NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural

Department of Computer Science & Engineering

Indian Institute of Technology Kharagpur

Lecture 47: Blockchain Interoperability - II

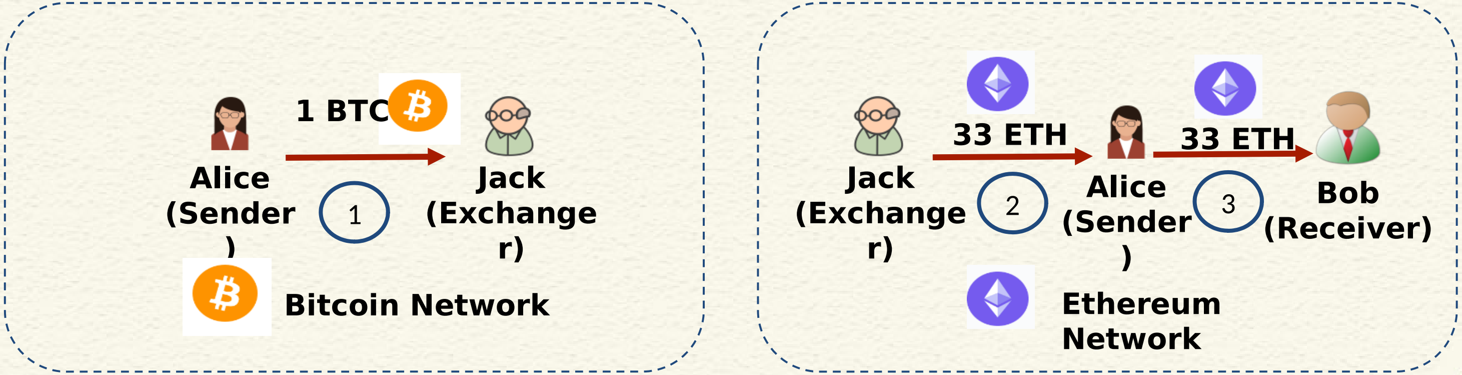
CONCEPTS COVERED

- Cross Chain Asset Exchange
- Atomic Swap
- Hashlock and Timelock
- Atomic Exchange

KEYWORDS

- Atomic Exchange
- Hashlock and Timelock
- Hashed Timelock Contract (HTLC)
- Two-party Atomic Exchange

Cross Chain Asset Transfer using Atomic Exchange



(1) (2) **Atomic Exchange** (3) **Transfer**

Solving atomic exchange will solve most challenges of asset transfer.

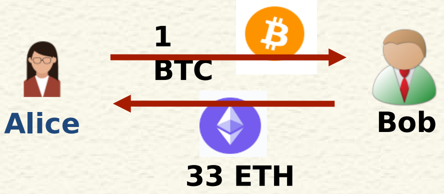
Atomic Cross-chain Swaps (PODC ‘18)

Atomicity: An atomic transaction is an indivisible series of operations, such that either all occur, or none occurs.

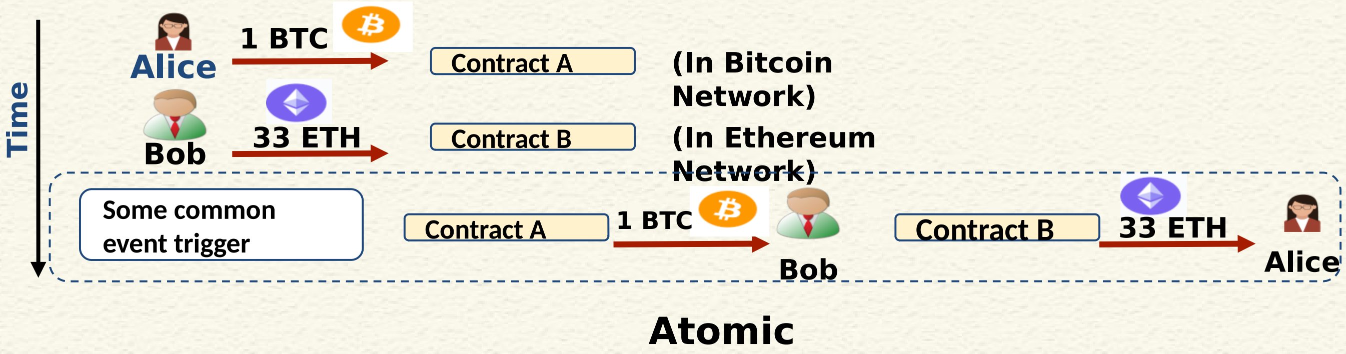
Atomic swap protocol guarantees

1. If all parties conform to the protocol, then all swaps take place
2. If some parties deviate from the protocol, then no conforming party ends up worse off
3. No coalition has an incentive to deviate from the protocol

Basic Idea



1. Initialize smart contracts on both ends with the amount.
2. Add a **common spending condition**, such that when the condition is met, **both the parties are paid simultaneously**



Hashlock and Timelock

- Hashlock: a function that restricts the spending of funds until a certain piece of data is publicly disclosed (as a cryptographic proof)
  - Hash of a secret pre-image is posted as a hashlock
  - When the secret is revealed, the funds are released
- Timelock: a function that restricts the spending of funds until a specific time (or block height) in the future

