



# Interoperability with Cryptocurrency-backed Tokens

**Alexei Zamyatin**

**Dominik Harz**

Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, William Knottenbelt

Scaling Bitcoin 2018, Tokyo

Imperial College  
London

 **SBA**  
Research

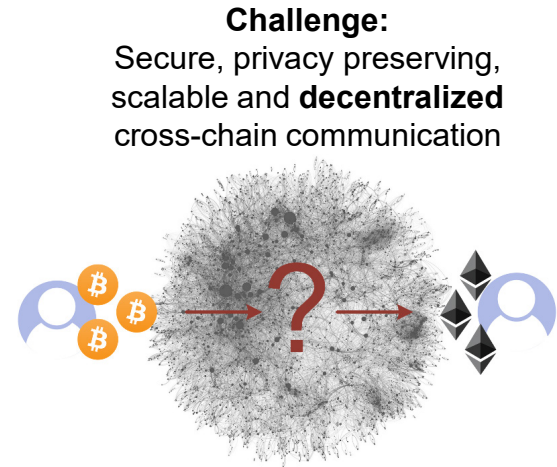
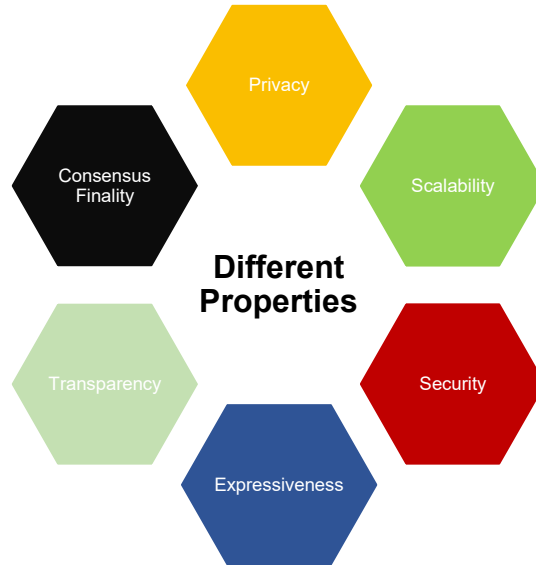
**OV**

 **BLOCKCHAIN**

# Motivation



**Today:**  
Over 2000 heterogeneous  
cryptocurrencies



# 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

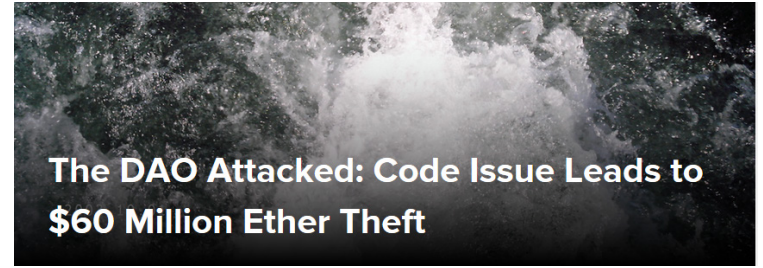


## Bitcoin exchange BitFloor shuttered after virtual heist

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

Scaling Bitcoin 2018



TECH • BITCOIN

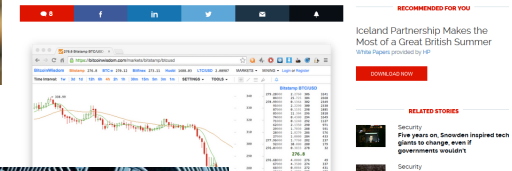
## Bitcoin Worth \$72M Was Stolen in Bitfinex Exchange Hack in Hong Kong



## 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 Zach Wissner for ZDNet | January 5, 2016 -- 20:22 GMT (20:22 GMT) | Topic: Security



Cryptocurrency-back

# 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 as Mt. Gox halted withdrawals of the digital currency, causing a panic in the market.



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

By Mark - May 9, 2017

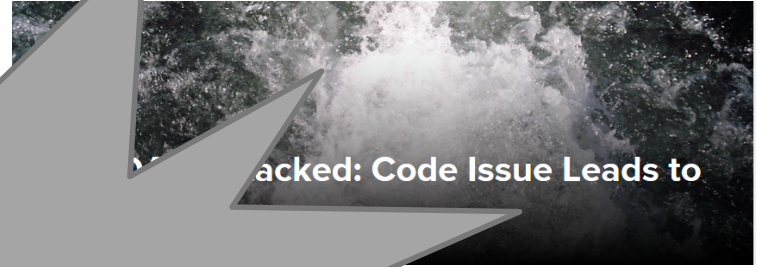
## Bitcoin exchange BitFloor shuttered in virtual heist

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

Scaling Bitcoin 2018

Cryptocurrency-backups: The most valuable item you own



Hacked: Code Issue Leads to

## Decentralized Exchanges?

## Polonex exchange hacked, \$5M worth of Bitcoin stolen

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

By Jason Witteback for ZDNet | January 5, 2018 -- 20:22 GMT (20:22 GMT) | Topic: Security



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

# 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  $A \rightarrow B$  and  $A \leftarrow B$  occur **atomically**
- Hashed Time-Lock Contracts (HTLCs)

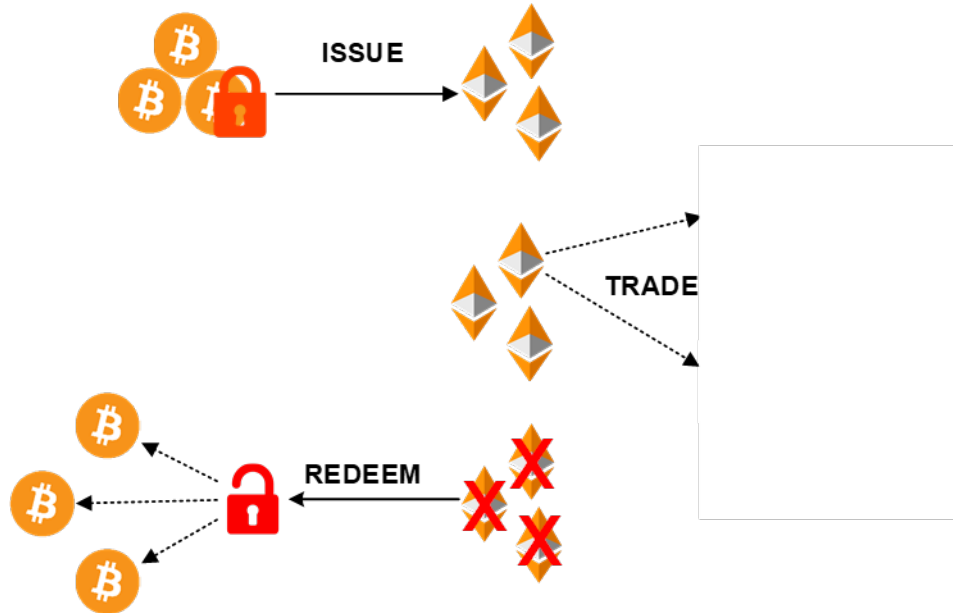
## Challenges:

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

\*we refer to the base form of ACCS. Other constructions possible

# Cryptocurrency-Backed Tokens

Tokens / on-chain assets backed 1:1 by an existing cryptocurrency  
e.g. **Bitcoin-backed tokens** on Ethereum



- Generality
- Fungibility
- Divisibility
- Value Redeemability**
- Transfer Atomicity**
- Consistency**

