Altex DEX

Mobile Decentralized Exchange

Elky Bachtiar
elky@iamdeveloper.io

February 22, 2018

ABSTRACT

Trading cryptocurrencies on centralized exchanges, where funds are stored on centralized servers, exposes users to hackers and regulatory risks. To date, decentralized exchanges are desktop oriented and difficult to use. While mobile usage has worked its way into daily life, blockchain companies mainly focus to advance blockchain users. However, decentralized exchanges focus only on one blockchain, such as Ethereum or NEO. This paper describes the technical side of the Alttex Decentralized Exchange (AltDEX), a brand new decentralized exchange that focus mainly on mobile users. AltDEX uses the latest technology such as **Atomic swaps**, the **Ethereum** blockchain, the open source decentralized platform of **0x Protocol, Dogethereum** technology of Truebit, and **Non-Interactive Proofs of Proof-of-Work (NIPOPOW),** to allow the interchangeability between various blockchain tokens.

---

[1] **Atomic swap** is a proposed feature in cryptocurrencies, that allows for the exchange of one cryptocurrency for another cryptocurrency without the need for a trusted third party.

[2] **Ethereum** is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

[3] **0x protocol** is 0x is a protocol using Etheereum smart contracts for anyone in the world to operate a decentralized exchange.

[4] **Dogethereum** will be a first-of-its-kind "bridge" between the Dogecoin and Ethereum blockchains. Once constructed, shibes will be able to send doge back-and-forth to Ethereum without using an exchange. This will allow shibes to trade dogecoin for other Ethereum-based tokens and use doge in smart contracts

[5] **Non-Interactive Proofs of Proof-of-Work:** the ability to save and check the proof of work of an blockchain and put it to another blockchain

CHAIN RELAY

The first chainrelay, BTCRelay of Ethereum, was developed by Joseph Chow. This is a very promising technology with the ability to connect the Ethereum blockchain with the Bitcoin blockchain. However, it has not gained much traction. This is because the relay is one way, meaning that Ethereum transactions cannot be relayed to Bitcoin. For decentralized exchanges, a two-way relay, like PeaceRelay, is necessary to allow interchain communication between different Ethereum based blockchains. AltDEX technology is inspired by PeaceRelay.

OUR LONG-TERM VISION IS TO SUPPORT TRADING BETWEEN ALL CRYPTOCURRENCIES, FOR EXAMPLE, BETWEEN BTC, BCH, DOGE, ETH, NEO, AND ANY ETH OR NEO TOKENS. ALTDEX WILL COMBINE THE PEACERELAY TECHNOLOGY WITH NIPOPOW, 0X PROTOCOL AND DOGETHEREUM.