Hash Locks

- **Hashlock** is a type of encumbrance that restricts the spending of an output until **a specified secret key is publicly revealed**
- **Inherent Property:** Once any hashlock is opened publicly, any other hashlock secured using the same key can also be opened

Hash Locks

Example:

- **Alice** generates a secret **key** **“I love strawberries”**
- Alice computes the Cryptographic Hash of the key: **f1b81571baac90bed544d1910f79ea5c31fa4509**
- Alice initiates a Hash Locked contract of **1 BTC** (some amount) which has the **conditions**:
  If **key is revealed** - **pay BOB** with 1 BTC
- The contract also contains the Hash, which allows any miner to verify the revealed key

Time Locks

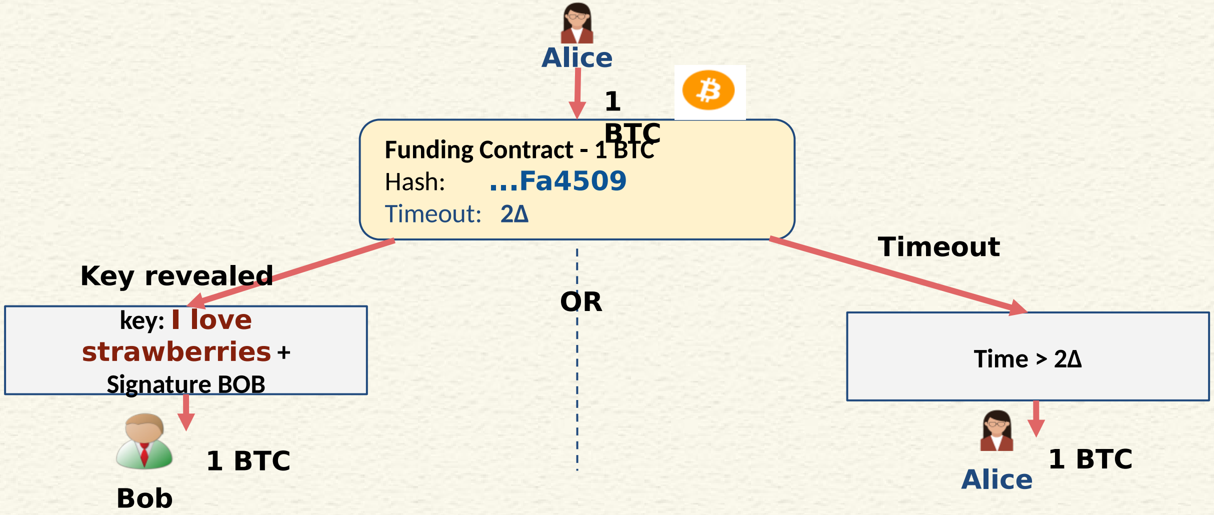
- **Timelock** is a type of smart contract primitive that restricts the spending/transfer of some currency until a specified future time
- Block height may be used as a proxy for time

Example:

- **Alice** generates a timelocked contract with 1 BTC, and time = 2Δ (Δ = some time unit)

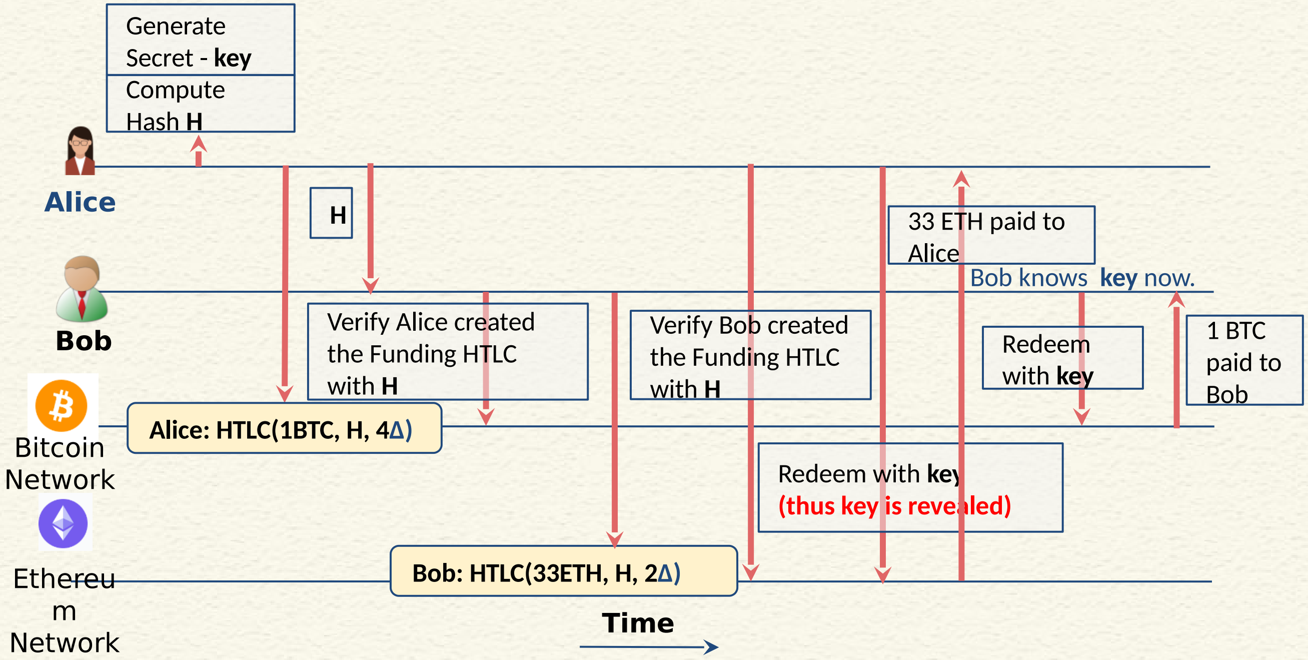
- After 2Δ time, 1 BTC will be transferred to a **target account**. (Target account can be Alice's own account)

