Breaking Blockchain Rationality with Out-of-Band Collusion

Haoqian Zhang, Mahsa Bastankhah, Louis-Henri Merino, Vero Estrada-GaliÃśanes, Bryan Ford

Decentralized and Distributed Systems Laboratory (DEDIS)

EPFL

Outline

- The Keynesian Beauty Contest
- Longest-chain Rule
- General Rational Attack on Rationality
- Implication

The Keynesian Beauty Contest[1]

[1]: Chapter 12, The General Theory of Employment, Interest and Money

Rational Strategy

- Choose the one based on your own judgement.
- Choose the one that average opinion thinks.
- Choose the one that average opinion expects the average opinion to be.
- …

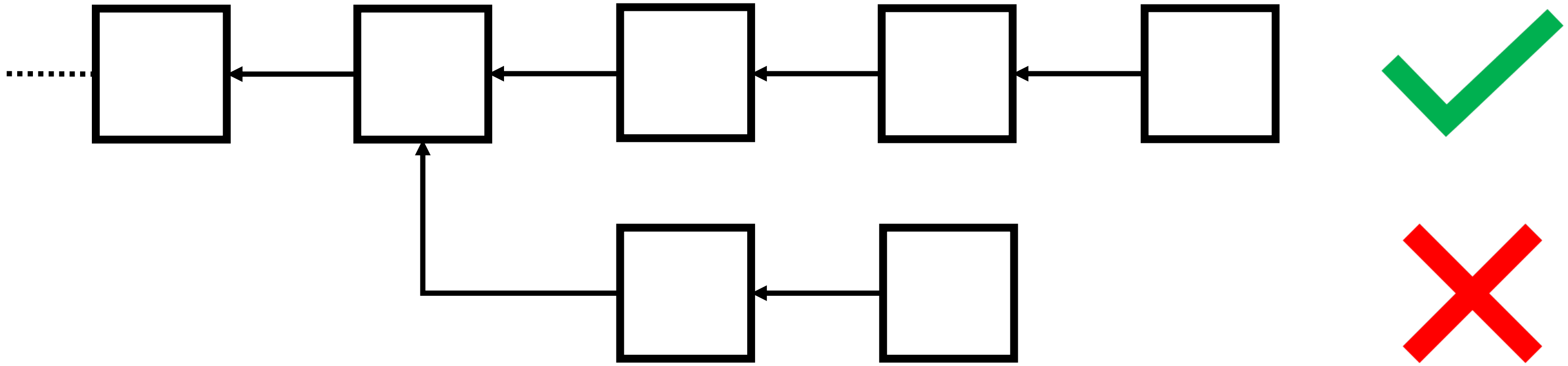
- Can we do better to let an arbitrary face win while each player remains rational?

Beauty Contest with Out-of-band Collusion

- A magnate announces a collusion aiming to let a face win.
- A participant can sign up for the collusion with a deposit.
- Enough participants signed up before the deadline?
  - Yes, ask everyone to vote for the face and return the deposit who honestly votes the face with an additional reward from magnate.
  - No, abort the attack and return the deposit to everyone.

- Rational Strategy: Sign up and follow the magnate’s order.

