Pool games in Various Information Environments

Constantinos Varsos[*,†] and Marina Bitsaki[‡]

[†]Centrum Winskunde & Informatica (CWI)
[‡]Computer Science Department, University of Crete

17th Symposium and Summer School On Service-Oriented Computing, Crete

June 25 - July 1, 2023

Outline

- digital environments, automated procedures, and big data
- intangible, crowd-sourcing, and sophisticated digital transaction methodologies
- transparent transactions, e.g. secured trading in distributed and decentralized environments

- digital environments, automated procedures, and big data
- intangible, crowd-sourcing, and sophisticated digital transaction methodologies
- transparent transactions, e.g. secured trading in distributed and decentralized environments

- Blockchain technology [Nakamoto '08]
- distributed synchronized secure database containing validated blocks of transactions
- blocks are containers holding a record of transactions on the blockchain

Blockchain

- a **block** is validated by special nodes, called **miners**, via the solution of a computationally demanding problem, called the proof-of-work puzzle
- miners compete against each other and the first one to solve the problem announces it
- the block is then verified by a predefined agreement protocol called **consensus**
- added to the distributed database
- the miner that generated the block is rewarded according to a commonly and apriori known protocol

Blockchain

- "Strength in unity", miners form mining **pools** implemented by a pool manager
- provide partial proof-of-work concurrently
  1. evaluates the miners' efforts
  2. estimates each miner's power

  and share their revenues accordingly
- **utility** of a pool is the total sum of the revenues received by its miners
- **block withholding attack**, a miner that solves a problem does not submit it after finding one block
- the cost to the miner is trivial but the cost to the pool is large

! Game theory [Eyal, IEEE'14], [Di et al, RESS'19]

Pool games

- The information available to a pool: set of its miners, set of adversary pools, and predefined protocols
- a pool may be attacked by a miner from an adversary pool by providing partial proof-of-work to the pool manager
- The attacking miner shares the revenue obtained in the pool but does not contribute, thus the utility of the attacked pool deteriorates and becomes less attractive to other miners [Eyal, IEEE'14]
- partial proof-of-work to opponent pools, called **infiltration rate**

Setting & Information environments

- Pool game with N pools, $N \in \mathbb{N}$
- pools are of equal capabilities
- all miners are atomic and identical

Setting & Information environments

Three different information environments

- Complete-correct information [Eyal, IEEE'14]

  "*pools know their mining power and estimate correctly the infiltration rates*"

- Incomplete information

  "*the pools are* **not** *aware about the size of the incoming attack*"

- Incorrect information

  "*they* **think** *they know the actual mining power of the pool and the accurate number of incoming attacks*"

Methodology

- Number of pools (N), number of choices (S), the gains that each choice provides to the pools (U)
- Pools try to maximize their gains
- Outcome of the interaction

Methodology

- Number of pools (N), number of choices (S), the gains that each choice provides to the pools (U)
- Pools try to maximize their gains

$$\left.\right\} G = \langle N, S, U \rangle$$

- Outcome of the interaction Nash equilibrium

- In a Nash equilibrium no agent has incentives to deviate

Methodology

Incomplete information

- Bayesian game, $BG = \langle N, S, \Theta, p, U \rangle$
- Pools' types Θ contain all relevant information about certain pools' private characteristics
- A type $\theta_i \in \Theta_i$ is only observed by pool i
- utilities are calculated by each pool by taking expectations over types using its own conditional beliefs about opponents' type (ex interim)
- Outcome, Bayes-Nash equilibrium

Methodology

Incomplete information

- Bayesian game, $BG = \langle N, S, \Theta, p, U \rangle$
- Pools' types Θ contain all relevant information about certain pools' private characteristics
- A type $\theta_i \in \Theta_i$ is only observed by pool i
- ex interim expected utility of pool i is

$$\mathbb{E}[U_i(\sigma, \theta_i)] = \sum_{\theta_{-i} \in \Theta_{-i}} p(\theta_{-i} | \theta_i) \mathbb{E}[U_i(\sigma, (\theta_i, \theta_{-i}))]$$

