



OST

Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

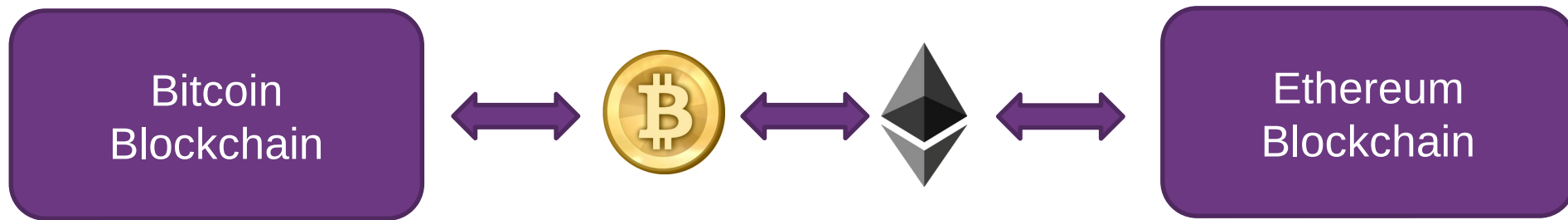
HTLCs, Cross-chain Atomic Swaps

Thomas Bocek

18.11.2021

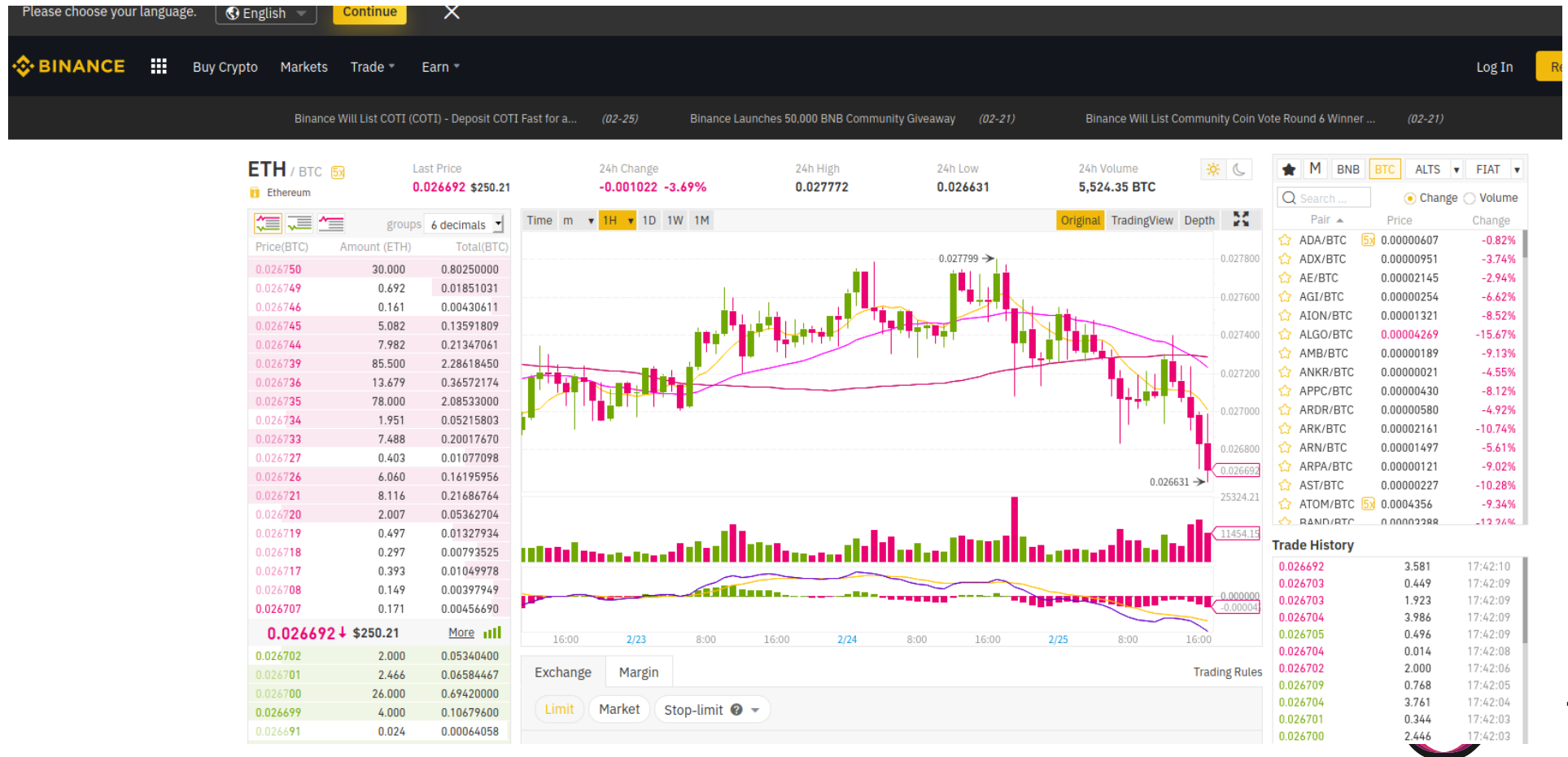
Cross-chain Atomic Swaps?