# 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 and Principles

**Creator:** locks coins to issue tokens

**Redeemer:** burns tokens to receive coins

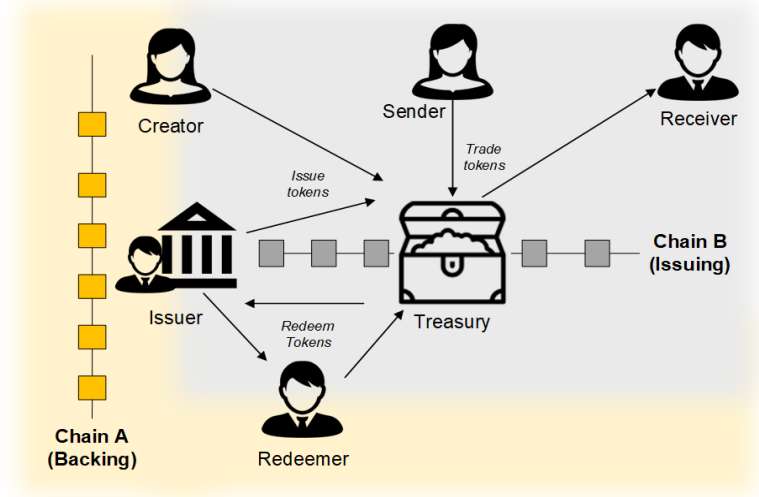
**Sender/Receiver:** Send/receive backed tokens

**Issuer:** ensures correct issuing/redeeming on backing chain.

*Non-trusted and collateralized*

**Treasury:** responsible for issuing, trading and redeeming on issuing chain

*Publicly verifiable smart contract*



**Intermediaries**

# Treasury Contract

## Base functionality:

Issue - Transfer - Redeem

## Chain Relay:

- Verify PoW
- Verify TX inclusion proof



## Collateralization:

- Lock
- Conditional release

**Optional:** Verify HTLC

# System Requirements

---

## Backing Chain

**Hashed-timelock contracts**  
(optional)

e.g. **Bitcoin**, Ethereum, Ethereum Classic, Litecoin, ...

---

## Issuing Chain (Smart Contracts)

### Chain relays

- Verify PoW of backing chain
- Verify transaction inclusion

### On-chain assets / meta information

- Tokens, colored coins, ....

### Conditional payments

- Collateralization

e.g. **Ethereum**, Ethereum Classic, Zilliqa, Cardano?, ...

---

# Cryptocurrency-Backed Tokens

## Achievable advantages:

- + Non-interactive
- + Logic handled by publicly verifiable smart contract
- + No need to monitor backing chains
- + Standardized token interface
- + Wallet in backing chain only needed when redeeming

# Cryptocurrency-Backed Tokens

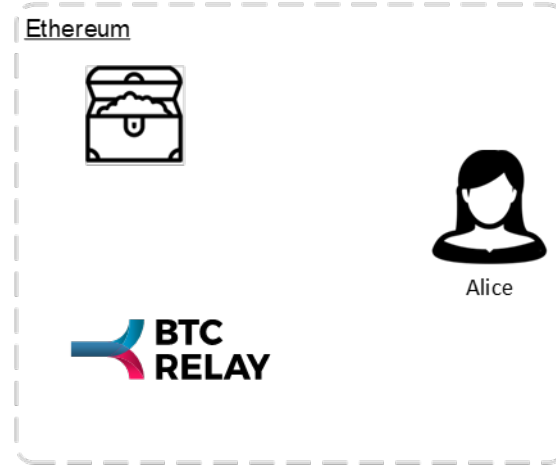
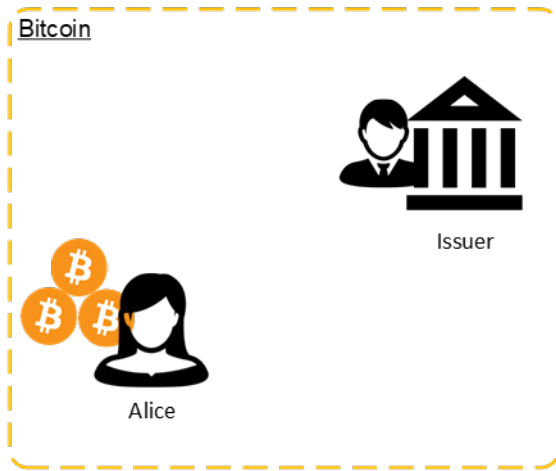
## Achievable advantages:

- + Non-interactive
- + Logic handled by publicly verifiable smart contract
- + No need to monitor backing chains
- + Standardized token interface
- + Wallet in backing chain only needed when redeeming

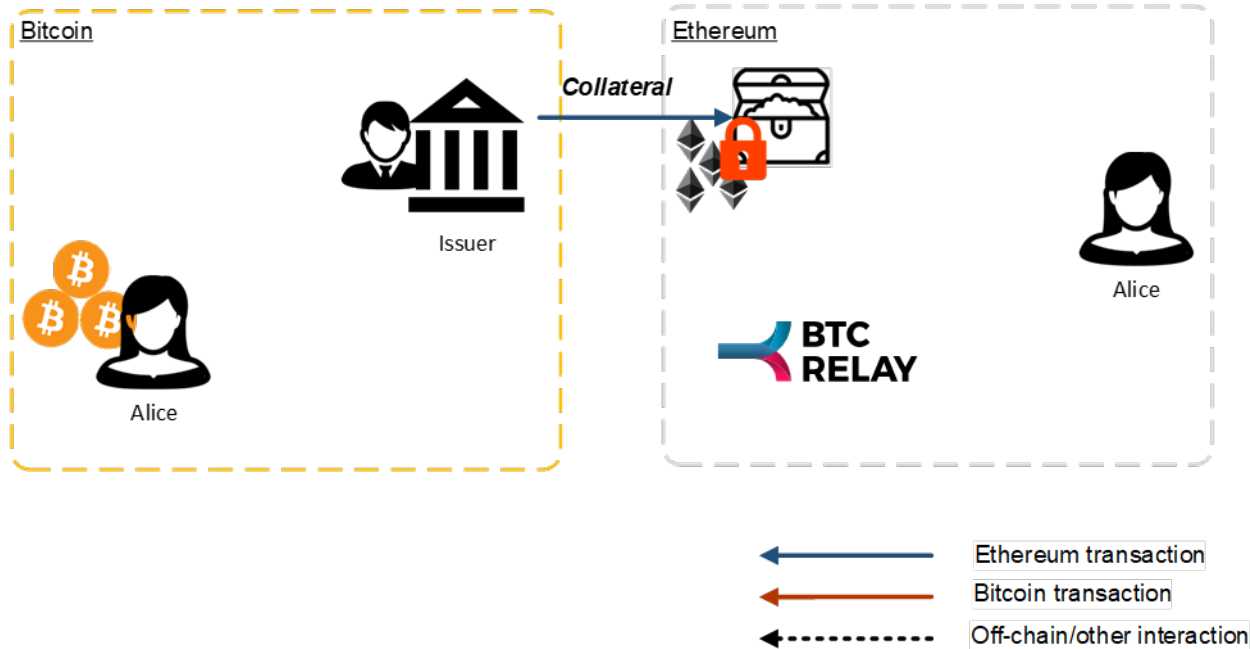
**→ Can be traded on decentralized exchanges**

# Protocols

# Issue



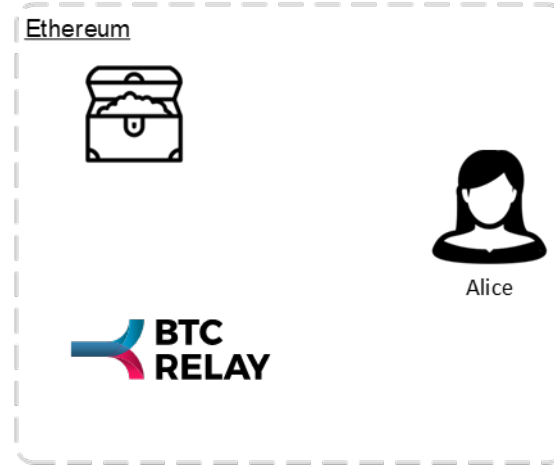
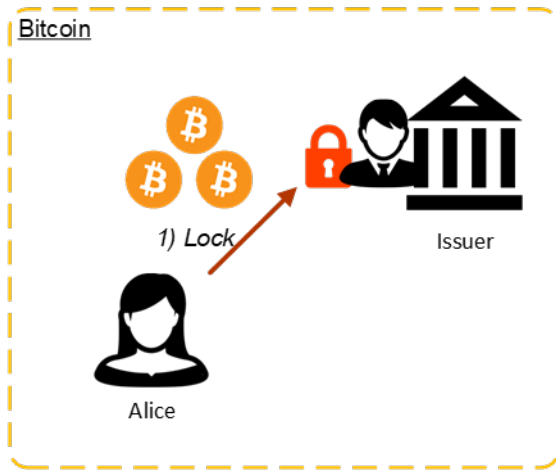
# Issue: Precondition



