



OST

Eastern Switzerland
University of Applied Sciences

Distributed Systems Advanced & Blockchain

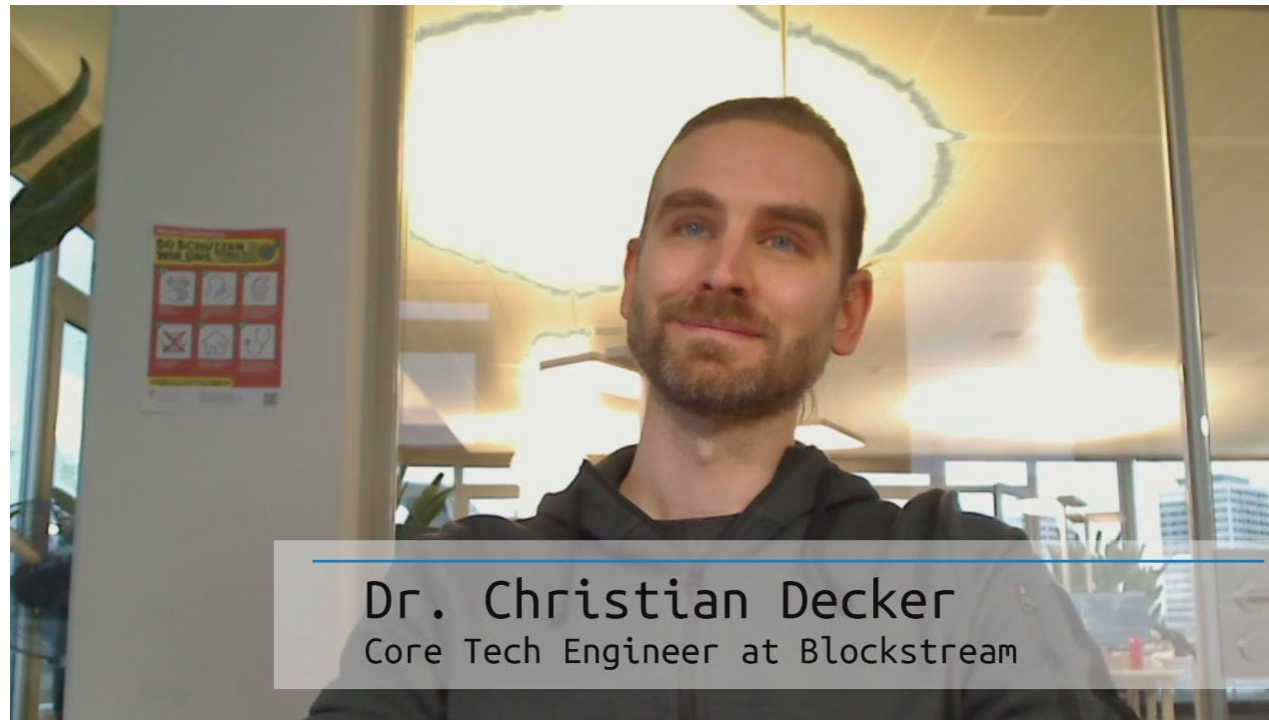
Payment Channels and Cross Chain Atomic Swaps

Thomas Bocek

29 November 2020

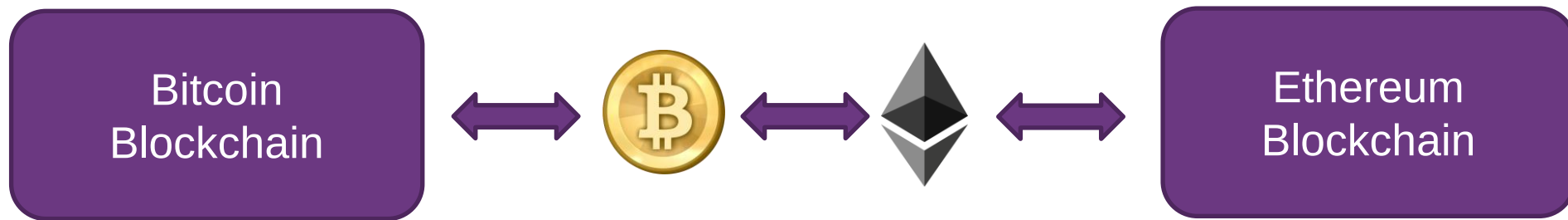
Payment Channel?