Longest-chain Rule



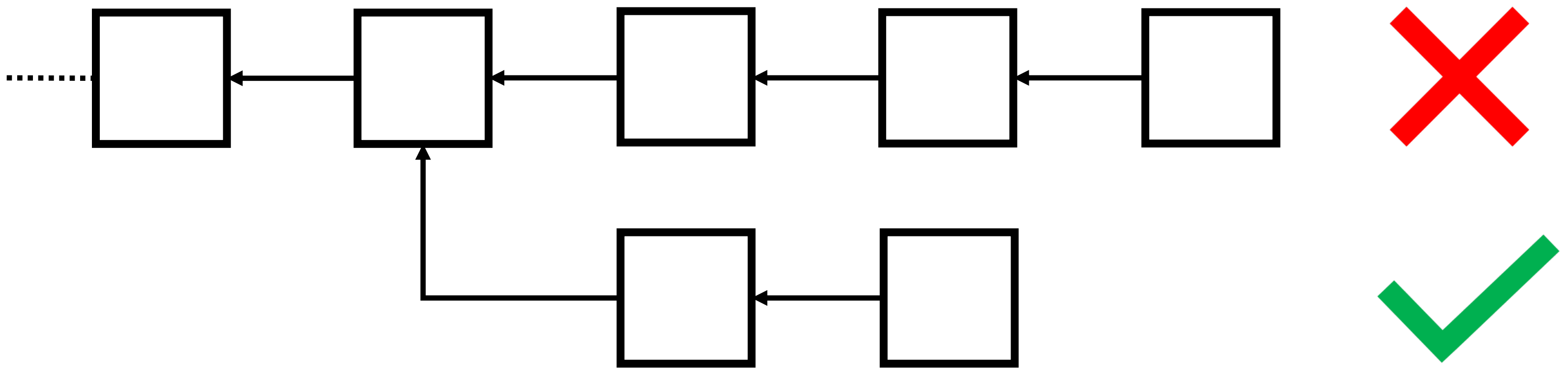
Rational Strategy

- Follow the longest-chain rule
- Selfish mining[1]
- Whale attack[2]
- …

- Can we do better to let an arbitrary fork win while each player remains rational?

[1]: Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable.
[2]: Liao, K., Katz, J.: Incentivizing blockchain forks via whale transactions.

Out-of-band Collusion Target

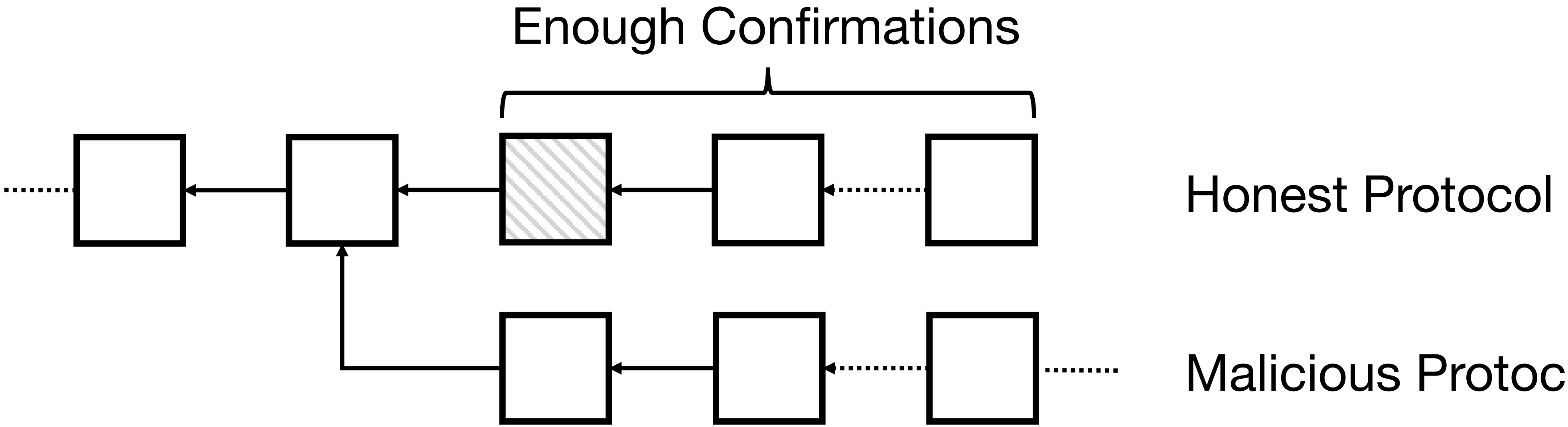


Out-of-band Collusion

- A magnate announces a collusion aiming to let a fork become the longest chain.
- A node can sign up for the collusion with a deposit.
- Enough nodes signed up before the deadline?
  - Yes, ask everyone to mine for the fork and return the deposit who honestly mines for the fork with an additional reward from magnate.
  - No, abort the attack and return the deposit to everyone.