- 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 **Binance**, **Bitstamp**, or **Kraken**



Why Cross-chain Atomic Swaps

- There was also Mt.Gox and BTC-e
 - You loose control over your funds (Mt. Gox)

Support The Guardian
Available for everyone, funded by readers

Contribute → Subscribe →

Search jobs Sign in Search International ed

The Guardian

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

70 39



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 down largest exchanges

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

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

f t SHARE



Illustration by Alex Castro / The Verge


This week, one of Bitcoin's largest and most notorious coin exchanges was brought down by law enforcement — and police and prosecutors are now beginning to explain why. On 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 @ianjosephyoung



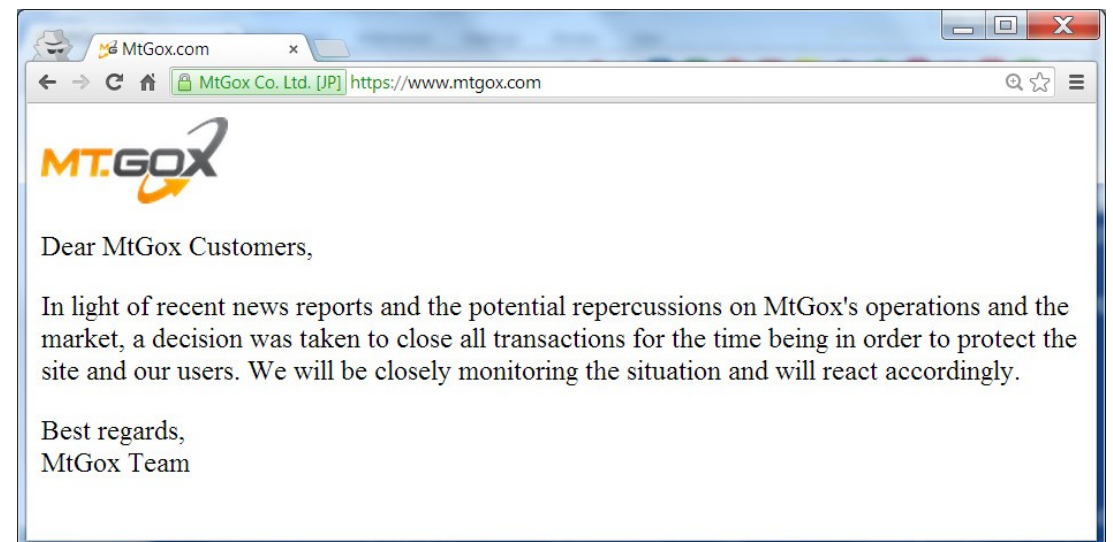
DON'T MISS:

- 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



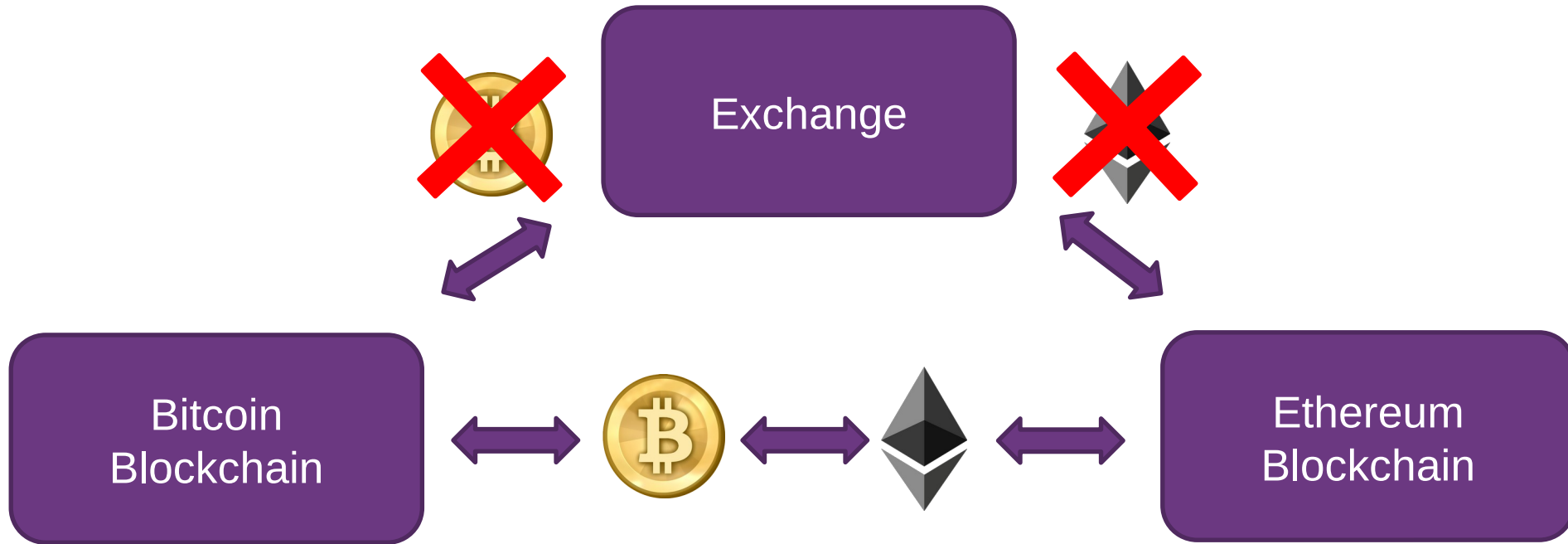
Mt. Gox

- **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
- 16.11.2021: Mt. Gox rehabilitation plan is now 'final and binding' [[link](#)]
 - Compensate creditors, \$460 million at the time, repaying 150k BTC (from lost 850k BTC)



Why Cross-chain Atomic Swaps

- With Atomic Swaps no trust in a centralized platform is needed



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

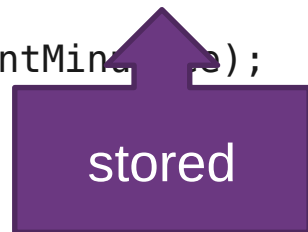
SHA256 Hash

Data:	<input type="text" value="aoeuaoeua0"/>
Hash:	<input type="text" value="8698bce64d5c921046ce61e7fd0f538ad44c8f5a44e0b7789daf660d653544d8"/>

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(amountMinimum);  
}
```



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");
```

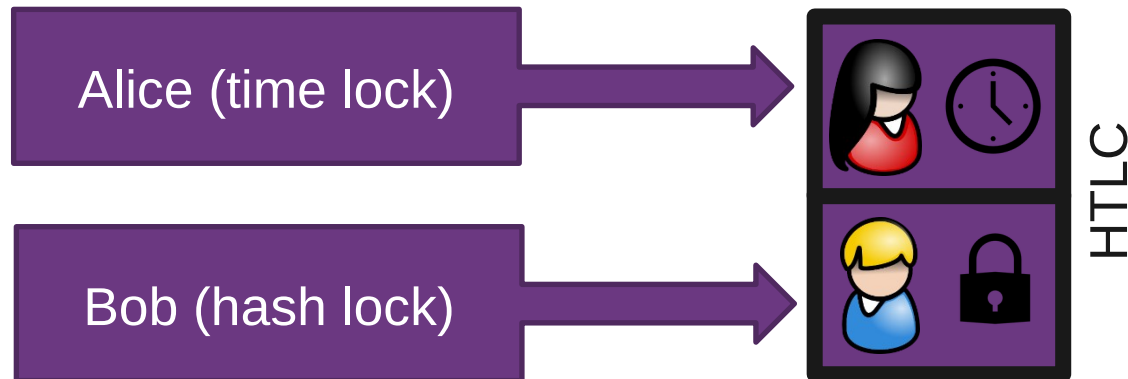
```
    c.sender.transfer(c.amount);
```

