Game Theoretical Analysis of Blockchain Users' Behaviors

presented by : **Marianna Belotti**
defended on : Decembre 16^{th}, 2021

HESAM UNIVERSITÉ
le cnam

THESIS directed by :
Stefano Secci, Professor, Cnam

Maria Potop-Butucaru, Professor, Sorbonne University

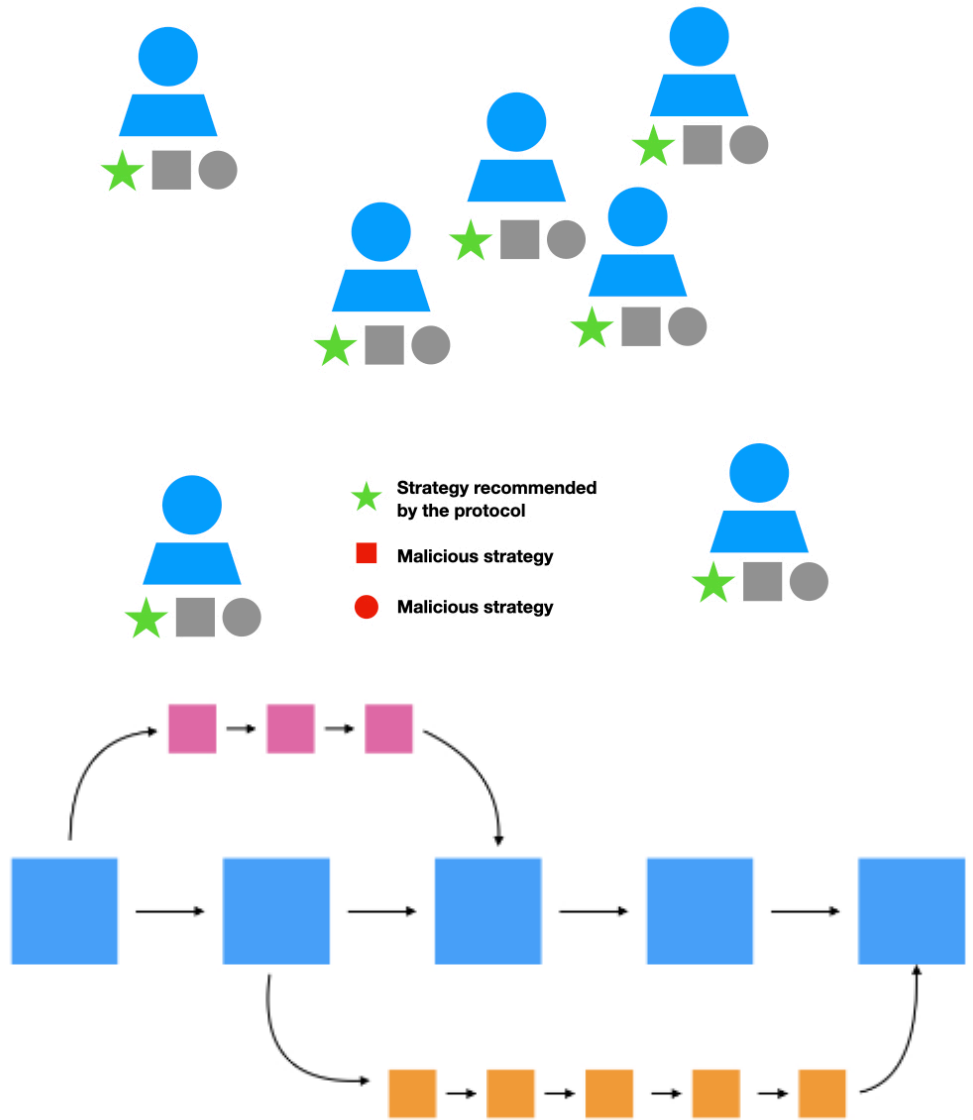
Caisse des Dépôts GROUPE

and co-advised by :
Stefano Moretti, Senior Researcher, CNRS, Paris Dauphine University PSL

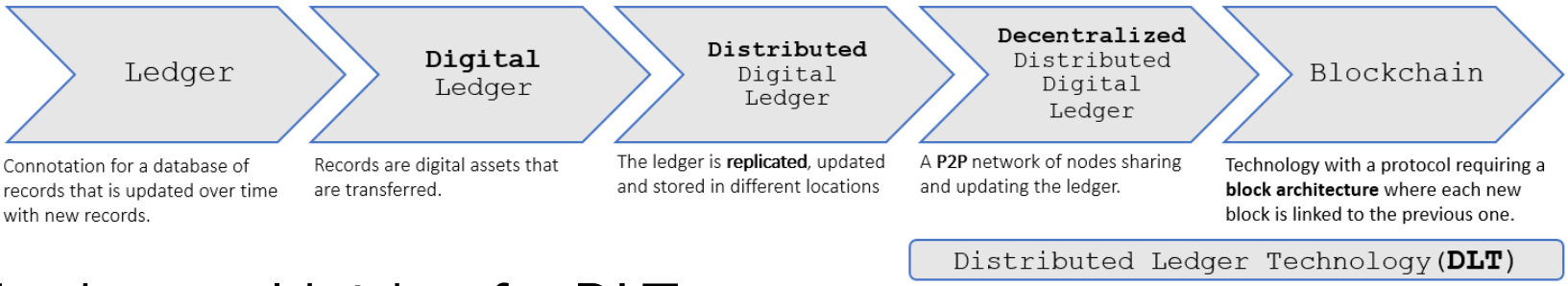
JURY

Maurice Herlihy	Professor, Brown University, USA	Reviewer
Emmanuelle Anceaume	Senior Researcher, IRISA, France	Reviewer
Nicolas Maudet	Professor, Sorbonne University, France	Examiner
Julien Prat	Professor, ENSAE, France	Examiner
Silvia Bonomi	Professor, La Sapienza University, Italy	Examiner
Henning Ahnert	European Central Bank, Germany	Invited
Nadia Filali	Caisse des Dépôts, France	Invited