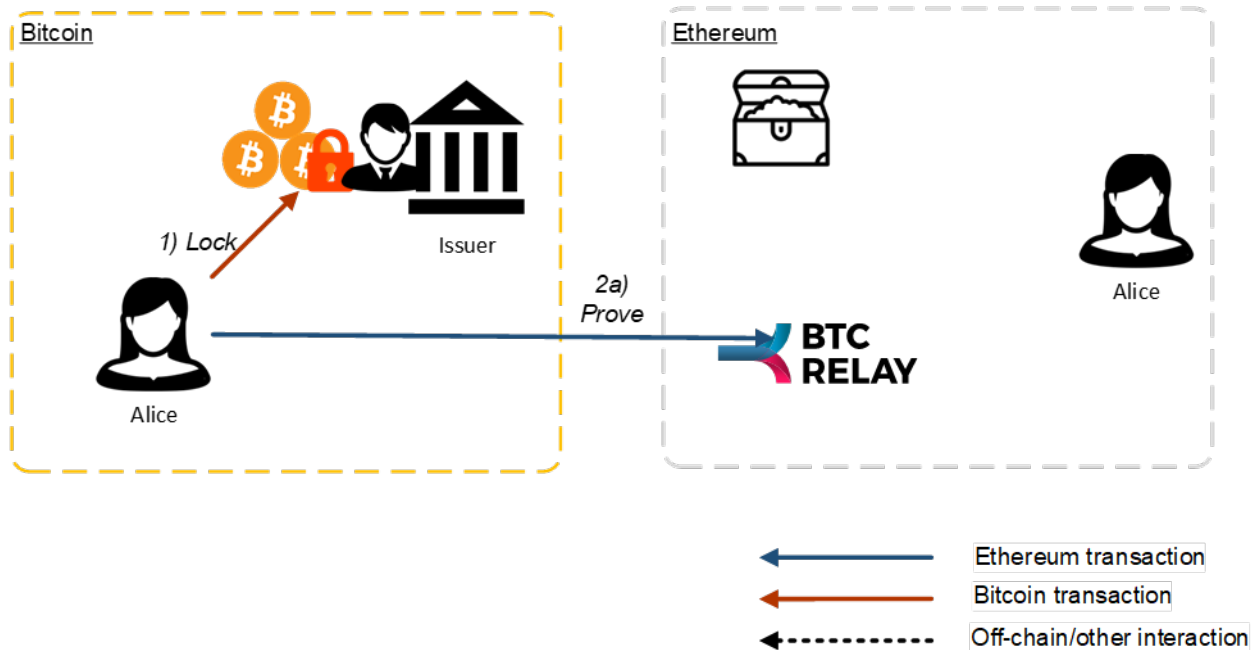
→ Over-collateralization to mitigate exchange rate fluctuations