- Rational Strategy: Sign up and follow the magnate’s order.

Double Spend



Enough Confirmations

Honest Protocol

Malicious Protocol

▨ : Targeted block with transactions that the magnate aims to double-spend.

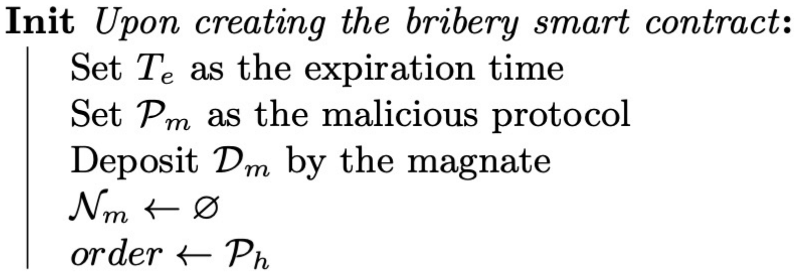
Magnate’s Incentive

- Aim to double-spend a transaction
- Obtain financial profit from the double-spent transaction
- Control the blockchain
- Fund the additional reward to colluded nodes

General Attack: Assumptions

- Assumption 1: Blockchain system **S** with a consensus group
- Assumption 2: External system **S’** has a perfect oracle on **S**
- Assumption 3: **S** leverages some fashion of rational assumptions
- Assumption 4: Malicious protocol can generate more profit

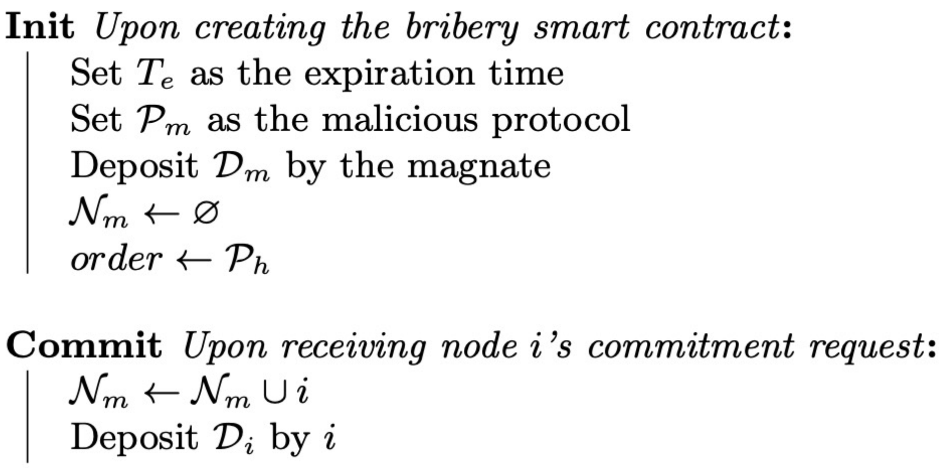
General Rational Attack on Rationality



```
Init Upon creating the bribery smart contract:
    Set $T_e$ as the expiration time
    Set $\mathcal{P}_m$ as the malicious protocol
    Deposit $\mathcal{D}_m$ by the magnate
    $\mathcal{N}_m \leftarrow \varnothing$
    $order \leftarrow \mathcal{P}_h$
```