THÈSE


Strategy recommended by the protocol
Malicious strategy
Malicious strategy

Introduction on DLTs



Fundamental bricks of a DLT:

- **Data Structure** (*e.g., Bitcoin UTXO*)
- **Communication Language** to update the ledger state (*e.g., transactions and smart-contract*)
- **Agreement Protocol** (*e.g., Bitcoin proof-of-work*)

Blockchain Actors and Transaction Journey

Transacting parties: a blockchain transaction involves two different types of actors related to single or multiple blockchain users: the *data-sender* and the *data-receiver*.

Validating nodes: run the consensus algorithm and are responsible for establishing the agreement on the proposals made by other validators or by leading nodes.

1. **Transaction Creation**
   - Signing transactions
2. Transaction Propagation
   - Collect transactions in blocks
4. **Transaction Validation**
5. Transaction Confirmation

Overview

Goal: We analyze the two main types of blockchain users (i.e., transacting parties and validating nodes) as well as different blockchains (i.e., permissionless and permissioned) with the scope of providing a general overview of the topic and formal results on **blockchain users' behaviors**.

		Behavior Model	
		Rational	*Byzantine*
Blockchain User	*Validating nodes*	*Miners*	*Robustness layer-1 blockchains*
	Transacting parties	*Interoperbility*	*Robustness layer-2 blockchains*

Rationality and Games

Pillars of game theory:

1. Agents **rationality**: players are fully able to analyze the problem (i.e., the game) and take the right decisions.
2. Each player is able to **order** the outcomes of the game according to consistent preferences.

Game $\longrightarrow$ blockchain consensus protocol, mining game, swap protocol
Players $\longrightarrow$ validating nodes, transacting parties
Strategy $\longrightarrow$ follow the instructions of a protocol or deviate
Payoff $\longrightarrow$ value of the final outcome (utility function)

How players play

- **Non-Cooperative Games**: individually as solo players
- **Cooperative Games**: in groups forming coalitions

Definitions

Definition (Non-cooperative or Strategic Game)

A game in a normal form representation is identified by a tuple $\boxed{\Gamma = \langle N, \mathcal{S}, u \rangle}$, where

- N is a finite set of n players
- $\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \times \mathcal{S}_n$ where $\mathcal{S}_i$ is the set of strategies of player i
- $u : \mathcal{S} \rightarrow \mathbb{R}^n$ is the utility function of the players.

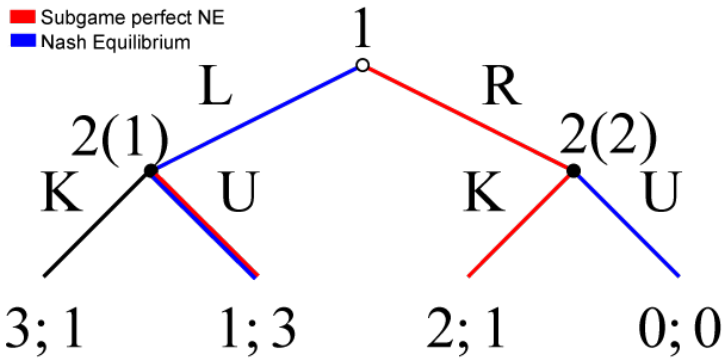
Definition (Nash equilibrium)

A strategy profile $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_i, \ldots, \sigma_n) \in \mathcal{S}$ is a Nash equilibrium if for every player i and for every strategy $\tau_i \in S_i$ we have that :

$$u_i(\sigma_1, \sigma_2, \ldots, \sigma_i, \ldots, \sigma_n) \geq u_i(\sigma_1, \sigma_2, \ldots, \tau_i, \ldots, \sigma_n)$$

Game Representations

- **Sequential games**: players play one after the other
- **Normal form games**: players' actions do not have an order (can take place simultaneously)

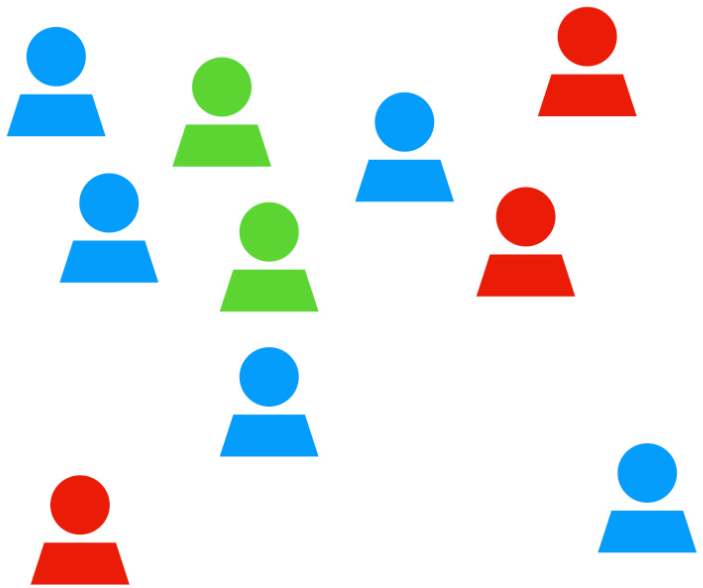


	(K,K)	(K,U)	(U,U)	(U,K)
L	3,1	3,1	1,3	1,3
R	2,1	0,0	0,0	2,1

BAR: Rational, Altruistic and Byzantine

Both blockchain users are at first modeled as **rational agents**. This game-theoretical modeling enables to capture several behaviors. To be more generic (i.e., including also irrational or unexpected malicious behaviors) blockchain users are modeled also as **Byzantine agents**. Users can be split into 3 categories:

- Byzantine, when they deviate arbitrarily from the protocol
- Altruistic, when they follow the protocol
- Rational, when they act to maximize their utility function



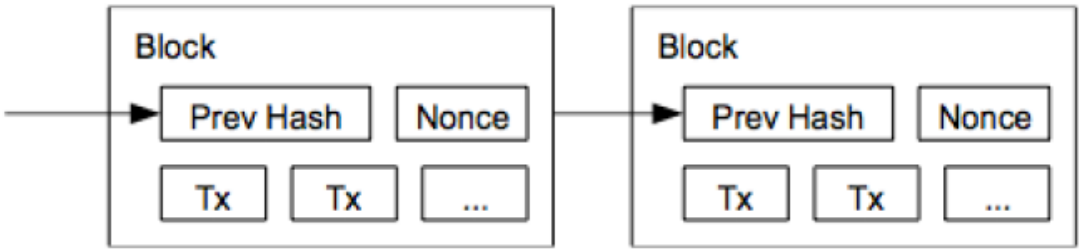
Overview

1. Belotti et al. "A vademecum on blockchain technologies: When, which, and how." IEEE Communications Surveys Tutorials 21.4 (2019): 3796-3838.
2. Belotti et al. "Bitcoin pool-hopping detection." 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI). IEEE, 2018.
3. Belotti et al. "Rewarding miners: bankruptcy situations and pooling strategies." Multi-Agent Systems and Agreement Technologies. Springer, Cham, 2020. 85-99. ⟵ *Bankruptcy (cooperative) games*
4. Belotti et al. "Game theoretical analysis of atomic cross-chain swaps." 40th IEEE International Conference on Distributed Computing Systems (ICDCS). 2020. ⟵ *Strategic games, NE*
5. Zappalà, Belotti et al. "Game theoretical Framework for Analyzing Blockchains Robustness." International Symposium on Distributed Computing (DISC). 2021. ⟵ *Strategic games, NE*

		Behavior Model	
		Rational	*Byzantine*
Blockchain User	*Validating nodes*	*Miners*	*Robustness layer-1 blockchains*
	Transacting parties	*Interoperbility*	*Robustness layer-2 blockchains*

Rational Miners

How to create bitcoins? Mining



SHA256(input, nonce) $\leq$ difficulty target

nonce = **full solution** and **share** = next to valid solution.
Pools' rewarding systems based on the number of **reported** shares.

The rewarding method adopted by a pool take into account that:

- Miners are **rational** agents.
- *Strategic behaviors:* WHEN reporting shares & WHERE directing the effort.

- Division into **rounds**: time elapsing between 2 full solutions.
- Reward allocation: $R : \mathrm{s} \rightarrow [0,1]^n$ where $\mathrm{s} \in \mathbb{N}^n$ vector of total number of shares reported by each miner in a **round**.

Original rewarding methods

Two types of malicious behaviors are analyzed; *pool-hopping* and *block-withholding*.

Original Rewarding Methods:

1. **proportional**: $R_i(\mathbf{s}) = \frac{s_i}{||\mathbf{s}||_1}$.
2. **pay-per-share**: $R_i(\mathbf{s}) = \frac{s_i}{D}$.

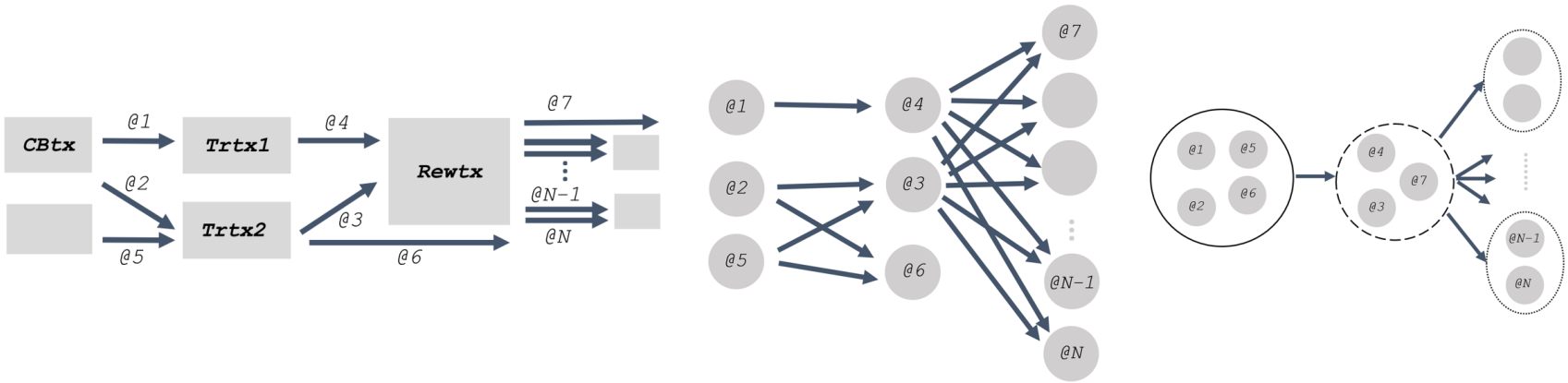
Issues:

- **Favoring Pool-Hopping** –> change pool during the round.
  The longer the round, the less each share is worth
- **Block Withholding** –> Pools go bankruptcy.
  The longer the round, the more each share is worth

Investigating the Network

Coinbase transactions, *Rewarding transactions*, *Transferring transactions*

- Identify miners –> **User sub-network** of a *subset* of transactions.
- Identify potential hoppers –> Filtering rewarding transactions.
- Identify real hoppers –> Transactions **reordering**.