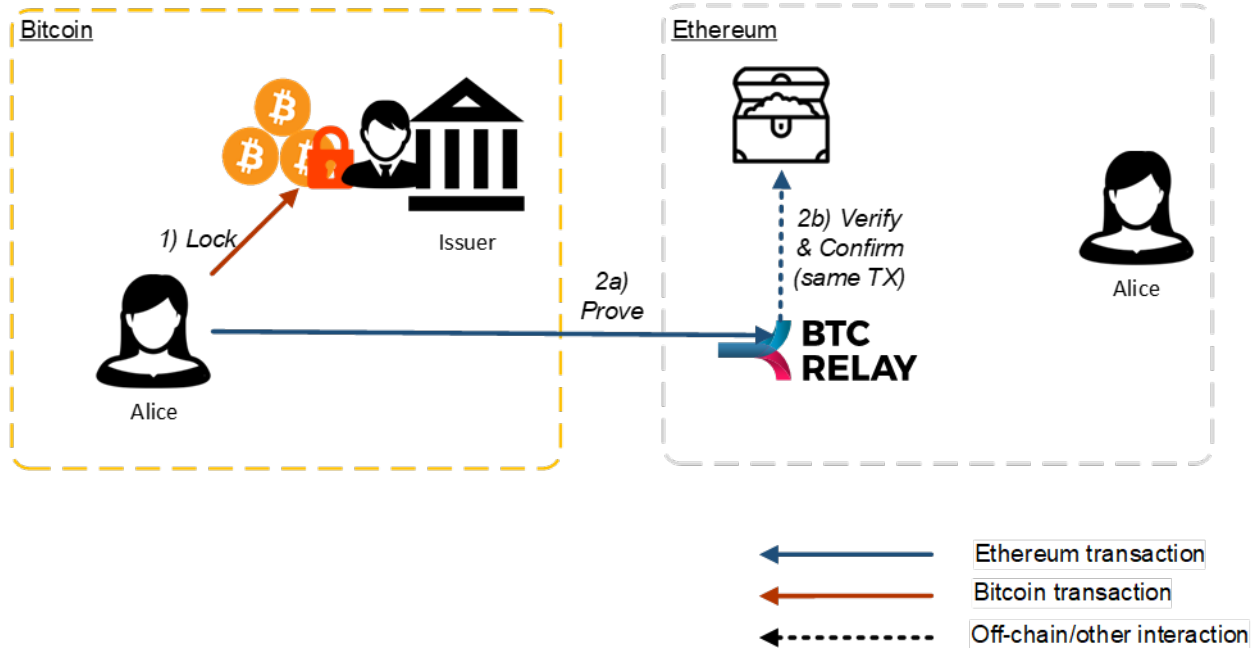
# Issue



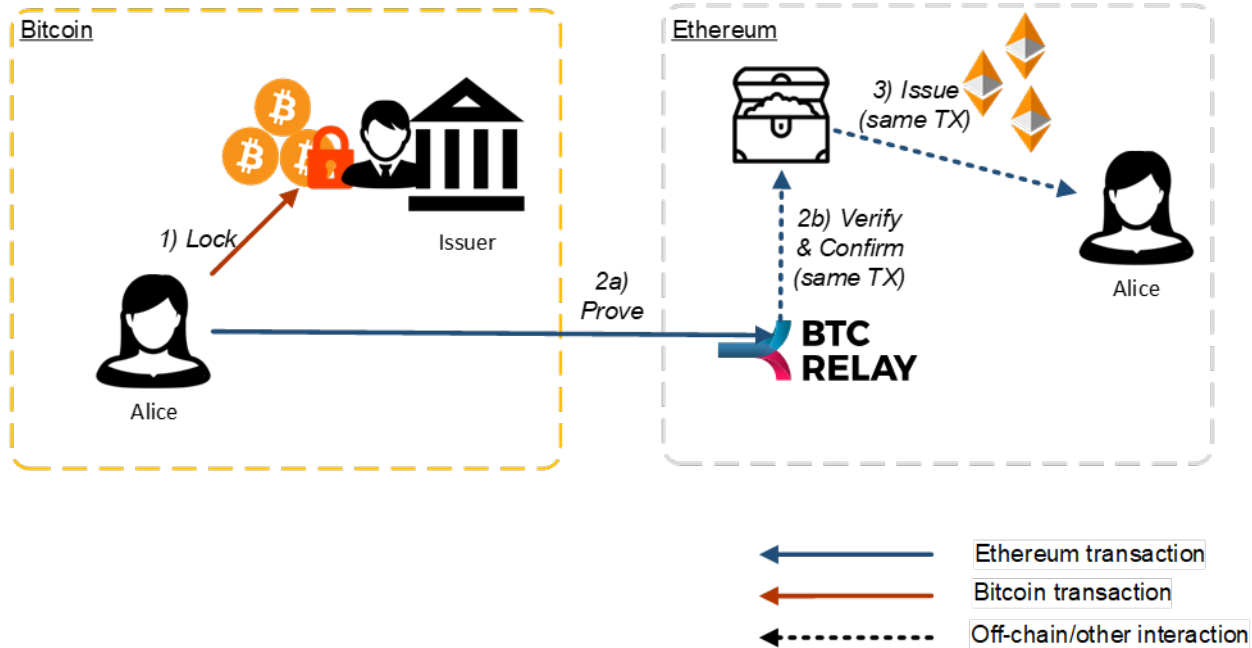
# Issue



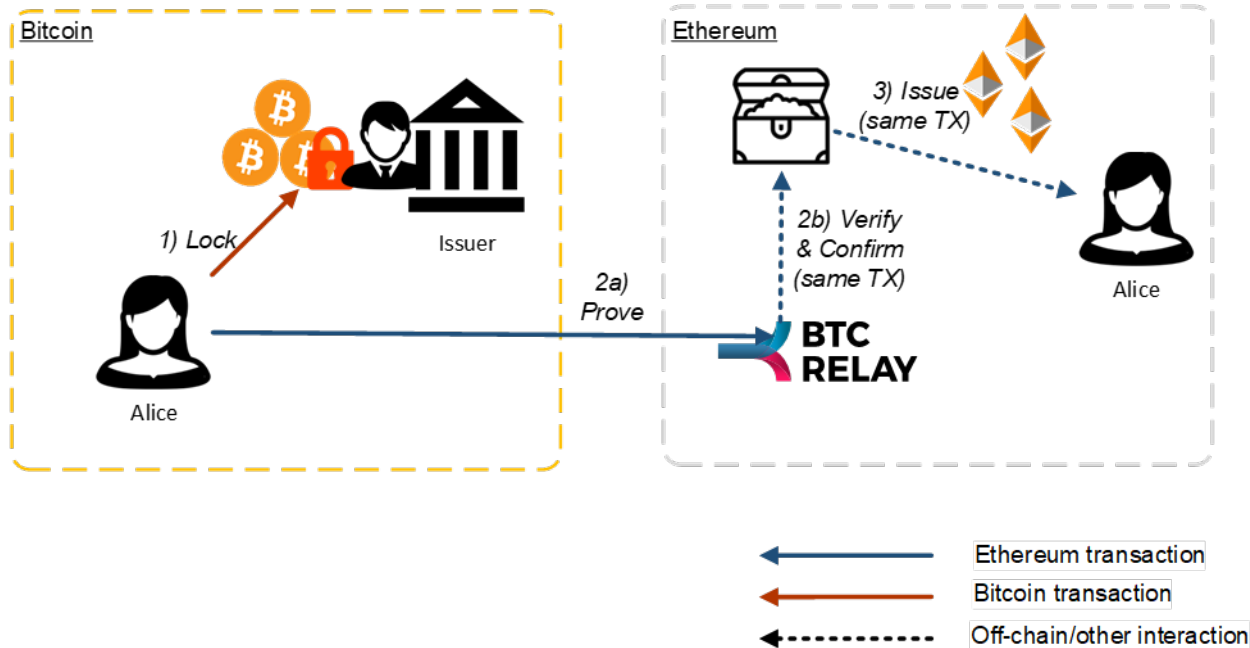
# Issue



# Issue



# 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 Issuer's collateral
  - Loser of the race loses BTC
- Issuer 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:

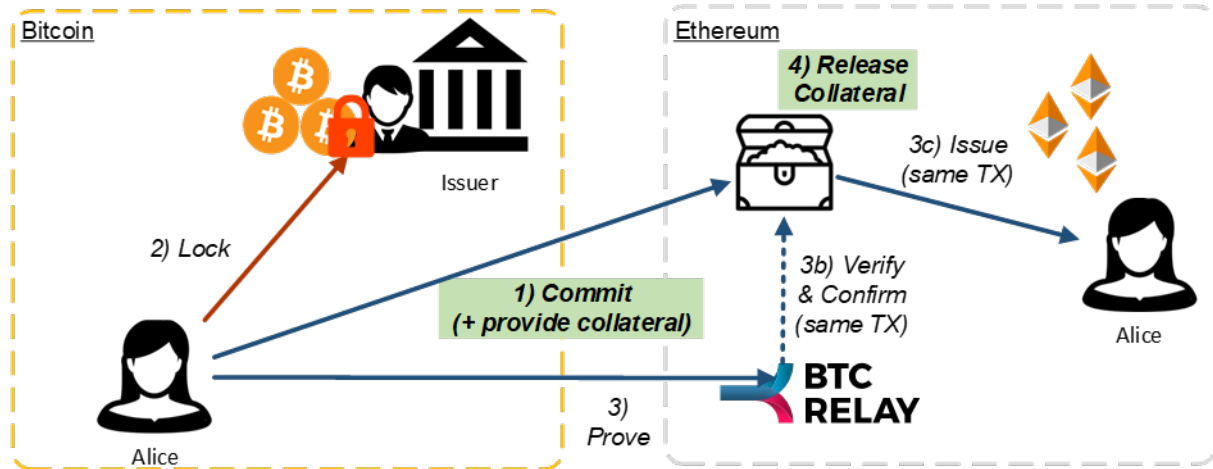
## 1) **Announce**

## 2) **Delay**

- finalize pending requests
- users know race conditions are now possible

## 3) **Withdraw**

# Mitigation 2 – Collateralized Commitments

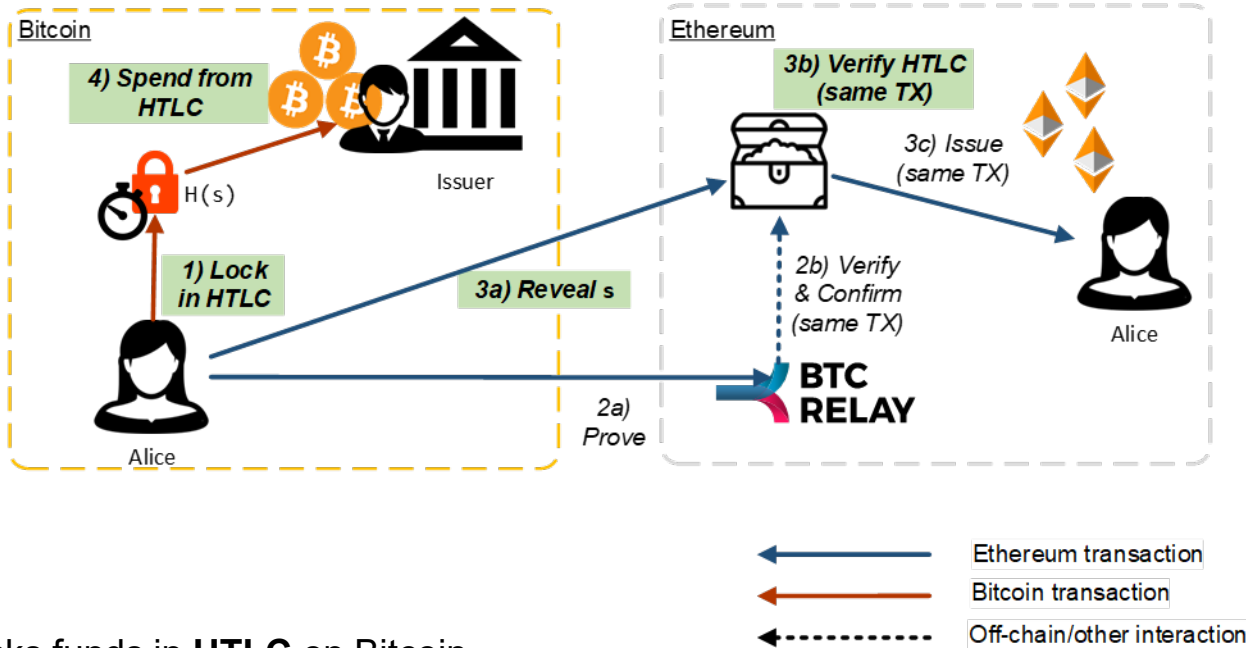


Alice registers **issue commitment** in treasury  
→ Temporarily locks Issuer's *eth* collateral

