Imperial College London

SBA Research

Trustless, Interoperable Cryptocurrency-Backed Assets

Research Paper
(IEEE S&P 2019)

PoC Code
(GPL-3.0)

Joint Work With

Alexei Zamyatin

Dominik Harz

Joshua Lind

Panayiotis Panayiotu

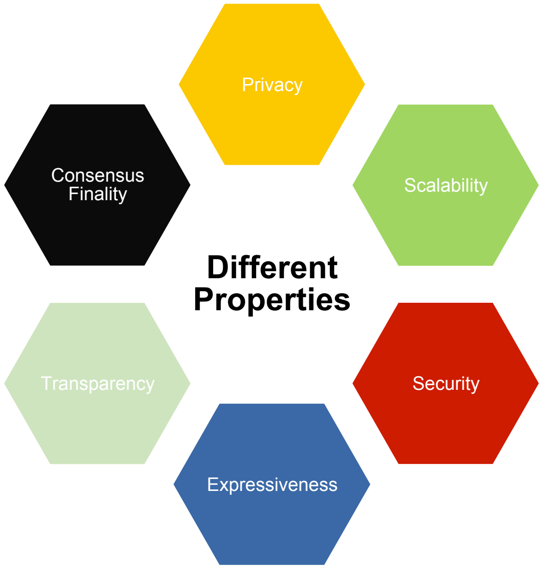
Arthur Gervais

William Knottenbelt

This research was co-funded by Blockchain.com, Outlier Ventures, Bridge 1 858561 SESC, Bridge 1 864738 PR4DLT (all FFG), the Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle (CDL-SQI), and the competence center SBA-K1 funded by COMET.

Motivation

Today:
Over 2000 heterogeneous cryptocurrencies



Privacy

Consensus Finality

Scalability

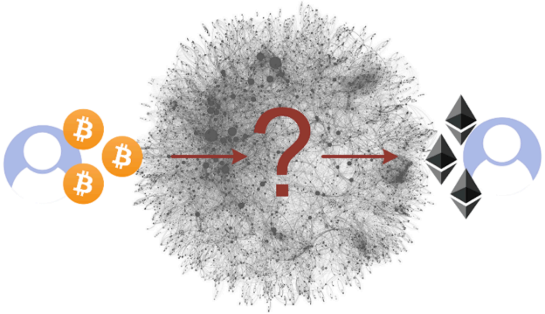
Different Properties

Transparency

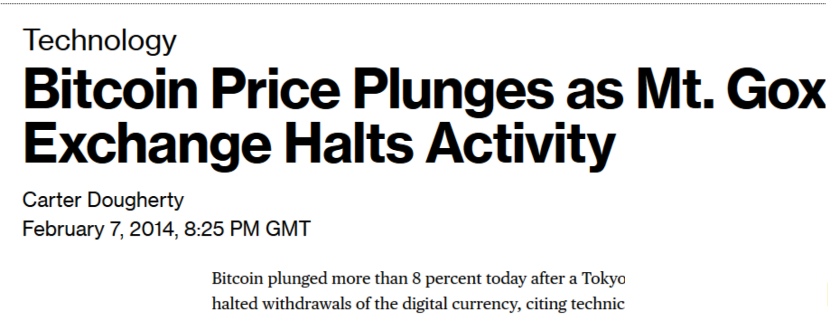
Security

Expressiveness

Challenge:
Trustless and scalabe
cross-chain communication



A History of Theft and Loss



Technology

Bitcoin Price Plunges as Mt. Gox Exchange Halts Activity

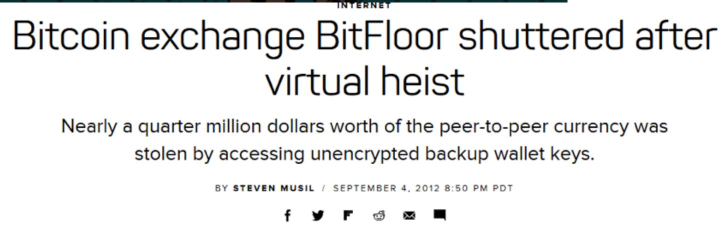
Carter Dougherty
February 7, 2014, 8:25 PM GMT

Bitcoin plunged more than 8 percent today after a Tokyo
halted withdrawals of the digital currency, citing technic

News Crypto

Poloniex Users Suffering From Frozen Accounts, Suspended Withdrawals, and Disabled Markets

By Mark - May 9, 2017

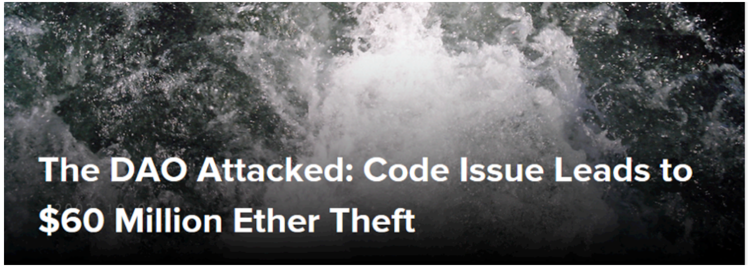


INTERNET

Bitcoin exchange BitFloor shuttered after virtual heist

Nearly a quarter million dollars worth of the peer-to-peer currency was stolen by accessing unencrypted backup wallet keys.

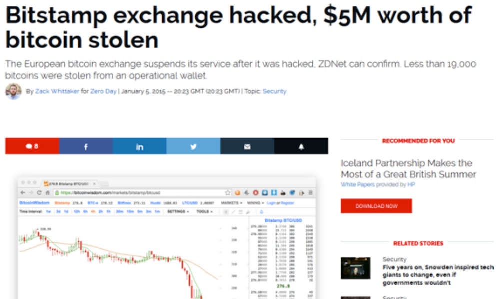
BY STEVEN MUSIL / SEPTEMBER 4, 2012 8:50 PM PDT



The DAO Attacked: Code Issue Leads to $60 Million Ether Theft

TECH • BITCOIN

Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong



Bitstamp exchange hacked, $5M worth of bitcoin stolen

The European bitcoin exchange suspends its service after it was hacked, ZDNet can confirm. Less than 19,000 bitcoins were stolen from an operational wallet.

By Zack Whittaker for Zero Day | January 5, 2015 -- 20:23 GMT (20:23 GMT) | Topic: Security

RECOMMENDED FOR YOU

Iceland Partnership Makes the Most of a Great British Summer
White Papers provided by HP

DOWNLOAD NOW

RELATED STORIES

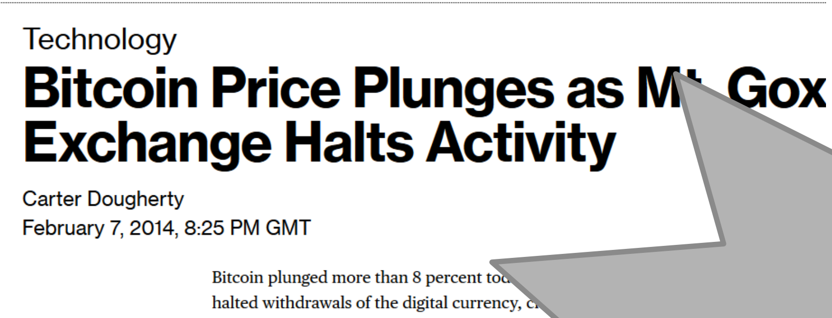
Security
Five years on, Snowden inspired tech giants to change, even if governments wouldn't

Security

INDY/TECH

COINCHECK HACK: BITCOIN EXCHANGE SECURITY UNDER SCRUTINY AFTER $534M CRYPTOCURRENCY THEFT

A History of Theft and Loss



Technology

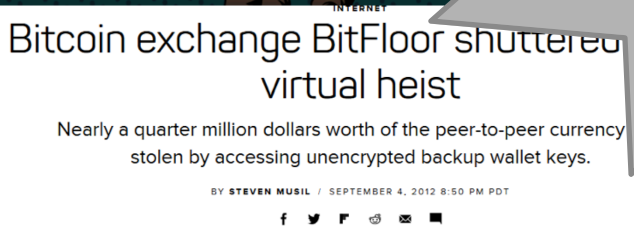
Bitcoin Price Plunges as Mt. Gox Exchange Halts Activity

Carter Dougherty
February 7, 2014, 8:25 PM GMT

Bitcoin plunged more than 8 percent tod
halted withdrawals of the digital currency, c

Poloniex Users Suffering From Frozen Accoun
Suspended Withdrawals, and Disabled Markets

By Mark - May 9, 2017



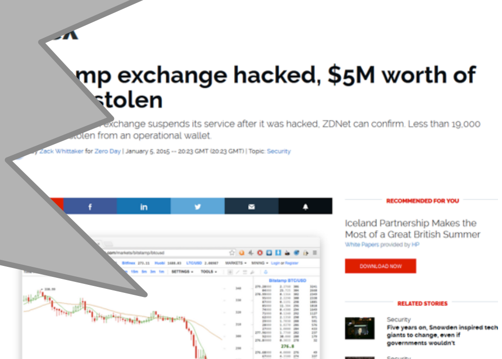
INTERNET

Bitcoin exchange BitFloor shuttered
virtual heist

Nearly a quarter million dollars worth of the peer-to-peer currency
stolen by accessing unencrypted backup wallet keys.

BY STEVEN MUSIL / SEPTEMBER 4, 2012 8:50 PM PDT

acked: Code Issue Leads to



mp exchange hacked, $5M worth of
stolen

exchange suspends its service after it was hacked, ZDNet can confirm. Less than 19,000
tolen from an operational wallet.

y Zack Whittaker for Zero Day | January 5, 2015 -- 20:23 GMT (20:23 GMT) | Topic: Security

RECOMMENDED FOR YOU

Iceland Partnership Makes the Most of a Great British Summer
White Papers provided by HP

DOWNLOAD NOW

RELATED STORIES

Security
Five years on, Snowden inspired tech giants to change, even if governments wouldn't

Security

ECH

COINCHECK HACK: BITCOIN EXCHANGE
SECURITY UNDER SCRUTINY AFTER
$534M CRYPTOCURRENCY THEFT

Decentralized
Exchanges?