- Interview with Christian Decker



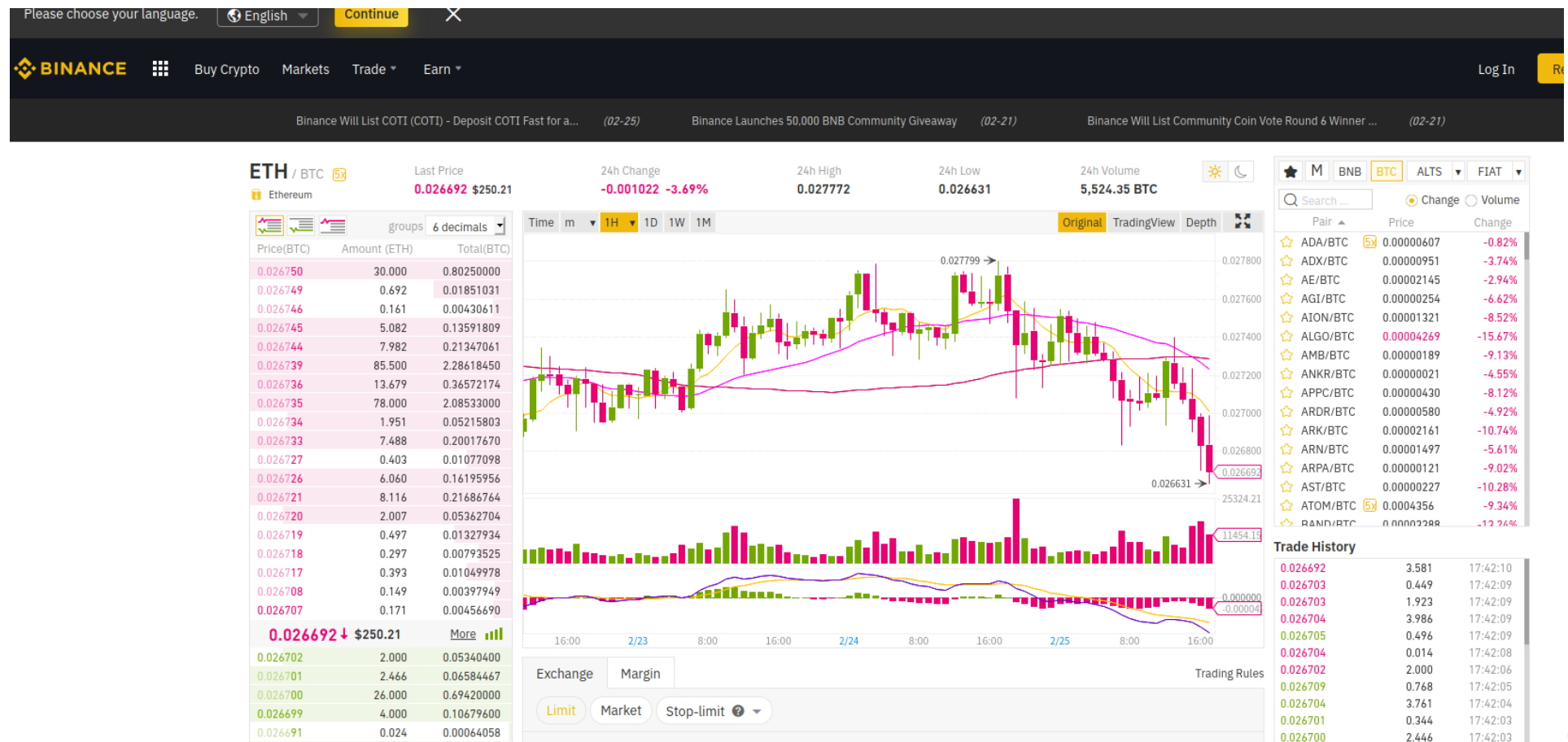
Cross-chain Atomic Swaps?

- 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



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



▲ MtGox CEO Mark Karpelles 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 Al

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

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 @iamjosephyoung



Kraken CEO Jesse Powell listens to the people, delists Bitcoin SV | Source: World Government Summit/YouTube

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

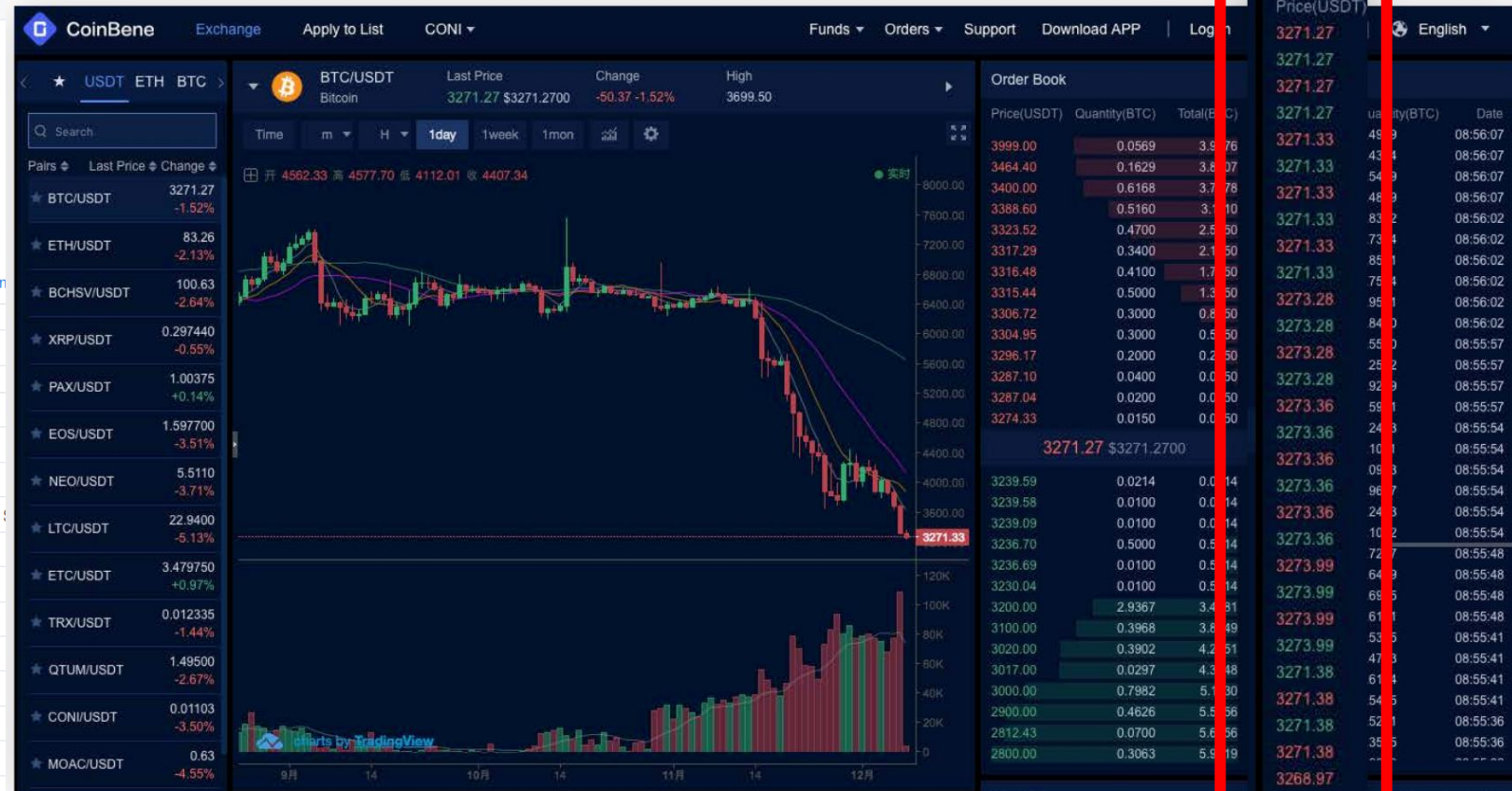
Why Cross-chain Atomic Swaps

- Exchanges caught trading against their customers - to boost their numbers

Rank 1	Market Cap	Volume (24h)
Website	\$171,765,938,910 USD	\$44,227,400,916 USD
Explorer (2 3 4 5)	18,236,850 BTC	4,695,742 BTC
Message Board		
Source Code		
Technical Documentation		
Coin	Mineable	