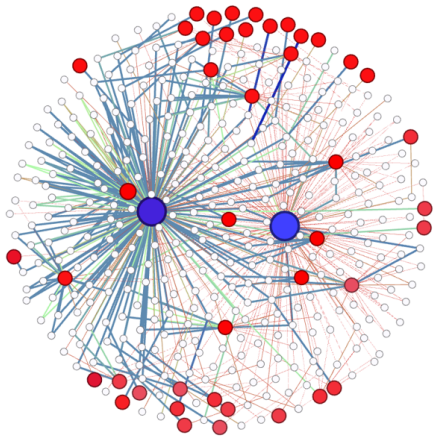


Transaction network –> **Address** network –> **User** network

mapping procedure: basic heuristics applied to all network addresses.

Results

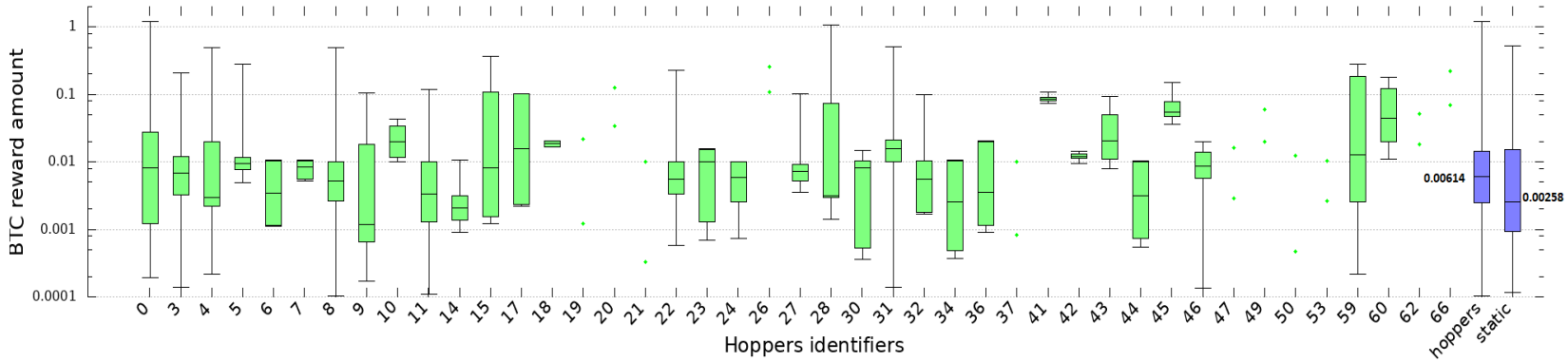
2-pool: Slush and Kano pool (*slush* and *pplns* methods) **time period**: April 6-20, 2016



Left blue: Kano pool
Right blue: Slush pool
Red nodes: detected hoppers

Edge **thickness** and **color** depend on the frequency of users interactions.

higher gains hopping i.e., earn on average more than the default miners.



Incentive Compatible Rewarding Function

Division into *rounds* where $||\mathbf{s}||_1$ shares are submitted.

1. **proportional**: $R_i(\mathbf{s}) = \frac{s_i}{||\mathbf{s}||_1}$.
2. **pay-per-share**: $R_i(\mathbf{s}) = \frac{s_i}{D}$.

Proposition

(**Incentive Compatibility**) A reward function R is *incentive compatible* when every miner's best response strategy $\sigma(R)$ reports full solutions immediately.

$$R_i^{(ic)}(\mathbf{s}, w) = \begin{cases} \frac{s_i}{D} + \mathbf{1}_{\{i=w\}}\left(1 - \frac{||\mathbf{s}||_1}{D}\right), & \text{if } ||\mathbf{s}||_1 < D \\ \frac{s_i}{||\mathbf{s}||_1}, & \text{if } ||\mathbf{s}||_1 \geq D \end{cases}$$

where w is the discoverer of the full solution.

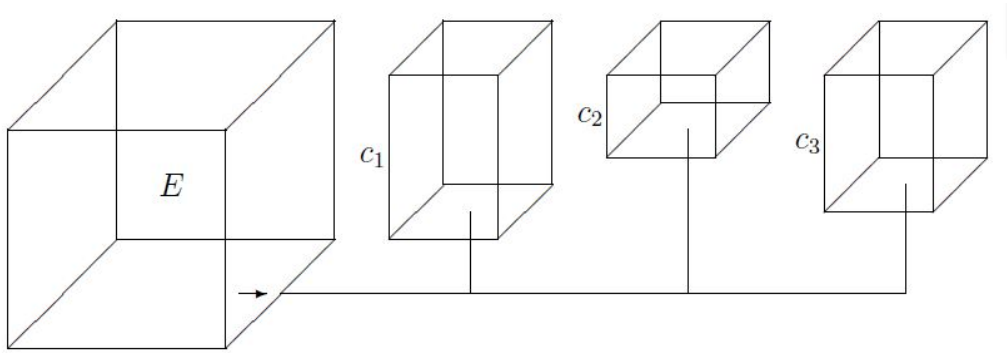
Reinterpretation as an outcome of a bankruptcy game

Bankruptcy Games - CEL

Definition

A *bankruptcy game* on the set N consists of a pair $(\mathbf{c}, E) \in \mathbb{R}^N \times \mathbb{R}$ with $c_i \geq 0$ for all $i \in N$ and $0 < E < \sum_{i \in N} c_i = C$. For each bankruptcy problem $(\mathbf{c}, E) \in \mathbb{B}^N$,

- **Proportional** rule **(P)**:
  $f(\mathbf{c}, E) = \lambda \mathbf{c}, \qquad \lambda : \sum_{i \in N} \lambda c_i = E$
- **Constrained equal losses** rule **(CEL)**:
  $f(\mathbf{c}, E) = \max\{c_i - \lambda, 0\}, \quad \lambda : \sum_{i \in N} \max\{c_i - \lambda, 0\} = E$



idea: CEL can prevent pool-hopping.

