Cross Chain Swaps with Preferences

Eric Chan*  Marek Chrobak  Mohsen Lesani

University of California at Riverside, USA
CSF 2023
Cross Chain Swap
Cross Chain Swap
Cross Chain Swap – Fair Exchange

[Diagram showing a circular exchange process involving two parties, A and B, with Bitcoin (₿) and Ethereum (Ξ) tokens.]
Cross Chain Swap – Fair Exchange
Formalization
Swap Digraph

A -> B
B -> C
C -> A
Outcomes

- **Deal**: \(\langle all \mid all\rangle\)
- **NoDeal**: \(\langle none \mid none\rangle\)
- **Discount**: \(\langle all \mid \neg all\rangle\)
- **FreeRide**: \(\langle \neg none \mid none\rangle\)
- **Underwater**: \(\langle \neg all \mid \neg none\rangle\) (everything else)
Outcomes

- **Deal:** \( \langle all \mid all \rangle \)
- **NoDeal:** \( \langle none \mid none \rangle \)
- **Discount:** \( \langle all \mid \neg all \rangle \)
- **FreeRide:** \( \langle \neg none \mid none \rangle \)
- **Underwater:** \( \langle \neg all \mid \neg none \rangle \) (everything else)
Outcomes

- **Deal**: \(\langle all \mid all \rangle\)
- **NoDeal**: \(\langle none \mid none \rangle\)
- **Discount**: \(\langle all \mid \neg all \rangle\)
- **FreeRide**: \(\langle \neg none \mid none \rangle\)
- **Underwater**: \(\langle \neg all \mid \neg none \rangle\) (everything else)
Outcomes

- Deal: \(\langle all \mid all \rangle\)
- NoDeal: \(\langle none \mid none \rangle\)
- Discount: \(\langle all \mid \neg all \rangle\)
- FreeRide: \(\langle \neg none \mid none \rangle\)
- Underwater: \(\langle \neg all \mid \neg none \rangle\) (everything else)
Outcomes

- **Deal**: \(<all | all>\)
- **NoDeal**: \(<none | none>\)
- **Discount**: \(<all | \neg all>\)
- **FreeRide**: \(<\neg none | none>\)
- **Underwater**: \(<\neg all | \neg none>\) (everything else)
Partial Ordering of Outcomes

- **Deal**: \( \langle all \mid all \rangle \)
- **NoDeal**: \( \langle none \mid none \rangle \)
- **Discount**: \( \langle all \mid \neg all \rangle \)
- **FreeRide**: \( \langle \neg none \mid none \rangle \)
- **Underwater**: \( \langle \neg all \mid \neg none \rangle \) (everything else)
Partial Ordering of Outcomes

- **Deal**: $\langle all \mid all \rangle$
- **NoDeal**: $\langle none \mid none \rangle$
- **Discount**: $\langle all \mid \neg all \rangle$
- **FreeRide**: $\langle \neg none \mid none \rangle$
- **Underwater**: $\langle \neg all \mid \neg none \rangle$ (everything else)
Partial Ordering of Outcomes

- **Deal**: \(\langle all \mid all\rangle\)
- **NoDeal**: \(\langle none \mid none\rangle\)
- **Discount**: \(\langle all \mid \neg all\rangle\)
- **FreeRide**: \(\langle \neg none \mid none\rangle\)
- **Underwater**: \(\langle \neg all \mid \neg none\rangle\) (everything else)
Partial Ordering of Outcomes

- **Deal:** \( \langle all \mid all \rangle \)
- **NoDeal:** \( \langle none \mid none \rangle \)
- **Discount:** \( \langle all \mid \neg all \rangle \)
- **FreeRide:** \( \langle \neg none \mid none \rangle \)
- **Underwater:** \( \langle \neg all \mid \neg none \rangle \) (everything else)
Protocol Properties
Atomic Protocol Properties