ALTTEXRELAY

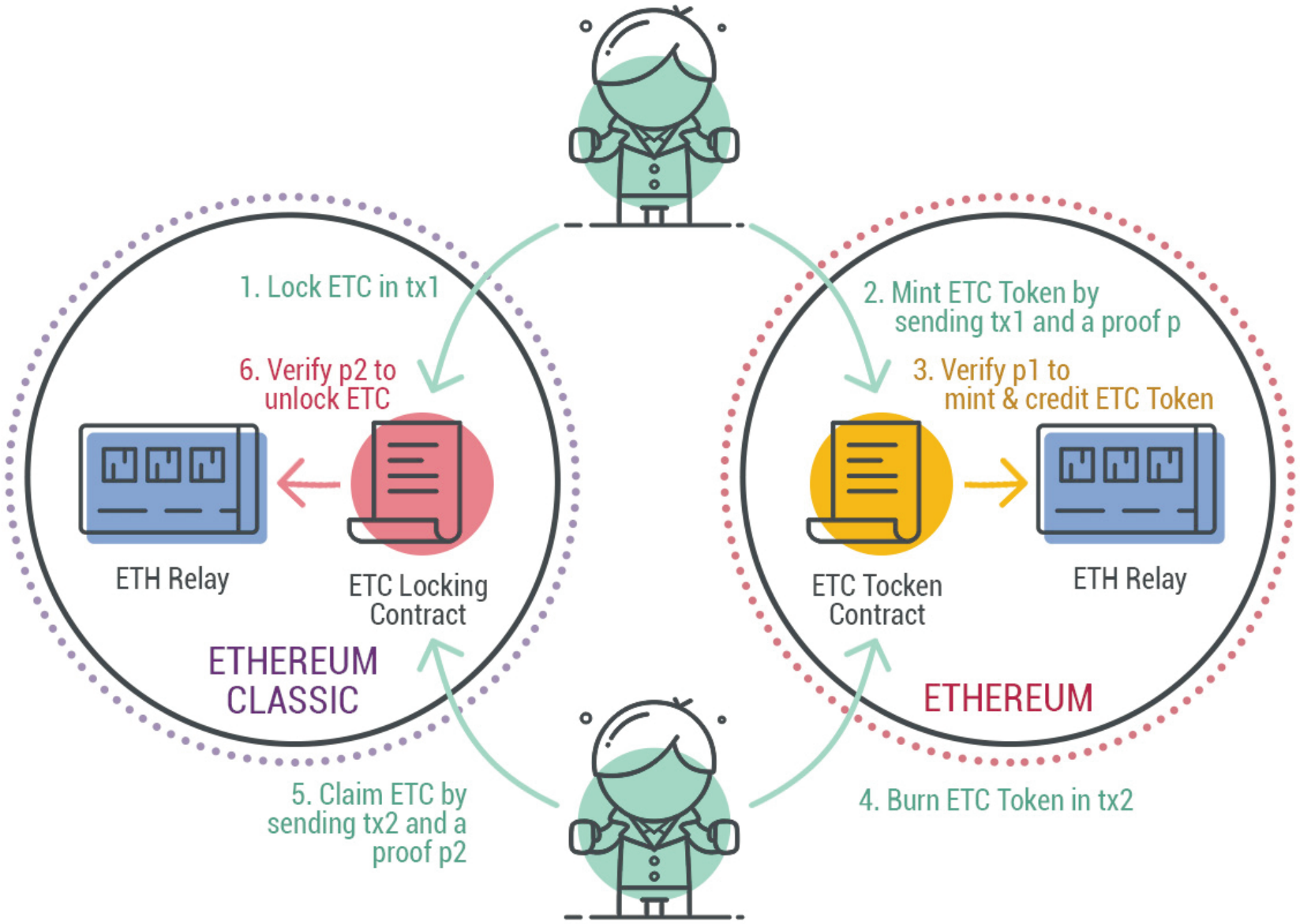
Before explaining the mechanics of AlttexRelay, we need to understand the mechanics of BTCRelay, and PeaceRelay.

BTCRELAY

BTCRelay is the bridge between Bitcoin's blockchain and Ethereum's smart contract. It is essentially a SPV client built on top of Ethereum. Anyone can run a program which fetches BTC block headers and sends it to the appropriate smart contract. The contract verifies the PoW and stores the headers. Other Ethereum contracts can then call the contract to get information about the BTC blockchain. It also has a "relay" function, where transactions and a merkle proof can be provided. The relay then verifies the transaction and sends the information to the selected contract. To verify transactions, a small fee must be paid, which is used to incentivize the relayers.