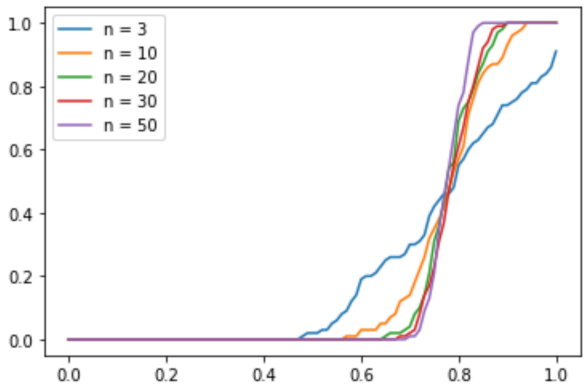
New Incentive Compatible Reward Function

$$\widehat{R}_i(\mathbf{s}, w) = \begin{cases} \frac{s_i}{D} + \mathbf{1}_{\{i=w\}}\left(1 - \frac{||\mathbf{s}||_1}{D}\right), & \text{if } ||\mathbf{s}||_1 < D \\ \frac{\mathbf{1}_{\{i=w\}}}{D} + \max\left(\frac{s_i}{D} - \lambda, 0\right) \quad \lambda : \text{efficiency}, & \text{if } ||\mathbf{s}||_1 \geq D \end{cases}$$

Proposition

The reward function R proposed by *Schrijvers et. al.* always gives miners a positive incentive $\delta_{\text{hop}} > 0$ to perform pool hopping. CEL-based reward function gives less incentive to pool hopping.

Estimate percentage $p(\alpha)$ non-hoppers and simulate its values.

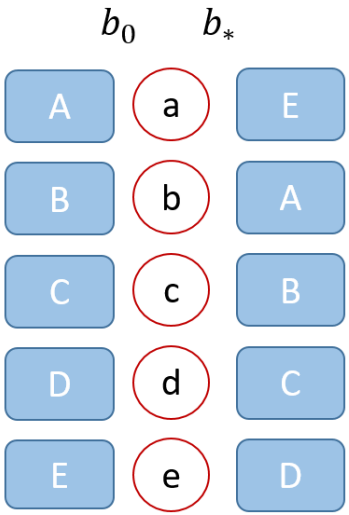


Swap Problem

Rational Agent: Rational Transacting Parties

A ***swap problem*** is a tuple $\boxed{\langle \mathcal{A}, \mathcal{O}, b_0, b_*, (u_i)_{i\in\mathcal{O}} \rangle}$ where:

- $\mathcal{A} = \{1, \ldots, m\}$ is the set of *assets*;
- $\mathcal{O} = \{1, \ldots, n\}$ is the set of *owners* or *agents*, with $m \geq n$;
- $b_0, b_* : \mathcal{A} \to \mathcal{O}$ (both **surjective**) the *original* and the *desired* ownership map;
- u_i is the payoff function for owner $i \in \mathcal{O}$ over bundles of assets in $2^{\mathcal{A}}$ such that $u_i(b_0^{-1}(i)) < u_i(b_*^{-1}(i))$ and for any $S, T \in 2^{\mathcal{A}}$ with $S \subseteq T$ we have $u_i(T) \geq u_i(S)$, $\forall i \in \mathcal{O}$.



Step 1: Decentralized Exchange protocols

Step 2: Decentralized Swap protocols

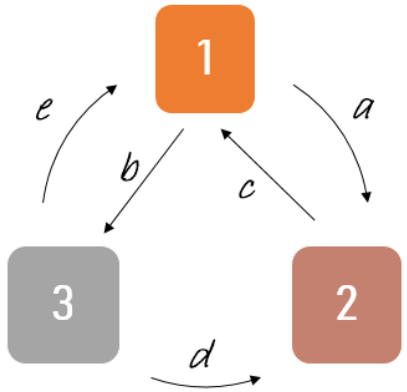
Step 3: Blockchain Swap protocols

Decentralized Exchange Protocols

A sequence $\boxed{\sigma = \{(A^k, O^k, X^k) : |A^k| \geq |O^k|\}_k}$, $k \in \{1, \ldots, t\}, t \in \mathbb{N} : t \leq m$ defines a **decentralized exchange protocol** where:

- $A^k \subseteq \mathcal{A}$ asset involved in the exchange at step k;
- $O^k \subseteq \mathcal{O}$ owners involved in the exchange at step k;
- $X^k : A^k \to O^k$ (surjective) specifies the owner $X^k(a) \in O^k$ of any asset $a \in A^K$ at step k;

A *decentralized swap protocol* is a decentralized exchange protocol where $\{A^k : k = 1, \ldots, t\}$ is a partition of $\mathcal{A}$.



Example. $\mathcal{A} = \{a, b, c, d, e\}, \mathcal{O} = \{1, 2, 3\}$, $b_0 = (1, 1, 2, 3, 3)$ and $b_* = (2, 3, 1, 2, 1)$.

$\sigma = (\{a, c\}, \{1, 2\}, \{X^1(a) = 2, X^1(c) = 1\}), (\{b, e\}, \{1, 3\}, \{X^2(b) = 3, X^2(e) = 1\}), (\{d\}, \{2\})$.

Decentralized Blockchain Swap Protocols

Assets involved in the swap should be ***locked*** for the following reasons:

(i) consequently to failures in the assets locking, the initial situation must be restored;

(ii) once an asset transfer is committed all the other transfers have to be committed, too.