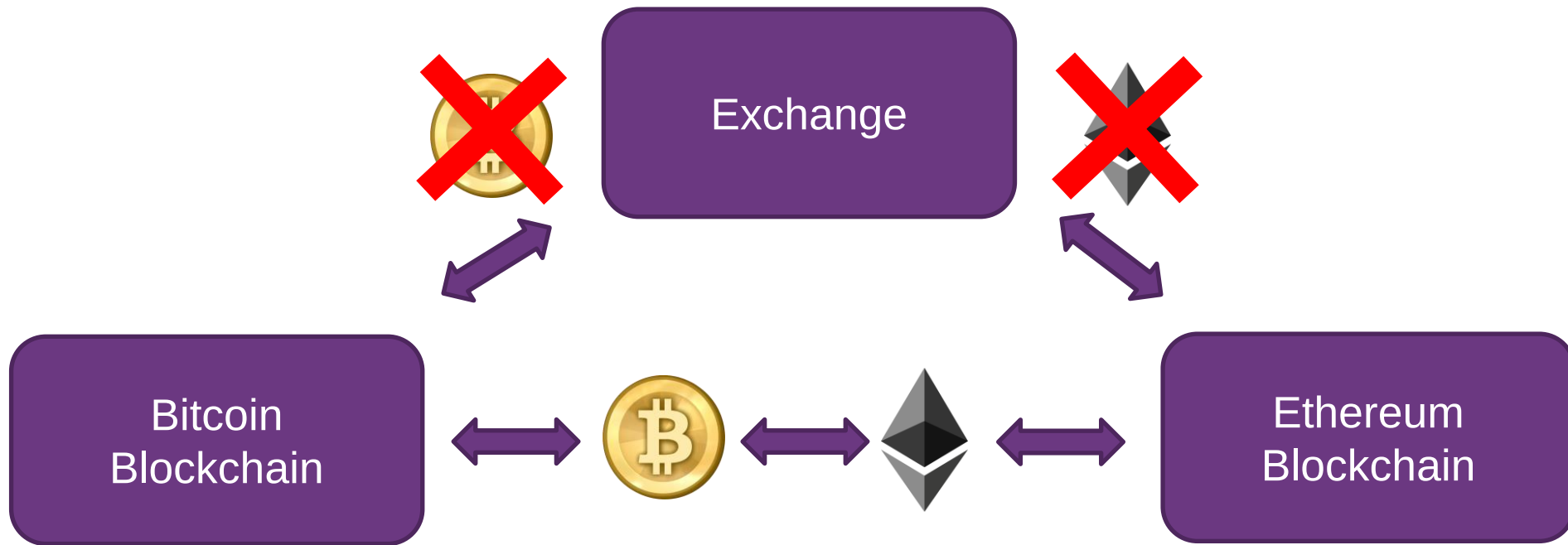
Bitcoin Market Pairs (Adjusted)

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	BHEX	BTC/USDT	\$1,419,901,861	\$9,416.74	3.21%
2	EtherFlyer	BTC/USDT	\$1,333,576,662	\$9,569.26	3.02%
3	Coinsbit	BTC/USDT	\$1,332,527,140	\$9,416.74	3.01%
4	ChainX	BTC/KRW	\$1,319,100,615	\$9,361.61	2.98%
5	LBANK	BTC/USDT	\$1,266,587,931	\$9,410.98	2.86%
6	BitForex	BTC/USDT	\$1,225,965,438	\$9,412.63	2.77%
7	Hotbit	BTC/USDT	\$1,076,692,891	\$9,413.41	2.43%
8	Bilaxy	BTC/USDT	\$987,764,643	\$9,409.37	2.23%
9	CoinBene	BTC/USDT	\$838,338,060	\$9,408.28	1.90%
10	Hubi	ETH/BTC	\$810,624,682	\$9,418.29	1.83%
11	Folgory	BTC/USDT	\$745,645,944	\$9,402.26	1.69%
12	BitMart	BTC/USDC	\$689,383,130	\$9,415.98	1.56%
13	BitForex	ETH/BTC	\$642,834,898	\$9,418.29	1.45%
14	PayBit	BTC/USD	\$632,525,870	\$9,385.98	1.43%



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

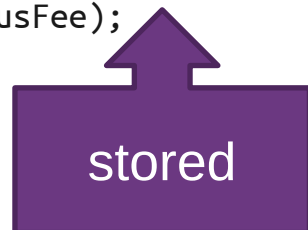
SHA256 Hash

Data:	aoeuaoeuao
Hash:	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(amountMinusFee);  
}
```



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

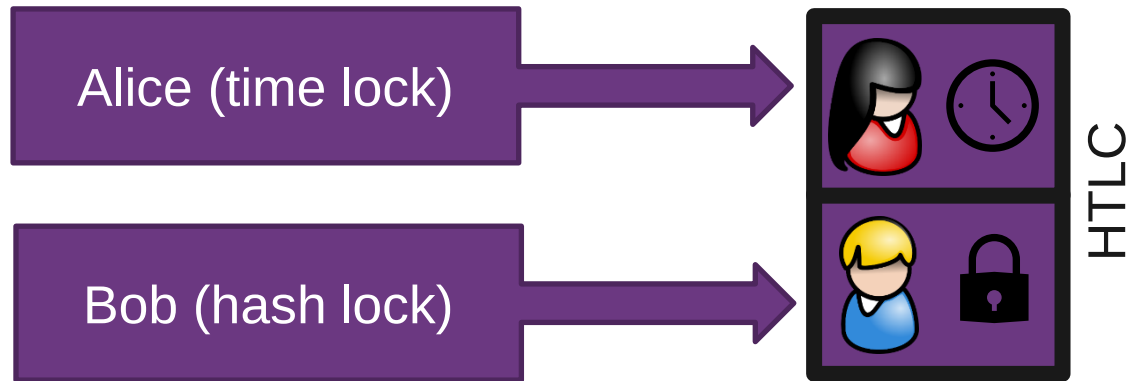
```
function recover(bytes32 contractId) external {
```

