Blockchain (BlCh)

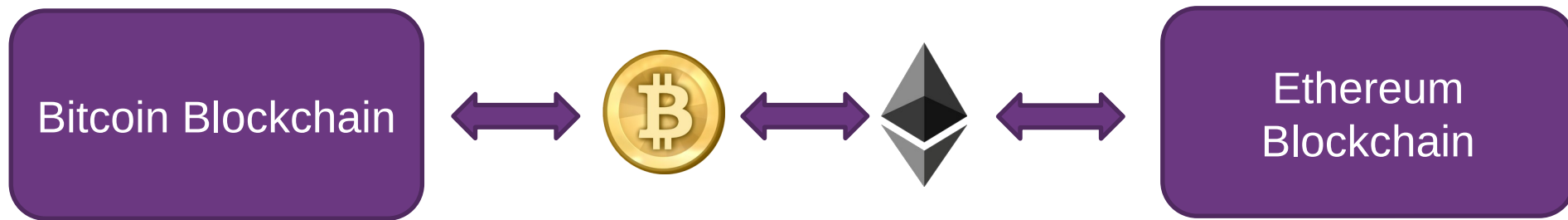**HTLCs, Cross-chain Atomic Swaps**

Thomas Bocek

05.11.2025

Learning Goals

- Lecture 10

  - HTLC – from simple operations (hash + timelock) to complex behavior

  - Understanding cross-chain atomic swaps and their trustless execution

  - Why decentralized exchanges are needed (Mt. Gox, FTX risks)

  - How HTLCs enable atomic swaps between different blockchains

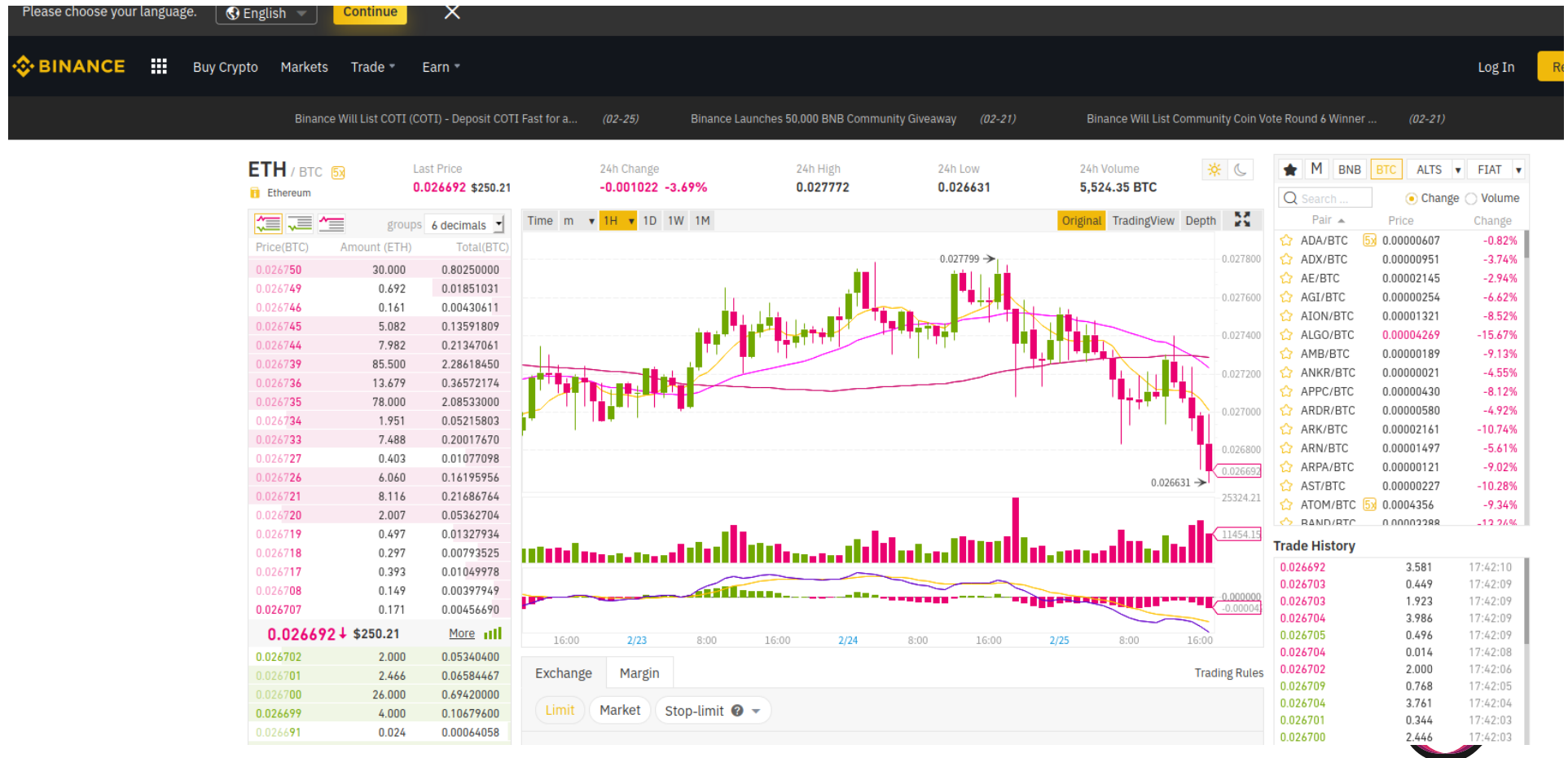 - The role of hash locks and time locks in secure cryptocurrency exchanges