- **Liveness**: if every party follows $\mathcal{P}$, then every party finishes $\text{Deal}$
- **Safety**: if a party follows $\mathcal{P}$, then it finishes in an acceptable outcome
- **Strong Nash Equilibria**: No coalition improves its payoff by deviating from $\mathcal{P}$
Atomic Protocol Properties

- **Liveness**: if every party follows $\mathbb{P}$, then every party finishes DEAL
- **Safety**: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- **Strong Nash Equilibria**: No coalition improves its payoff by deviating from $\mathbb{P}$
Atomic Protocol Properties

- **Liveness**: if every party follows $\mathcal{P}$, then every party finishes DEAL
- **Safety**: if a party follows $\mathcal{P}$, then it finishes in an acceptable outcome
- **Strong Nash Equilibria**: No coalition improves its payoff by deviating from $\mathcal{P}$
Herlihy’s Protocol

[Herlihy’18] gives an atomic protocol so long that:

- the swap digraph is strongly connected
- each party has the preference structure:

```
UNDERWATER  →  NO DEAL  →  FREE RIDE  →  DISCOUNT
```

Acceptable →
Can We Do Better?
The Underwater Class
Preferences

\[
\begin{align*}
&\langle \text{T} | \text{P} \rangle_{\text{UNDERWATER}} \quad \text{Acceptable} \rightarrow \\
&\langle \text{P} | \text{P} \rangle_{\text{UNDERWATER}}
\end{align*}
\]
User-defined Preferences

- **NoDeal** ➔ **Deal**

- *Inclusive Monotonicity:*

  \[
  \langle \text{T}, \text{P} \mid \text{T}, \text{P} \rangle \rightarrow \langle \text{T}, \text{P} \mid \text{T} \rangle
  \]

  \[
  \langle \text{T}, \text{P} \mid \text{T}, \text{P} \rangle \rightarrow \langle \text{T}, \text{P}, \text{S} \mid \text{T}, \text{P} \rangle
  \]
General Atomic Protocol?

- *Liveness*: if every party follows $\mathbb{P}$, then every party finishes *Dear or better*

- *Safety*: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome

- *Strong Nash Equilibria*: No coalition improves its payoff by deviating from $\mathbb{P}$
General Atomic Protocol?

- **Liveness**: if every party follows $\mathbb{P}$, then every party finishes **DEAL or better**
- **Safety**: if a party follows $\mathbb{P}$, then it finishes in an acceptable outcome
- **Strong Nash Equilibria**: No coalition improves its payoff by deviating from $\mathbb{P}$

No, there is no atomic protocol (scheme) that works for every swap system.
No General Atomic Protocol

Preference of A:

Deal

\langle \text{T-shirt} , \text{Shirt} \rangle
No General Atomic Protocol

Preference of A:

Preference of B:
No General Atomic Protocol

Preference of A:

Preference of B:
No General Atomic Protocol – Case 1

Preference of A:

Preference of B:

Case 1
No General Atomic Protocol – Case 1

Preference of A:
\[
\text{Deal} \rightarrow \langle \text{ } | \text{ } \rangle
\]

Preference of B:
\[
\text{Deal} \rightarrow \langle \text{ } | \text{ } \rangle
\]

Case 1: Not strong Nash equilibria
No General Atomic Protocol – Case 2

Preference of A:

Preference of B:

Case 2
No General Atomic Protocol – Case 2

Preference of A:

Preference of B:

Case 2: Not live
Sometimes, There Is a Protocol
Theorem

Theorem. $S = (D, P)$ has an atomic protocol iff there exists a spanning subgraph $G$ of $D$ such that:

- $G$ is piece-wise strongly connected and has no isolated vertices
- $G$ dominates $D$
- no subgraph $H$ of $D$ strictly dominates $G$
Example

Preference of A:

Preference of B:
Example

Preference of A:

\[
\text{Deal} \rightarrow \langle \text{T-shirt} | \text{T-shirt} \rangle
\]

