《Game Theory》 Group Presentation

Incentives in Blockchain system

Jiahao Yao, Junhao Dai

2024.6.4

Overview

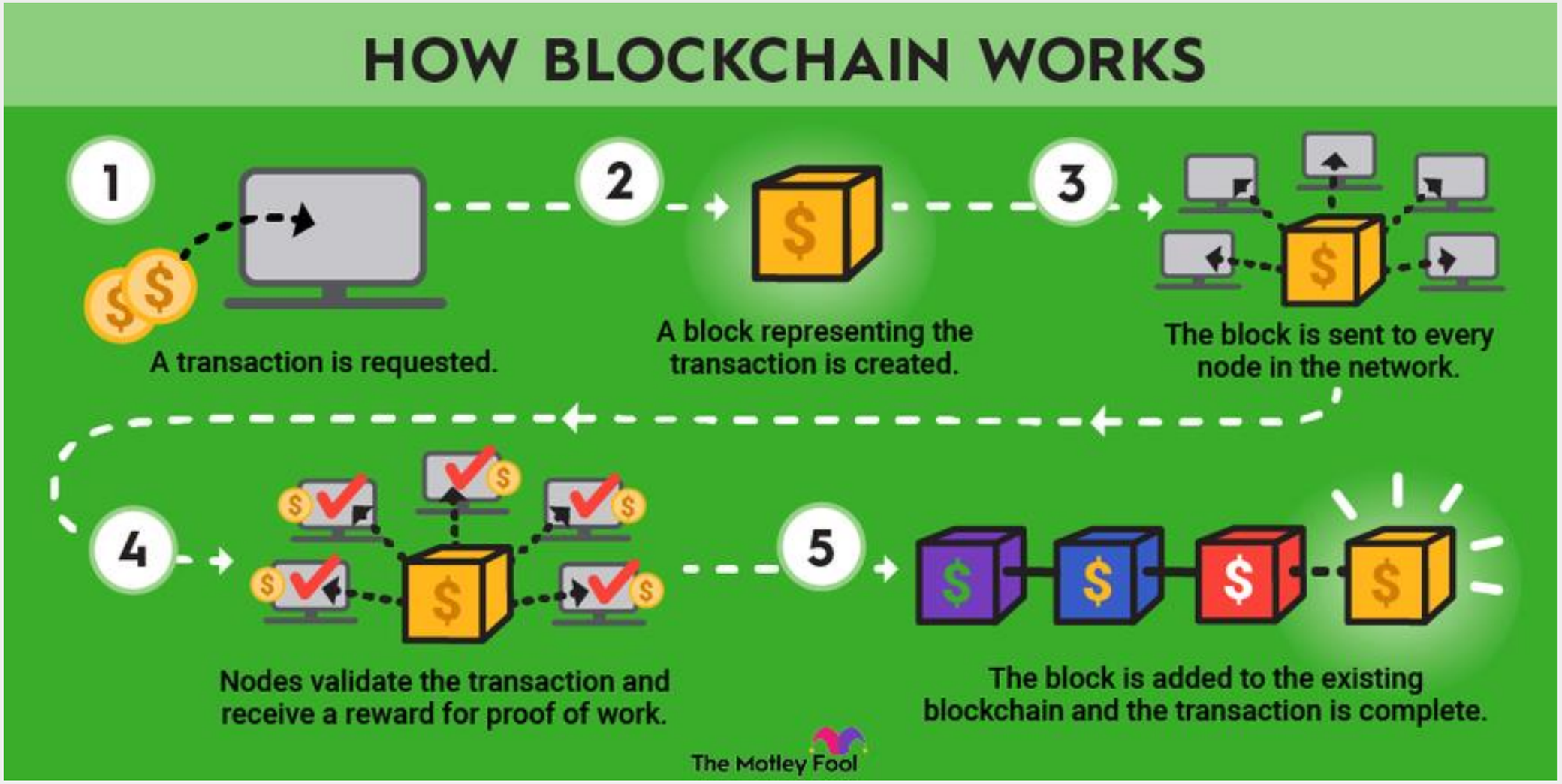
Blockchain Intro

Incentive Mechanism

Game Theory For Mining

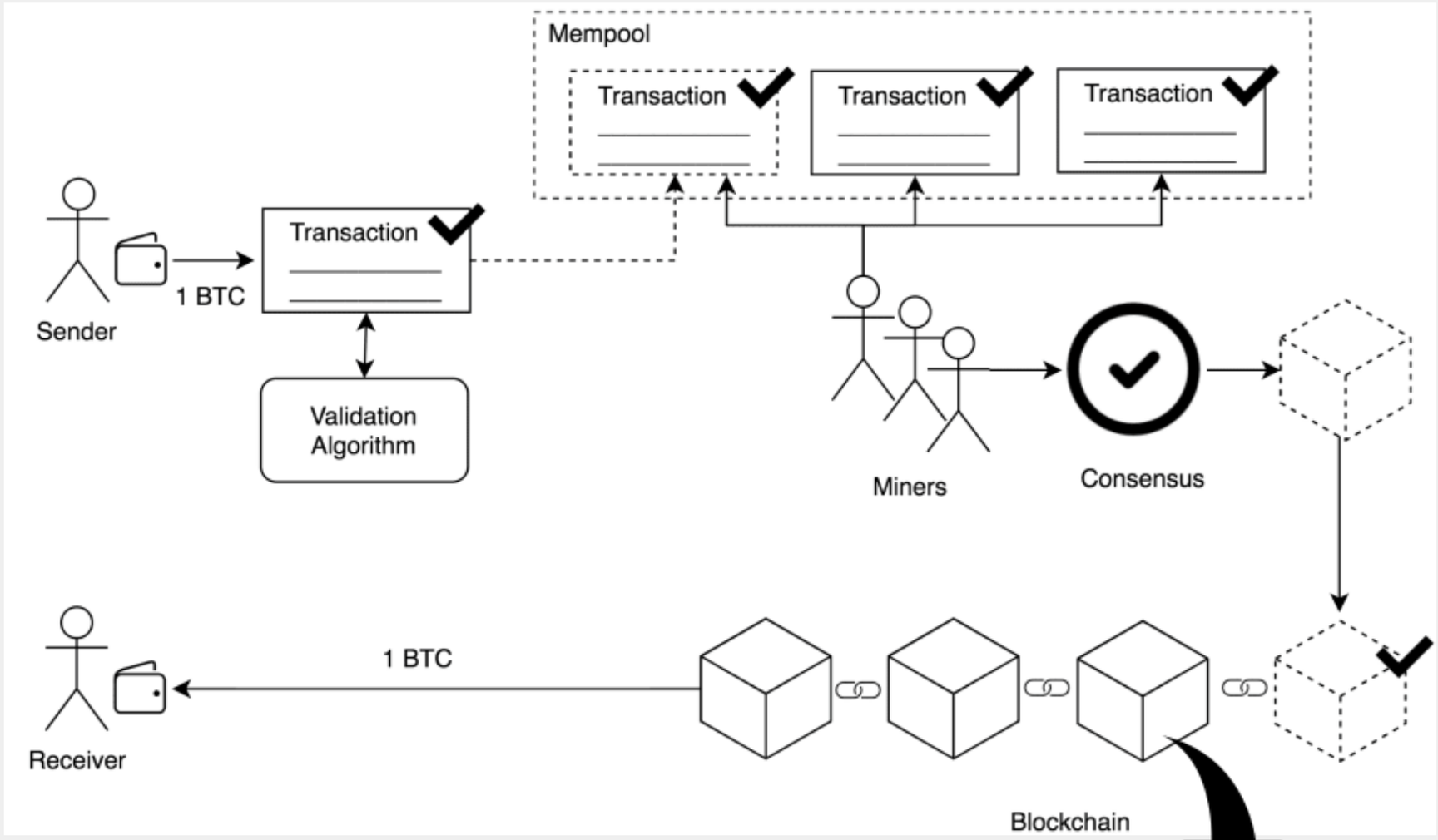
Game Theory For Security

Blockchain Intro



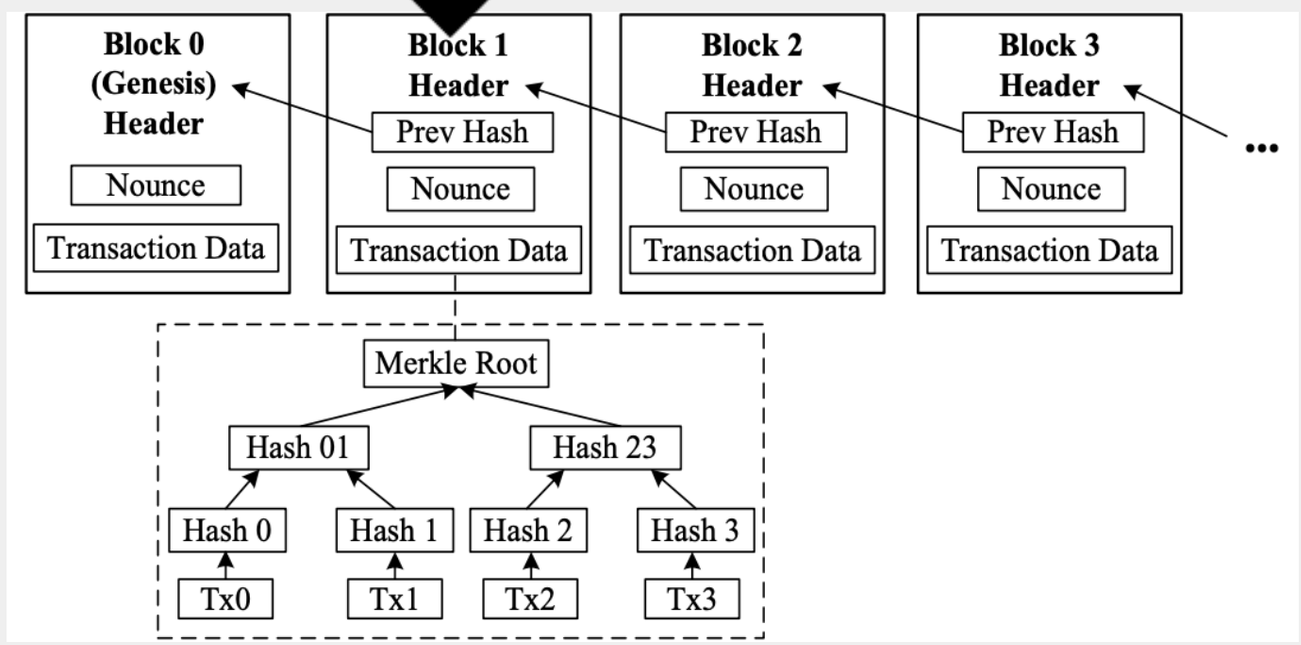
Blockchain is a decentralized, distributed ledger technology that securely records transactions across multiple computers, ensuring data integrity and transparency without the need for a central authority.

Blockchain Intro



Basic Components:

- Transaction
- Block
- Hash pointer
- Merkle Tree



Blockchain Intro

Some Widely-used Blockchain Platforms

Platform Name	**Ledger type**	**Consensus Protocol**
Bitcoin [1]	Public	Proof of Work (PoW)
Ethereum [3]	Public	PoW & Proof of Stake
Hyperledger Fabric [21]	Consortium	Pluggable algorithm
EOS [5]	Private	Delegated Proof of Stake
Stellar [23]	Public & Private	Stellar consensus protocol
Quorum [24]	Private	Majority voting
Ripple [4]	Private	Probabilistic voting

Incentive Mechanism

> “ Expending resources to mine gold and inject it into circulation ”

- **Objective**

To ensure all participants are motivated to maintain and secure the network.