Any transfer should be conditioned on the correct asset locking.

A **decentralized blockchain swap protocol** is defined by the pair $\boxed{(\sigma_P, \sigma_T)}$ where

- $\sigma_P = \{(A^j, O^j)\}_{j \in \{1,\dots,t_P\}}$, $t_P \in \mathbb{N} : t_P \leq m$, $A^j \subseteq \mathcal{A}, O^j \subseteq \mathcal{O}$ is a sequence such that $\forall j \in \{1, \dots, t_P\}$, $O^j = \{o \in \mathcal{O} : o \in b_*(A^j) \vee o \in b_0(A^j)\}$;
- $\sigma_T = \{(A^k, O^k, X^k)\}_{k \in \{1,\dots,t_T\}}$ is a swap protocol engendering the sequence of maps $b_1^{\sigma_T}, \dots, b_{t_T}^{\sigma_T} : \mathcal{A} \to \mathcal{O}$.

Strategic and Extensive form Games

Definition

A *decision function* as a map $F : \{1, \ldots, t\} \to \mathcal{O} \cup \mathcal{T}$ that specifies which owner $F(k)$ has the power to decide at step k whether to transfer A^k to O^k. F_T is **effective** on σ_T iff $F_T(k) = O^k$ for any $k \in \{1, \ldots, t_T\}$.

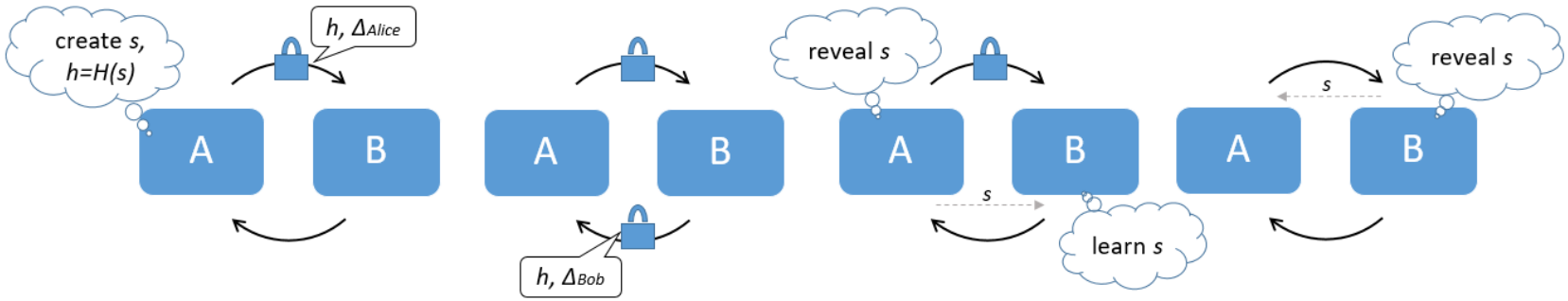
1. Swap protocols with *sequential publishing* and *commitment*.
2. Swap protocols with *concurrent publishing* and *snap commitment*.

1. **Extensive games**: sequential phases.
2. **Normal form games**: concurrent phase.

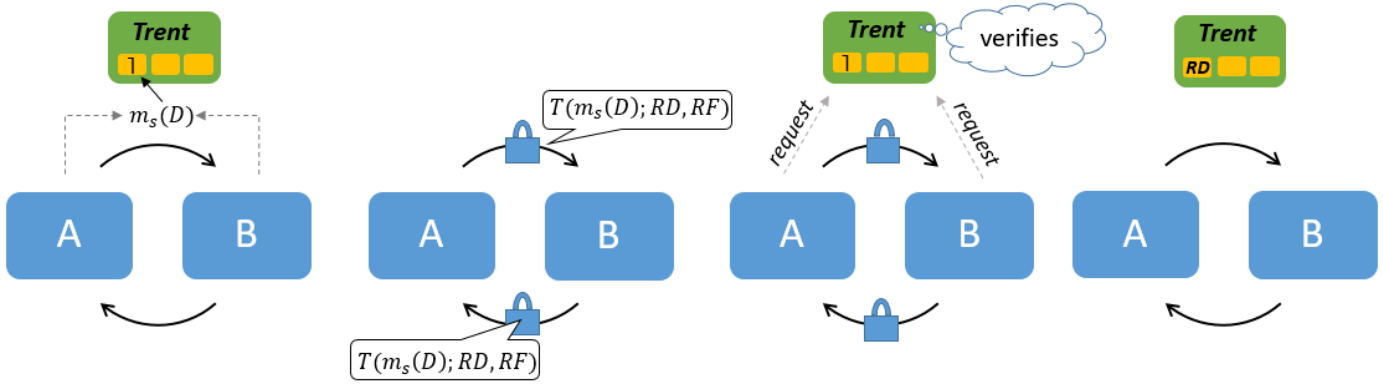
Strategies:

- **Follow**: each player follow the protocol in every step.
- **Deviate**: the player decide to behave *irrationally* or *maliciously* and decide not to publish or not to trigger a transaction.