```
    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)

Hash lock – to Bob

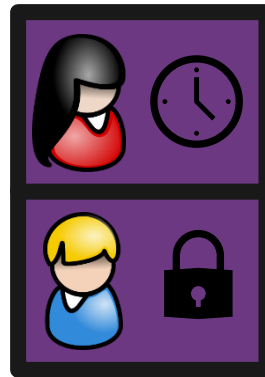
```
OP_IF
  OP_SIZE
  AddInt64(secretSize)
  OP_EQUALVERIFY
  OP_SHA256
  AddData(secretHash)
  OP_EQUALVERIFY)
  OP_DUP
  OP_HASH160
  AddData(pkhThem[:])
```

Time lock – to Alice

```
OP_ELSE
  AddInt64(locktime)
  OP_CHECKLOCKTIMEVERIFY
  OP_DROP
  OP_DUP
  OP_HASH160
  AddData(pkhMe[:])
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

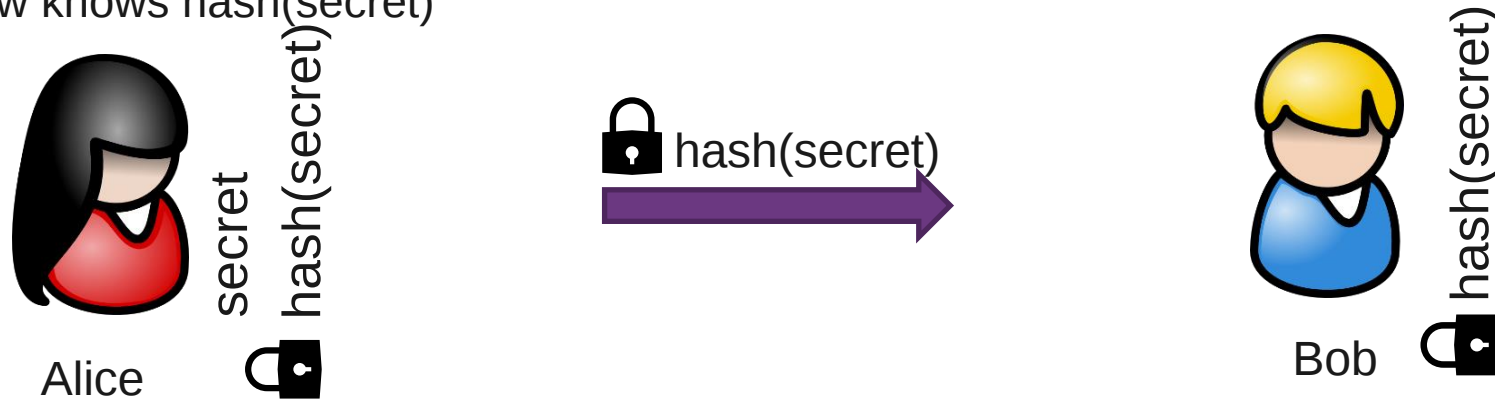
Hashed Time-Locked Contracts

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



Atomic Swaps

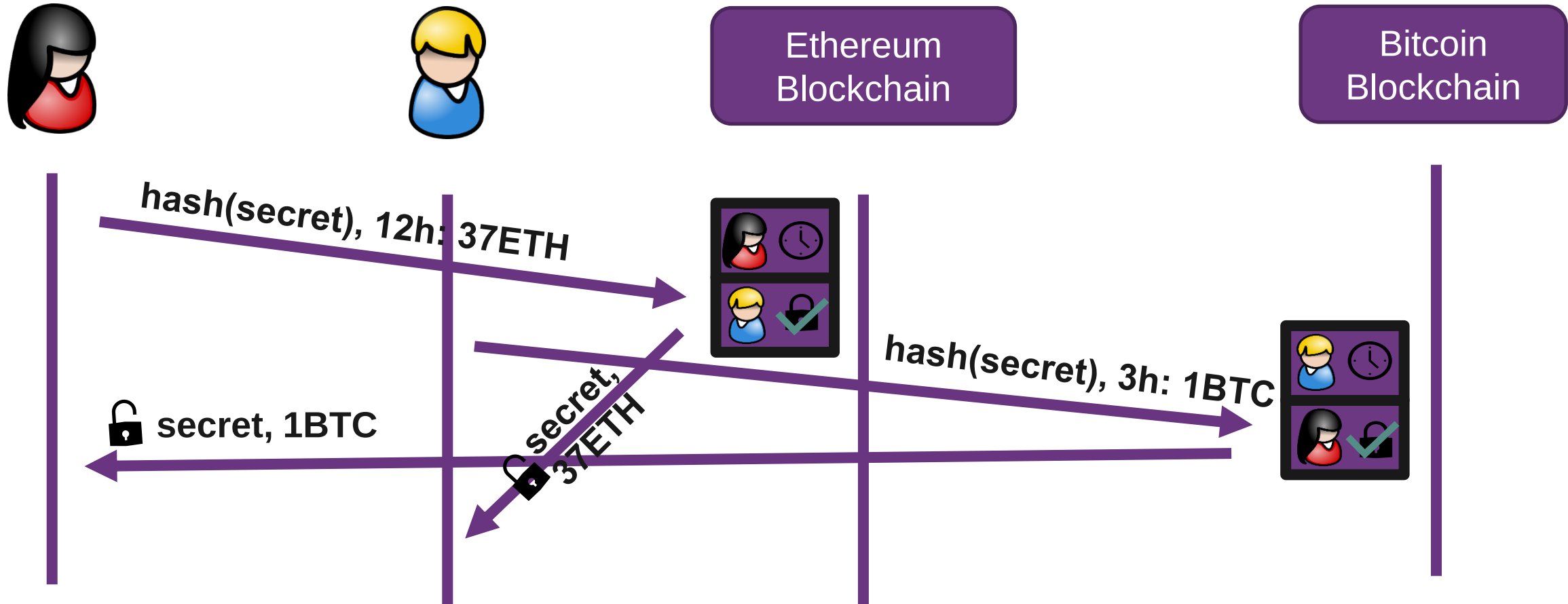
- Now we are ready to do an atomic swap with Alice and Bob with HTLC
 - Alice (initiator) creates “secret”, shares with Bob, hash(secret)
 - Bob now knows hash(secret)



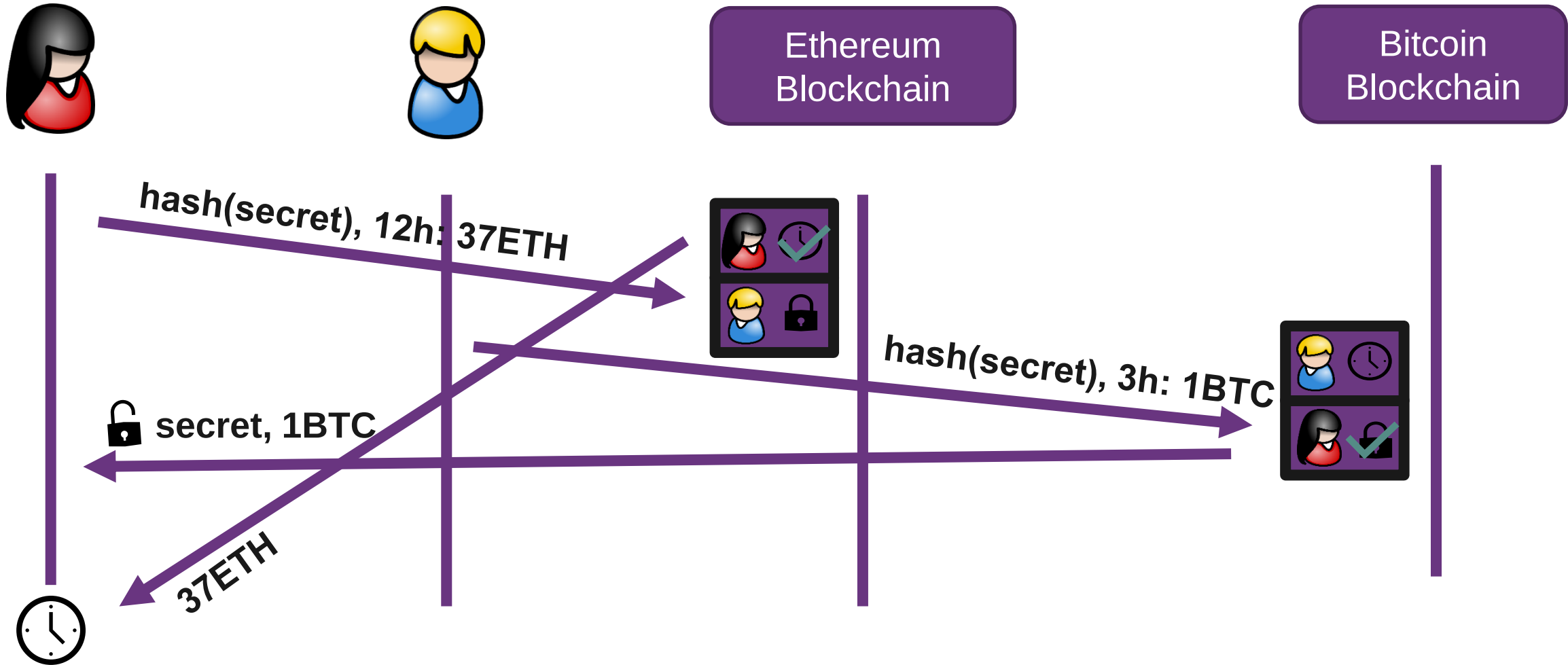
Blockchain BTC

Blockchain ETH