Cross-Chain Communication Today

Centralized exchanges (CeX)

- Predominant method to exchange assets cross-chain
- > 99% of volume

Decentralized Exchanges (DeX):

- < 1% of volume
- Mostly **limited to ERC20** tokens on Ethereum

→ **Not „Cross-chain“!**

Atomic Cross-Chain Swaps* (2012)

- Ensure A → B and A ← B occur atomically
- Hashed Time-Lock Contracts (HTLCs)

Challenges:

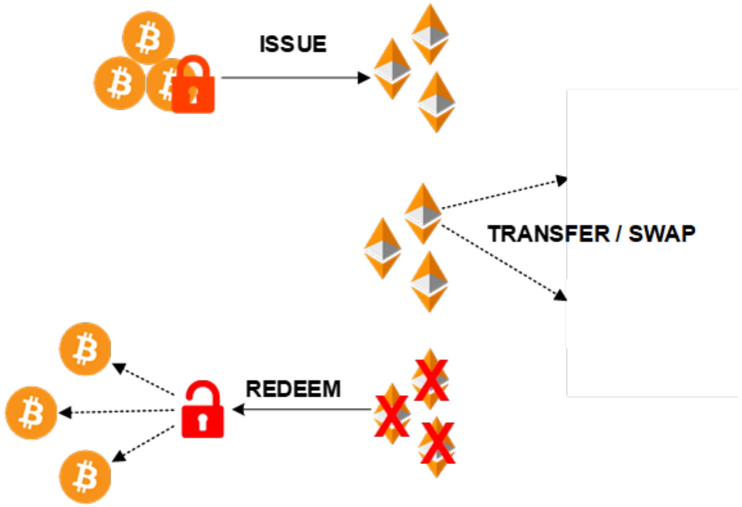
- All parties must be online
- Need out-of-band channel (censoring!)
- Require monitoring of all involved chains
- No standardized interface for locks
- Race conditions, mempool sniffing, …

*we refer to the HTLC-based form of ACCS. Other constructions possible

Cryptocurrency-Backed Assets

On-chain assets backed 1:1 by an existing cryptocurrency

e.g. **Bitcoin-backed tokens** on Ethereum



- Cross-chain DeX
- Cross-chain payment channels,
- Improved atomic swaps
- Stablecoins
- …

Challenge: Conditional Locks in Bitcoin

Goal:

Unlock funds on Bitcoin only when tokens are *burned*

Challenge:

We cannot verify the state of e.g. Ethereum

Can we use **hashlocks**?

Publicly verifiable contracts **cannot generate random secret**

→ We need an intermediary

System Model

Requester: locks coins to issue tokens

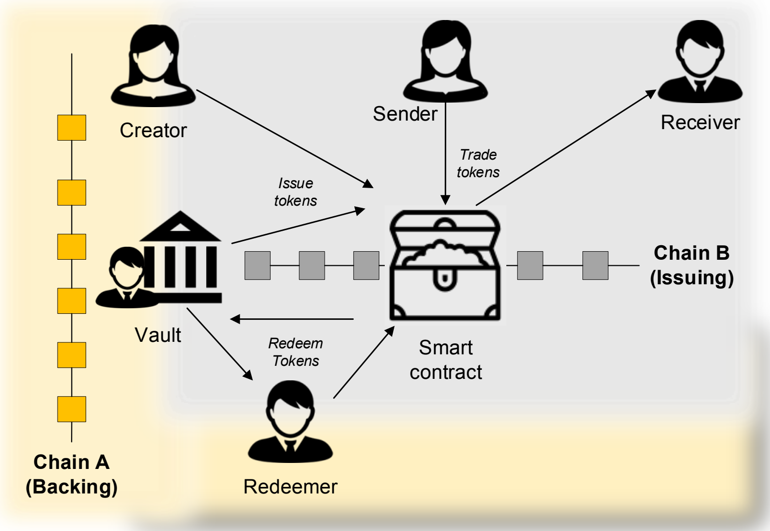
Redeemer: burns tokens to receive coins

Sender/Receiver: Send/receive backed tokens

Vault: ensures correct redeeming on backing chain.
Non-trusted and collateralized

`Smart Contract`: responsible for issuing, trading and redeeming on issuing chain. Enforces correctness of Vaults.

Intermediaries



Smart Contract

Base functionality:

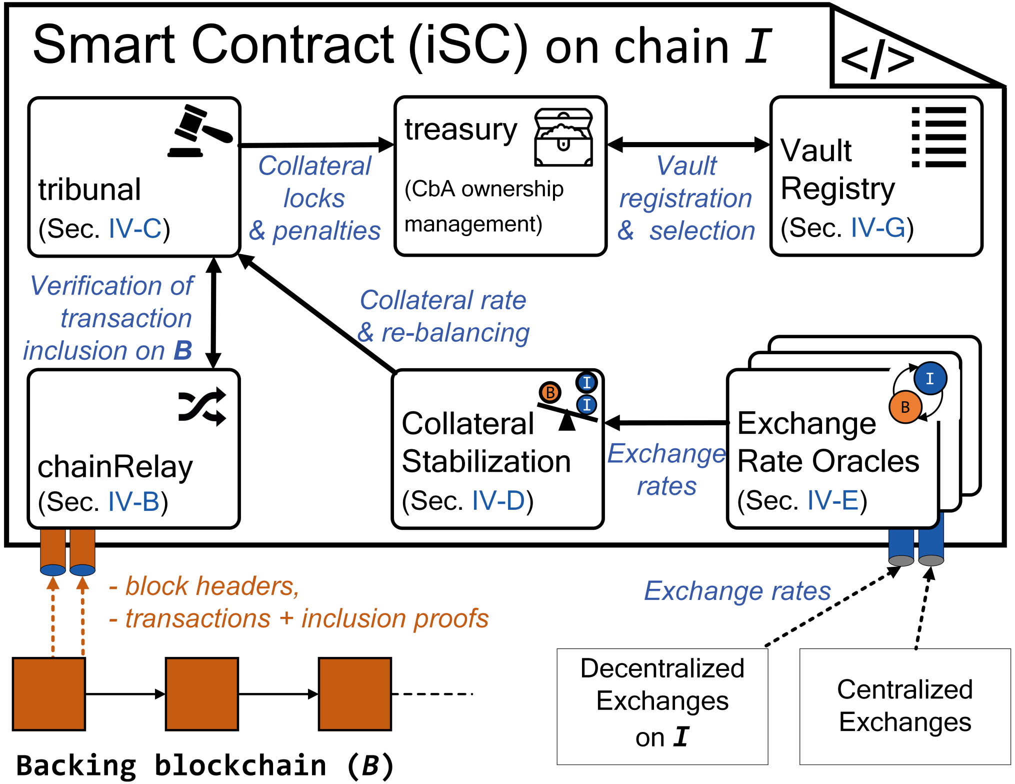
- Issue
- Transfer / Swap
- Redeem

Chain Relay:

- Verify PoW
- Verify TX inclusion proof

Collateralization:

- Lock
- Conditional release / Liquidate


Smart Contract (iSC) on chain *I*
</>
tribunal
(Sec. IV-C)
Collateral locks & penalties
treasury
(CbA ownership management)
Vault registration & selection
Vault Registry
(Sec. IV-G)
*Verification of transaction inclusion on **B***
Collateral rate & re-balancing
chainRelay
(Sec. IV-B)
B
I
I
Collateral Stabilization
(Sec. IV-D)
Exchange rates
I
B
Exchange Rate Oracles
(Sec. IV-E)
- block headers,
- transactions + inclusion proofs
Exchange rates
Backing blockchain (*B*)
Decentralized Exchanges on *I*
Centralized Exchanges