OST

Cross-chain Atomic Swaps?

- A Showcase of Cross-chain Atomic Swaps

  - Either swap happens or becomes void

Why Cross-chain Atomic Swaps

- Use case: I want to exchange my 1 BTC to 37 ETH

  - Obvious approach: use a centralized exchange, such as FTX, Binance, Bitstamp, or Kraken

Why Cross-chain Atomic Swaps

- There was also Mt.Gox, BTC-e, and FTX

  - You loose control over your funds (Mt. Gox)

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

The Guardian

Search jobs · Sign in · Search · International ed

News · Opinion · Sport · Culture · Lifestyle · More ⌄

World UK Environment Science Global development Football **Tech** Business Obituaries

Bitcoin

⊙ This article is more than **5 years old**

MtGox files for bankruptcy in Japan after collapse of bitcoin exchange

The bitcoin exchange has debts of £38m and assets of just £22.6m, it reported on Friday

Alex Hern
🐦 @alexhern
Fri 28 Feb 2014 13.30 GMT

▲ MtGox CEO Mark Karpeles bows in apology at a press conference at the Justice Ministry in Tokyo Friday night, Feb. 28, 2014. Photograph: i/AP

MtGox filed for bankruptcy protection in Tokyo on Friday, with the world's former biggest bitcoin exchange blaming "a weakness in our system" for its collapse.

Why the feds took d... largest exchanges

Tracing Mt. Gox's stolen coins led feds to...

By Russell Brandom and Sarah Jeong | Jul 29, 2017, 10:00am E

f 🐦 SHARE

Illustration by Alex Castro / The Verge

This week, one of Bitcoin's largest and most notorious coin excha...
law enforcement — and police and prosecutors are now beginnin...
Thursday, the Department of Justice unsealed an indictment against Alexander Vinnik —
thought to be the operator, or one of the operators of Bitcoin exchange BTC-e — charging

ARCHIVE Published: January 17, 2019 12:21 PM UTC

Please Do Not Store Crypto on Any Exchange, Warns CEO of Major Crypto Exchange Kraken

Jesse Powell, the CEO of a major crypto exchange Kraken, warned users of digital assets to not store funds on trading platforms. The warning of Powell follows a high profile security breach suffered by Cryptopia, a New Zealand-based crypto exchange known for its listing of…