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



# Mitigation 3 – HTLCs



- 1) Alice locks funds in **HTLC** on Bitcoin
- 2) **Reveals pre-image** via treasury **ONLY IF** Issuer's collateral available
- 3) Issuer withdraws from HTLC

Requirement: treasury must verify HTLC → Give Issuer **enough time** to withdraw

# Trade...

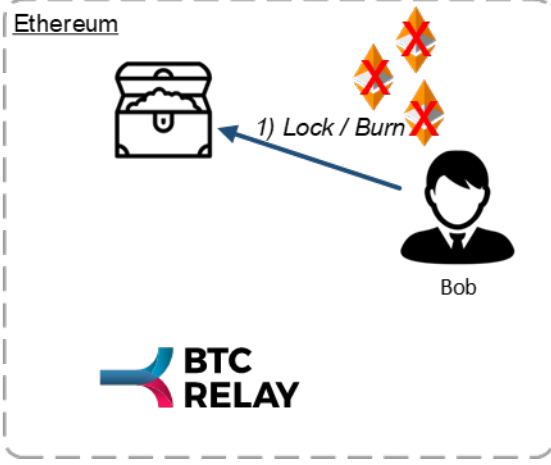
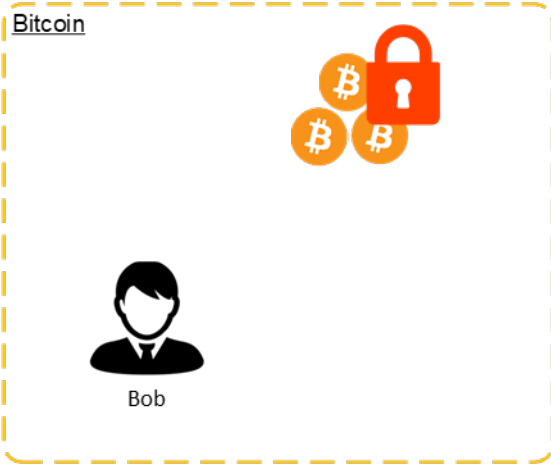
# Trade...

Simple ERC20 transfer!  
Alice → Bob

# Redeem



Issuer

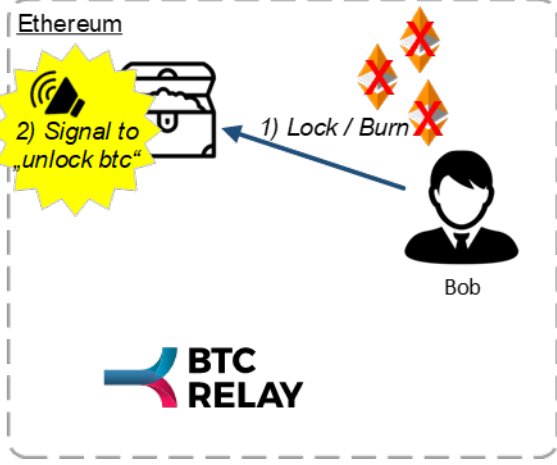
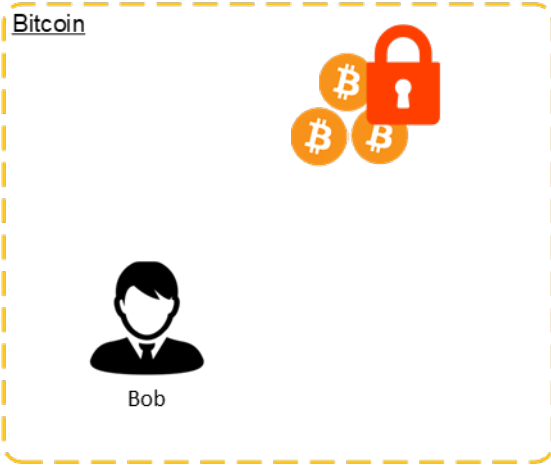