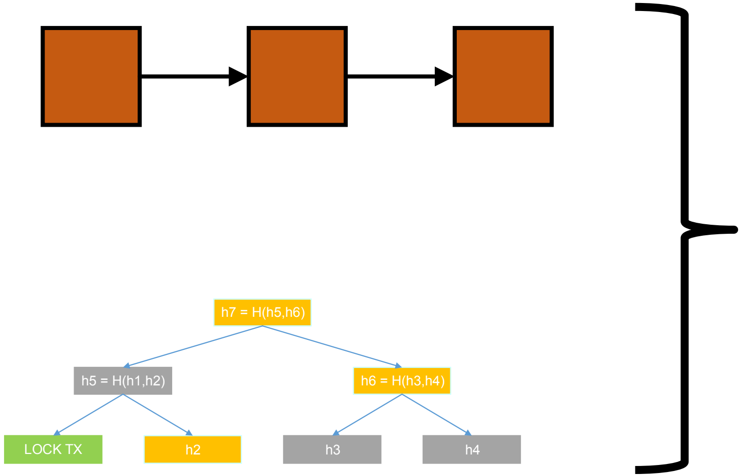
Chain Relay

Cross-chain SPV / light client

E.g. deployed on Ethereum to verify transactions in Bitcoin

Block Headers

Transaction
+
Merkle Path



BTC RELAY

System Requirements

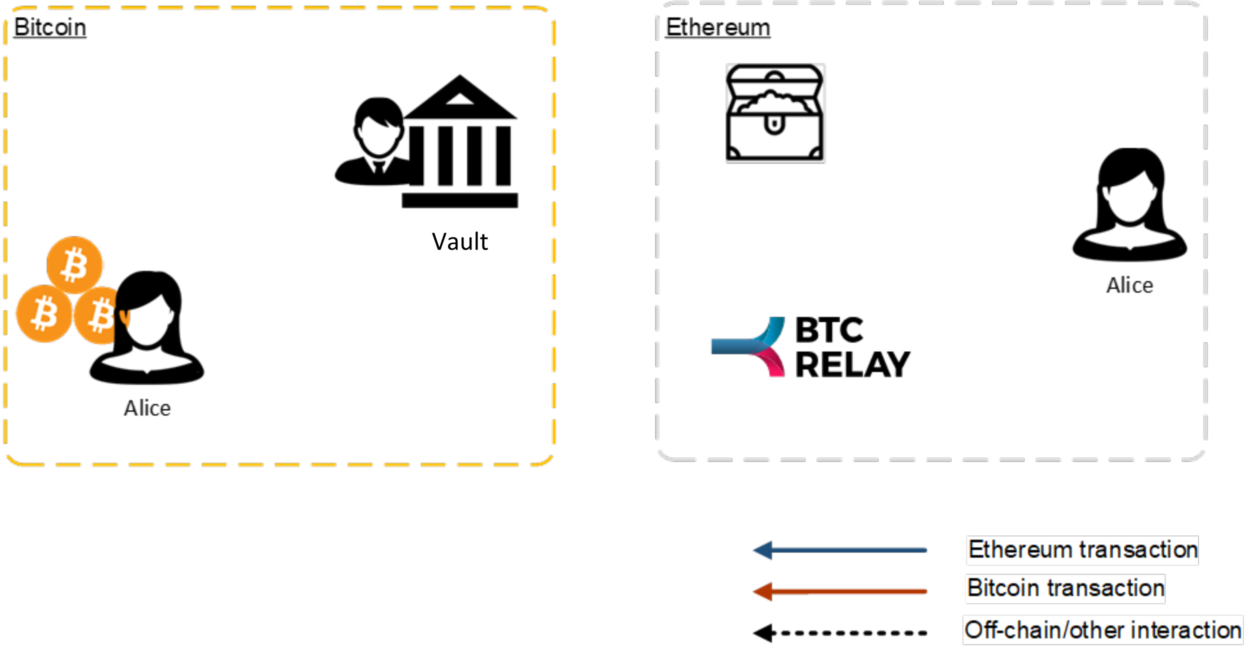
Backing Chain	**Issuing Chain** (Smart Contracts)
None (Basic ledger functionality)	**Chain relays** • Verify PoW of backing chain • Verify transaction inclusion **On-chain assets / meta information** • Tokens, colored coins, …. **Conditional payments** • Collateralization
e.g. **Bitcoin**, Ethereum, Ethereum Classic, Litecoin, …	e.g. **Ethereum**, Ethereum Classic, Zilliqa, Cardano?, …

System Requirements

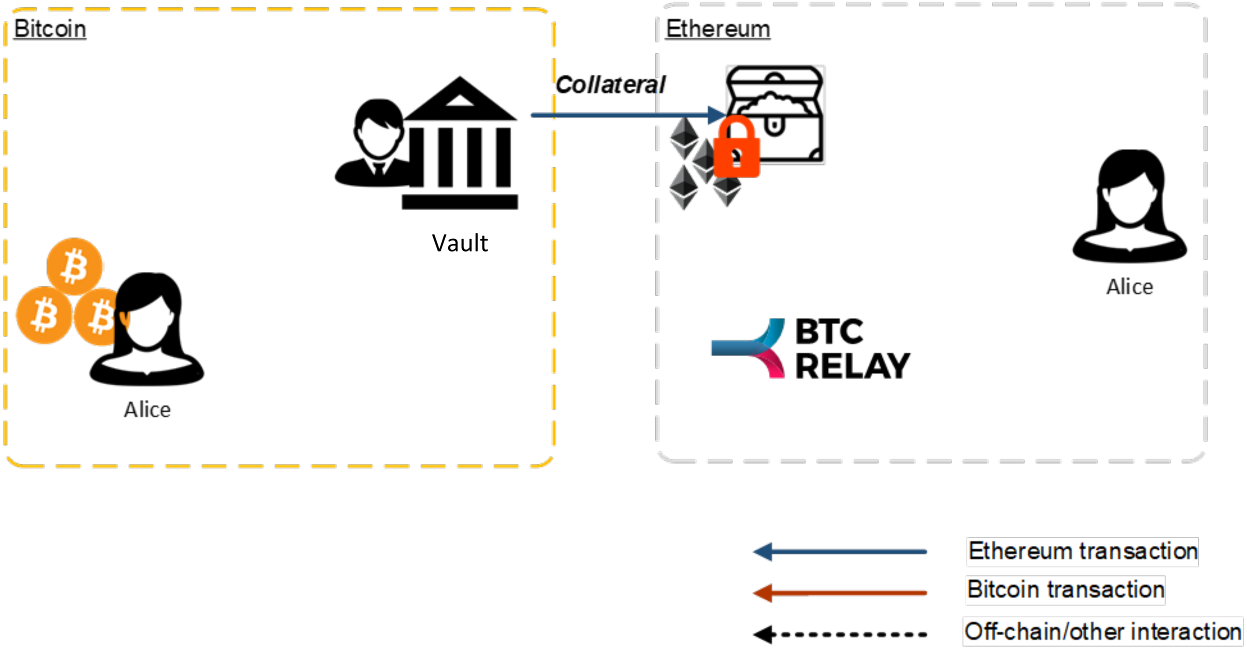
Backing Chain	**Issuing Chain** (Smart Contracts)
None (Basic ledger functionality) Smart contracts allow to automate/optimize the process	**Chain relays** • Verify PoW of backing chain • Verify transaction inclusion **On-chain assets / meta information** • Tokens, colored coins, …. **Conditional payments** • Collateralization
e.g. **Bitcoin**, Ethereum, Ethereum Classic, Litecoin, …	e.g. **Ethereum**, Ethereum Classic, Zilliqa, Cardano?, …

Protocols

Issue

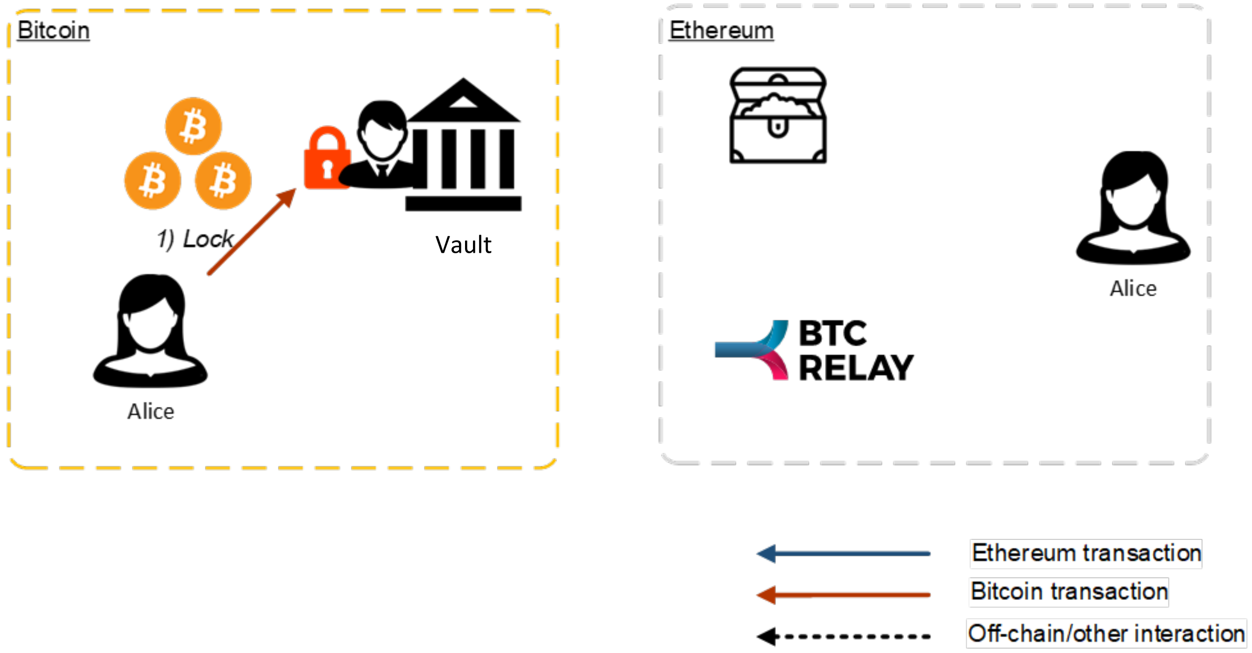

Bitcoin
Vault
Alice
Ethereum
Alice
BTC RELAY
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Issue: Precondition