Atomic Swaps - Alice needs to reveal secret to redeem 1 BTC

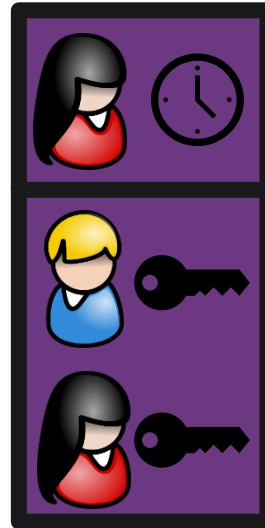


Atomic Swaps - Bob goes offline (worst case)

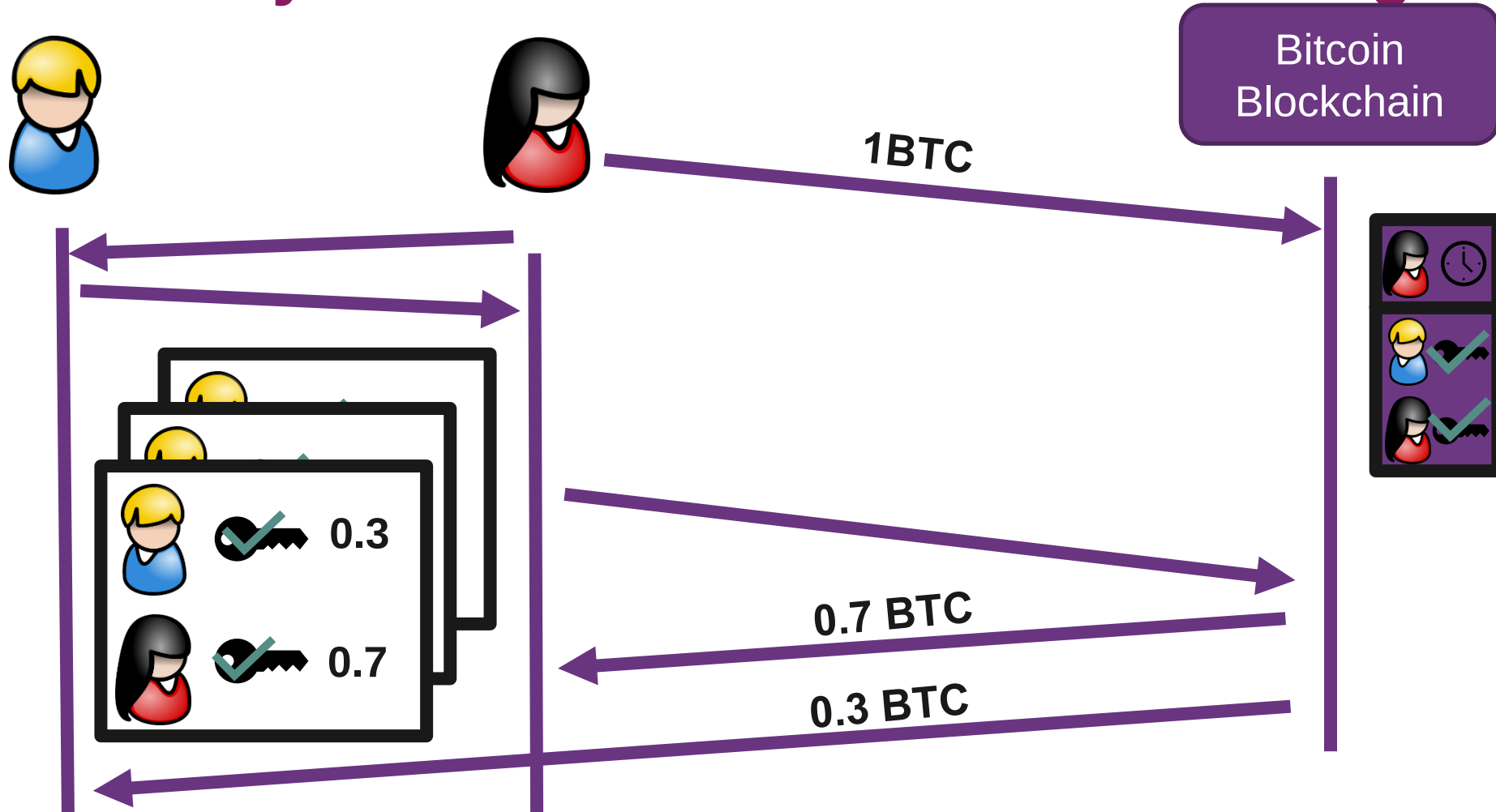


Direct Payment Channel with 2-of-2 Multisig Contracts

- Now we are ready to open a payment channel between Alice and Bob
 - 1 BTC each
 - 2-of-2 multisig



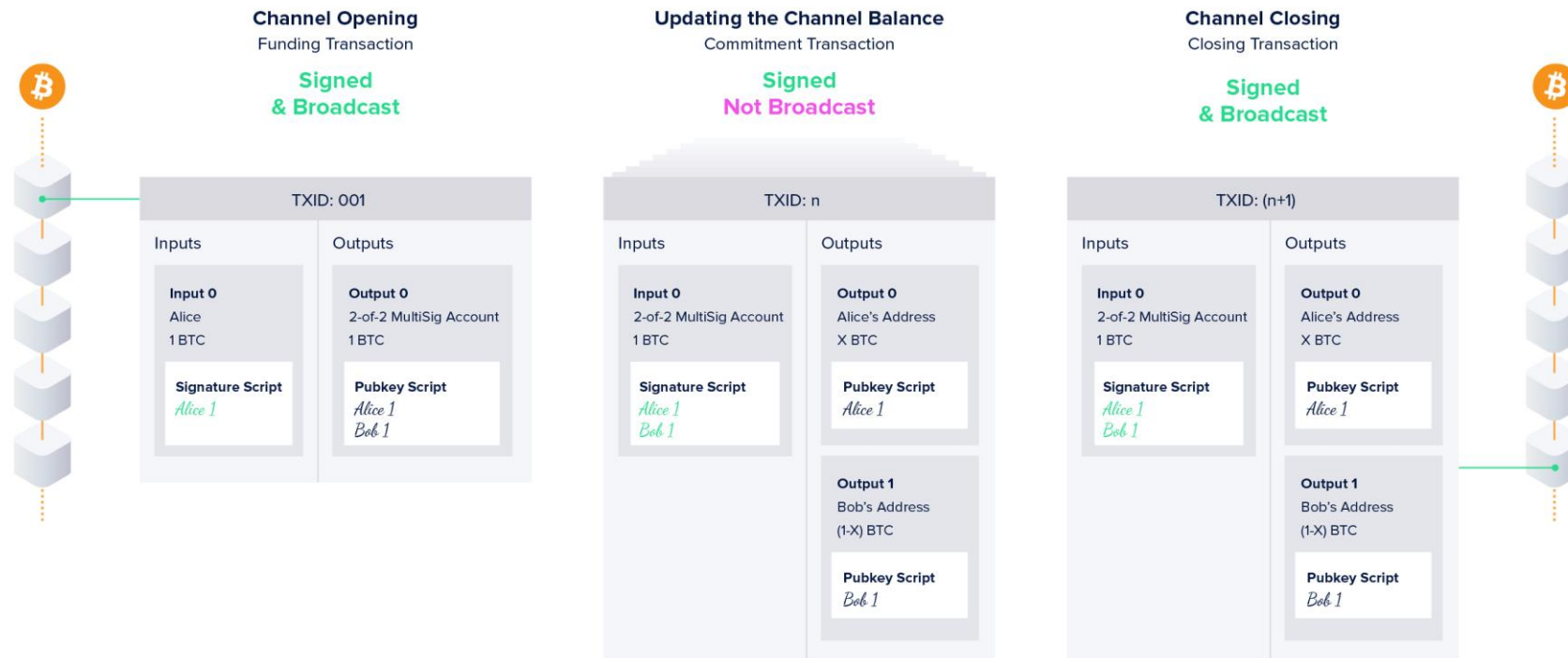
Direct Payment Channel with 2-of-2 Multisig Contracts



