A brief history of bridging cryptocurrencies

PhD Ciobanu Andrei
@
unibuc

Events

- 2009 Bitcoin genesis
- 2011 Namecoin and altcoins
- 2013 Tier Nolan describing the atomic swap concept on the BitcoinTalk forum
- 2015 Smart contracts era: apparition of the quasi-Turing complete EVM
- 2017 ICO boom and popularization of ERC-20 standard
- 2018 Uniswap AMM
- 2018 ECDSA Threshold Signature Schemes
- 2020 Thorchain TSS Whitepaper
- 2021 Taproot upgrade and Schnorr signatures for Bitcoin

Fair exchange

The problem of exchanging value or data in such a manner that either all involved participants receive what they want or of them neither do.

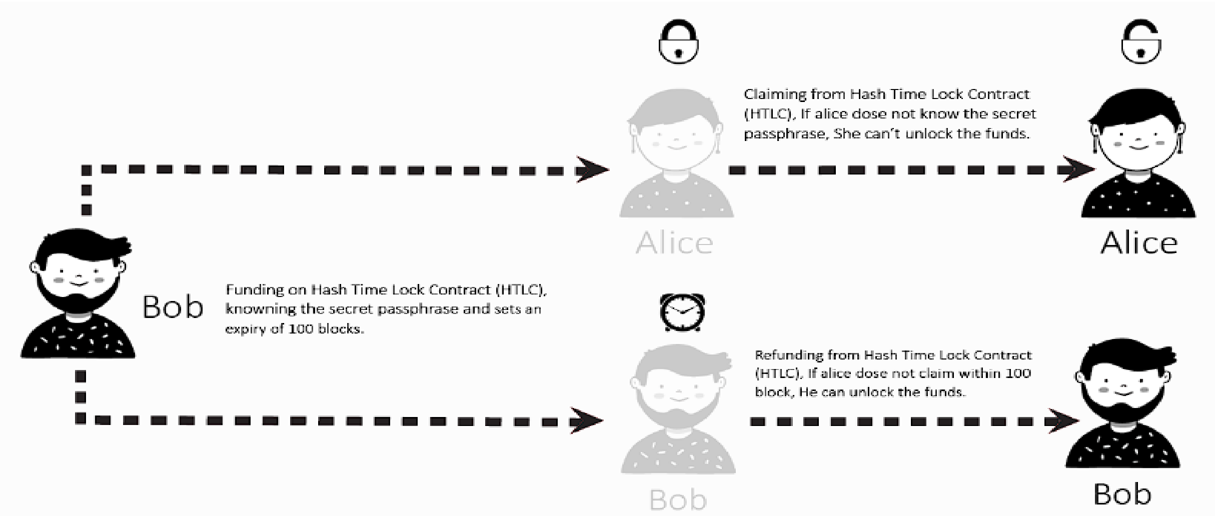
Unfortunately, there is a known result by Henning Pagnia and Felix Gartner which shows that this fundamental problem is impossible to solve without the involvement of a trusted third party (TTP).

The TPP in the case of atomic swaps is represented by each blockchain consensus protocol.

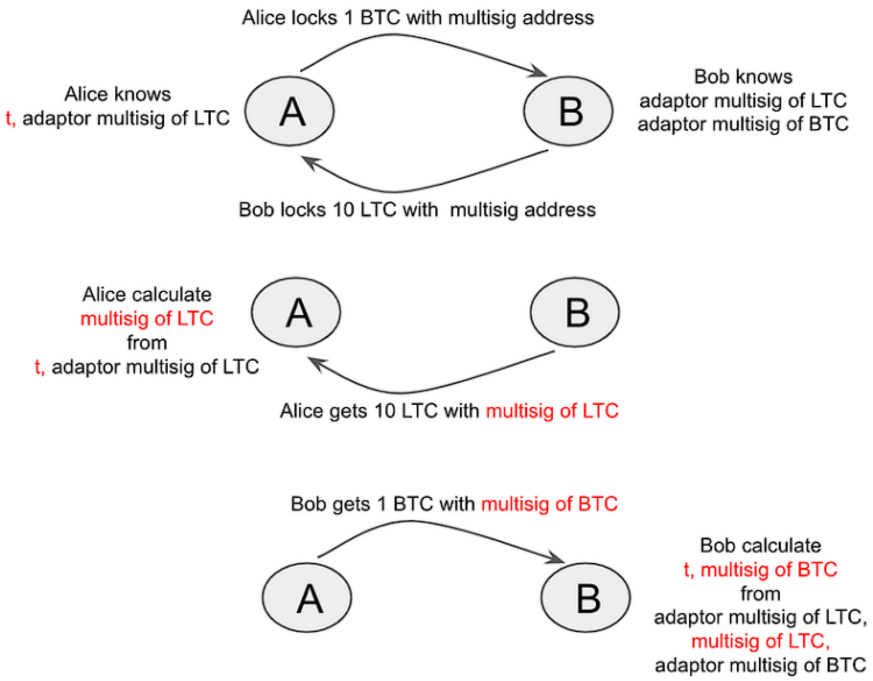
The TPP in the case of bridges is represented by the nodes participating in the signing ceremonies.

