Bazaar – Anonymous Resource Sharing
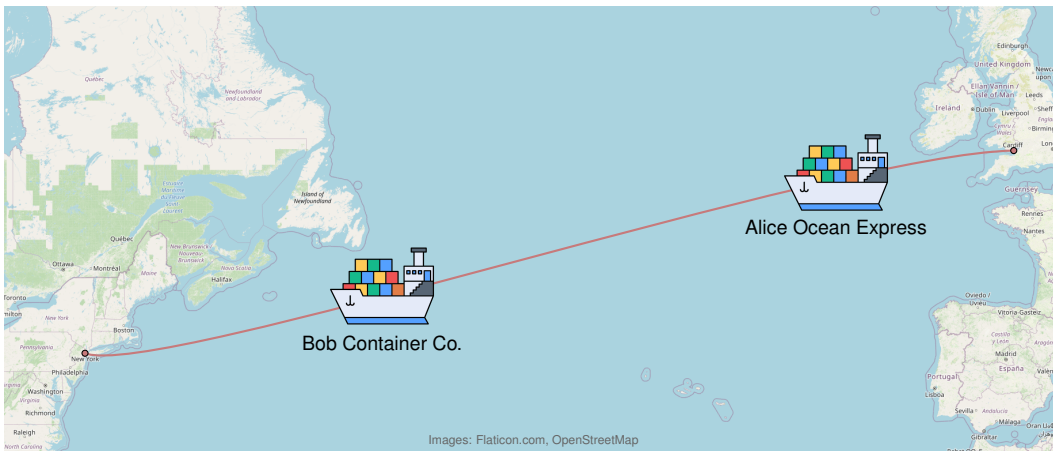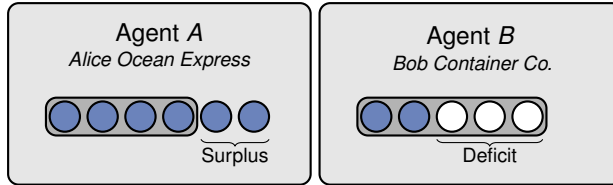
Christoph Coijanovic, Daniel Schadt, Christiane Weis, and Thorsten Strufe | 11/26/2023

Alice Ocean Express
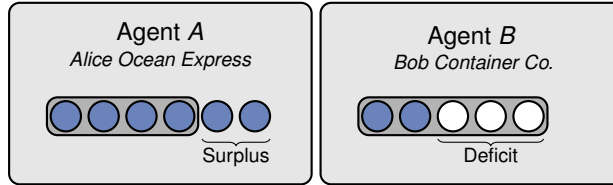
Bob Container Co.

Images: Flaticon.com, OpenStreetMap

Setting

Agent *A*
Alice Ocean Express

Surplus
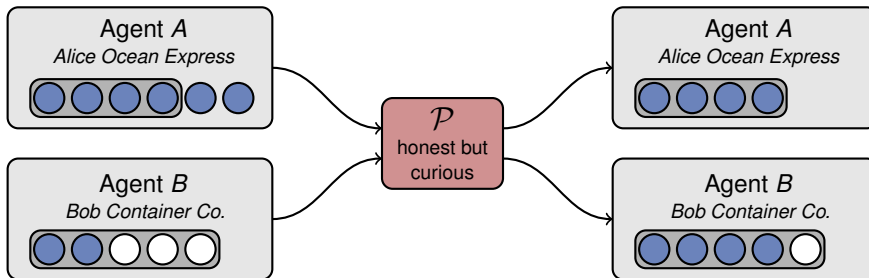
Agent *B*
Bob Container Co.

Deficit

Resource Usage Function RU.
Maps agents to their resource usage:

$$RU(A) = +2 \quad RU(B) = -3$$

Functionality

Privacy Goals

Agent-Usage Unlinkability

It should not be possible to link agents to their usage value.

Is *Bob Container Co.* failing?

Privacy Goals

Agent-Usage Unlinkability

It should not be possible to link agents to their usage value.

Is *Bob Container Co.* failing?

Usage Unobservaiblity

It should not be possible determine the distribution of usage values.

Is *someone* failing?

Bazaar

| Token Accumulation | Token Matching | Agent Coordination |

Require anonymous channel (e.g., Tor) that hides link between Agents and messages from $\mathcal{P}$.

Token Accumulation: Submit Resource Usage to $\mathcal{P}$

| Token Accumulation | Token Matching | Agent Coordination |

$(pk, sk) \leftarrow \text{KEYGEN}()$

$\texttt{type} \leftarrow \begin{cases} + & \text{if } RU(A) > 0 \\ - & \text{else} \end{cases}$