- ← Ethereum transaction
- ← Bitcoin transaction
- ← Off-chain/other interaction

# Redeem

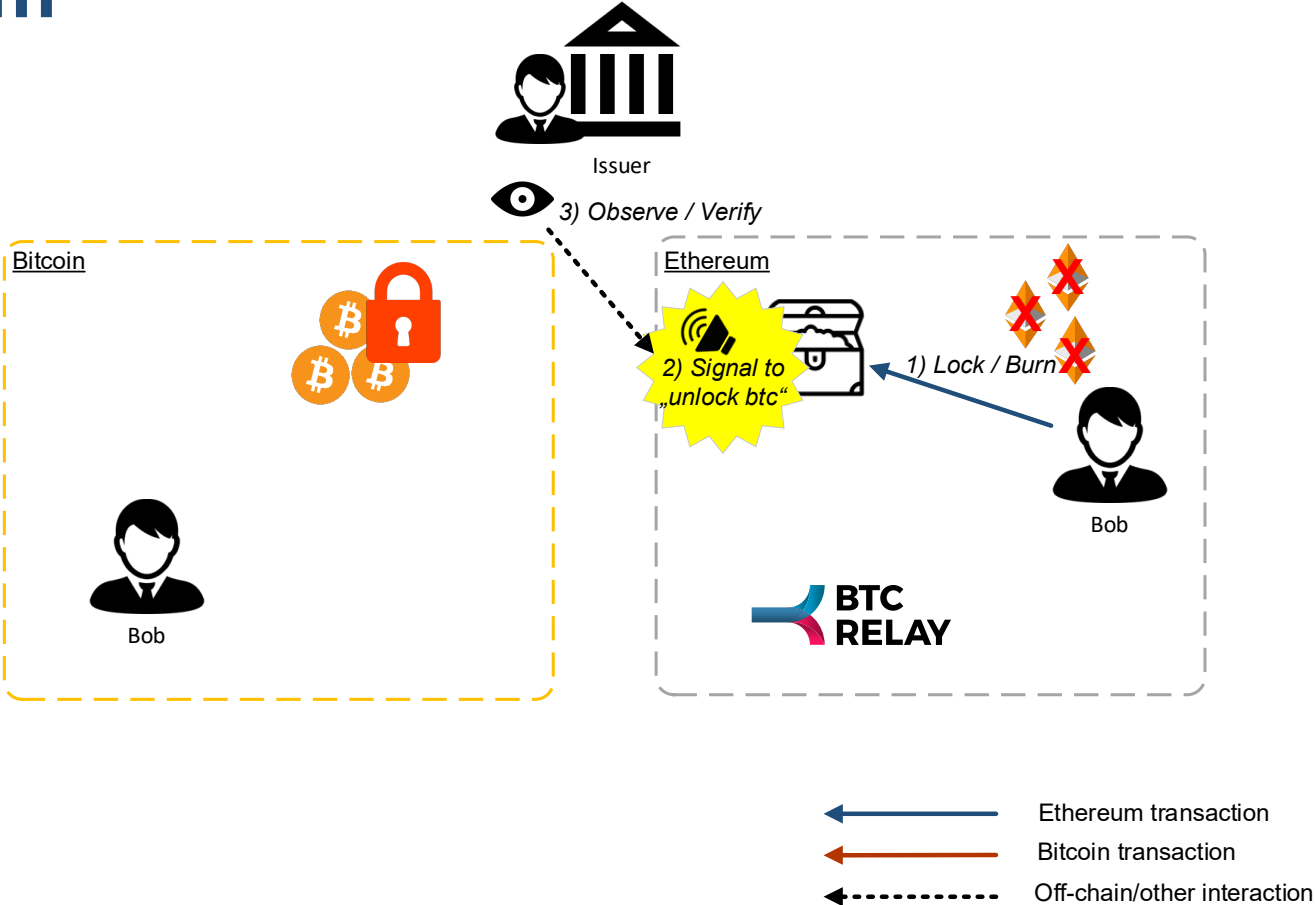


Issuer

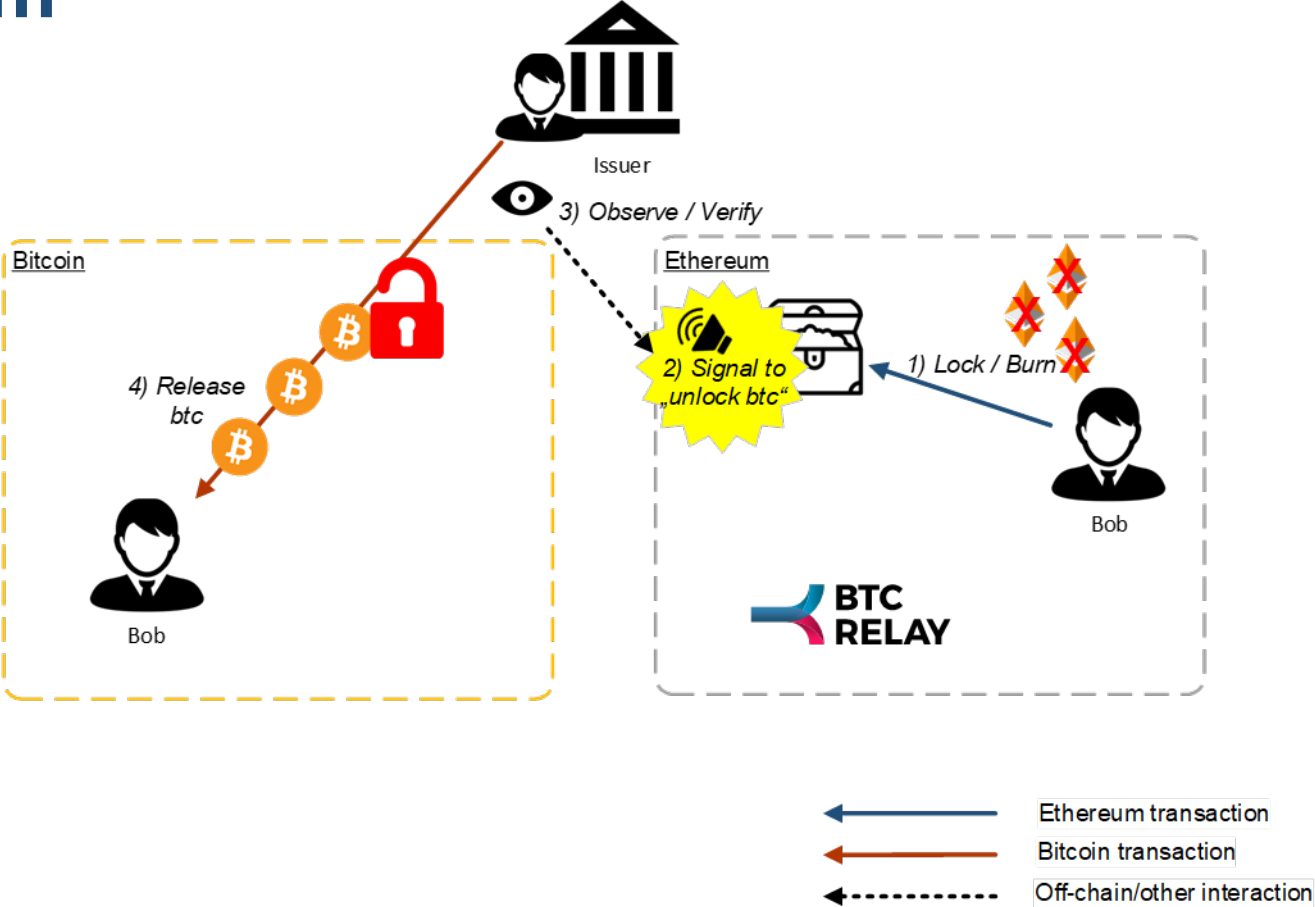


- ← Ethereum transaction
- ← Bitcoin transaction
- ← Off-chain/other interaction

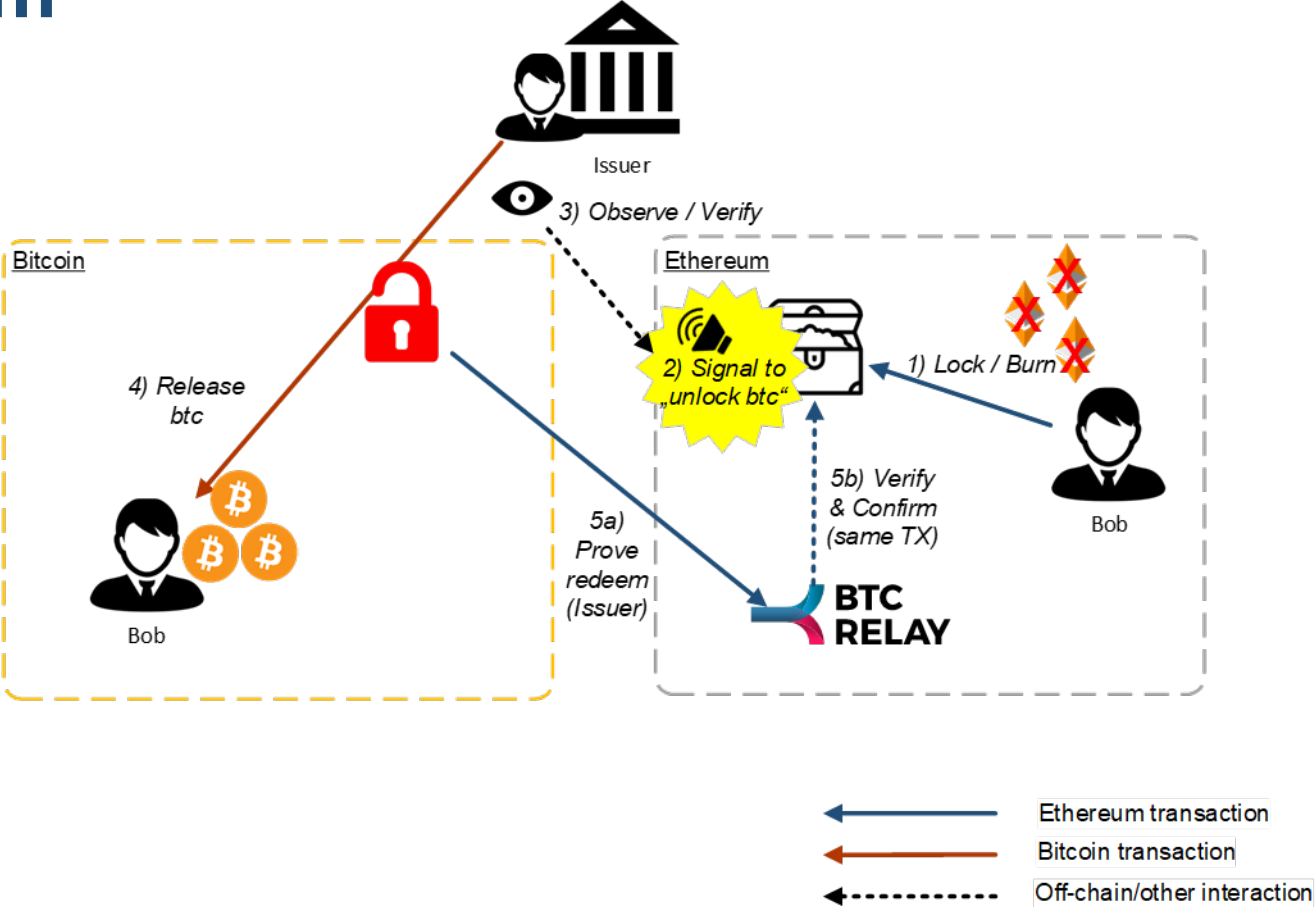