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



Hash time lock (HTLC)

```

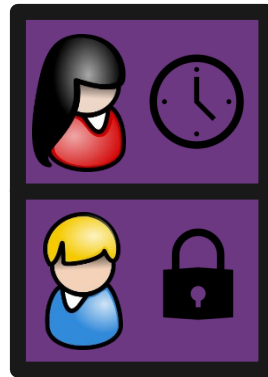
OP_IF
  OP_SIZE
  AddInt64(secretSize)
  OP_EQUALVERIFY
  OP_SHA256
  AddData(secretHash)
  OP_EQUALVERIFY)
  OP_DUP
  OP_HASH160
  AddData(pkhThem[:])
OP_ELSE
  AddInt64(locktime)
  OP_CHECKLOCKTIMEVERIFY
  OP_DROP
  OP_DUP
  OP_HASH160
  AddData(pkhMe[:])
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
    
```

Annotations on the code block:

- A bracket on the left groups the top half of the code (from `OP_IF` to `AddData(pkhThem[:])`) and labels it "Hash lock to Bob".
- A bracket on the left groups the bottom half of the code (from `OP_ELSE` to `AddData(pkhMe[:])`) and labels it "Time lock to Alice".

Hashed Time-Locked Contracts

- Now we are ready to do an atomic swap with Alice and Bob
 - 1 BTC for 37 ETH



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)



Blockchain BTC

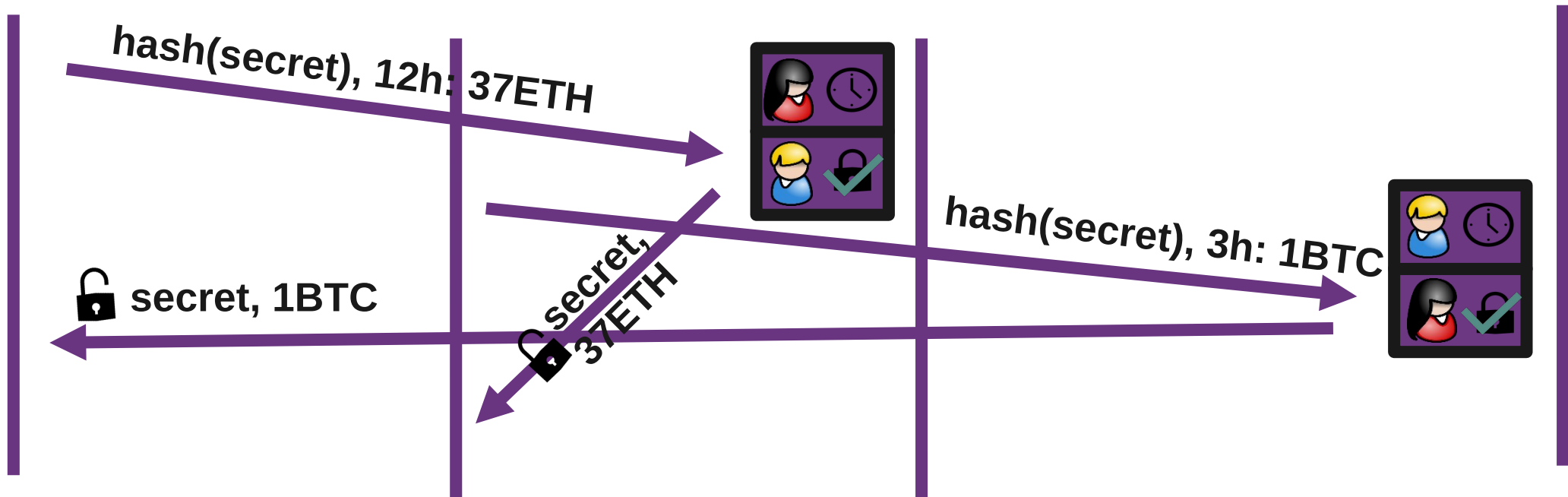
Blockchain ETH

Atomic Swaps - Alice reveals secret to redeem 1 BTC



Ethereum
Blockchain

Bitcoin
Blockchain



Atomic Swaps - Bob goes offline (worst case)



Ethereum Blockchain

Bitcoin Blockchain