- **Importance**

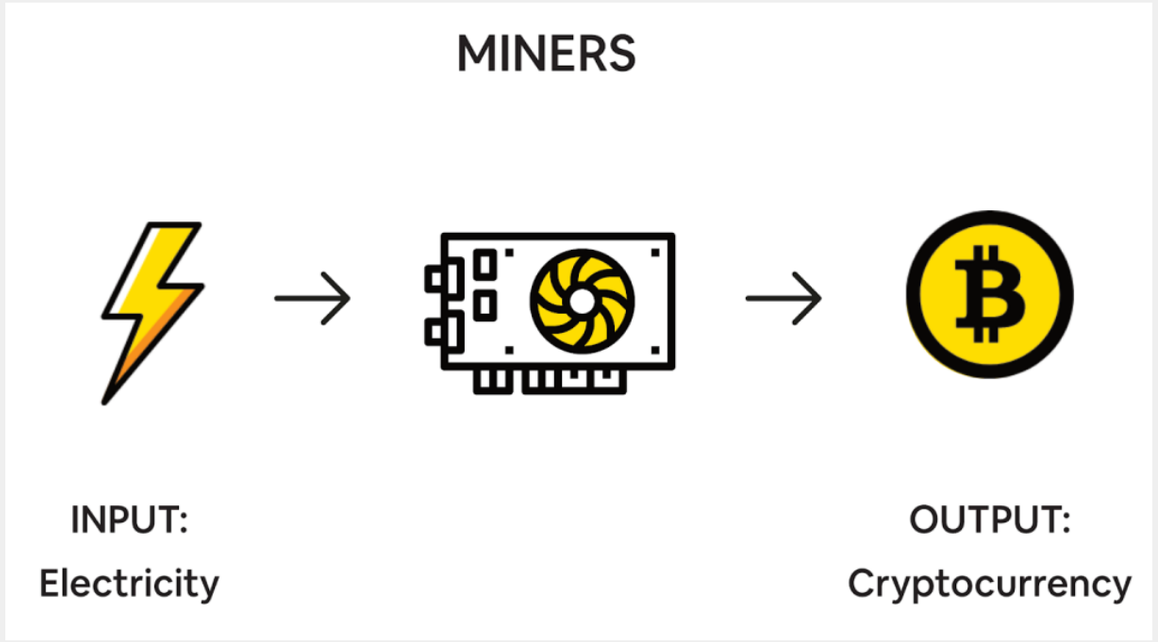
Essential for the prevention of fraudulent activities and ensuring fidelity and security.

- **Agreement**

Participants are rewarded for contributing computational power.

- **Types**

- Mining Rewards: Reward miners for validating transactions and securing the blockchain.
- Transaction Fees: Fees paid by users to have their transactions included in the blockchain.



Game Theory For Mining

Three challenges and Game Theory Approach for minig

1. Computational Power Allocation

- Challenge: inding the right amount of resources to deploy for maximum efficiency and profit.
- Game Theory Approach: Miners optimize the cost-benefit ratio of resource use to maximize returns.

2. Reward Allocation

- Challenge: Distributing rewards to motivate ongoing participation and honesty.
- Game Theory Approach: Design reward systems that encourage cooperation and align miner incentives with network health.