# Redeem



# Redeem

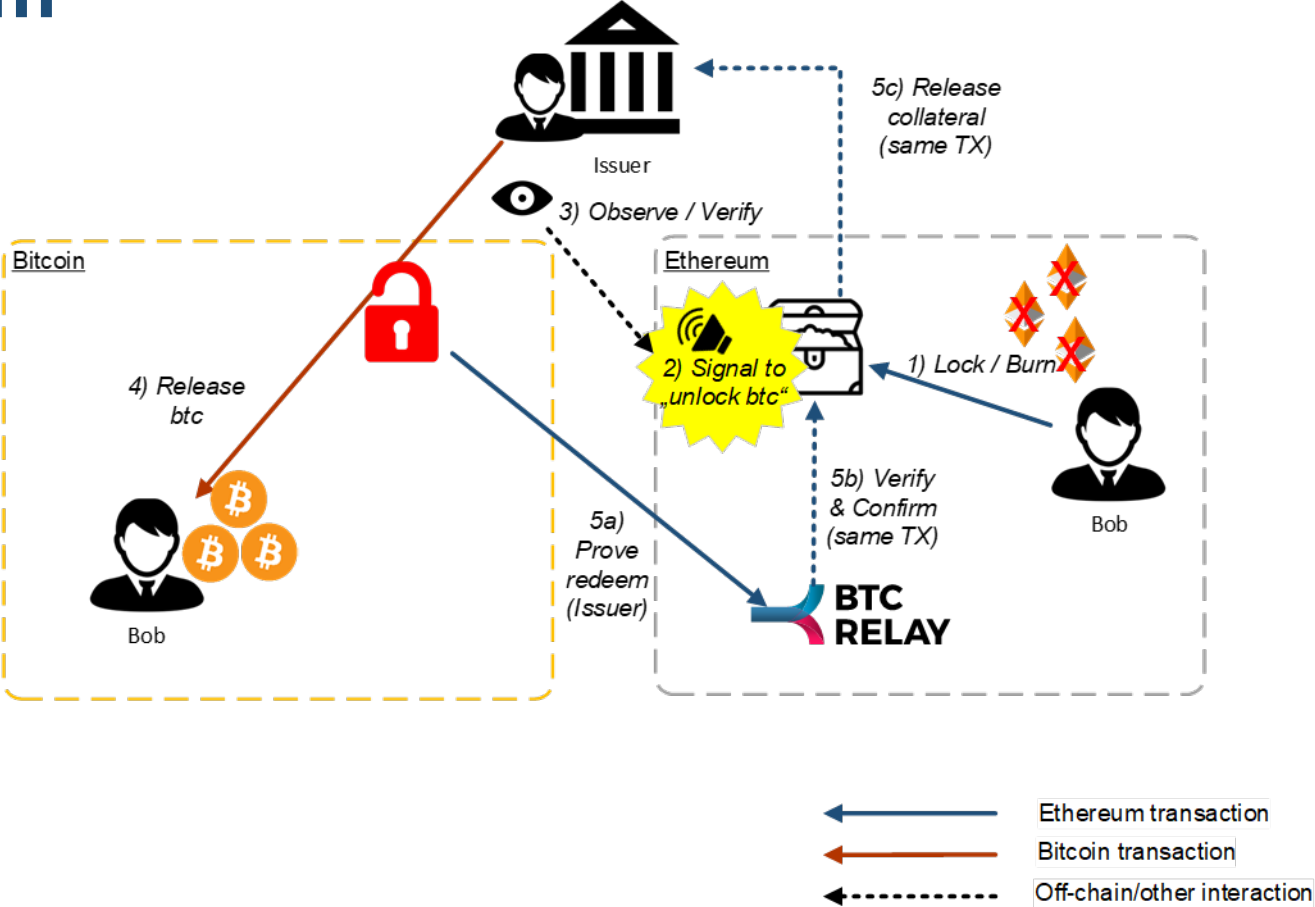


# Redeem

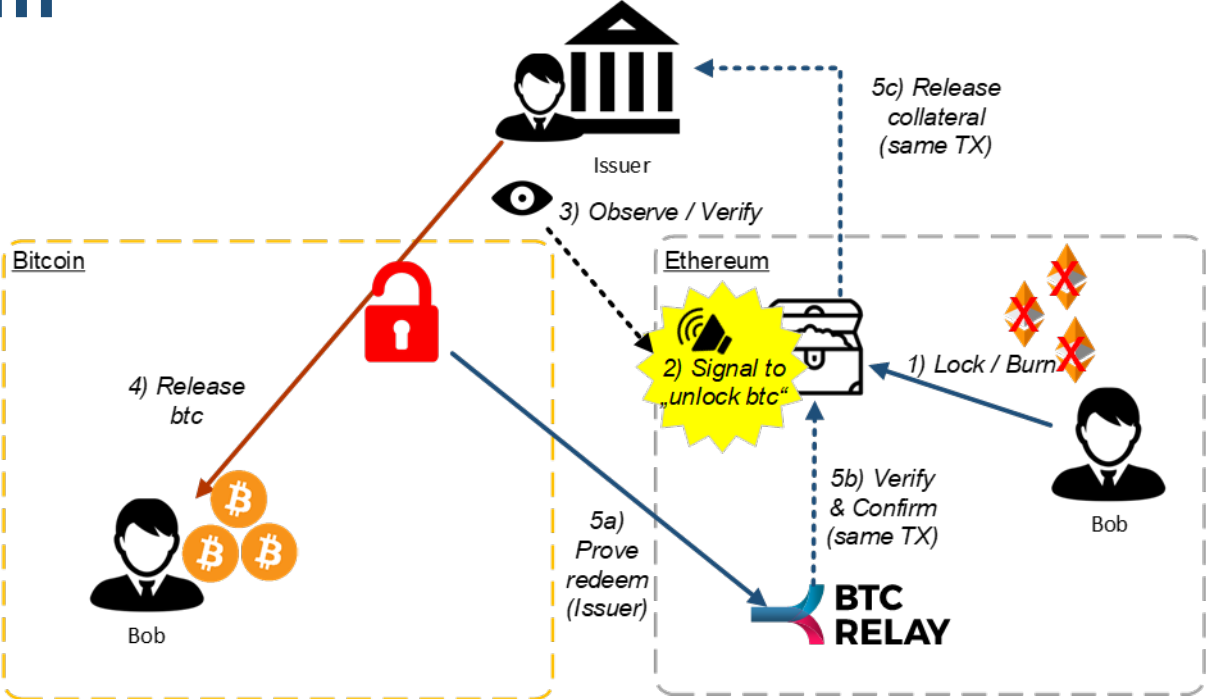




# Redeem

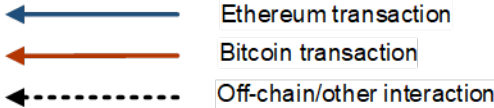


# Redeem



If the Issuer cannot provide proof of correct behavior:

- Collateral slashed
- Bob reimbursed

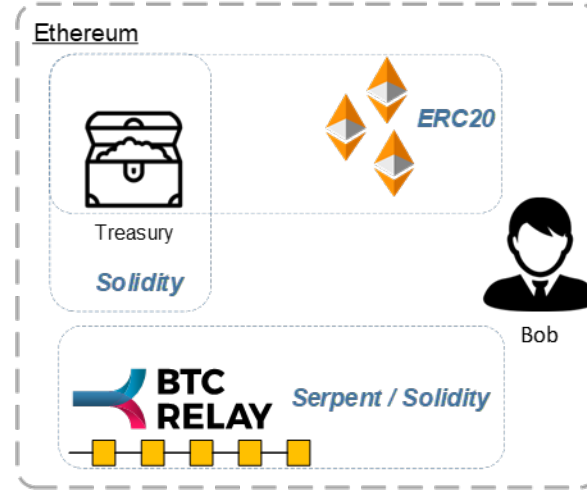
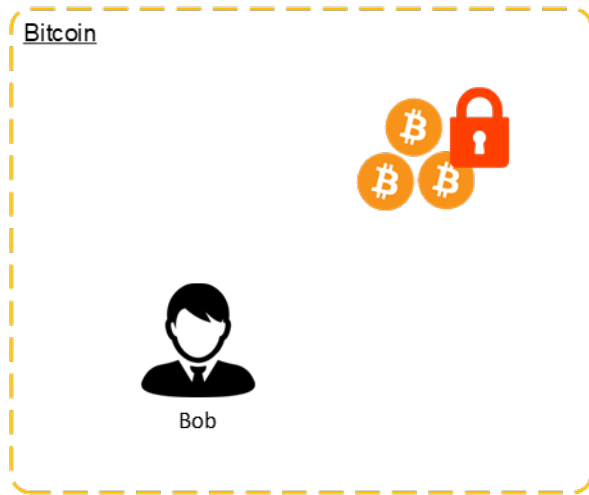