Other View on Direct Payment Channels

HORIZEN ACADEMY

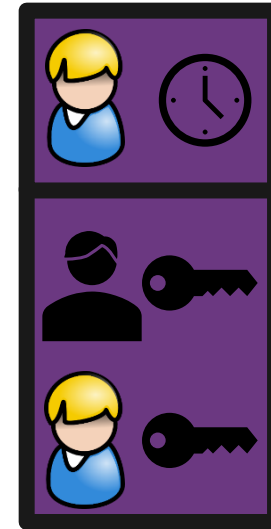
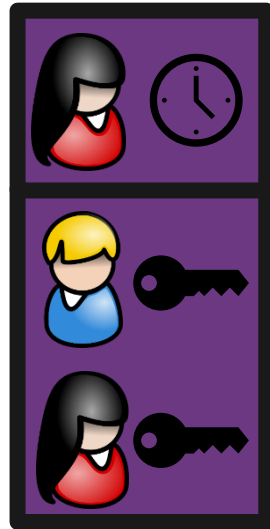
PAYMENT CHANNEL CONCEPT



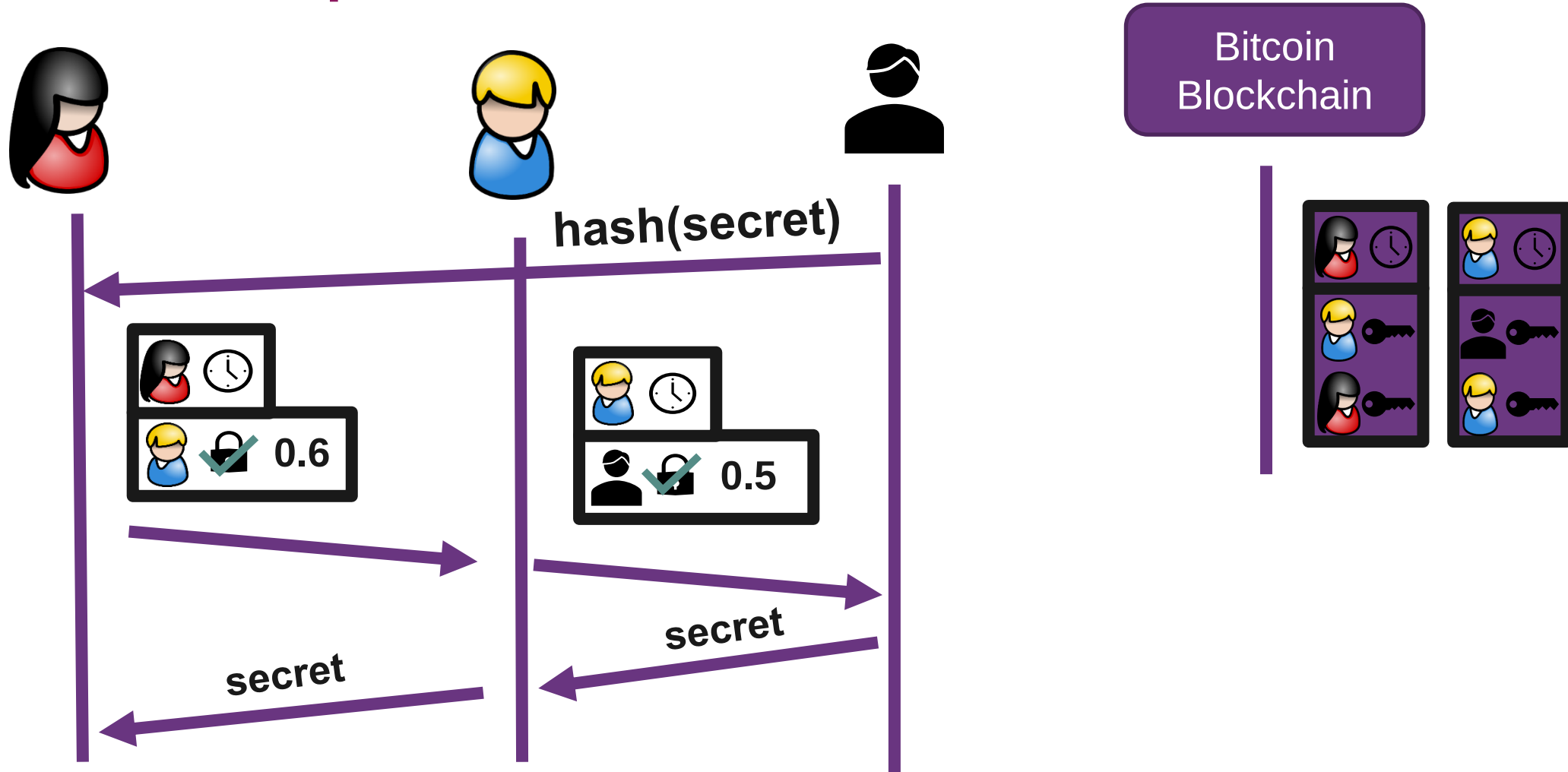
<https://academy.horizen.io/technology/expert/state-and-payment-channels/>

Indirect Payment Channel with HTLC

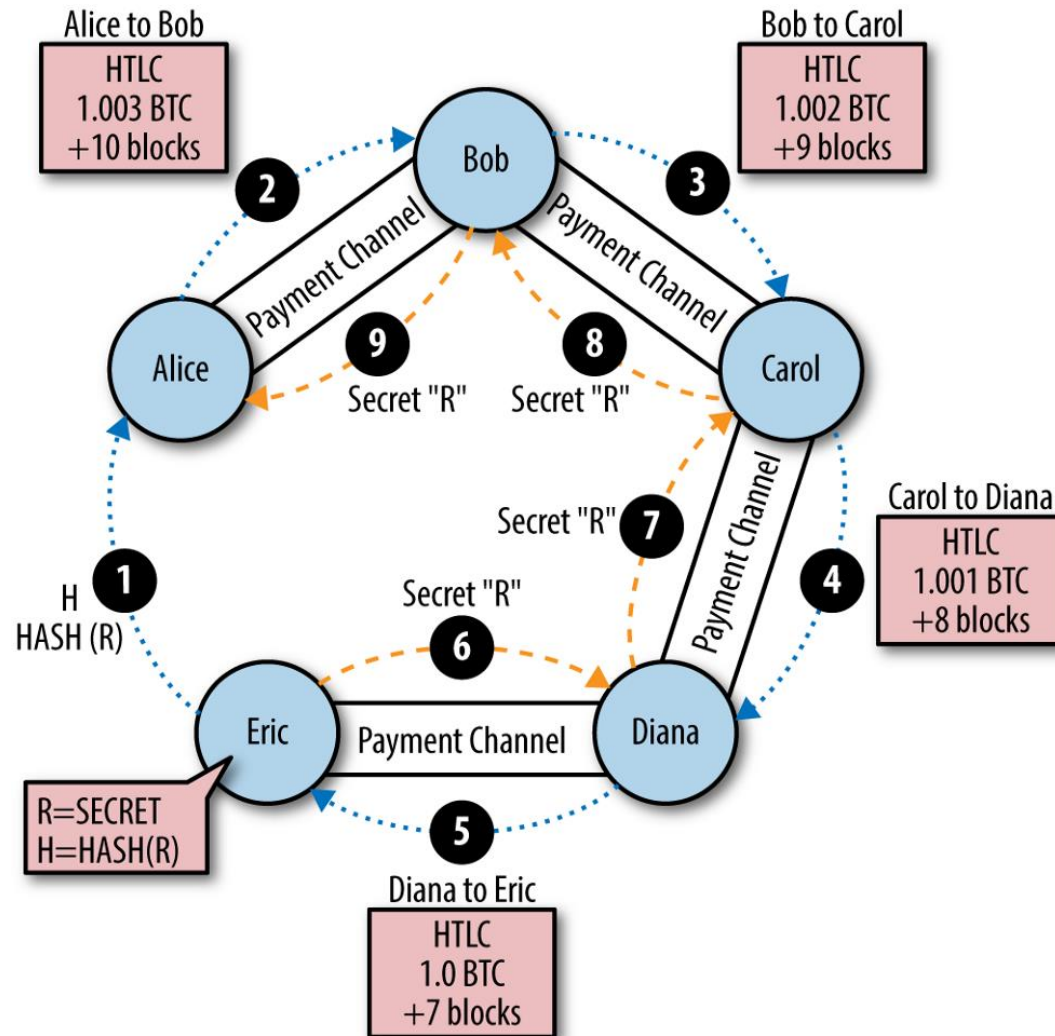
- Now we are ready to open a payment channel between Alice and Bob and Charlie
