Interoperability with Cryptocurrency-backed Tokens

Alexei Zamyatin  Dominik Harz
Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, William Knottenbelt

Scaling Bitcoin 2018, Tokyo
Motivation

Challenge: Secure, privacy preserving, scalable and decentralized cross-chain communication

Today: Over 2000 heterogeneous cryptocurrencies

Different Properties
- Privacy
- Consensus
- Finality
- Transparency
- Scalability
- Expressiveness
- Security

Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l

Scaling Bitcoin 2018
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

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

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.

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

Bitstamp exchange hacked, $5M worth of bitcoin stolen

Coincheck hack: Bitcoin exchange security under scrutiny after $534M cryptocurrency theft
A History of Theft and Loss

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 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

<table>
<thead>
<tr>
<th>Backing Chain</th>
<th>Issuing Chain (Smart Contracts)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hashed-timelock contracts (optional)</strong></td>
<td><strong>Chain relays</strong></td>
</tr>
<tr>
<td></td>
<td>• Verify PoW of backing chain</td>
</tr>
<tr>
<td></td>
<td>• Verify transaction inclusion</td>
</tr>
<tr>
<td>e.g. <strong>Bitcoin</strong>, Ethereum, Ethereum Classic, Litecoin, …</td>
<td><strong>On-chain assets / meta information</strong></td>
</tr>
<tr>
<td></td>
<td>• Tokens, colored coins, …</td>
</tr>
<tr>
<td></td>
<td><strong>Conditional payments</strong></td>
</tr>
<tr>
<td></td>
<td>• Collateralization</td>
</tr>
<tr>
<td></td>
<td>e.g. <strong>Ethereum</strong>, Ethereum Classic, Zilliqa, Cardano?, …</td>
</tr>
</tbody>
</table>
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
- Wallet in backing chain only needed when redeeming
- No need to monitor backing chains

→ Can be traded on decentralized exchanges
Protocols
Issue

Cryptocurrency-backed Tokens

Bitcoin

Issuer

Alice

Ethereum

Alice

BTC RELAY

Ethereum transaction
Bitcoin transaction
Off-chain/other interaction
Issue: Precondition

→ Over-collateralization to mitigate exchange rate fluctuations

Scaling Bitcoin 2018
Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l_
Issue

Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l

Scaling Bitcoin 2018

1) Lock
Issue

1. Lock
2a) Prove
2b) Verify & Confirm (same TX)

Ethereum transaction
Bitcoin transaction
Off-chain/other interaction
Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l

Scaling Bitcoin 2018

20
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 looses 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 grieving**
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…
Simple ERC20 transfer!
Alice → Bob
Redeem

Issuer

Bitcoin

Ethereum

1) Lock / Burn

Bob

BTC RELAY

Ethereum transaction
Bitcoin transaction
Off-chain/other interaction
Redeem

**Bitcoin**

Issuer

**Ethereum**

1) Lock / Burn

2) Signal to 'unlock btc'

Bob

**BTC RELAY**

Ethereum transaction

Bitcoin transaction

Off-chain/other interaction
Redeem

Issuer

3) Observe / Verify

Ethereum

2) Signal to "unlock btc"

1) Lock / Burn

Bob

Bob

Ethereum transaction
Bitcoin transaction
Off-chain/other interaction

Bitcoin

Ethereum

Scaling Bitcoin 2018

Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l_
Redeem

 cryptographic-backed Tokens - @alexeiZamyatin @nud3l_

Scaling Bitcoin 2018
Redeem Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l

1) Lock / Burn

2) Signal to "unlock btc"

3) Observe / Verify

4) Release btc

5a) Prove redeem (Issuer)

5b) Verify & Confirm (same TX)

5c) Release collateral (same TX)

Issuer

Ethereum

BTC RELAY

Bob

Bob

Bitcoin

Ethereum transaction

Bitcoin transaction

Off-chain/other interaction
If the Issuer cannot provide proof of correct behavior:

- Collateral slashed
- Bob reimbursed
Implementation
Trustless via BTC Relay

Cryptocurrency-backed Tokens - @alexeiZamyatin @nud3l_
Optimization 1: SGX Relay

[Diagram showing the interaction between Bitcoin and Ethereum, with a focus on SGX relay for cryptocurrency-backed tokens.]
Optimization 2: SGX Issuer

Bitcoin

SGX Issuer

Ethereum

Treasury

Solidity

ERC20

Bob
## Performance and Costs

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

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

* Exchange rate: USD 220 / ETH; Gas cost: 5 gwei
## Security Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure DoS</td>
<td>Multiple issuers and/or chain relays to distribute responsibility</td>
</tr>
<tr>
<td>Eclipse Attacks</td>
<td></td>
</tr>
<tr>
<td>Collateral deterioration</td>
<td>Over-collateralize issuer</td>
</tr>
<tr>
<td>Chain reorganizations and forking attacks</td>
<td>Dynamic contestation period based on tx value</td>
</tr>
<tr>
<td>User privacy (cross-chain linking)</td>
<td>Encrypt the public key of redeeming address</td>
</tr>
<tr>
<td></td>
<td>Mixing services in treasury contract</td>
</tr>
<tr>
<td></td>
<td>Privacy techniques (zk-proof and ring-signatures)</td>
</tr>
</tbody>
</table>
Challenges and Ongoing Work

Feasibility of chain relays
- Off-chain verification games: TrueBit, Arbitrage, …
- Compact proofs: NiPoPoWs, …

Multi-signatures to prevent theft
- Fund freeze still possible → Collateral on backing-chain?
- Higher costs and less usable → payment channels?

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

Exchange rate stabilization
- Optimal parametrization of security parameters?
- Interactive re-negotiation of collateral