- σ s.t. $\sigma_i \in BR_i(\sigma_{-i}), \forall i \in N$, where $BR_i(\sigma_{-i})$ is the best response of i against $\{-i\}$
- Repeated case, utility formulas

$$\frac{1}{T} \sum_{t \in [T]} U_i(\sigma^t, \theta_i), \qquad (1-\delta) \sum_{t \in [T]} \delta^t U_i(\sigma^t, \theta_i), \;\; i \in [|N|], \;\; \delta \in (0,1), T > 0$$

Methodology

Incorrect information

- Misinformation game, $mG = \langle G^0, G^1, \ldots, G^{|N|} \rangle$
- Pool i has the G^i game
- G^0 is the actual interaction
- Here, misinformation affects only the values of the payoffs
- Outcome, natural misinformed equilibrium (**nme**)

Methodology

Incorrect information

- Misinformation game, $mG = \langle G^0, G^1, \ldots, G^{|N|} \rangle$
- Pool i has the G^i game
- G^0 is the actual interaction
- Here, misinformation affects only the values of the utilities
- Outcome, natural misinformed equilibrium (**nme**)
- Repeated case, Adaptation Procedure ($\mathcal{AD}$)

$$\mathcal{AD}^{(t)}(M) = \{mG_{\vec{u}} \mid mG \in M, \vec{u} \in \chi(\sigma), \sigma \in NME(mG)\}$$

$$\mathcal{AD}^{(t)}(M) = \mathcal{AD}^{(t+1)}(M)$$

- N pools, m miners
- goal: maximize revenue density

- N pools, m miners
- goal: maximize revenue density $\rightsquigarrow$ optimize infiltration rates

- N pools, m miners
- goal: maximize revenue density $\rightsquigarrow$ optimize infiltration rates
- revenue density of a pool i, $r_i(t)$:

$$\frac{\text{average revenue that miner } i \text{ earns}}{\text{average revenue it would have earned as a solo miner}}$$

! discrete-time step interaction

! the total number of miners per pool remains constant throughout the game

At time step t a pool i,

- has in total $m_i(t)$ miners
- commits to the pool j $m_{ij}(t)$ miners

  Clearly, $m_i(t) = \sum_j m_{ij}(t)$
- mines with power $m_i(t) - \sum_{j \in [|N|] \setminus \{i\}} m_{ij}(t)$,
  - divided by total mining rate then direct mining, R_i
- shares reward among $m_{ii}(t) + \sum_{j \in [|N|] \setminus \{i\}} m_{ji}(t)$
- infiltration matrix

At time step t a pool i,

- has in total $m_i(t)$ miners
- commits to the pool j $m_{ij}(t)$ miners

  Clearly, $m_i(t) = \sum_j m_{ij}(t)$
- mines with power $m_i(t) - \sum_{j \in [|N|] \setminus \{i\}} m_{ij}(t)$,
  - divided by total mining rate then direct mining, R_i $\Bigg\}$ $\mathbf{m}(t)$
- shares reward among $m_{ii}(t) + \sum_{j \in [|N|] \setminus \{i\}} m_{ji}(t)$
- infiltration matrix $\mathbf{IR}(t)$

At time step t a pool i,

- has in total $m_i(t)$ miners
- commits to the pool j $m_{ij}(t)$ miners

  Clearly, $m_i(t) = \sum_j m_{ij}(t)$
- mines with power $m_i(t) - \sum_{j \in [|N|] \setminus \{i\}} m_{ij}(t)$,
  - divided by total mining rate then direct mining, R_i $\quad \mathbf{m}(t)$
- shares reward among $m_{ii}(t) + \sum_{j \in [|N|] \setminus \{i\}} m_{ji}(t)$
- infiltration matrix $\quad \mathbf{IR}(t)$

$$\boxed{\mathbf{r}(t) = \mathbf{m}(t) + \mathbf{IR}(t) \cdot \mathbf{r}(t-1), \quad \mathbf{r}(0) = \mathbf{m}(0)}$$