→ **Over-collateralization to mitigate exchange rate fluctuations**

Issue



Bitcoin

1) Lock

Vault

Alice

Ethereum

BTC RELAY

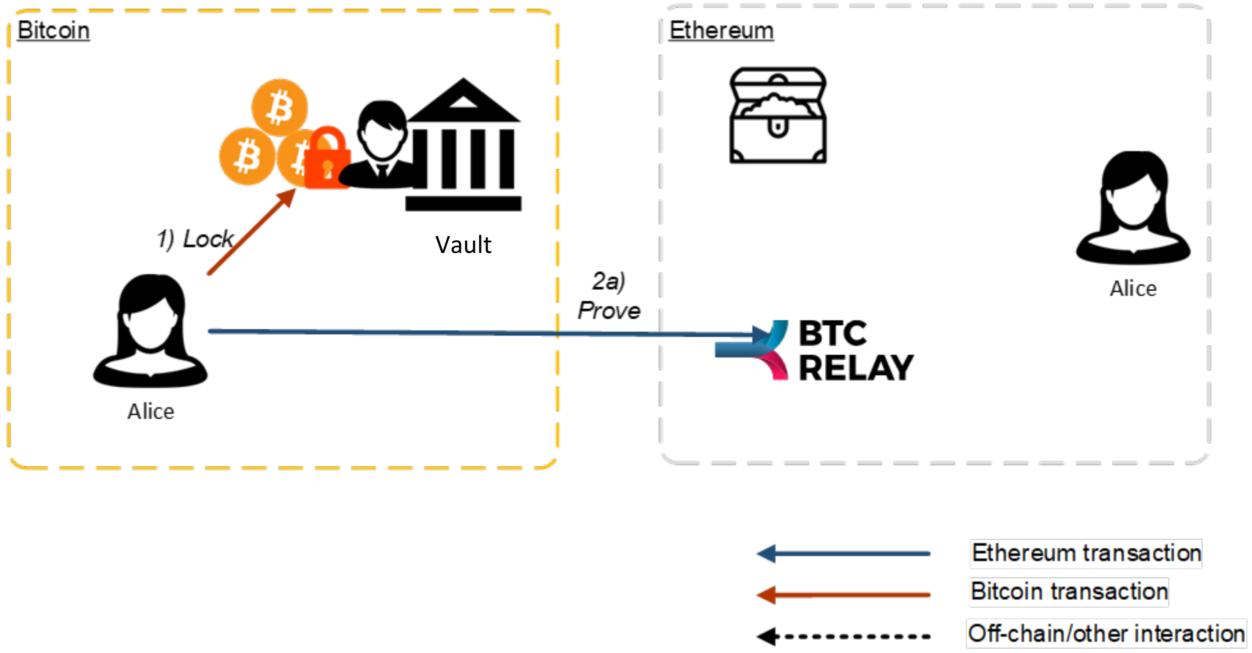
Alice

Ethereum transaction

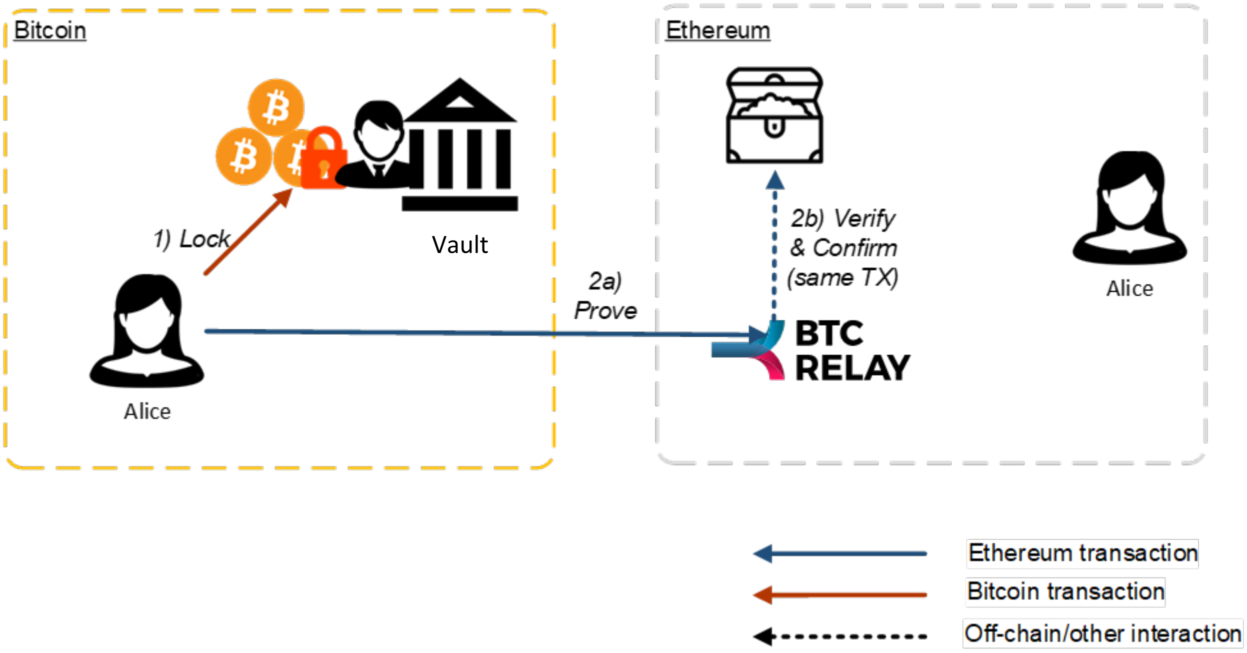
Bitcoin transaction

Off-chain/other interaction

Issue


Bitcoin
1) Lock
Vault
Alice
2a) Prove
Ethereum
BTC RELAY
Alice
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Issue



Bitcoin

1) Lock

Vault

Alice

2a) Prove

Ethereum

2b) Verify & Confirm (same TX)

BTC RELAY

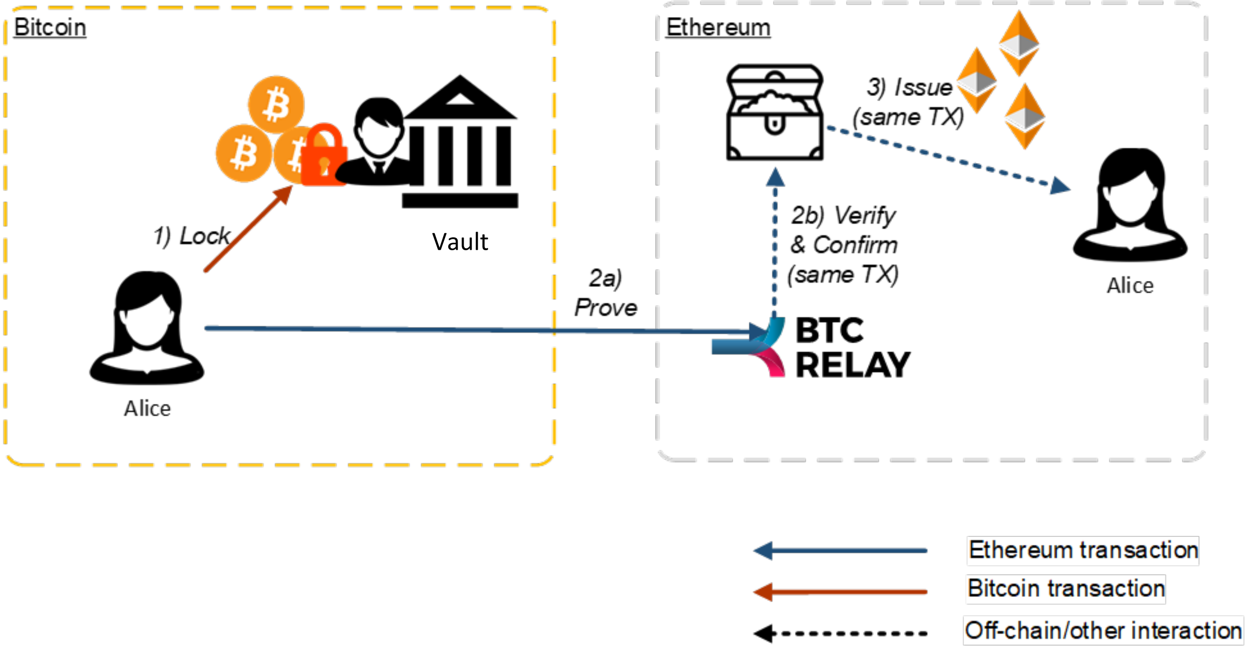
Alice

Ethereum transaction

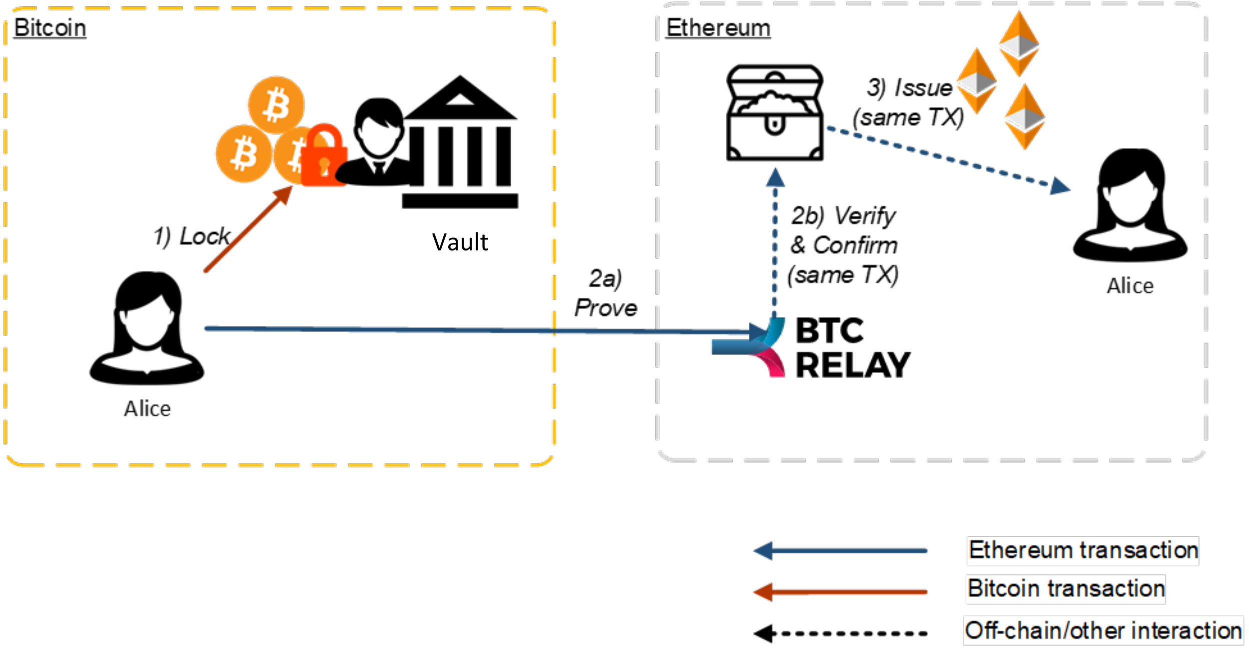
Bitcoin transaction

Off-chain/other interaction

Issue


Bitcoin
1) Lock
Vault
Alice
2a) Prove
Ethereum
3) Issue (same TX)
2b) Verify & Confirm (same TX)
BTC RELAY
Alice
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Issue



Only issue if Issuer locked sufficient collateral!
→ Challenge: race conditions

Issue – Race Conditions

Potential Problems:

- **Simultaneous issuing**
  - Alice and Carol try to lock same portion of the vault‘s collateral
  - Loser of the race looses BTC
- **Vault withdraws collateral before Alice can finalize process**
  - Security waiting period for inclusion proof
  - Ethereum transaction inclusion time
  - Latency
  - DoS