Sequential (*Nolan*) and Concurrent-Snap protocols



Alice swaps x Acoins for y Bcoins owned by Bob.Nolan's first protocol for UTXO-based blockchains (**not atomic**).
$\sigma_P = \{(x, B), (y, A)\}, F_P(j) = \{A, B\}, j = \{1, 2\}; \sigma_T = \{(y, A), (x, B)\}, F_T(k) = \{A, B\}, k = \{1, 2\}.$

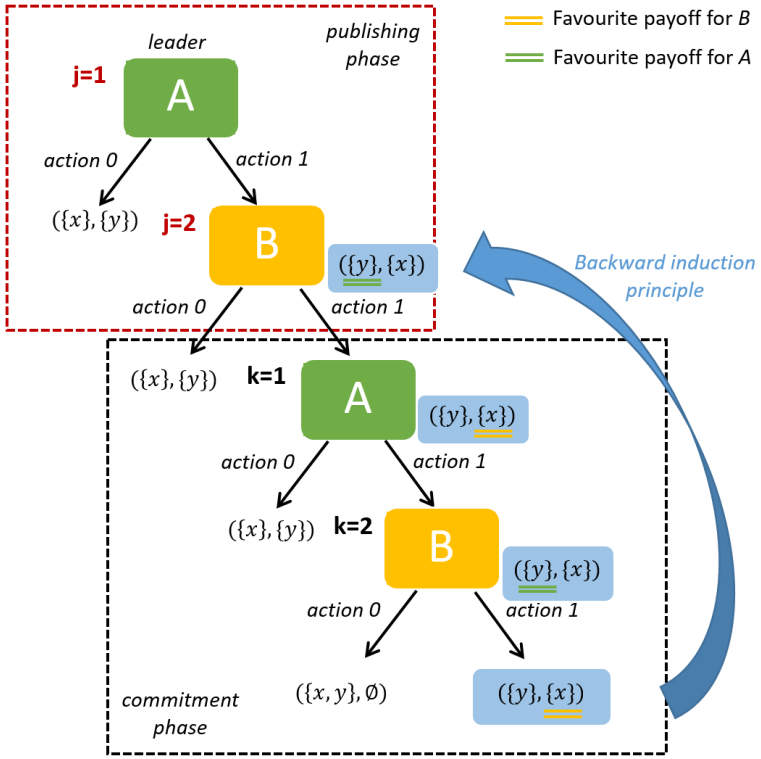


Atomic protocol with central authority. $\sigma_P = \{(\{x, y\}, \{A, B\})\}, F_P(j) = \{A, B\}, j = \{1\};$
$\sigma_T = \{(\{x, y\}, \{A, B\}, \{X^1(x) = B, X^1(y) = A\})\}, F_T(k) = T, k = \{1\}.$

Results

Proposition

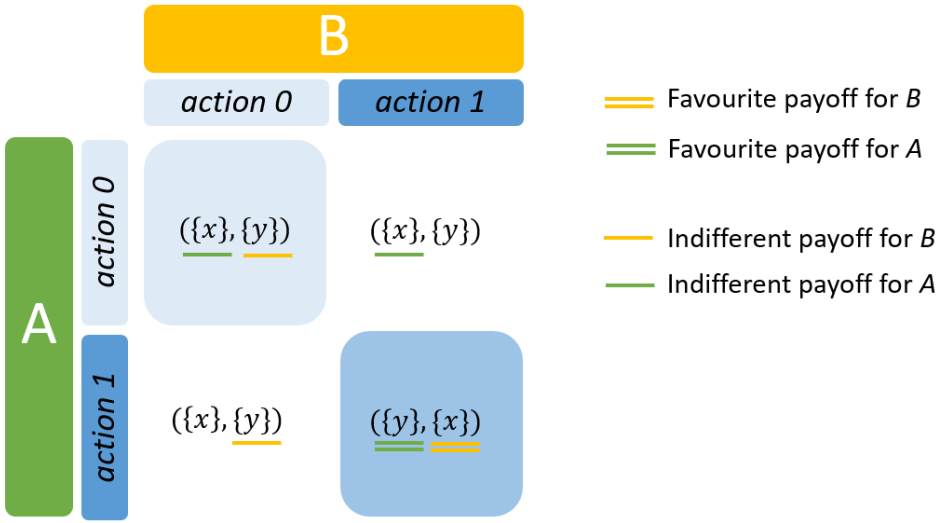
Let Γ^{σ} be the extensive form game associated with a sequential swap problem, if F is **effective**, then the strategy profile $(\hat{s}_1, \ldots, \hat{s}_n)$ that specifies action 1 (follow the protocol) at any node is the **unique subgame perfect equilibrium**.



Results - part 2

Proposition

Let Γ be the strategic form game associated with a swap problem characterized by a *concurrent publishing and a snap commitment* where the decision function F_T is such that $F_T(k) = T \in \mathcal{T}\ \forall k \in \{1, \ldots, t_T\}$. Then, the strategy profile $(\hat{s}_1, \ldots, \hat{s}_n)$ that specifies action 1 for every player i is a **Nash equilibrium**.



Goal and Approach

- Byzantine, when they deviate arbitrarily from the protocol
- Altruistic, when they follow the protocol
- Rational, when they act to maximize their utility function

		Behavior Model	
		Rational	*Byzantine*
Blockchain User	*Validating nodes*	*Miners*	*Robustness layer-1 blockchains*
	Transacting parties	*Interoperbility*	*Robustness layer-2 blockchains*

Goal. **Characterize** and **measure** in a formal and general way the robustness of a blockchain protocol.
Approach.

- List all the protocol instructions
- Identify all the possible behaviors of the users when facing the protocol
- List and evaluate all the possible outcomes

Model - Mechanism and Robustness Properties

Definition

A game in a normal form representation is identified by a tuple $\Gamma = \langle N, \mathcal{S}, u \rangle$.
A **mechanism** is a pair $\boxed{(\Gamma, \sigma)}$ in which $\Gamma = \langle N, \mathcal{S}, u \rangle$ is a game and $\sigma \in \mathcal{S}$ is a joint strategy.

We fix the **maximum number of rational players allowed in a game such that the protocol still provides the same utility to altruistic players**.

