Marianna Belotti

Swap Introduction

Preliminary results

Swap as Games

Protocols

Equilibria

Game Theoretical Analysis of Cross-Chain Swaps

Marianna Belotti[1] , Maria Potop-Butucaru [2] , Stefano Moretti[3] and Stefano Secci[4]

Tokenomics 2020, Toulouse, France

26/10/2020

[1] Groupe Caisse des Dépôts - Cnam

[2] Sorbonne Université

[3] Université Paris Dauphine

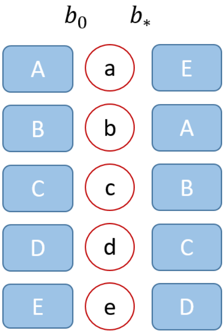
[4] Cnam

Swap Problem

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

Swap Problem



- 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 $u_i(T) \geq u_i(S)$, for each $i \in \mathcal{O}$.

Decentralized Swap Protocols

Let $\sigma = \{(A^k, O^k, X^k) : |A^k| \geq |O^k|\}_k$, $k \in \{1, \ldots, t\}, t \in \mathbb{N} : t \leq m$ be a sequence of exchanges 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 sequence σ defines a **decentralized exchange protocol** that engenders a sequence of maps $b_1^\sigma, b_2^\sigma, \ldots, b_t^\sigma : \mathcal{A} \to \mathcal{O}$ such that for all $k \in \{1, 2, \ldots, t\}$:

- $b_k^\sigma(z) = b_{k-1}^\sigma(z), \; \forall z \in \mathcal{A} \setminus A^k$;
- $b_k^\sigma(z) = X^k(z), \forall z \in A^k$,

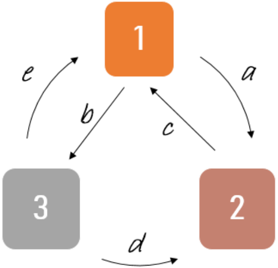
where we set $b_0^\sigma = b_0$.

Decentralized Swap Protocols - example

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

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

$b_1 = (2, 1, 1, 3, 3), b_2 = (2, 3, 1, 3, 1), b_3 = (2, 3, 1, 2, 1) = b_*$.



Decentralized Atomic Swap Protocols

1. A **decentralized swap protocol** is a decentralized exchange protocol where $\{A^k : k = 1, \ldots, t, t \in \mathbb{N} : t \leq m\}$ is a partition of $\mathcal{A}$.
2. σ is *efficient* if the engendered sequence is such that $b_t^\sigma = b_*$.
3. σ is *atomic* if efficient or $b_t^\sigma = b_0$.

How to reach **all-or-nothing atomicity**?

Assets involved in the swap should be *locked*. Once locked, the transfer commitment allows every participant to redeem the new swapped asset(s).

Decentralized Blockchain Swap Protocols

(i) any commitment should be conditioned on the correct asset locking;

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

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

- A **decentralized blockchain swap protocol** is defined by the pair (σ_P, σ_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 $b_1^{\sigma_T}, \dots, b_{t_T}^{\sigma_T} : \mathcal{A} \to \mathcal{O}$.

Preliminary Results - pt.1

1. (σ_P, σ_T) is *atomic* if $b^{\sigma_T}_{t_T} = b_0$ or $b^{\sigma_T}_{t_T} = b_*$.

Definition (commitment requirement)

Given (σ_P, σ_T) if in σ_P, $\exists \bar{j} \in \{1, \ldots, t_P\} : O^{\bar{j}} \cap b_0(A^{\bar{j}}) \neq \emptyset$ then, in σ_T, $b^{\sigma_T}_k = b_0 \; \forall k \in \{1, \ldots, t_T\}$.

Whenever there exists an asset transfer that is not correctly published, then no asset transfer is committed.
The commitment requirement is a **necessary condition** (not sufficient) for a blockchain swap protocol to be atomic.

Preliminary Results - pt.2

Proposition

Given a commitment protocol then, replacing O^k by $b^{\sigma_T}_{k-1}(A^k)$ in σ_T, i.e., considering a new sequence $\sigma^k_T = (A^1, O^1),$ $\dots, (A^{k-1}, O^{k-1}), (A^k, b^{\sigma_T}_{k-1}(A^k)), (A^{k+1}, O^{k+1}), \dots, (A^{t_T}, O^{t_T}),$ implies that:

(i) $\left(b^{\sigma^k_T}_{t_T}\right)^{-1}(O^k) \subseteq \left(b^{\sigma_T}_{t_T}\right)^{-1}(O^k)$ and,

(ii) $\left(b^{\sigma^k_T}_{t_T}\right)^{-1}(b^{\sigma_T}_{k-1}(A^k)) \supseteq \left(b^{\sigma_T}_{t_T}\right)^{-1}(b^{\sigma_T}_{k-1}(A^k)).$

Preliminary Results - pt.3

Marianna Belotti

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.