Author: Joseph Young @iamjosephyoung
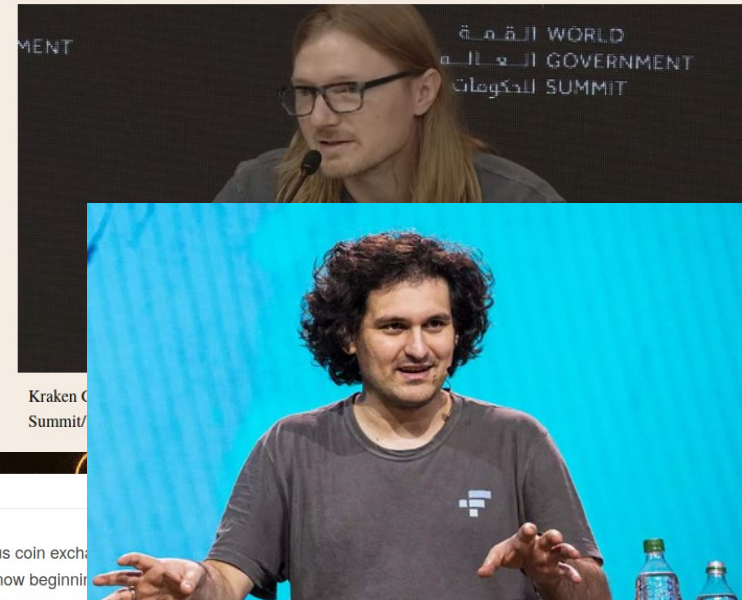
DON'T MISS:

Crypto Trading Is the New Wall Street: Kraken Pro Trader

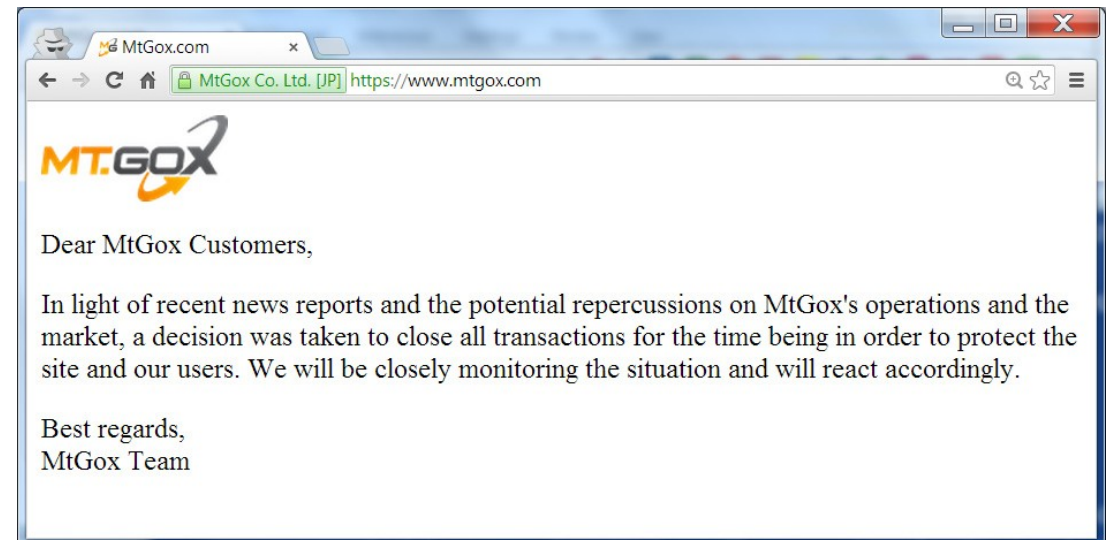Winklevoss Twins Foster Mainstream Adoption with Bitcoin Giveaway

Crypto Mom Bemoans 'Regulatory Escape Room' Feel for Crypto

Gemini Exchange Expands into Windy City to Capture Institutional Wave

New York Kraken Ex-Employee Sues Crypto Exchange Over Failure to Pay $900,000

5

OST

Mt. Gox

- Mt. Gox (short for Magic: The Gathering Online Exchange)
  - July 2010 reused domain name, started Bitcoin trading platform

- April 2013, handled 70% of Bitcoin trades

- November 2013, users reported payout delays
  - Exchange rates different from other trading platforms

- 7. February 2014, suspended all BT withdrawals
  - "Bug in the Bitcoin system": transaction malleability

- 20. February, suspended all withdrawals

- 24. February, all trading suspended, blank page

- 9. March 2014, filed for bankruptcy
  - 850k Bitcoins missing

- 27.10.2025: Mt. Gox Delays Creditor Repayment to October 2026 [link]
  - Compensate creditors, $460 million at the time, repaying 150k BTC (from lost 850k BTC)

Dear MtGox Customers,

In light of recent news reports and the potential repercussions on MtGox's operations and the market, a decision was taken to close all transactions for the time being in order to protect the site and our users. We will be closely monitoring the situation and will react accordingly.