$\mathcal{N}_m$ is the collusion set

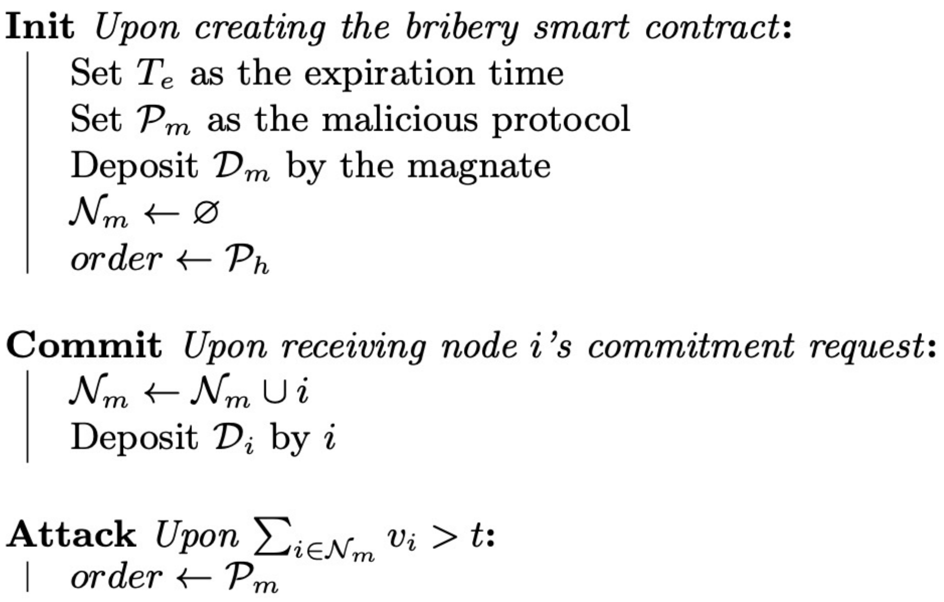
General Rational Attack on Rationality



```
**Init** *Upon creating the bribery smart contract*:
    Set $T_e$ as the expiration time
    Set $\mathcal{P}_m$ as the malicious protocol
    Deposit $\mathcal{D}_m$ by the magnate
    $\mathcal{N}_m \leftarrow \varnothing$
    $order \leftarrow \mathcal{P}_h$

**Commit** *Upon receiving node i's commitment request*:
    $\mathcal{N}_m \leftarrow \mathcal{N}_m \cup i$
    Deposit $\mathcal{D}_i$ by $i$
```