Preference of B:

\[
\text{Deal} \rightarrow \langle \text{T-shirt} | \text{Dark T-shirt} \rangle
\]
Example

Preference of A:

Deaf

Preference of B:

Deaf

Preference of C:

Deaf

Preference of D:

Deaf
Condition 1

$G$ is piece-wise strongly connected and has no isolated vertices
Condition 1

$G$ is piece-wise strongly connected and has no isolated vertices.
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2

Preference of A:

Deal \rightarrow \{ \text{t-shirt} \mid \text{t-shirt} \}
Condition 2

Preference of A:
Condition 2

\( G \) dominates \( D \): each party in \( G \) ends at least as good as they do in \( D \)
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2

Preference of B:

\[ \langle \text{Deal} | \text{Deal} \rangle \]
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 2
Condition 2

$G$ dominates $D$: each party in $G$ ends at least as good as they do in $D$
Condition 3

no subgraph $H$ of $D$ strictly dominates $G$
Condition 3

no subgraph $H$ of $D$ strictly dominates $G$
Condition 3

no subgraph $H$ of $D$ strictly dominates $G$
Condition 3

Preference of A:

Preference of B:

Preference of C:

Preference of D:
Condition 3

no subgraph $H$ of $D$ strictly dominates $G$
Condition 3

no subgraph $H$ of $D$ strictly dominates $G$
Protocol
Applying Herlihy’s Protocol
Applying Herlihy’s Protocol
Applying Herlihy’s Protocol
Applying Herlihy’s Protocol

Condition 3: no subgraph $H$ of $D$ strictly dominates $G$
Complexity
SwapAtomic

SwapAtomic:

- **input**: swap system $S = (D, P)$
- **output**: Yes if $S$ has an atomic swap protocol, otherwise No
SwapAtomic

SwapAtomic:

- **input**: swap system $S = (D, P)$
- **output**: Yes if $S$ has an atomic swap protocol, otherwise No

*Theorem.* SwapAtomic is $\Sigma_2^P$-complete.
\( \Sigma_2^P \)-completeness

**Theorem.** \( S = (D, P) \) has an atomic protocol **iff** there exists a spanning subgraph \( G \) of \( D \) such that:

- \( G \) is piece-wise strongly connected and has no isolated vertices
- \( G \) dominates \( D \)
- no subgraph \( H \) of \( D \) strictly dominates \( G \)

\[ \exists G. \neg \exists H. \pi(G, H) \]
\( \Sigma_2^P \)-completeness

Theorem. \( S = (D, P) \) has an atomic protocol \( \text{iff} \) there exists a spanning subgraph \( G \) of \( D \) such that:

- \( G \) is piece-wise strongly connected and has no isolated vertices
- \( G \) dominates \( D \)
- no subgraph \( H \) of \( D \) strictly dominates \( G \)

\[ \exists G. \neg \exists H. \pi(G, H) \]
$\Sigma^P_2$-completeness

Theorem. $S = (D, P)$ has an atomic protocol iff there exists a spanning subgraph $G$ of $D$ such that:

- $G$ is piece-wise strongly connected and has no isolated vertices
- $G$ dominates $D$
- no subgraph $H$ of $D$ strictly dominates $G$

$\exists G. \neg \exists H. \pi(G, H)$
$\Sigma_2^P$-completeness

*Theorem.* $S = (D, P)$ has an atomic protocol iff there exists a spanning subgraph $G$ of $D$ such that:

- $G$ is piece-wise strongly connected and has no isolated vertices
- $G$ dominates $D$
- no subgraph $H$ of $D$ strictly dominates $G$

$$\exists G. \neg \exists H. \pi(G, H)$$
Example
Example

Diagram $D$ and $G$ show the connections between different elements.
Summary

- Relax structure of preference posets
- Characterize when swap systems have an atomic protocol
- If there is an atomic protocol, we give one
- Complexity of deciding whether a swap system has an atomic protocol
Thank You