Best regards,
MtGox Team

Why Cross-chain Atomic Swaps

- Exchanges caught trading against their customers - to boost their numbers [link]

Why Cross-chain Atomic Swaps

- With Atomic Swaps no trust in a centralized platform is needed: non-custodial
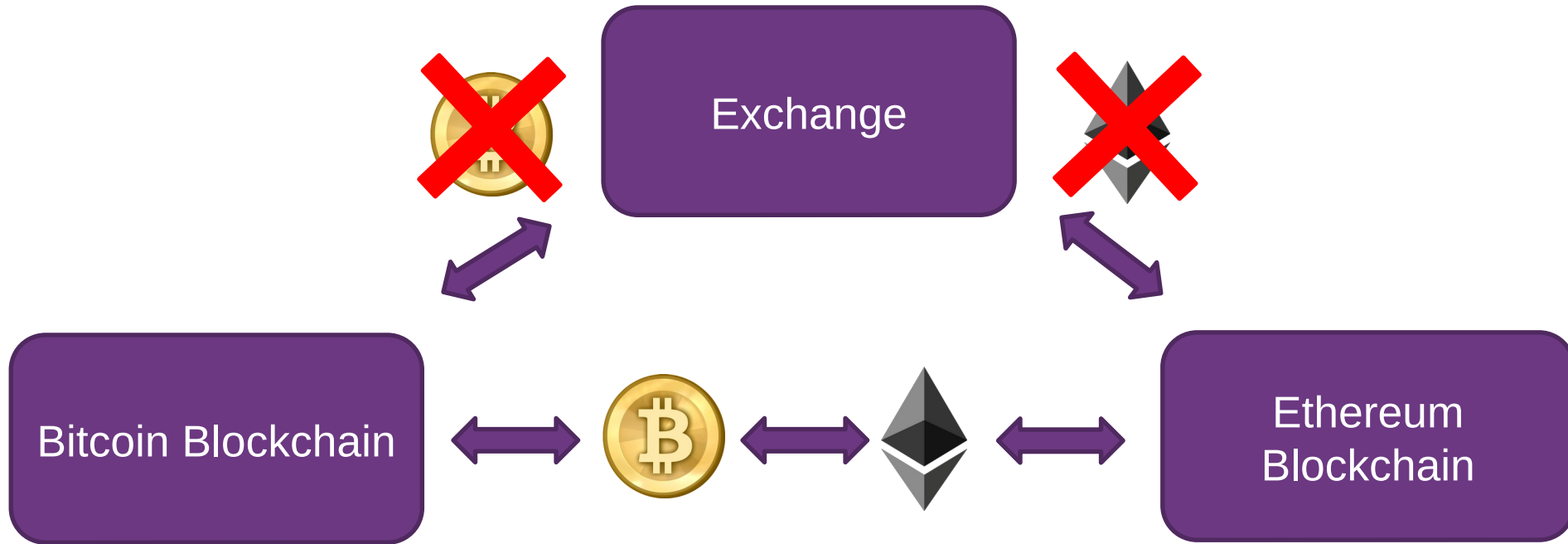
Hashed Time-Locked Contracts

- Building Blocks of Cross-chain Atomic Swaps

- Cryptographic hashing:

  - one-way function - computationally efficient in one way, computationally highly expensive the other way

  - deterministic – same input – same output

  - collision resistant – highly expensive to find two inputs that hash to the same output

SHA256 Hash

Data: aoeuaoeuao

Hash: 8698bce64d5c921046ce61e7fd0f538ad44c8f5a44e0b7789daf660d653544d8

https://dsl.i.ost.ch/lect/bl/hash.html

OST

Hashed Time-Locked Contracts

- Building block for cross-chain atomic swaps and payment channels

- Hash lock:

  - store hashed secret – publicly stored in a smart contract

  - unlock – only if secret is provided (publicly)

```
function redeem(bytes32 contractId, bytes32 secret) external {
  require(contracts[contractId].sender != address(0), "contract needs to exist");
  //encodePacked -> unpadded encoding
  require(contracts[contractId].hashedSecret == sha256(abi.encodePacked(secret)),"hashlock hash does
not match");
  ...
  c.receiver.transfer(amountMinusFee);
```

stored

provided

OST

Hashed Time-Locked Contracts

- Building block for cross-chain atomic swaps and payment channels

- Hash time lock:

  - store hashed secret – publicly stored in a smart contract

  - unlock – only if secret is provided (publicly) before timeout

Or

  - unlock – after timeout

```
function recover(bytes32 contractId) external {
  require(contracts[contractId].lockTime <= now, "refundable: timelock not yet passed");
  ...
  c.sender.transfer(c.amount);
```
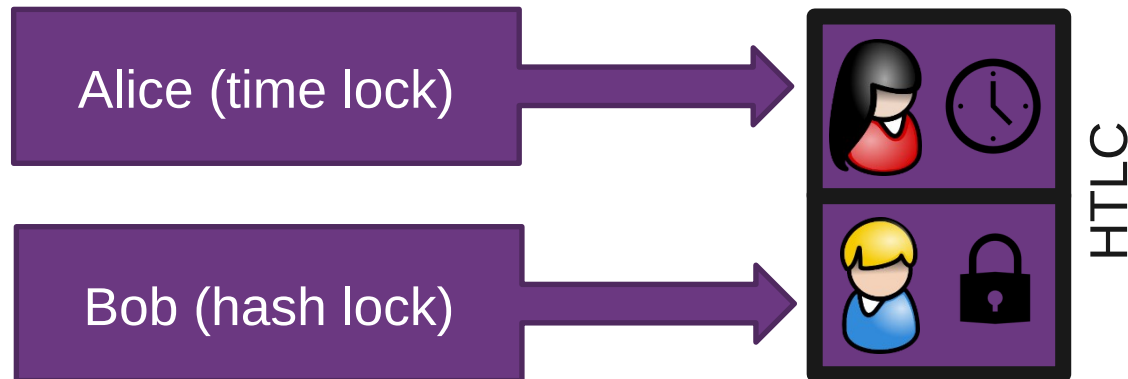
OST

Hashed Time-Locked Contracts

- Building block for cross-chain atomic swaps and payment ch.

- Hash time lock:

  - store hashed secret – publicly stored in a smart contract

  - unlock – only if secret is provided (publicly) before timeout

Or

  - unlock – after timeout

Alice (time lock)

Bob (hash lock)

HTLC

Hash time lock (HTLC)