$\mathcal{N}_m$ is the collusion set

General Rational Attack on Rationality



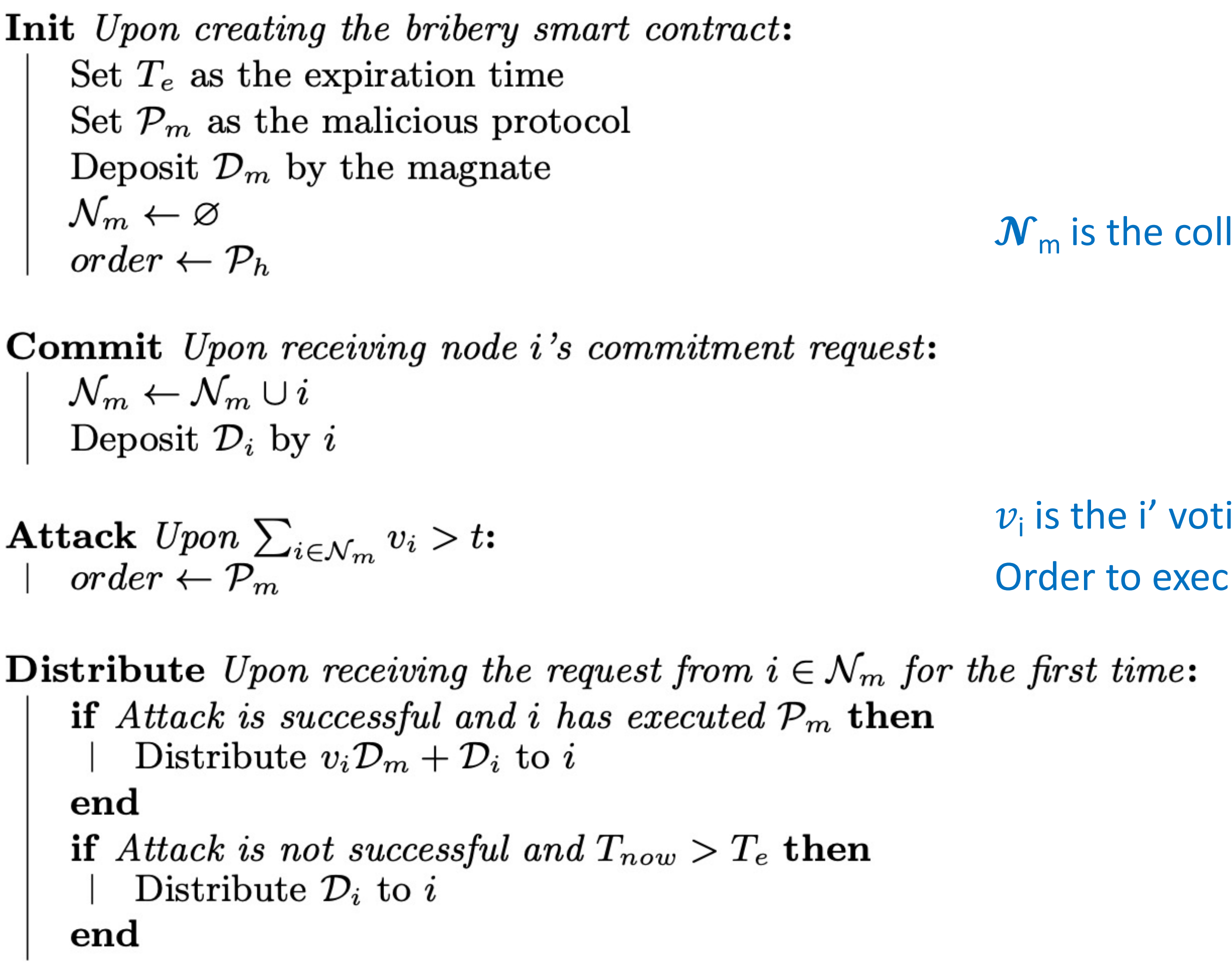
```
**Init** *Upon creating the bribery smart contract*:
    Set $T_e$ as the expiration time
    Set $\mathcal{P}_m$ as the malicious protocol
    Deposit $\mathcal{D}_m$ by the magnate
    $\mathcal{N}_m \leftarrow \varnothing$
    $order \leftarrow \mathcal{P}_h$

**Commit** *Upon receiving node i's commitment request*:
    $\mathcal{N}_m \leftarrow \mathcal{N}_m \cup i$
    Deposit $\mathcal{D}_i$ by $i$

**Attack** *Upon* $\sum_{i \in \mathcal{N}_m} v_i > t$:
    $order \leftarrow \mathcal{P}_m$
```

$\mathcal{N}_m$ is the collusion set

v_i is the i' voting power in consensus

Order to execute the malicious protocol

General Rational Attack on Rationality



```
**Init** *Upon creating the bribery smart contract*:
    Set $T_e$ as the expiration time
    Set $\mathcal{P}_m$ as the malicious protocol
    Deposit $\mathcal{D}_m$ by the magnate
    $\mathcal{N}_m \leftarrow \varnothing$
    $order \leftarrow \mathcal{P}_h$

**Commit** *Upon receiving node i's commitment request*:
    $\mathcal{N}_m \leftarrow \mathcal{N}_m \cup i$
    Deposit $\mathcal{D}_i$ by $i$

**Attack** *Upon* $\sum_{i \in \mathcal{N}_m} v_i > t$:
    $order \leftarrow \mathcal{P}_m$

**Distribute** *Upon receiving the request from* $i \in \mathcal{N}_m$ *for the first time*:
    **if** *Attack is successful and i has executed* $\mathcal{P}_m$ **then**
        Distribute $v_i \mathcal{D}_m + \mathcal{D}_i$ to $i$
    **end**
    **if** *Attack is not successful and* $T_{now} > T_e$ **then**
        Distribute $\mathcal{D}_i$ to $i$
    **end**
```

$\mathcal{N}_m$ is the collusion set

v_i is the i' voting power in consensus

Order to execute the malicious protocol

Implication

- Rationality is insufficient for security
- Provide a false sense of security
- Must rely on non-rational assumptions
  - E.g. threshold assumptions or police enforcement.

Conclusion

- General rational attack on rationality
- Out-of-band smart contract to establish collusion
- Irrational can be rational
- Welcome to the era of irrationality

Preprint QR code