NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 48: Blockchain Interoperability - III

CONCEPTS COVERED

- Multi-party Cross-chain Swap
- Permissioned Blockchain Interoperability
- Data Transfer Across Multiple Hyperledger Fabric Networks in Two Verticals

KEYWORDS

- Cross Chain Swap
- Permissioned Blockchain Interoperability
- Interconnection Relay

Multi-Party Atomic Cross-chain Swap

- Carol wants to sell her Cadillac for bitcoins
- Alice can buy Carol's Cadillac, but wants to pay in an "alt-coin" cryptocurrency
- Bob ready to trade alt-coins for bitcoins
- Alice, Bob and Carol arrange a three-way swap:
  - Alice will transfer her alt-coins to Bob
  - Bob will transfer his bitcoins to Carol
  - Carol will transfer title of her Cadillac to Alice

M. Herlihy, "Atomic cross-chain swaps," in PODC, 2018

Multi-Party Atomic Cross-chain Swap

- Alice creates a secret s, h = H(s)
- Publishes a contract on the alt-coin blockchain with hashlock h and timelock 6Δ in the future, to transfer her alt-coins to Bob
- Bob first confirms that Alice's contract has been published on the alt-coin blockchain
- He then publishes a contract on the Bitcoin blockchain with the same hashlock h but with timelock 5Δ in the future, to transfer his bitcoins to Carol

M. Herlihy, "Atomic cross-chain swaps," in PODC, 2018

Multi-Party Atomic Cross-chain Swap

- Carol confirms Bob's contract is published on Bitcoin
- She publishes a contract on the automobile title blockchain with the same hashlock h, but with timeout 4Δ to transfer the Cadillac's title to Alice
- Alice confirms that Carol's contract has been published on the title blockchain
- she sends *s* to Carol's contract, acquiring the title and revealing *s* to Carol
- Carol sends *s* to Bob's contract, acquiring the bitcoins and revealing *s* to Bob
- Bob sends *s* to Alice's contract, acquiring the alt-coins and completing the swap

M. Herlihy, "Atomic cross-chain swaps," in PODC, 2018

Multi-Party Atomic Cross-chain Swap

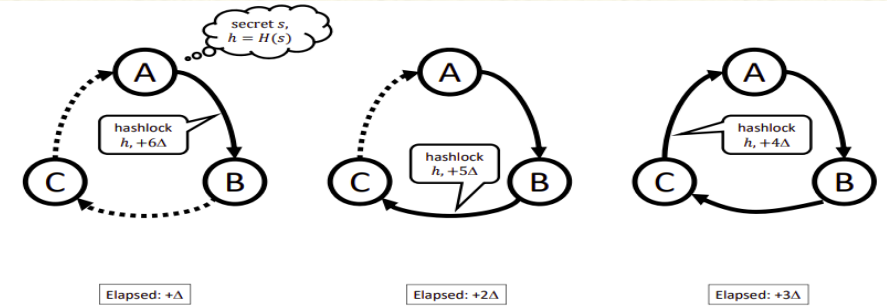


Figure 1: Atomic cross-chain swap: deploying contracts

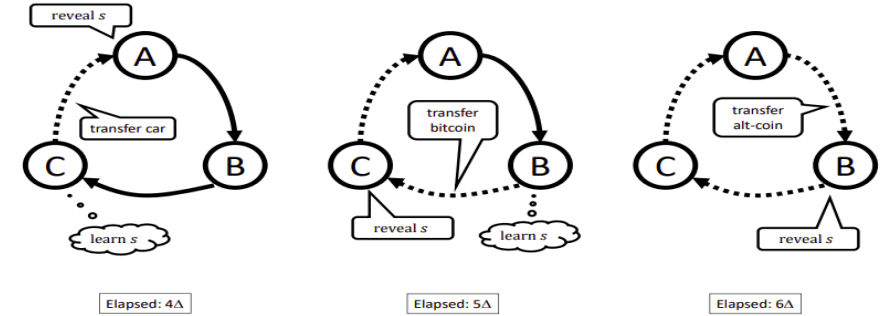


Figure 2: Atomic cross-chain swap: triggering arcs

M. Herlihy, “Atomic cross-chain swaps,” in PODC, 2018.

Validity of the Protocool

- If any party halts while contracts are being deployed, then all contracts eventually time out and trigger refunds
- If any party halts during triggering of contracts, only that party ends up worse off
    - If Carol halts without triggering her contract, then Alice gets the Cadillac and Bob gets a refund, so Carol's misbehavior harms only herself

M. Herlihy, "Atomic cross-chain swaps," in PODC, 2018

Interoperation in Permissioned Blockchains

- Permissioned blockchain networks are designed to be **private**, for a closed consortium
- **Different business sectors** tend to have different groups of organizations, thus have **separate blockchain networks**
- **TradeLens -** Logistics, **We.Trade** Trade finance, **IBM Food Trust** - Food Supply Chain, etc.
- **Continue to operate in complete isolation**
- N**eed for interoperation** between different isolated networks to achieve business goals

Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

Interoperation in Permissioned Blockchains

Challenges

- Here interoperation is specifically **Verifiable Data Transfer** between two separate permissioned blockchain networks
- Data in a blockchain network is generated by transactions going through **consensus process**
- Data **consistent with the source network's state**
- **Multiparty Trust - When one network consumes state from another, it needs to establish the state validity as per shared consensus view of parties in the network**

Use Case

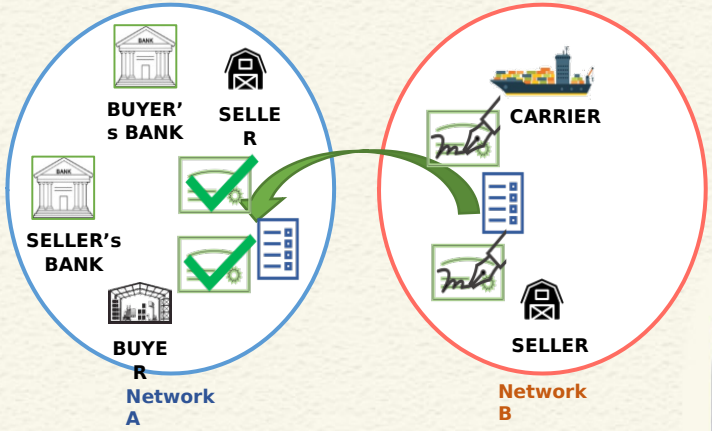
Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

- **We.Trade** is a trade financing network
- **TradeLens** is trade logistics network
- **Letter of Credit (L/C)** – a bank confirmation that ensures payment will be made by the buyer
- **Bill of lading** proves that the seller has dispatched the goods via the carrier,
- It enforces an obligation on the buyer (as per letter of credit terms) to make a payment.

Verifiable Data Transfer in Permissioned Blockchain

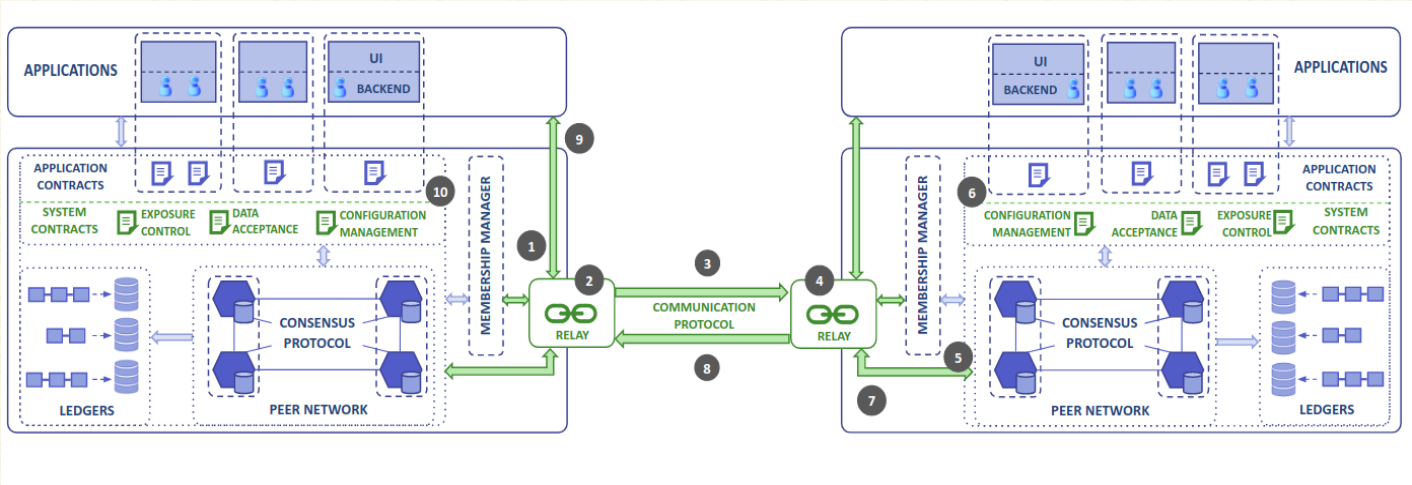
- Each data (block) in a network has a set of **endorsements** (signatures) **for consensus**
- This set of endorsements confirm the validity of a block in the network
- Thus, from the source, **data is accompanied with the set of signatures - Attestations**
- The attestations are **validated** in the destination network according to an **data acceptance policy**

Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Middleware '2019)



Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

Architecture



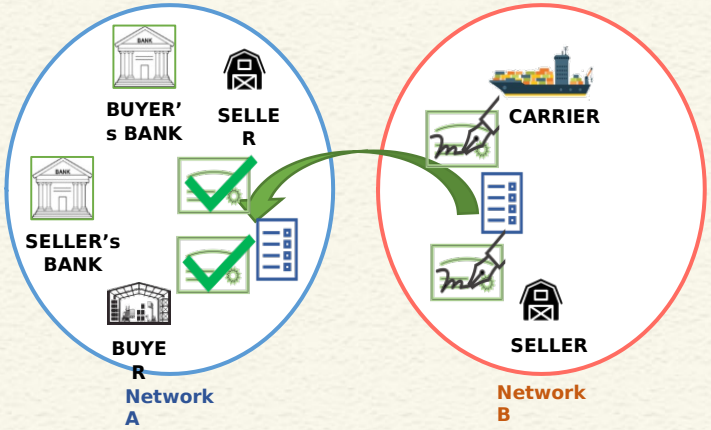
Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

- **Relay Service:** Provides the means of communication between the two separate networks
- **Configuration Management Contract:** Maintain identity (public keys) of the interoperating networks
- **Exposure Control Contract:** Define and enforce policies on what data to expose to which network
- **Data Acceptance:** Validate the data received from a foreign network against the policy that defines how many signatures are required (and other conditions) to verify a data

Protocol Overview

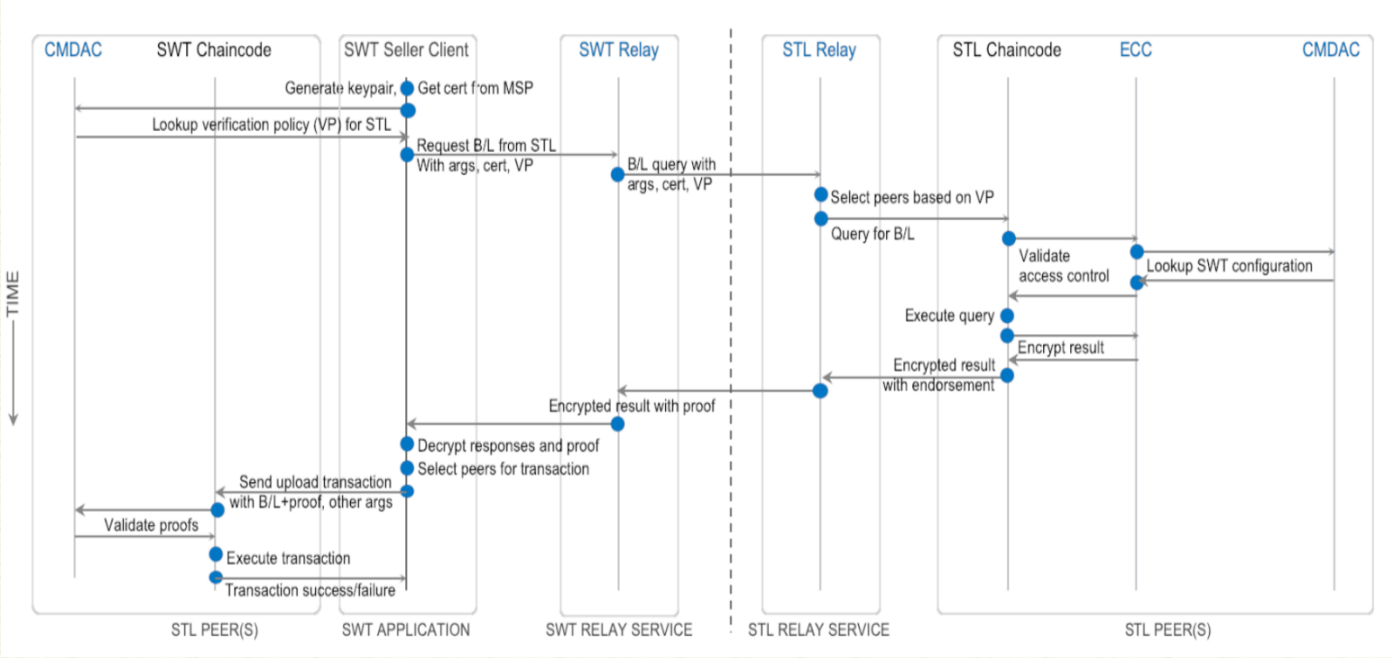
Steps:

1. Proof request is generated consisting of a verification policy which has to be met by the source network
2. Access control policies are checked
3. Response data along with proofs (endorsements) sent back through relay
4. Proofs validated against verification policy



Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

Protocol Details



Abebe, E. et al., 2019, December. Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th International Middleware Conference Industrial Track

CONCLUSIONS

- Explained how HTLC is used for three-party swap
- Permissioned blockchain interoperability
- Data transfer across different Hyperledger Fabric networks

REFERENCES

- Web resources as mentioned from time to time


Thank
you