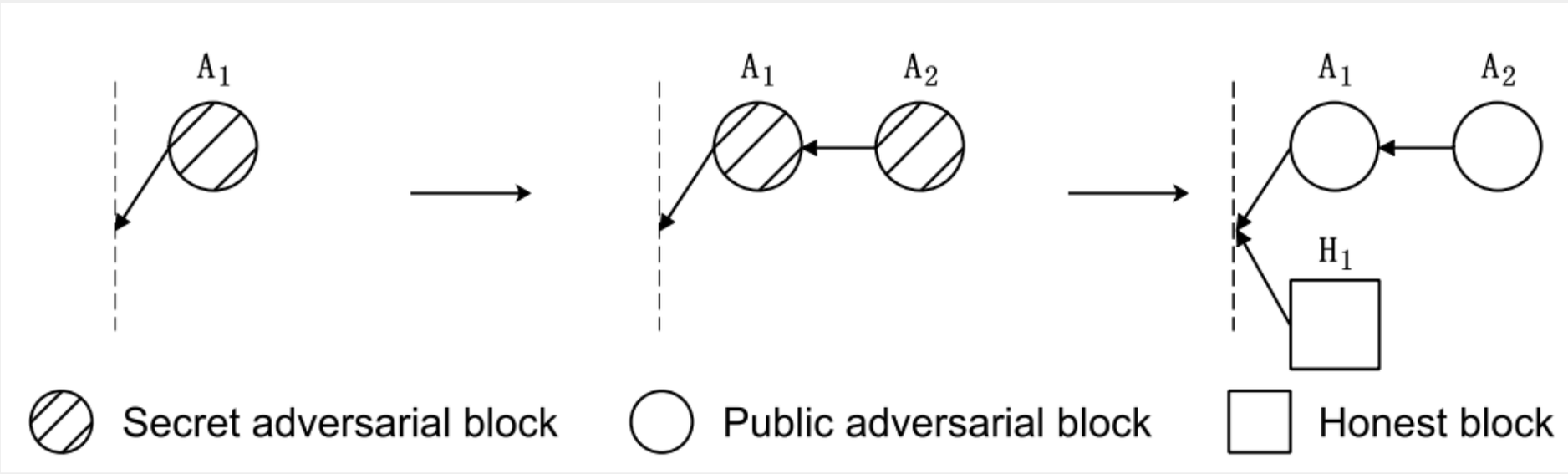
3. Pool Selection

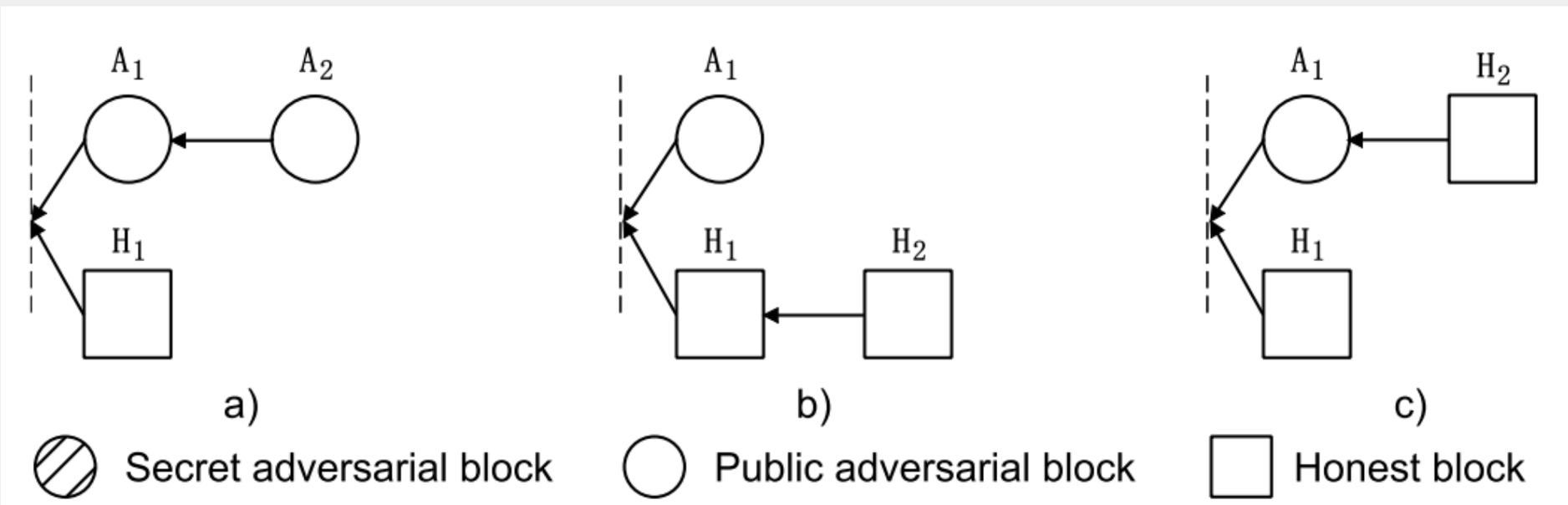
Solo, PPS, PPLNS...