Mitigation 1 – Delayed Collateral Withdraw

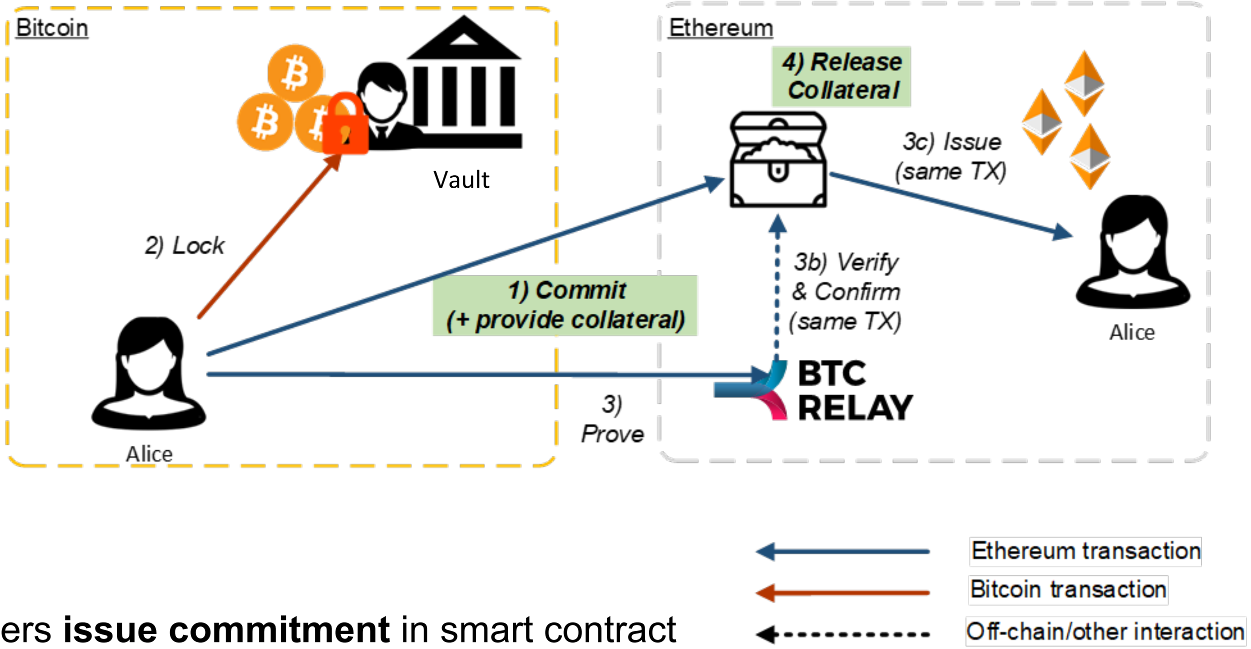
Issuer must announce withdrawal of unused collateral:

1) **Announce**

2) **Delay**
   - finalize pending requests
   - users know race conditions are now possible

3) **Withdraw**

Mitigation 2 – Collateralized Commitments



Alice registers **issue commitment** in smart contract

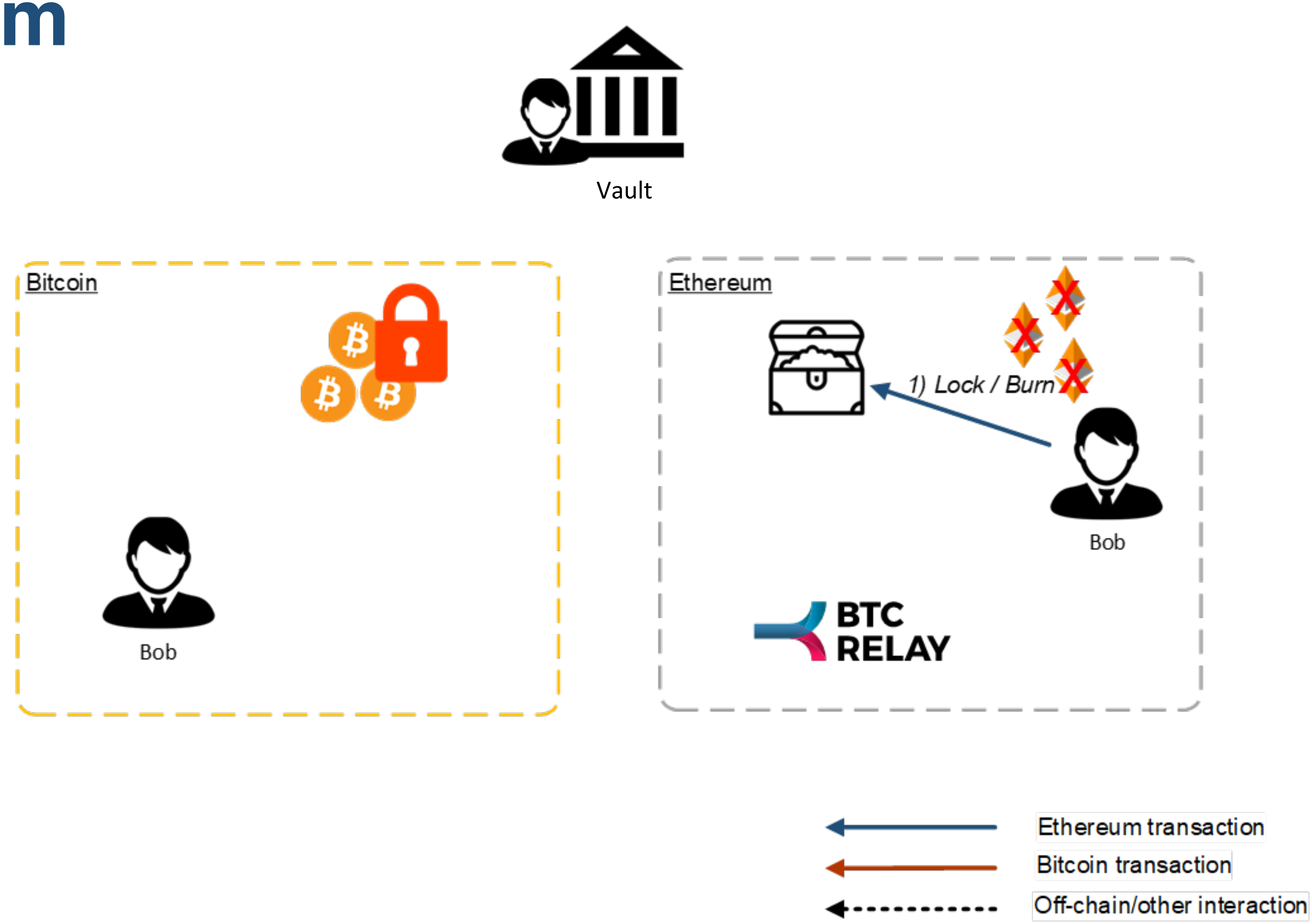
→ Temporarily locks vault‘s *eth* collateral