$N = 2$

- the infiltration rates are $m_{12}(t)$ and $m_{21}(t)$

$$r_1(m_{12}(t), m_{21}(t)) = \frac{m_{22}(t)R_1(t) + m_{12}(t)(R_1 + R_2)}{m_{11}(t)m_{22}(t) + m_{11}(t)m_{12}(t) + m_{22}(t)m_{21}(t)},$$

$$r_2(m_{12}(t), m_{21}(t)) = \frac{m_{11}(t)R_2(t) + m_{21}(t)(R_1 + R_2)}{m_{11}(t)m_{22}(t) + m_{11}(t)m_{12}(t) + m_{22}(t)m_{21}(t)}$$

  with $m_{11}(t), m_{22}(t) > 0$ and $m_1(t) + m_2(t) \leq m$.

- a pool i has two pure strategies, either to attack or to non-attack the adversary [strategy profiles are (attack, attack), (attack, non-attack), (non-attack, attack), and (non-attack, non-attack)]

- ordering for the density revenues of the pools [Eyal, IEEE'14]

$$\text{For Pool}_1 : \begin{cases} (attack, non-attack) > (non-attack, non-attack) \\ (attack, attack) > (non-attack, attack) \end{cases}$$

$$\text{For Pool}_2 : \begin{cases} (non-attack, attack) > (non-attack, non-attack) \\ (attack, attack) > (attack, non-attack) \end{cases}$$

- payoff matrix

Pool$_1$ \ Pool$_2$	attack	non-attack
attack	(r_1, r_2)	$(r_1, \tilde{r}_2)$
non-attack	$(\tilde{r}_1, r_1)$	$(\tilde{r}_1, \tilde{r}_2)$

- ordering for the density revenues of the pools [Eyal, IEEE'14]

$$\text{For Pool}_1 : \begin{cases} (attack, non-attack) > (non-attack, non-attack) \\ (attack, attack) > (non-attack, attack) \end{cases}$$

$$\text{For Pool}_2 : \begin{cases} (non-attack, attack) > (non-attack, non-attack) \\ (attack, attack) > (attack, non-attack) \end{cases}$$

- payoff matrix

Pool$_1$ \ Pool$_2$	**attack**	non-attack
attack	(r_1, r_2)	$(r_1, \tilde{r}_2)$
non-attack	$(\tilde{r}_1, r_1)$	$(\tilde{r}_1, \tilde{r}_2)$

- Prisoners' Dilemma (unique Nash equilibrium)

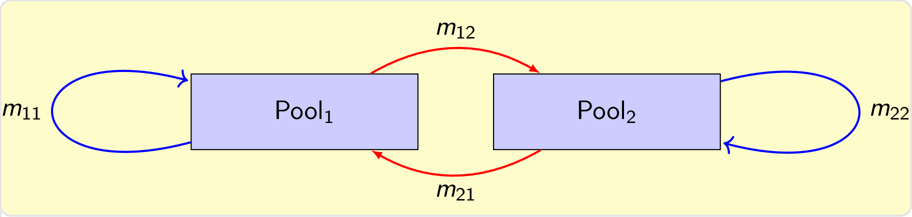


Figure: Pool game with $N = \{\mathrm{Pool}_1, \mathrm{Pool}_2\}$.

Setting

- Infiltration rates estimation has a level of uncertainty. At time step t,
  - Pool_2 estimates with probability p_1 that Pool_1 attacks with the correct infiltration rate $m_{12}(t)$ and with probability p_2 that Pool_1 attacks with infiltration rate $\hat{m}_{12}(t)$, with $p_1 + p_2 = 1$
  - Pool_1 does not experience any uncertainty in the estimations, and believes that Pool_2 attacks with the correct infiltration rate $m_{21}(t)$