- Challenge: Selecting a mining pool that maximizes rewards, reliability, and overall returns.
- Game Theory Approach: Miners choose pools based on the best projected earnings and stability.

Game Theory For Security

Selfish Mining in Bitcoin





Game Theory For Security

- **A2 Mining on A1**

The selfish miners produce the next blocks A2 after their block and publish it. By LCR, all selfish miners' blocks are accepted by honest miners, whereas honest block H1 is abandoned.

- **H2 Mining on H1**

Some honest miners produce the next block H2 after the previous honest block H1. If the selfish miners accept these two honest blocks H1 and H2 and mine after them, its block A1 will be abandoned.

- **H2 Mining on A1**

Some honest miners produce the next block H2 after the selfish miners' block A1. Both blocks A1 and H2 will be accepted, whereas the block H1 will be abandoned by LCR.

α fraction of computation power owned by the selfish miners

γ fraction of honest computation power working on the selfish miners' blocks

the relative revenue for the selfish miner

$$\frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+(2-\alpha)\alpha)}$$

selfish miner can obtain a revenue larger than its honest mining when:

$$\frac{1-\gamma}{3-2\gamma}<\alpha<\frac{1}{2}$$

Game Theory For Security

The Pool Game of Selfish Mining

1. The average time to find a solution is proportional to its hash rate or mining power.
2. Block discard is random, factor this event into the probability of finding a block.
3. A mining pool is a group of miners who share revenue in proportion to their computing power.
4. Block withholding is an attack launched by mining pool members against other mining pools.

m_i the number of miners loyal to pool i

$x_{i,j}(t)$ the number of miners from pool i that infiltrate pool j at step t.

the direct mining rate of pool i at step t :

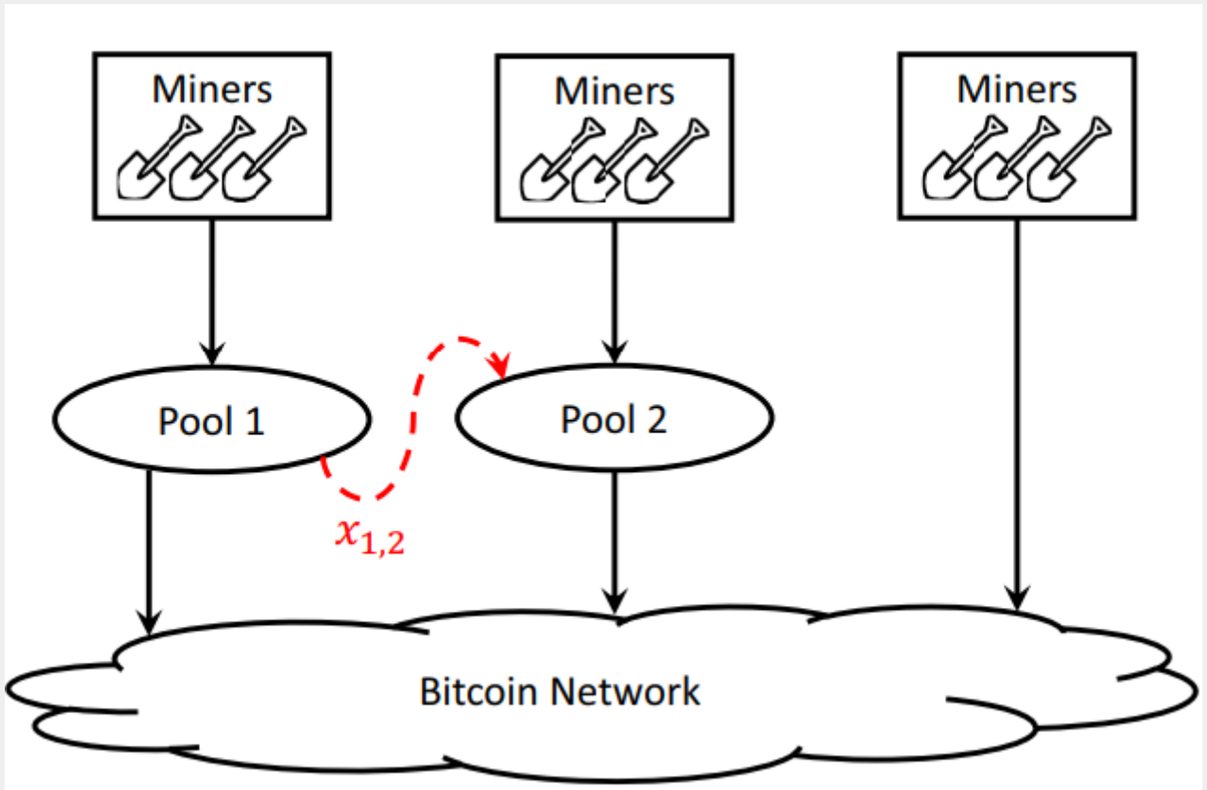
$$R_i \triangleq \frac{m_i - \sum_{j=1}^{p} x_{i,j}}{m - \sum_{j=1}^{p} \sum_{k=1}^{p} x_{j,k}}$$