Requirement: Alice must provide collateral to **prevent griefing**

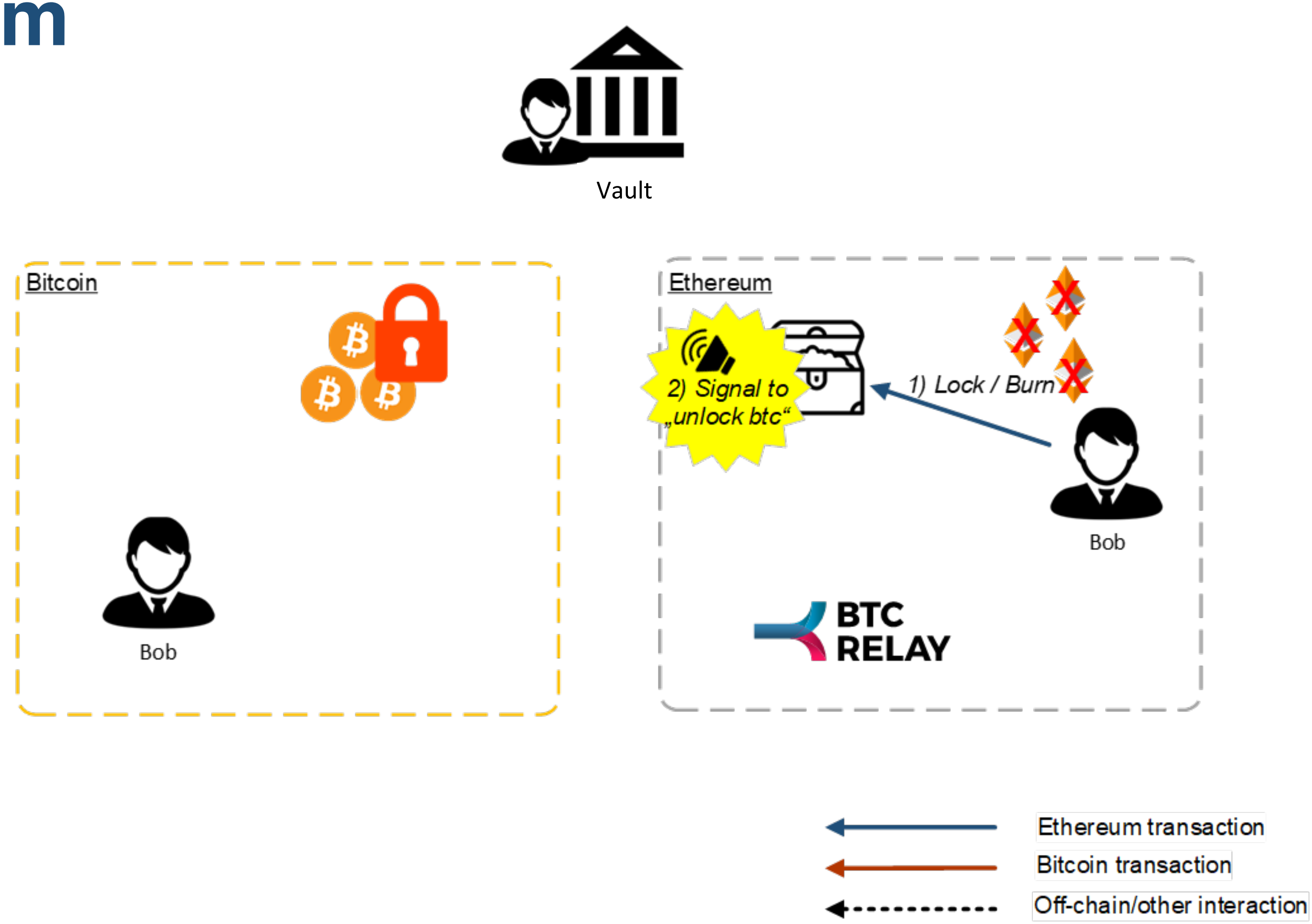
Swap & Transfer…

Simple ERC20 transfer / atomic swap!
Alice → Bob

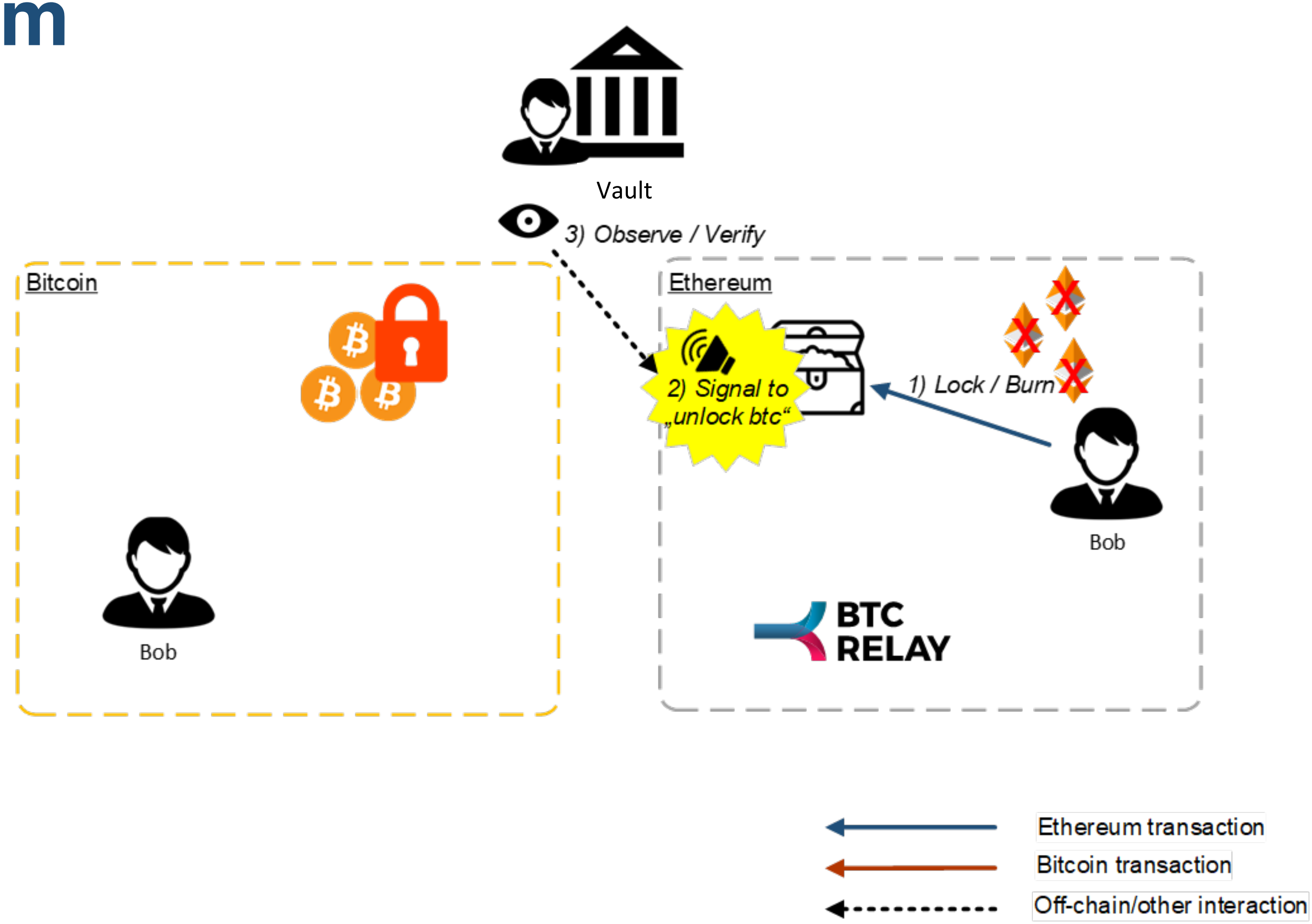
Redeem


Vault
Bitcoin
Bob
Ethereum
1) Lock / Burn
Bob
BTC RELAY
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

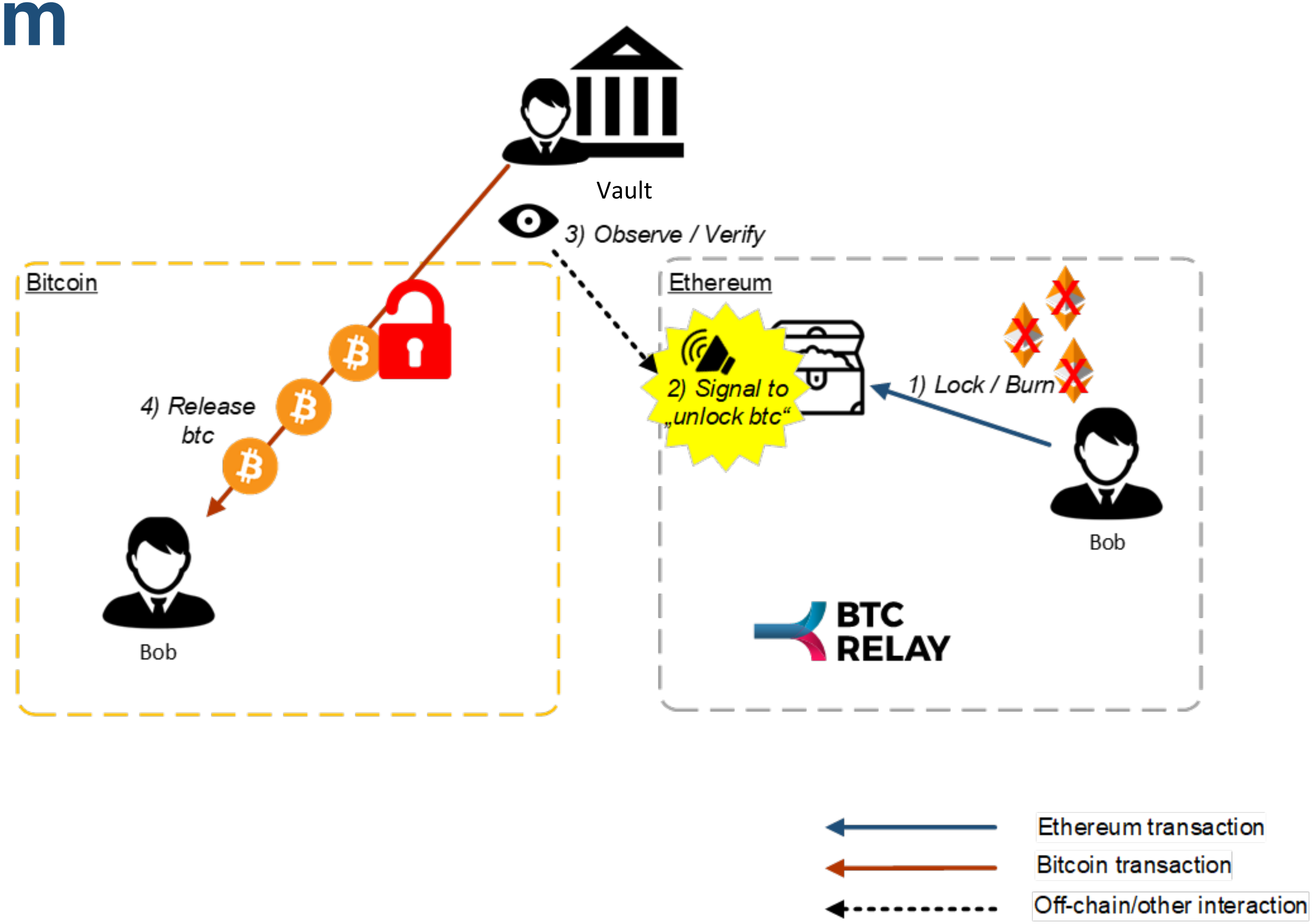
Redeem


Vault
Bitcoin
Bob
Ethereum
2) Signal to „unlock btc"
1) Lock / Burn
Bob
BTC RELAY
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