Setting

- Bayesian game, $BG = \langle N, S, \Theta, p, U \rangle$
  - Pool_1 has one type $\Theta_{\text{Pool}_1} = \{\theta_{\text{Pool}_1,1}\}$
  - Pool_2 has two types $\Theta_{\text{Pool}_2} = \{\theta_{\text{Pool}_2,1}, \theta_{\text{Pool}_2,2}\}$

Pool₁ \ Pool₂	attack	non-attack
attack	(r_1, r_2)	$(r_1, \tilde{r}_2)$
non-attack	$(\tilde{r}_1, r_2)$	$(\tilde{r}_1, \tilde{r}_2)$

Table 1. Types: $\theta_{\text{Pool}_1,1}, \theta_{\text{Pool}_2,1}$

Pool₁ \ Pool₂	attack	non-attack
attack	(r_1, r_2')	$(r_1, \hat{r}_2)$
non-attack	$(\tilde{r}_1, r_2')$	$(\tilde{r}_1, \hat{r}_2)$

Table 2. Types: $\theta_{\text{Pool}_1,1}, \theta_{\text{Pool}_2,2}$

Theoretical results

Lemma: Polynomial infiltration rates

Consider a Bayesian Pool game BG with $|N|$ pools. If for all Information types $i \in \Theta$ in the BG, $m^i_j(t)$, $m^i_{jk}(t)$ are non-zero polynomials of equal degree $d \in \mathbb{N}$ with non-negative coefficients such that $m^i_{jj}(t) \geq \sum_{k \setminus \{j\}} m^i_{jk}(t)$ $\forall i \in [|N|]$ and $\forall t \in \mathbb{N}$, then the pool density revenues converge.

Lemma: Spectrum of IR

Consider a Bayesian Pool game BG with $|N|$ pools. If for all Information types $i \in \Theta$ in the BG, $\mathbf{m}^i(t)$ are bounded, and $\mathbf{IR}^i(t)$ are such that $\|\mathbf{IR}^i(t)\| \leq 1$ $\forall t \in \mathbb{N}$, then the pool revenues converge.

Numerical results

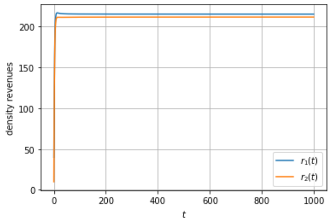
(upper) $m_{ij}(t) \in \mathbb{P}_1$

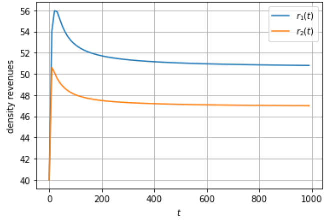
(lower) $m_{ij}(t) \in \mathbb{P}_3$

non-negative coefficients

Initial infiltration rates

$m_{11}(0)$	$m_{12}(0)$	$m_{21}(0)$	$m_{22}(0)$	p
80	20	30	70	.7
90	10	40	60	.3





Setting

- the pools have incorrect information regarding the mining power and the density revenues. At time step t,
  - actual situation in Table 3
  - Pool_1 knows the Pool game in Table 4
  - Pool_2 knows the Pool game in Table 5

	s_1	s_2
s_1	(r_1, r_2)	$(r_1, \tilde{r}_2)$
s_2	$(\tilde{r}_1, r_2)$	$(\tilde{r}_1, \tilde{r}_2)$

Table 3. Actual Game

	s_1	s_2
s_1	$(\dot{r}_1, \dot{r}_2)$	$(\dot{r}_1, \hat{r}_2)$
s_2	$(\hat{r}_1, \dot{r}_2)$	$(\tilde{r}_1, \hat{r}_2)$

Table 4. Pool_1 game

	s_1	s_2
s_1	$(\bar{r}_1, \bar{r}_2)$	$(\bar{r}_1, \hat{r}_2')$
s_2	$(\hat{r}_1', \bar{r}_2)$	$(\tilde{r}_1, \hat{r}_2')$