the revenue density of pool i at end of step t :

$$r_i(t) = \frac{R_i(t) + \sum_{j=1}^{p} x_{i,j}(t) r_j(t)}{m_i + \sum_{j=1}^{p} x_{j,i}(t)}$$

Game Theory For Security

One Attacker



$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2}}$$

$$R_2 = \frac{m_2}{m - x_{1,2}}$$

$$\Rightarrow \quad r_2 = \frac{R_2}{m_2 + x_{1,2}}$$

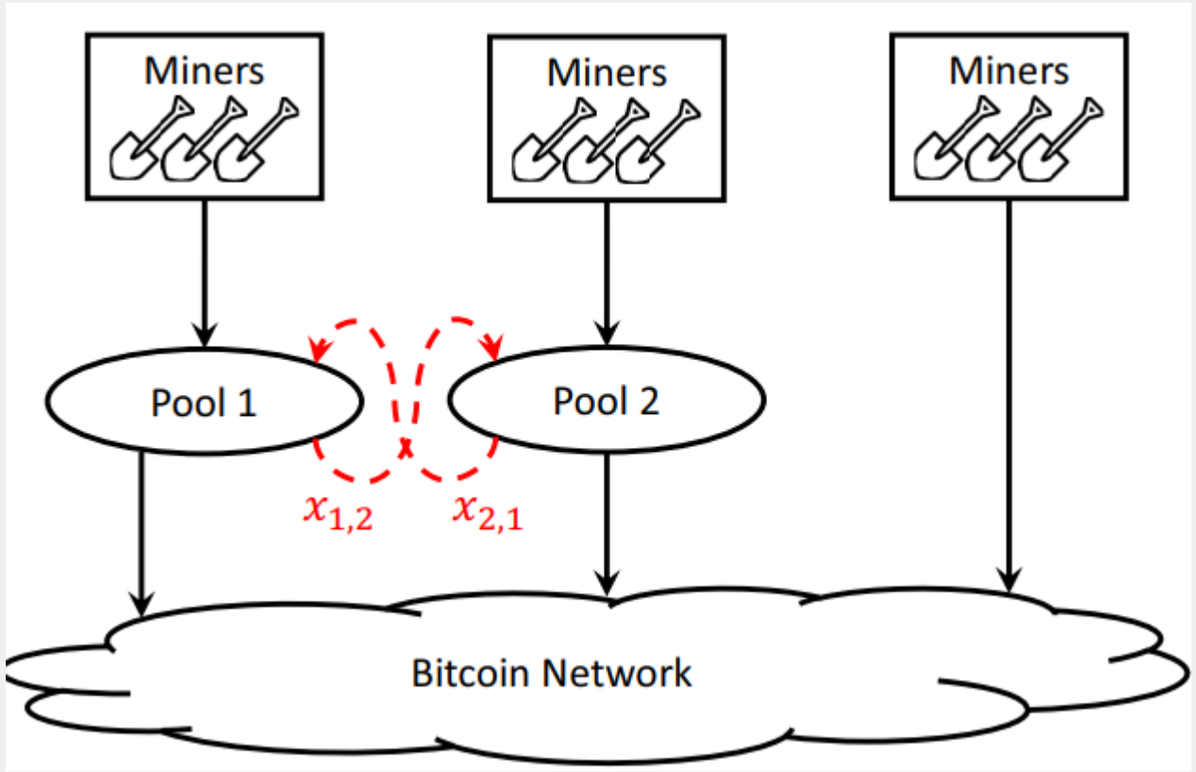
$$r_1 = \frac{R_1 + x_{1,2} \cdot r_2}{m_1}$$