# Implementation

# Trustless via BTC Relay



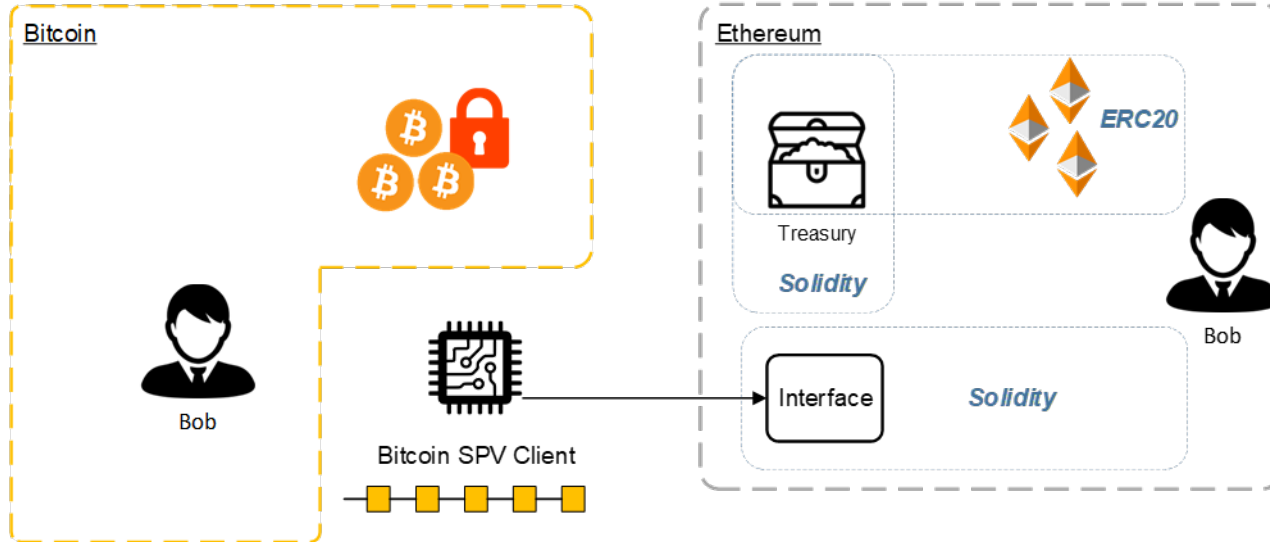
Issuer



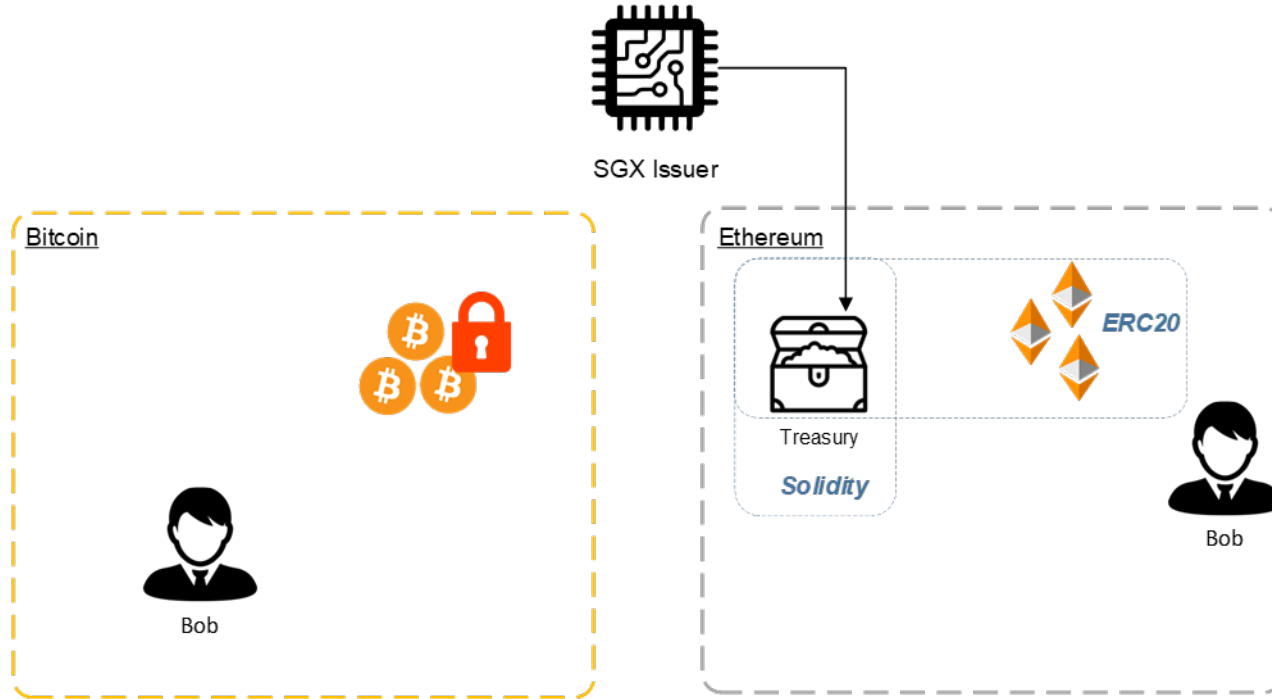
# Optimization 1: SGX Relay



Issuer



# Optimization 2: SGX Issuer








# Performance and Costs

Protocol	# Tx	Cost	SGX relay	SGX Issuer
Issue - HTLC	4	0.63 USD	- 35% (0.41 USD)	- 35% (0.41 USD)
Issue – Collateral	3	0.36 USD	- 33% (0.24 USD)	- 33% (0.24 USD)
Trade	1	0.02 USD	+/- 0% (0.02 USD)	+/- 0% (0.02 USD)
Redeem	3	0.39 USD	- 32% 0.26 USD	- 73% 0.10 USD

BTC Relay cost **per day** ~25 million gas ~27 USD

\* Exchange rate: USD 220 / ETH; Gas cost: 5 gwei

# Security Challenges

Challenge	Mitigation
	Infrastructure DoS
	Eclipse Attacks
	Collateral deterioration
	Chain reorganizations and forking attacks
	User privacy (cross-chain linking)

Multiple issuers and/or chain relays to distribute responsibility

Over-collateralize issuer

Dynamic contestation period based on tx value

Encrypt the public key of redeeming address

Mixing services in treasury contract

Privacy techniques (zk-proof and ring-signatures)



# Challenges and Ongoing Work

## Feasibility of chain relays

- Off-chain verification games: TrueBit, Arbitrage, ...
- Compact proofs: NiPoPoWs, ...

## Issuer committees

- Optimistic improvement of safety and liveness
- Single view for users despite dynamic membership

## Multi-signatures to prevent theft

- Fund freeze still possible  
→ Collateral on backing-chain?
- Higher costs and less usable  
→ payment channels?

## Exchange rate stabilization

- Optimal parametrization of security parameters?
- Interactive re-negotiation of collateral

# Questions?

**Alexei Zamyatin**

@alexeiZamyatin

a.zamyatin@imperial.ac.uk

**Dominik Harz**

@nud3l\_

d.harz@imperial.ac.uk

## Resources

**Paper  
(pre-print):**



**Poster  
on multisigs:**



**Join our Slack:**