Hash lock to Bob

Time lock to Alice

```
OP_IF
  OP_SIZE
  AddInt64(secretSize)
  OP_EQUALVERIFY
  OP_SHA256
  AddData(secretHash)
  OP_EQUALVERIFY)
  OP_DUP
  OP_HASH160
  AddData(pkhThem[:])
OP_ELSE
  AddInt64(locktime)
  OP_CHECKLOCKTIMEVERIFY
  OP_DROP
  OP_DUP
  OP_HASH160
  AddData(pkhMe[:])
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```
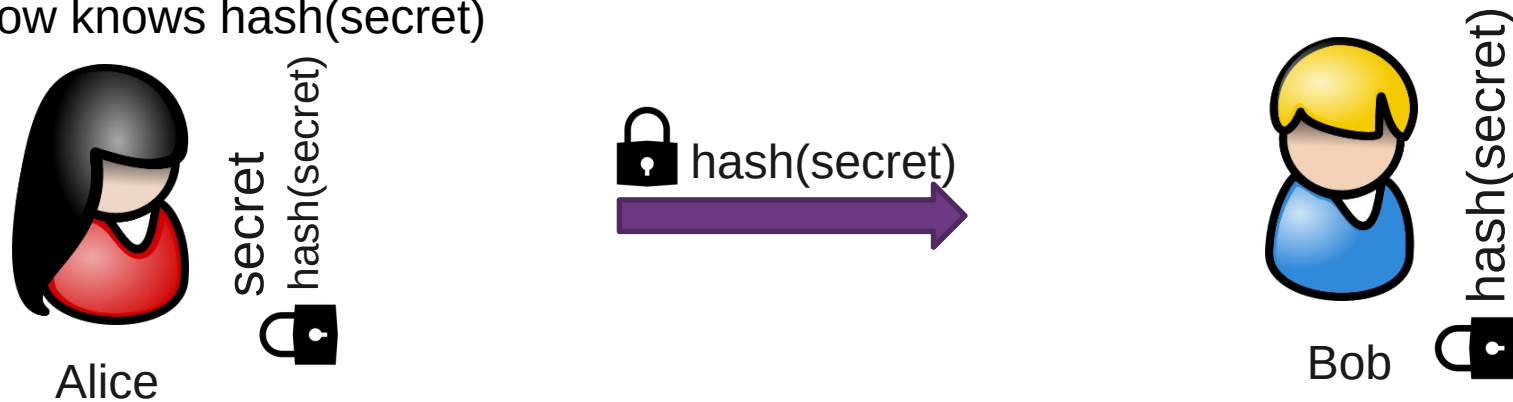
OST

Hashed Time-Locked Contracts

- Now we are ready to do an atomic swap with Alice and Bob

  - 1 BTC for 37 ETH

OST
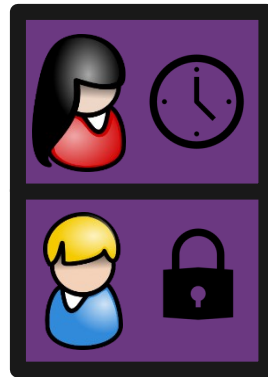
Atomic Swaps

- Now we are ready to do an atomic swap with Alice and Bob with HTLC

  - Alice (initiator) creates "secret", shares with Bob, hash(secret)
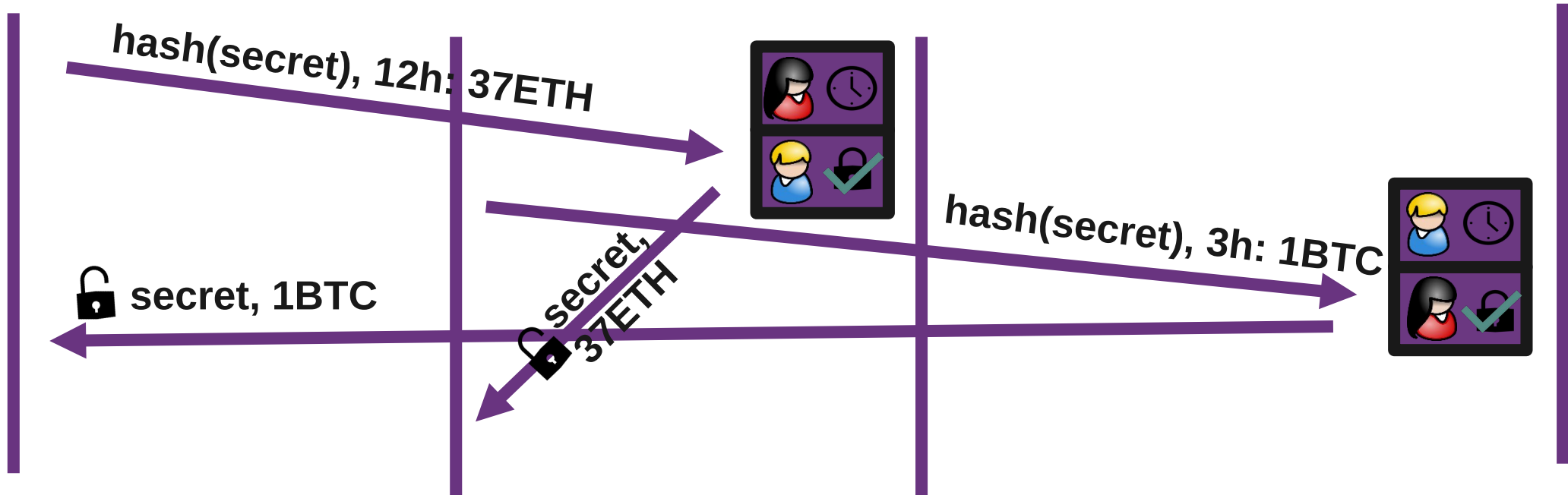
  - Bob now knows hash(secret)

hash(secret)

Alice

Bob

Blockchain BTC

Blockchain ETH

OST

Atomic Swaps - Alice reveals secret to redeem 1 BTC

Ethereum Blockchain

Bitcoin Blockchain

hash(secret), 12h: 37ETH

hash(secret), 3h: 1BTC

secret, 1BTC

secret, 37ETH

OST

Atomic Swaps - Bob goes offline (worst case)