$$\Rightarrow \quad r_1 = \frac{m_1 (m_2 + x_{1,2}) - x_{1,2}^2}{m_1 (m - x_{1,2}) (m_2 + x_{1,2})}$$

To find the optimal permeability, we need to calculate $\overline{x}_{1,2} \triangleq \arg\max_{x_{1,2}} r_1$

Game Theory For Security

Two Pools



$$R_1 = \frac{m_1 - x_{1,2}}{m - x_{1,2} - x_{2,1}} \quad \Rightarrow \quad r_1 = \frac{R_1 + x_{1,2} r_2}{m_1 + x_{2,1}}$$

$$R_2 = \frac{m_2 - x_{2,1}}{m - x_{1,2} - x_{2,1}} \qquad r_2 = \frac{R_2 + x_{2,1} r_1}{m_1 + x_{1,2}}$$

$$r_1(x_{1,2}, x_{2,1}) = \frac{m_2 R_1 + x_{1,2}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}$$

$$r_2(x_{2,1}, x_{1,2}) = \frac{m_1 R_2 + x_{2,1}(R_1 + R_2)}{m_1 m_2 + m_1 x_{1,2} + m_2 x_{2,1}}$$

No attack is not an equilibrium point, Nash equilibrium exists and satisfies :

$$\begin{cases} \dfrac{\partial r_1(x_{1,2}, x_{2,1})}{\partial x_{1,2}} = 0 \\ \dfrac{\partial r_2(x_{2,1}, x_{1,2})}{\partial x_{2,1}} = 0 \end{cases}$$

$$\begin{cases} \arg\max\limits_{x_{1,2}} r_1(x_{1,2}, x'_{2,1}) = x'_{1,2} \\ \arg\max\limits_{x_{2,1}} r_2(x'_{1,2}, x_{2,1}) = x'_{2,1} \end{cases}$$

$$s.t. \quad 0 < x'_1 < m_1$$

$$0 < x'_2 < m_2$$

Game Theory For Security

Two Pools

Pool 1 / Pool 2	no attack	attack
no attack	$(r_1 = 1, r_2 = 1)$	$(r_1 > 1, r_2 = \tilde{r}_2 < 1)$
attack	$(r_1 = \tilde{r}_1 < 1, r_2 > 1)$	$(\tilde{r}_1 < r_1 < 1, \tilde{r}_2 < r_2 < 1)$

q Identical Pools

$$R_1 = \frac{m_i - (q-1)x_{1,\neg 1}}{m - (q-1)(q-1)x_{\neg 1,*} - (q-1)x_{1,\neg 1}} \quad \Rightarrow \quad r_1 = \frac{R_1 + (q-1)x_{1,\neg 1}r_{\neg 1}}{m_i + (q-1)x_{\neg 1,1}}$$

$$R_{\neg 1} = \frac{m_i - (q-1)x_{\neg 1,*}}{m - (q-1)(q-1)x_{\neg 1,*} - (q-1)x_{1,\neg 1}} \quad r_{\neg 1} = \frac{R_{\neg 1} + (q-2)x_{\neg 1,*}r_{\neg 1} + x_{\neg 1,*}r_1}{m_i + (q-2)x_{\neg 1,*} + x_{1,\neg 1}}$$

Division of Work

Jiahao Yao:

Game Theory For Mining in blockchain

Junhao Dai:

Game Theory For Security in blockchain

Thanks