Definition

A decision function F_T is **effective** on σ_T if and only if $F_T(k) = O^k$ for any $k \in \{1, \ldots, t_T\}, t_T \in \mathbb{N} : t_T \leq m$.

Strategic and Extensive form Games

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

1. **Extensive games**: sequential phases .
2. **Strategic 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.

Result for sequential protocols

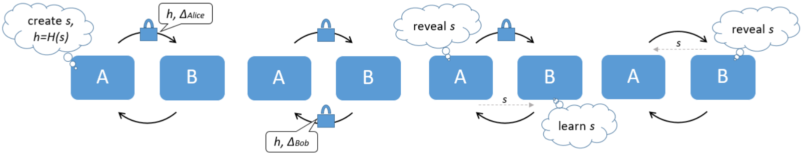
Proposition

Let Γ^{σ} be the extensive form game associated with a swap problem, let (σ_P, σ_T) be a blockchain swap protocol and let $F_T : \{1, \ldots, t_T\} \to \mathcal{O} \cup \mathcal{T}$ be a decision function.
If F is **effective** on σ_T, 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 (in dominant strategies).

Proof: By the first claim of Proposition 1, the deviating player ends up with a set of assets that is contained in the one that the player would obtain if she/he specifies action 1. Then, proved for the monotonicity of the utility function.

Blockchain Sequential Protocol

Tier Nolan's first protocol for UTXO-based blockchains (not atomic). Alice aims swapping x bitcoins for y litecoins owned by Bob.



$\Delta_{Alice} < \Delta_{Bob}$

$$\sigma_P = \{(x, B), (y, A)\}, \quad F_P(j) = \{A, B\}, \quad j = \{1, 2\};$$

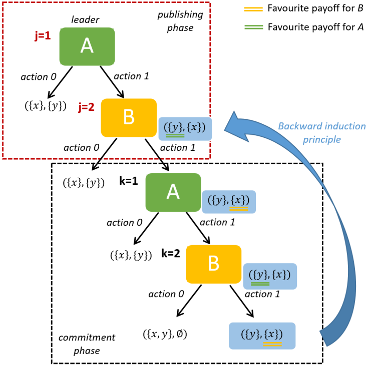
$$\sigma_T = \{(y, A), (x, B)\} \quad F_T(k) = \{A, B\}, \quad k = \{1, 2\}.$$

Blockchain Sequential Protocol

Marianna Belotti

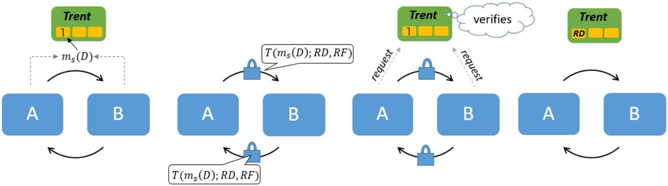
Corollary

In the protocol (σ_P, σ_T) presented above the strategy profile $(\hat{s}_1, \ldots, \hat{s}_n)$ specifying action 1 (follow the protocol) at any node is the unique subgame perfect equilibrium (in dominant strategies).



Blockchain Concurrent-Snap Protocol

Alice aims swapping x bitcoins for y litecoins owned by Bob. Atomic protocol for the role of Trent (central authority).



$$\sigma_P = \{(\{x, y\}, \{A, B\})\}, \quad F_P(j) = \{A, B\}, \quad j = \{1\};$$

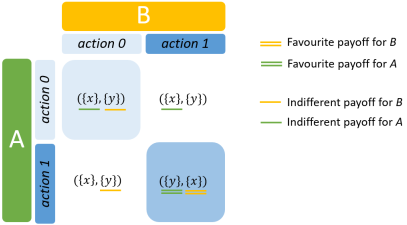
$$\sigma_T = \{(\{x, y\}, \{A, B\}, \{X^1(x) = B, X^1(y) = A\})\}$$

$$F_T(k) = T, k = \{1\}.$$

Blockchain Concurrent-Snap Protocol

Proposition

Let Γ be the strategic form game associated with a swap problem, let (σ_P, σ_T) be a blockchain swap protocol 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 (follow the protocol) for every player i is a **Nash equilibrium**.



Thank you for the attention