$\texttt{sig} \leftarrow \text{SIGN}(sk, pk \mid \texttt{type})$

pk
type
sig

- Agent A generates $|RU(A)|$ *tokens*
- A sends tokens individually over anonymous channel to $\mathcal{P}$
- Crucial: Anonymous channel ensures that $\mathcal{P}$ cannot tell which or how many tokens it receives from whom
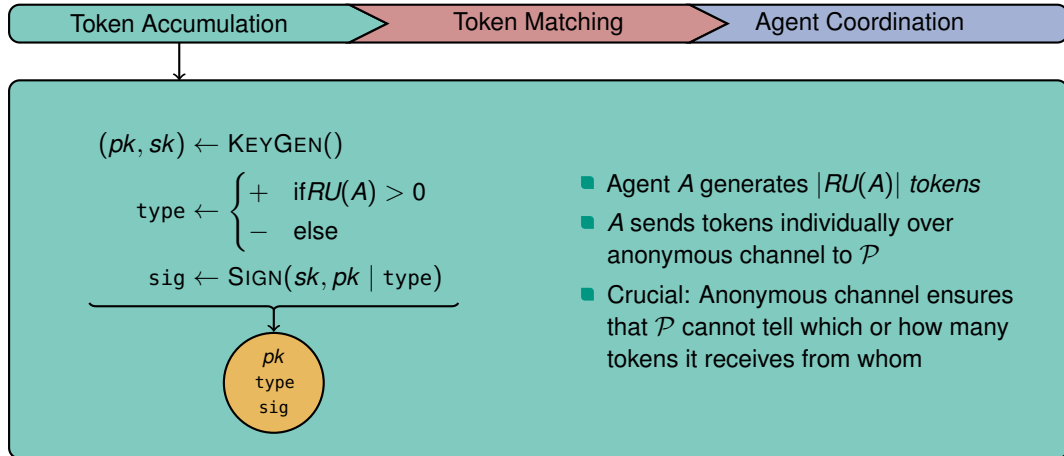
Token Matching: Determine Who Shares With Whom
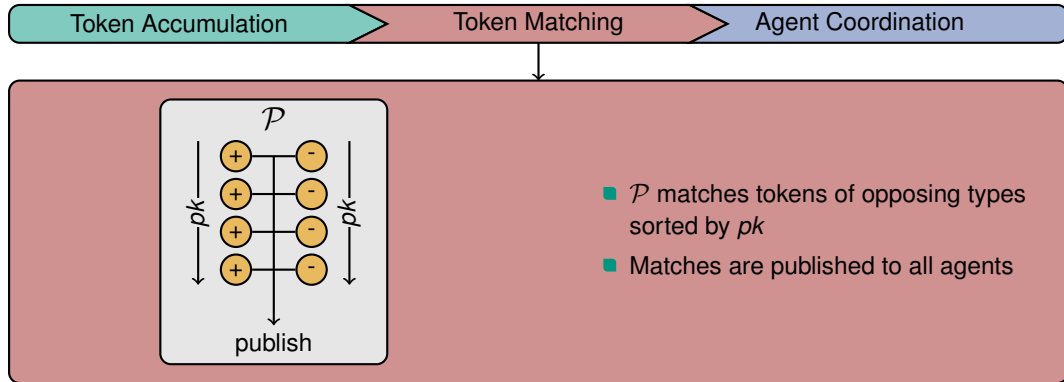
Agent Coordination: Let Matched Agents Communicate

| Token Accumulation | Token Matching | Agent Coordination |

$\mathrm{addr}_{AB} \leftarrow H(pk_A \parallel pk_B)$
$c_A \leftarrow \mathrm{ENC}(pk_B, m_A)$
$\mathrm{sig}_A \leftarrow \mathrm{SIGN}(sk_A, \mathrm{addr}_{AB} \parallel c_A)$

$\mathcal{P}$

addr_{AB} = addr_{AB}

c_a, sig_A c_B, sig_B

A B

c_B, sig_B c_A, sig_A

Dashed arrows indicate use of anonymous channel.

C. Coijanovic et al.: Bazaar – Anonymous Resource Sharing Chair of Privacy & Security – KASTEL
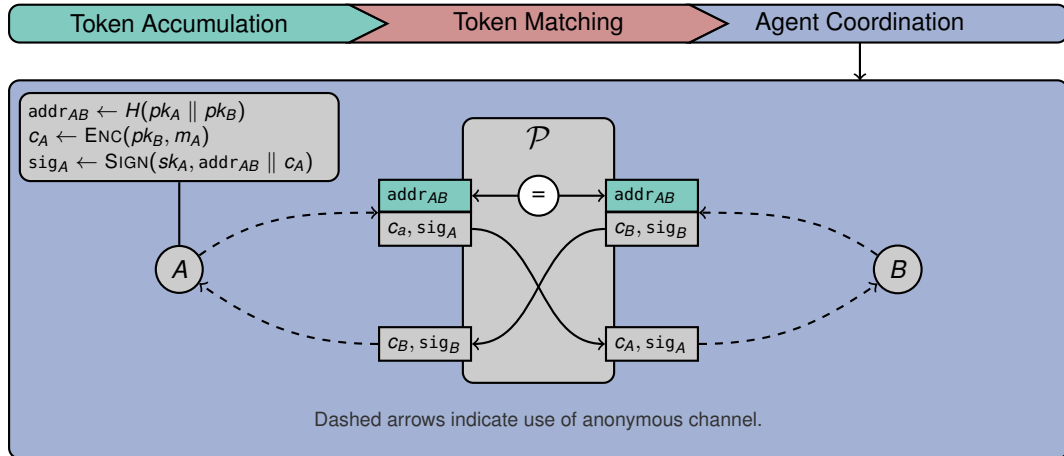
Future Directions

Stronger Adversaries

Enable protocol to protect against, e.g., GPA or malicious agents.

Bulk Resource Matching

Enable Alice to give all her surplus to one other party.

Multi Resource Settings

Enable multiple resources to be exchanged on the same market.

Summary

Resource sharing is nice and efficient. → Sharing should not introduce privacy risks. → Our protocol BAZAAR enables just that!