Types of Atomic Swaps

- ## Hash Timelock Contract (HTLC)

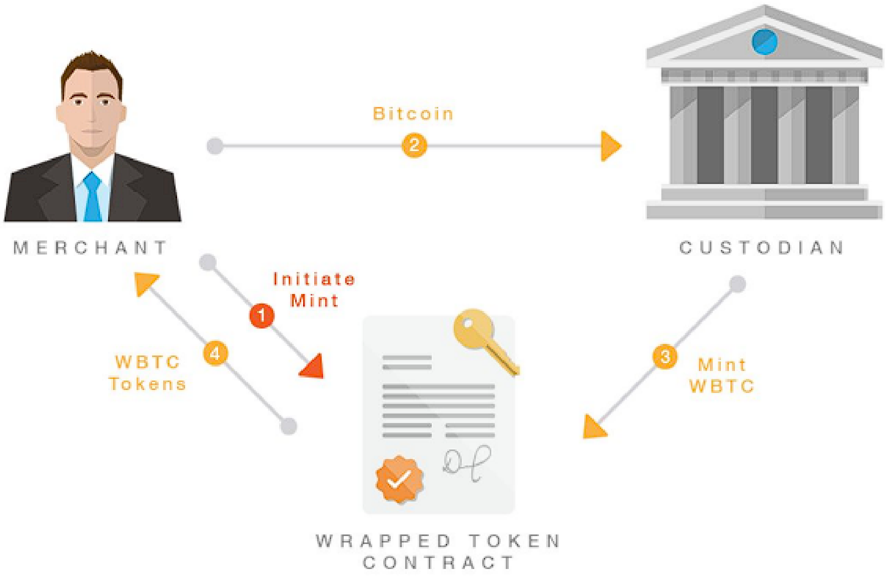

Claiming from Hash Time Lock Contract (HTLC), If alice dose not know the secret passphrase, She can't unlock the funds.
Alice
Alice
Bob
Funding on Hash Time Lock Contract (HTLC), knowning the secret passphrase and sets an expiry of 100 blocks.
Refunding from Hash Time Lock Contract (HTLC), If alice dose not claim within 100 block, He can unlock the funds.
Bob
Bob

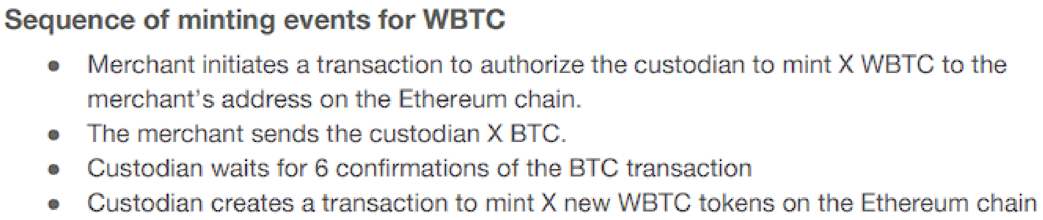
- ## Point Timelock Contract (PTLC)



Early bridge designs

Nov 2018 WBTC by BitGo





Sequence of minting events for WBTC

- Merchant initiates a transaction to authorize the custodian to mint X WBTC to the merchant's address on the Ethereum chain.
- The merchant sends the custodian X BTC.
- Custodian waits for 6 confirmations of the BTC transaction
- Custodian creates a transaction to mint X new WBTC tokens on the Ethereum chain

Decentralized Bridge Architectures

Wormhole relying on multi-sig

- 19 guardians
- 13/19 t schnorr

Avalanche relying on Intel Software Guard Extension (SGX)

- 8 wardens
- 6/8 to submit the same transaction
- shares are distributed using Shamir Secret Share

Thorchain and Multichain relying on TSS

Bridging wrapped assets: problem abstraction

- Two blockchain networks involved
- A network of nodes that observe events
- Key custody based on cryptography or trusted hardware
- Mint/Burn Release/Lock mechanism

Conclusions and future work

- 50% + 1 attack still not solved
- Solutions with high degree of decentralization and security focus will gain more traction in the future e.g Hardware Security Module to store key shards
- Post-quantum threshold schemes
- Multi-chain vs Cross-chain (native assets vs wrapped assets)