Property

A joint strategy $\sigma \in \mathcal{S}$ is a **k-resilient** equilibrium if for all $C \subseteq N$ with $1 \leq |C| \leq k$, all $\tau_C \in \mathcal{S}_C$ and all $i \in C$, we have $u_i(\sigma_C, \sigma_{-C}) \geq u_i(\tau_C, \sigma_{-C})$.

Model - Mechanism and Robustness Properties

We fix the **maximum number of byzantine players allowed in a game such that the altruistic players always get at least the utility of the initial state**.

Property

A joint strategy $\sigma \in \mathcal{S}$ is **t-weak-immune** if for all $T \subseteq N$ with $|T| \leq t$, all $\tau_T \in \mathcal{S}_T$ and all $i \in N \setminus T$, we have $u_i(\sigma_{-T}, \tau_T) \geq 0$.

Definition

Given 2 games A, B with the same set of players N it is possible to define a new game $\boxed{C = A \odot B}$, called **composition** of A and B, which is characterized as follows.
$C = \langle N, (s_{Ai}, s_{Bi}), u_A + u_B \rangle$.

The compositions preserves the robustness properties

Results

Here some **indices** to measure robustness of *layer-1* (users = **validating nodes**) and *layer-2* (user = **transacting parties**) blockchain protocols

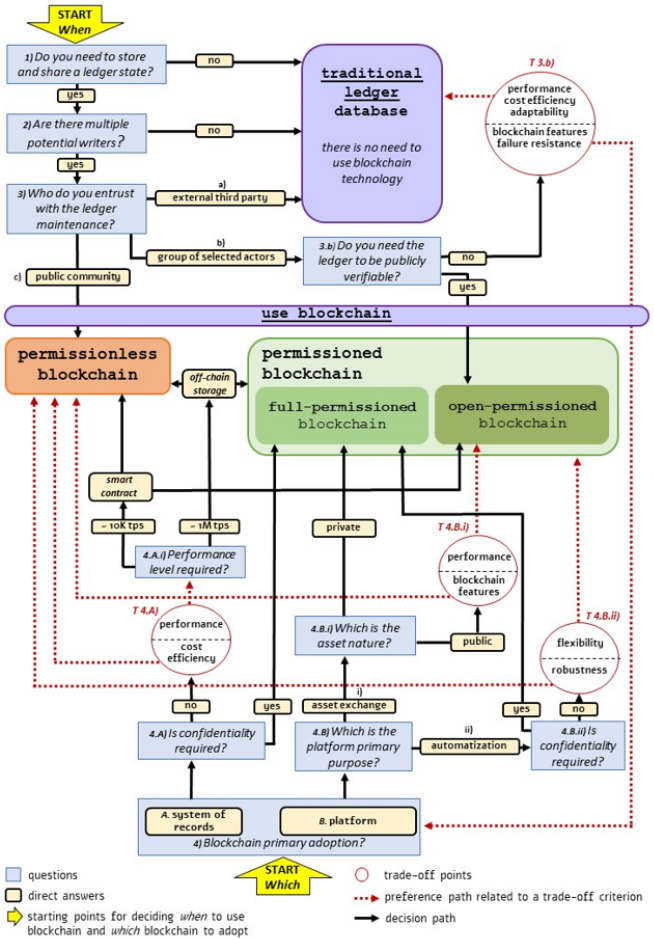
Protocol	k-Resilience	t-Weak Immunity
Tendermint	**Yes, k** $< n/3$	**Yes, t** $< n/3$
Bitcoin	**Yes, k** $< 3n/20$	**No**
Lightning Network	**Yes, k** $< 3n/20$	**No**
Closing module	Yes	No
(Alternative closing module)	(Yes)	(Yes)
Other modules	Yes	Yes
Side-chain (Platypus)	**Yes, k** $< n/3$	**Yes, t** $< n/3$
Cross-chain Swap	**Yes**	**Yes**

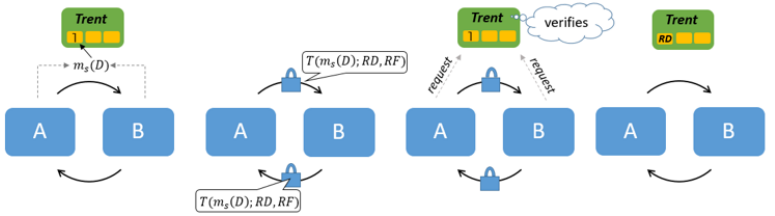
Present Works

1. Belotti et al. "A vademecum on blockchain technologies: When, which, and how." IEEE Communications Surveys Tutorials 21.4 (2019): 3796-3838.
2. Belotti et al. "Bitcoin pool-hopping detection." 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI). IEEE, 2018.
3. Belotti et al. "Rewarding miners: bankruptcy situations and pooling strategies." Multi-Agent Systems and Agreement Technologies. Springer, Cham, 2020. 85-99.
4. Belotti et al. "Game theoretical analysis of atomic cross-chain swaps." 40th IEEE International Conference on Distributed Computing Systems (ICDCS). 2020.
5. Zappalà, Belotti et al. "Game theoretical Framework for Analyzing Blockchains Robustness." International Symposium on Distributed Computing (DISC). 2021.

Present Works - Industrial Side

User as **early adopter** facing several challenges: using the technology, respecting the regulation and which role to assume in a blockchain protocol.





Future Works

Future working directions.

1. **Rational Behaviors**. modeling blockchain systems with fewer assumptions.
2. **Solution Concepts**. analysis of blockchain users' behaviors with other solution concepts.

3. **Blockchain Users' Behaviors**. extend analysis not only to new blockchain protocols but also to include new protocol deviations.
4. **Rewarding Miners**. applying the analysis to other crypto-currencies with comparable and new consensus methods.

Thanks for the Attention