Table 5. Pool_2 game

Setting

- the pools have incorrect information regarding the mining power and the density revenues. At time step t,
  - actual situation in Table 3
  - Pool_1 knows the Pool game in Table 4
  - Pool_2 knows the Pool game in Table 5

	s_1	s_2
s_1	(r_1, r_2)	$(r_1, \tilde{r}_2)$
s_2	$(\tilde{r}_1, r_2)$	$(\tilde{r}_1, \tilde{r}_2)$

Table 3. Actual Game

	s_1	s_2
s_1	$(\dot{r}_1, \dot{r}_2)$	$(\dot{r}_1, \hat{r}_2)$
s_2	$(\hat{r}_1, \dot{r}_2)$	$(\tilde{r}_1, \hat{r}_2)$

Table 4. Pool_1 game

	s_1	s_2
s_1	$(\bar{r}_1, \bar{r}_2)$	$(\bar{r}_1, \hat{r}'_2)$
s_2	$(\hat{r}'_1, \bar{r}_2)$	$(\tilde{r}_1, \hat{r}'_2)$

Table 5. Pool_2 game

- misinformed Pool game mG

Adaptation procedure

- Given the *nme*, $\mathcal{AD}$ will evaluate the information of the pools
- $\mathcal{AD}$ will proceed to the next time step. The density revenues matrices will take the form

	s_1	s_2
s_1	(r_1, r_2)	$(r_1, \tilde{r}_2)$
s_2	$(\tilde{r}_1, r_2)$	$(\tilde{r}_1, \tilde{r}_2)$

Table 3. Actual Game

	s_1	s_2
s_1	(r_1, r_2)	$(\dot{r}_1, \tilde{r}_2)$
s_2	$(\hat{r}_1, \dot{r}_2)$	$(\tilde{r}_1, \hat{r}_2)$

Table 6. Pool_1 game

	s_1	s_2
s_1	(r_1, r_2)	$(\bar{r}_1, \hat{r}'_2)$
s_2	$(\hat{r}'_1, \bar{r}_2)$	$(\tilde{r}_1, \hat{r}'_2)$

Table 7. Pool_2 game

Theoretical results

Lemma: Polynomial infiltration rates

Consider the finite misinformation Pool game mG, then if $m^i_j(t)$, $m^i_{jk}(t)$ are non-zero polynomials of equal degree $d \in \mathbb{N}$ with non-negative coefficients such that $m^i_{jj}(t) \geq \sum_{k \setminus \{j\}} m^i_{jk}(t)\ \forall i \in [|N|]$ and $\forall t \in \mathbb{N}$, then the pool density revenues converge.

Lemma: Spectrum of IR

Consider the finite misinformation Pool game mG, $\mathbf{m}^i(t)$ are bounded, and $\mathbf{IR}^i(t)$ are such that $\|\mathbf{IR}^i(t)\| \leq 1\ \forall t \in \mathbb{N}$, then the pool revenues converge.

Numerical results

(upper) $m_{ij}(t) \in \mathbb{P}_1$

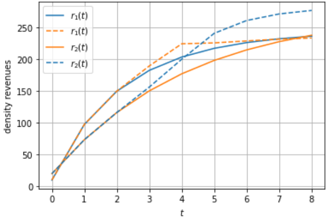
(lower) $m_{ij}(t) \in \mathbb{P}_3$

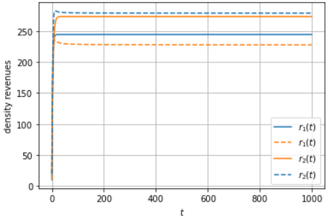
non-negative coefficients

Initial infiltration rates

Game	$m_{11}(0)$	$m_{12}(0)$	$m_{21}(0)$	$m_{22}(0)$
G^0	80	20	30	70
G^{Pool_1}	90	10	40	60
G^{Pool_2}	70	30	20	80

Adaptation procedure





- Blockchain interactions, pool games
- improve the results of [Eyal, IEEE'14]
- transfuse the pool game setting to the incomplete and the incorrect information cases
- provide theoretical results

! develop mechanisms/protocols to regulate the efficiency of a pool game

! study situations other than the block withholding attack scenario

Thank you!