HTLC - Hashed Timelock Contract



Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." (2016).

HTLC for Atomic Swap



Generate Secret - **key**

Compute Hash **H**

Alice

H

Bob

Bitcoin Network

Ethereum Network

Verify Alice created the Funding HTLC with **H**

Alice: HTLC(1BTC, H, 4Δ)

Verify Bob created the Funding HTLC with **H**

Bob: HTLC(33ETH, H, 2Δ)

Redeem with **key**
(thus key is revealed)

33 ETH paid to Alice

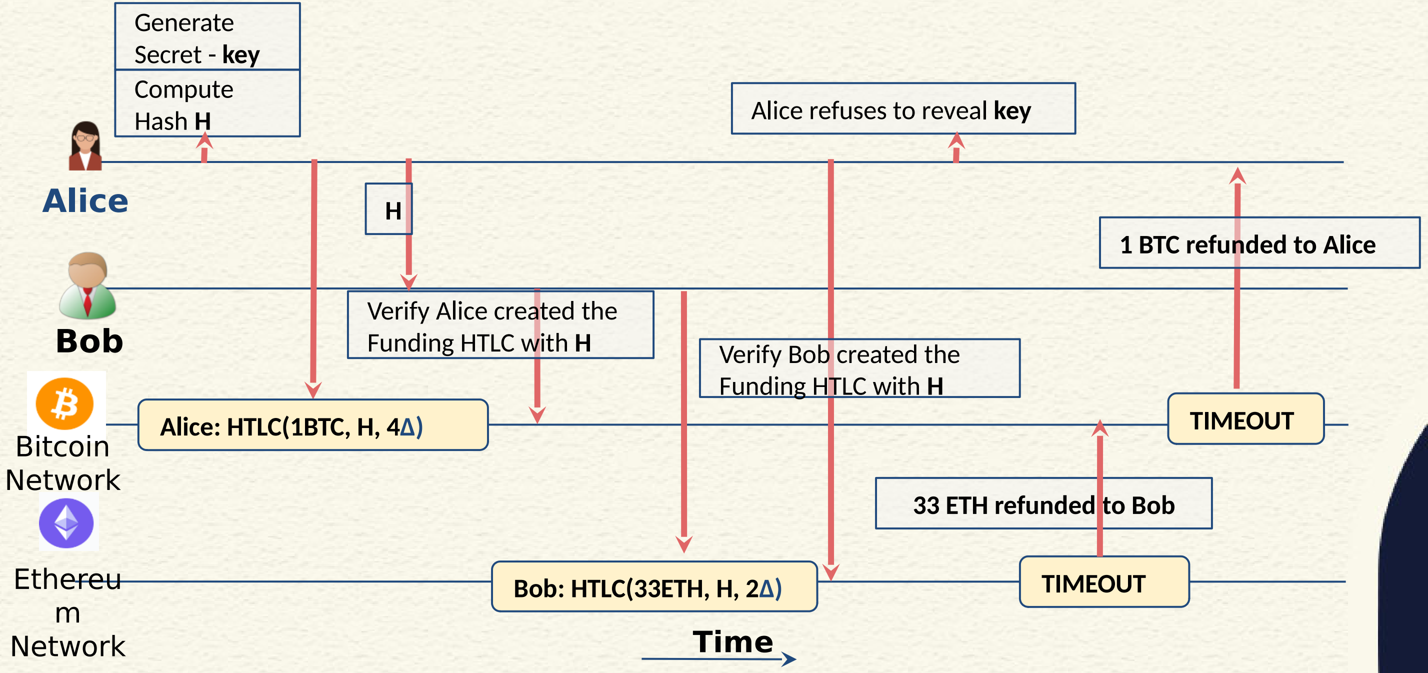
Bob knows **key** now.

Redeem with **key**

1 BTC paid to Bob

Time

What if Alice does not Reveal Key?



CONCLUSIONS

- Explained how hashed timelock contracts work
- Cross-chain atomic swap operations
- Two-party atomic exchange

REFERENCES

- **Web resources as mentioned from time to time**

Thank you