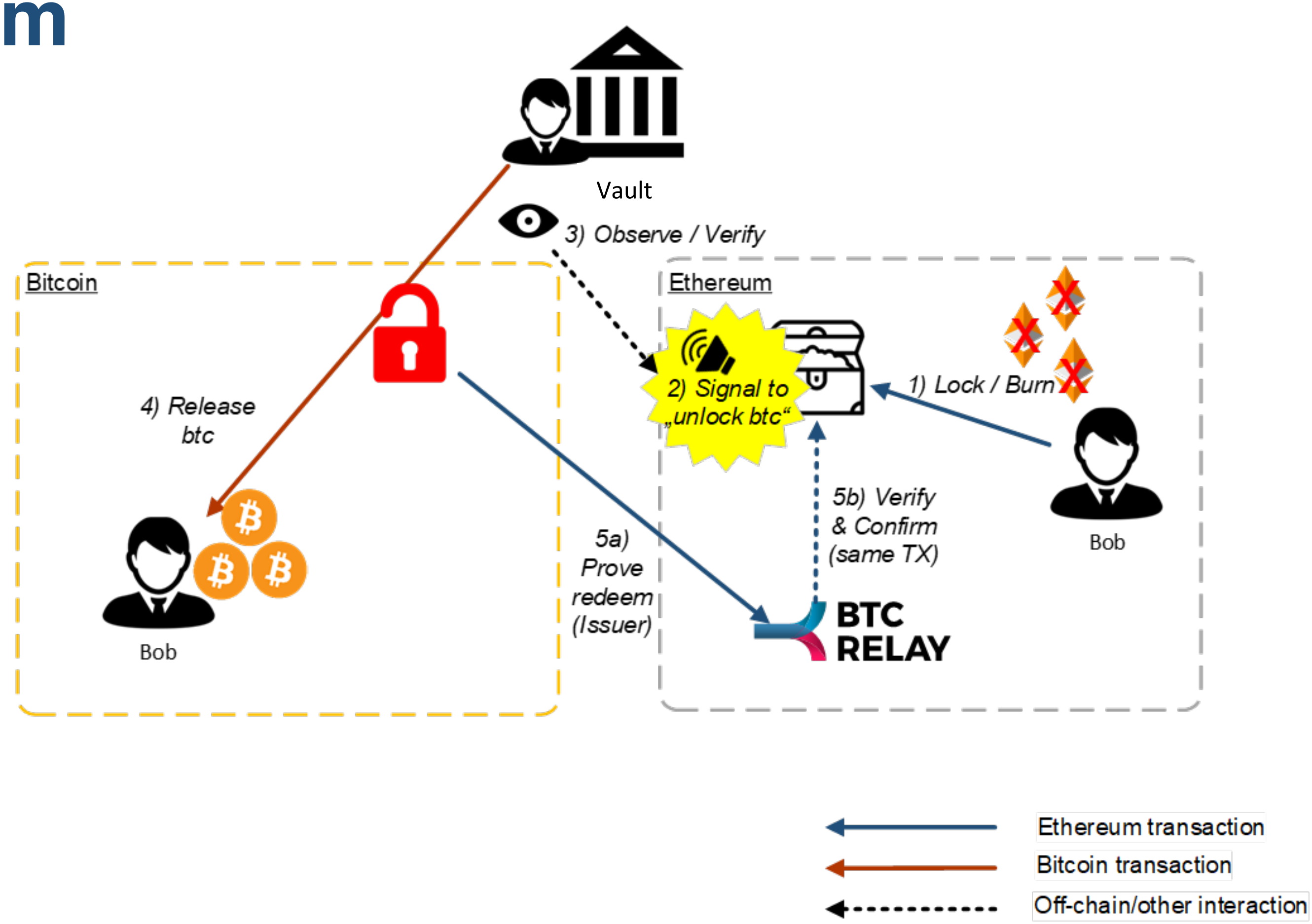
Redeem


Vault
3) Observe / Verify
Bitcoin
Ethereum
2) Signal to „unlock btc“
1) Lock / Burn
Bob
Bob
BTC RELAY
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Redeem

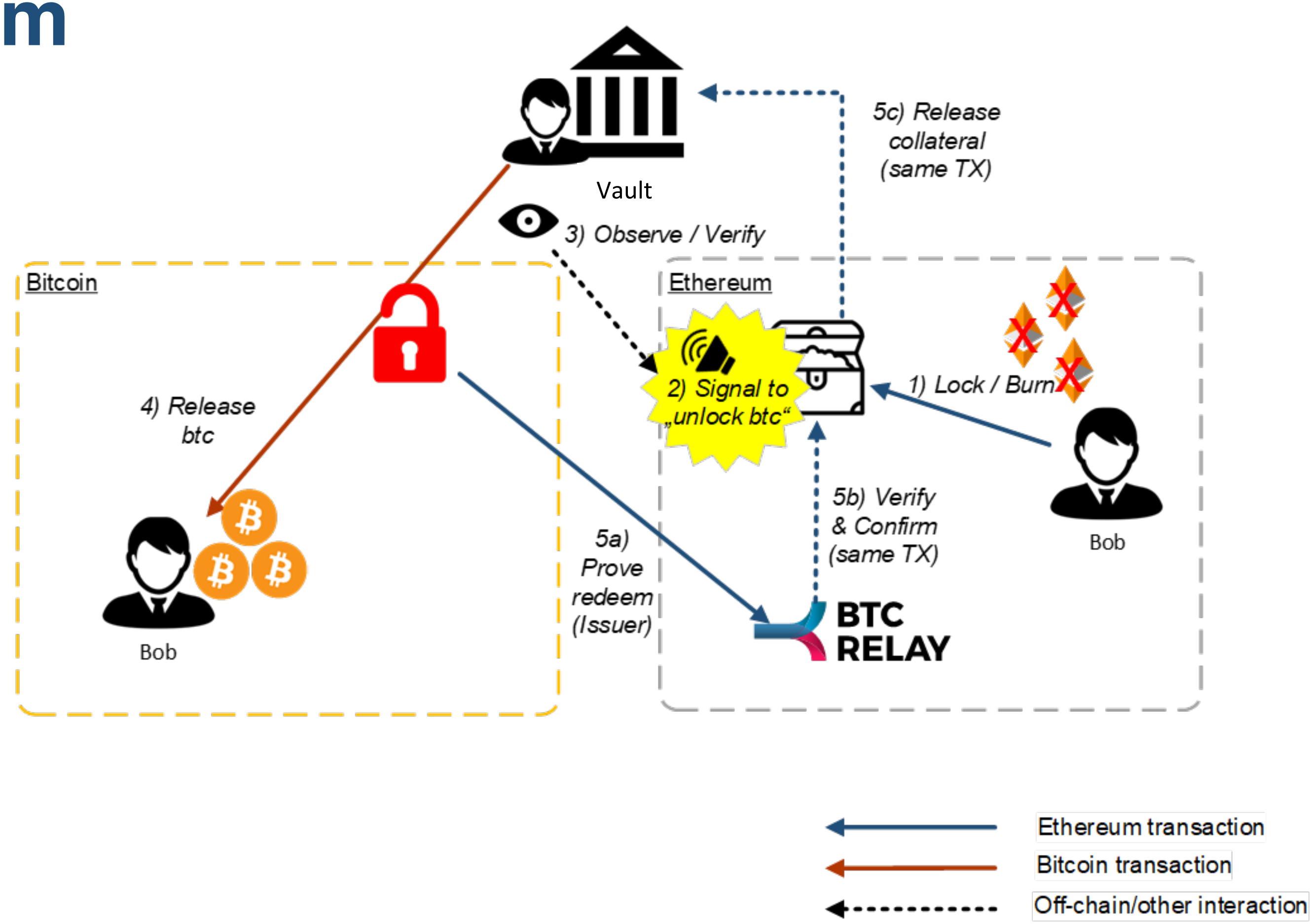

Vault
3) Observe / Verify
Bitcoin
Ethereum
2) Signal to „unlock btc“
1) Lock / Burn
4) Release btc
Bob
Bob
BTC RELAY
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Redeem

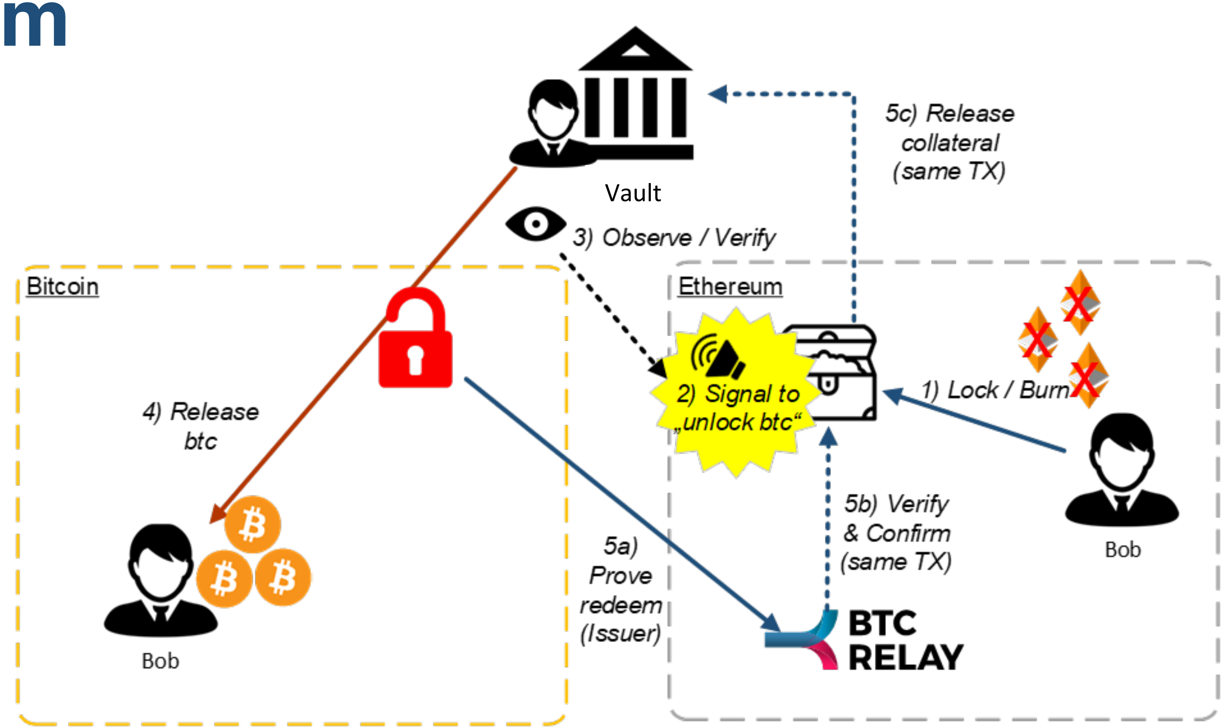


Vault
3) Observe / Verify
Bitcoin
Ethereum
2) Signal to „unlock btc“
1) Lock / Burn
4) Release btc
5b) Verify & Confirm (same TX)
Bob
5a) Prove redeem (Issuer)
BTC RELAY
Bob
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Redeem


Vault
3) Observe / Verify
5c) Release collateral (same TX)
Bitcoin
Ethereum
2) Signal to „unlock btc“
1) Lock / Burn
4) Release btc
5b) Verify & Confirm (same TX)
Bob
5a) Prove redeem (Issuer)
BTC RELAY
Bob
Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Redeem


Vault
3) Observe / Verify
5c) Release collateral (same TX)
Bitcoin
Ethereum
2) Signal to „unlock btc“
1) Lock / Burn
4) Release btc
5b) Verify & Confirm (same TX)
5a) Prove redeem (Issuer)
BTC RELAY
Bob
Bob