 - 1 BTC lockup, Alice – Bob, Bob – Charlie
 - Alice wants to send 0.5 BTC to Charlie (no direct channel)



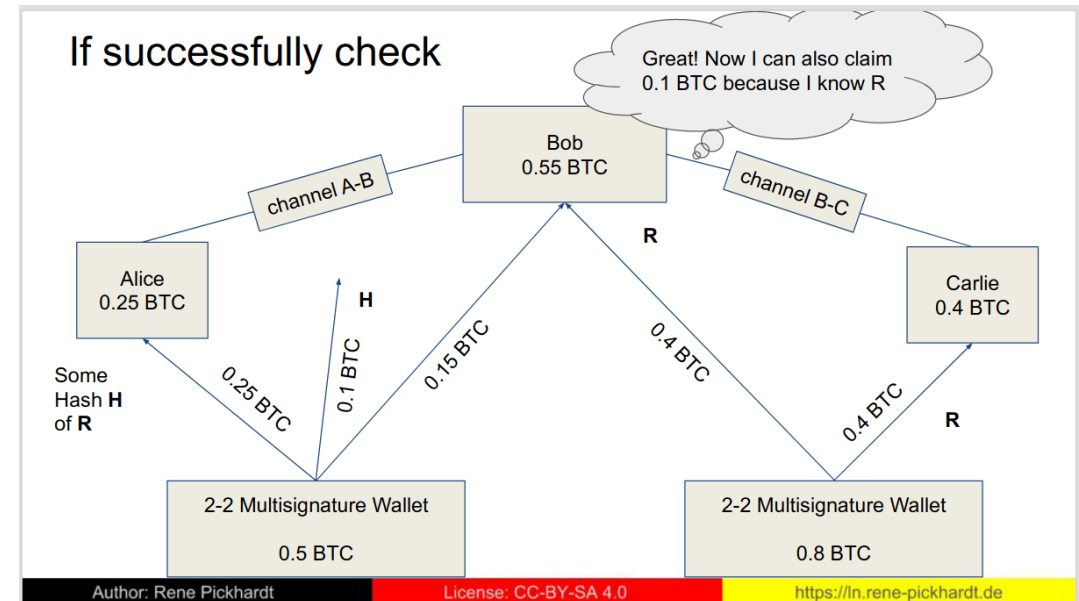
Atomic Swaps - Alice needs to reveal secret to redeem 1 BTC



Other View on Indirect Payment Channels



<http://site.ieee.org/icbc-2019/files/2019/05/ICBC-2019-Tutorial-3-Lightning-Network-Protocol.pdf>



<https://medium.com/softblocks/lightning-network-in-depth-part-2-htlc-and-payment-routing-db46aea445a8>