Wang and Z. Han, "Incentive Mechanism Design for Mitigating Frontrunning and Transaction Reordering in Decentralized Exchanges," in IEEE Access, doi: 10.1109/ACCESS.2023.3236891.
2. D. M. Doe, D. Chen, K. Han, H. Wang, J. Xie and Z. Han, "DSORL: Data Source Optimization With Reinforcement Learning Scheme for Vehicular Named Data Networks," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2023.3292033.
3. D. M. Doe, J. Li, N. Dusit, Z. Gao, J. Li and Z. Han, "Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design," in IEEE Open Journal of the Computer Society, vol. 4, pp. 171-184, 2023, doi: 10.1109/OJCS.2023.3260829.
4. Edge-Assisted Indexing for Highly Dynamic and Static Data in Mixed Reality Connected Autonomous Vehicles: Daniel Doe, Dawei Chen, Haoxin Wang, Kyungtae Han, Linda Xie, and Zhu Han

CONFERENCES:

1. D. M. Doe, D. Chen, K. Han, Y. Dai, J. Xie and Z. Han, "Real-Time Search-Driven Content Delivery in Vehicular Networks for AR/VR-Enabled Autonomous Vehicles," 2023 IEEE/CIC International Conference on Communications in China (ICCC), Dalian, China, 2023, pp. 1-6, doi: 10.1109/ICCC57788.2023.10233627.
2. High definition map data optimization for autonomous driving in vehicular named data networks: Daniel Doe, Dawei Chen, Haoxin Wang, Kyungtae Han, Linda Xie, and Zhu Han IEEE International Conference on Communications (ICC), June 2023
3. Z. Zhan et al., "Mitigate Gender Bias in Construction: Fusion of Deep Reinforcement Learning-Based Contract Theory and Blockchain," 2023 IEEE International Conference on Blockchain (Blockchain), Danzhou, China, 2023, pp. 86-91, doi: 10.1109/Blockchain60715.2023.00023.

WORKING PAPERS AND SUBMISSIONS:

1. D. M. Doe, D. Chen, K. Han, H. Wang, J. Xie and Z. Han, "Enhancing AR/VR Performance via Optimized Edge-based Object Detection for Connected Autonomous Vehicles," for IEEE International Conference on Communications.
2. D. M. Doe, D. Chen, K. Han, H. Wang, J. Xie and Z. Han, "Edge-Assisted Indexing for Highly Dynamic and Static Data in AR/VR-Connected Autonomous Vehicles," for IEEE International Conference on Communications.
3. D. M. Doe et al., "Harnessing Tullock Contests and Signaling Games: A Novel Weight Assignment Strategy for Ethereum 2.0" for IEEE Transactions on Blockchain and Security.
4. D. M. Doe et al., "A Contract-Stackelberg Framework for Mitigating Timing Games in Proof-of-Stake Blockchain Networks”

PATENTS:

1. Doe, D. M., Chen, D., Han, K. (October 2023). "Systems and Methods for Reducing Latency and Bandwidth Usage in Mixed Reality Devices Through Selective Frame Transmission."
2. Doe, D. M., Chen, D., Han, K. (October 2023). “Systems and Methods for Resource-Optimized Mixed Reality Using User-Centric Adaptive Object Detection."
3. Doe, D. M., Chen, D., Han, K. (October 2023). "Systems and Methods For Edge-Driven Object Detection for Resource Optimization in Mixed Reality Systems of Autonomous Vehicles."
4. Doe, D. M., Chen, D., Han, K. (October 2023). "Systems and Methods for Computation Offloading Determination Using Multi-Modal User Input in Autonomous Vehicles."


Incentive Mechanism Design for Blockchain Networks: Bridging Decentralized Exchanges, Web 3.0, and the Metaverse
Presented by: Daniel Mawunyo Doe
Advisor: Dr. Zhu Han
Electrical and Computer Engineering Department
University of Houston
Committee Members: Dr. Miao Pan, Dr. David Mayerich, Dr. Yuqing Hu, Dr. Niyato Dusit, and Dr. Zhu Han
Department of Electrical and Computer Engineering
Cullen College of Engineering
Should we approve Daniel's defense?

Thank you