If the vault cannot provide proof of correct behavior:

→ Collateral slashed

→ Bob reimbursed

←	Ethereum transaction
←	Bitcoin transaction
⇠	Off-chain/other interaction

Mitigating Exchange Rate Fluctuations

Stage	Meaning	Action	Example threshold
Secure Operation	Collateral surplus	**Vault:** Withdrawal of unused collateral possible. **Users**: can issue new assets	> 2.0
Buffered Collateral	Sufficient collateral buffer	**SC**: no new Issue requests accepted **Vault**: Increase collateral.	
Liquidation	Collateral buffer critically low	**Vault**: increase collateral **Users**: redeem recommended **SC: automatic liquidation (opt-in/out)***	< 1.05

* Triggered by exchange rate oracle or user/watchtower

System Properties

1. **Auditability**: all actions on both chains logged
2. **Consistency**: backed-assets only issued if proof provided
3. **Redeemability**: receive Bitcoin or be reimbursed in Ether
4. **Liveness**: no third party required to use XCLAIM. Any user can become a vault!!
5. **Atomic Swaps**: swap Bitcoin vs Ether via smart contract
6. **Scale-out**: the more vaults / collateral locked, the more assets can be issued
7. **Compatibility**: minimal requirements for backing chain

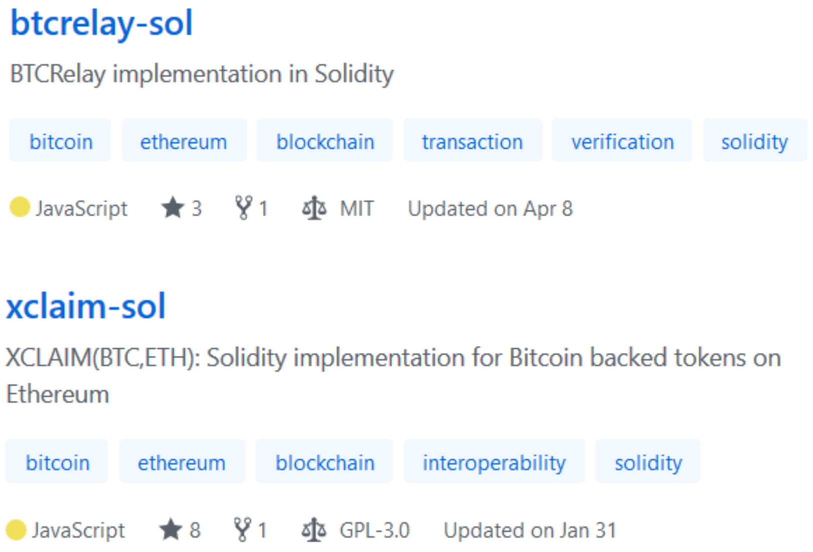
Implementation

- XCLAIM smart contract: Solidity v0.5.x (~ 820 LOC)

- BTCRelay: Serpent (https://github.com/ethereum/btcrelay)

→ new Solidity implementation is WIP

- Tested on Ropsten



btcrelay-sol

BTCRelay implementation in Solidity

bitcoin ethereum blockchain transaction verification solidity

● JavaScript ★ 3 ⑂ 1 ⚖ MIT Updated on Apr 8

xclaim-sol

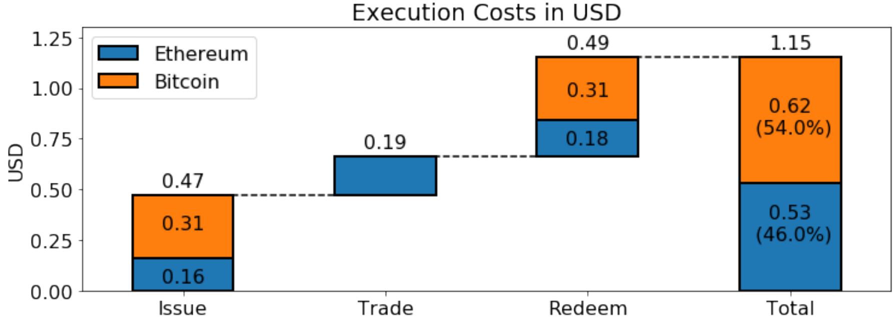
XCLAIM(BTC,ETH): Solidity implementation for Bitcoin backed tokens on Ethereum

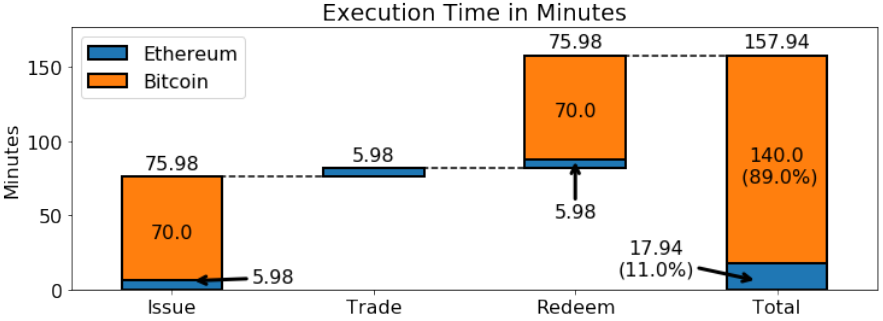
bitcoin ethereum blockchain interoperability solidity

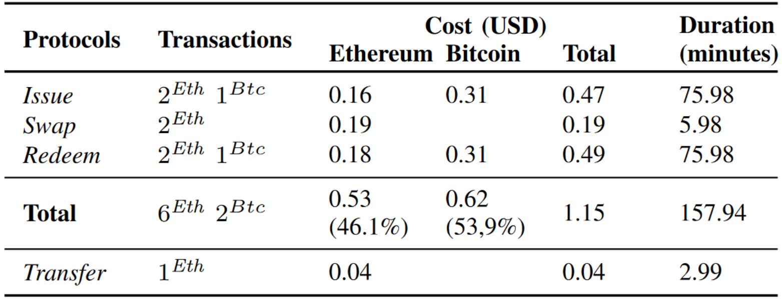
● JavaScript ★ 8 ⑂ 1 ⚖ GPL-3.0 Updated on Jan 31

https://github.com/crossclaim

Performance and Costs



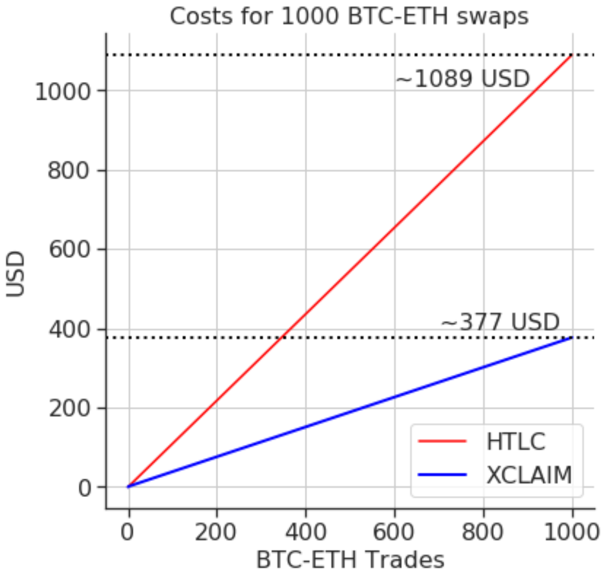


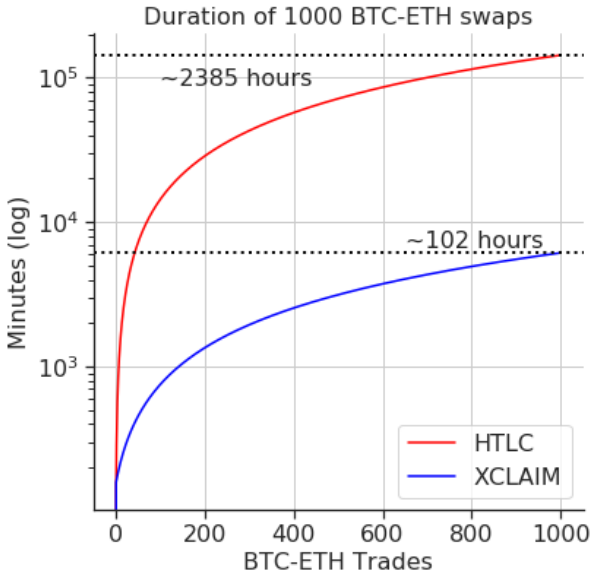


Protocols	Transactions	Cost (USD)			Duration
		Ethereum	Bitcoin	Total	(minutes)
Issue	2^{Eth} 1^{Btc}	0.16	0.31	0.47	75.98
Swap	2^{Eth}	0.19		0.19	5.98
Redeem	2^{Eth} 1^{Btc}	0.18	0.31	0.49	75.98
Total	6^{Eth} 2^{Btc}	0.53 (46.1%)	0.62 (53,9%)	1.15	157.94
Transfer	1^{Eth}	0.04		0.04	2.99

Exchange rate: USD 220 / ETH (Gas cost: 5 gwei); USD 4.497 / BTC
“Recommended” security parameters: 14 sec x 12 ETH Tx confs; 10 min x 6 BTC Tx confs.

Comparison to HTLC Atomic Swaps





BTC-ETH swaps with XCLAIM are 95.7% faster and 64.5% cheaper for 1000 independent swaps.

Challenges and Ongoing Work

Feasibility of chain relays

- ***Off-chain verification games**: TrueBit, Arbitrum, …*
- ***Compact proofs**: NiPoPoWs, FlyClient*
- ***Combination: Game + Fallback NIZK Proof***
  → PoW verification (hash preimage → hash?)

Multi-signatures to prevent theft
(feasible via off-chain channels)

Incentives for Vault F(r)ee Market

Decentralized Exchange Rate
Oracles & Stabilization

Questions?

Trustless, Interoperable Cryptocurrency-Backed Assets

Research Paper
(IEEE S&P 2019)

PoC Code
(GPL-3.0)

eprint.iacr.org/2018/643

github.com/crossclaim

Website: xclaim.io