PEACERELAY

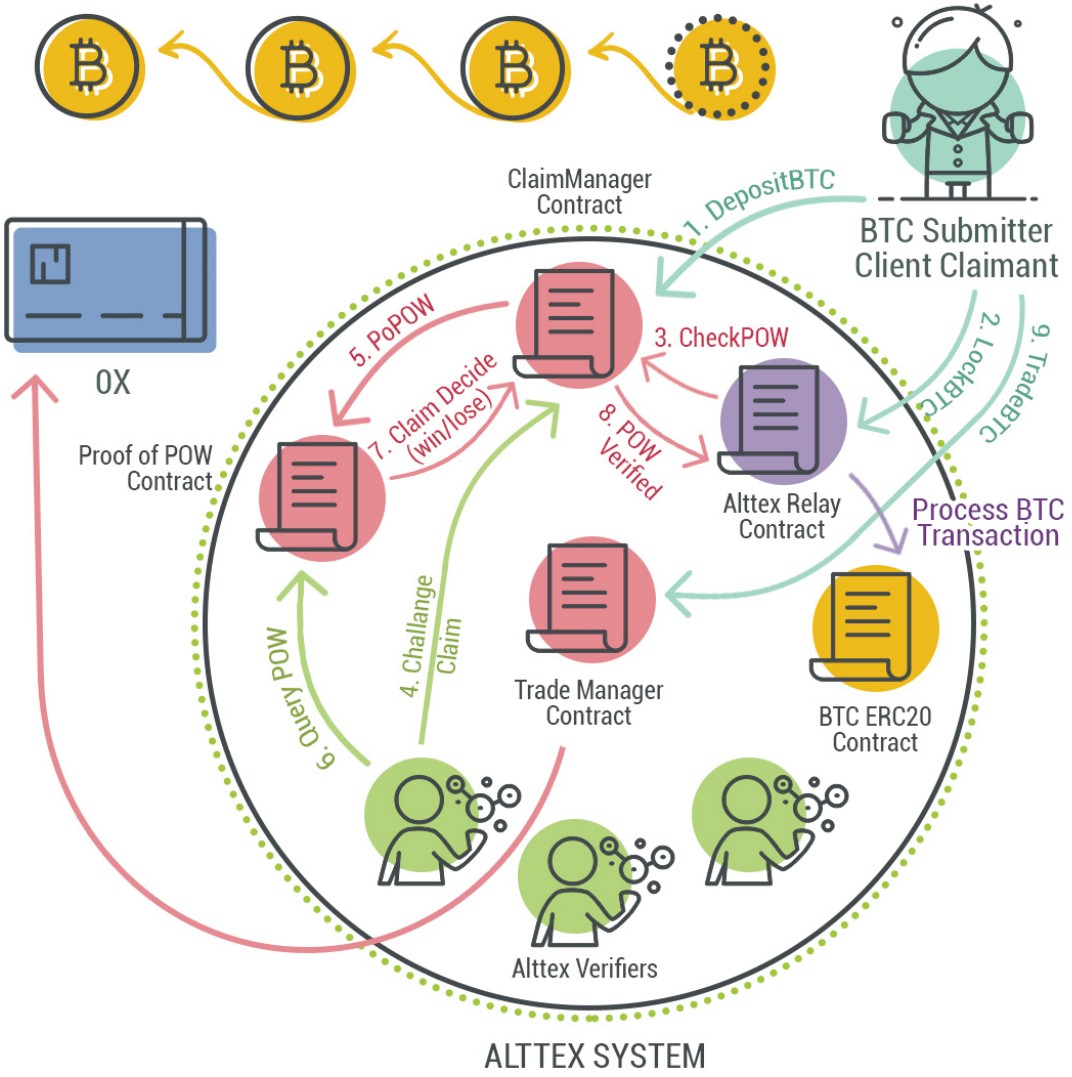
Peacerelay is the interchain communication between different Ethereum based blockchains that allows for the transfer of ETC to and from the Ethereum blockchain. PeaceRelay is a two-way peg. One can lock their ETC in a locking contract running on Ethereum Classic, and use this locking transaction to create new ETC tokens in a ETCToken contract running on Ethereum. To claim the ETC tokens on the Ethereum Classic network from the ETC tokens on the Ethereum network, one needs to burn their ETC tokens using the ETCToken contract. The transaction that burns ETC tokens is used to claim the owner's ETC from the ETC locking contract running on Ethereum Classic. The explanation of the lock/claim mechanism is illustrated below:



By using PeaceRelay, a trustless move of ETC to and from the Ethereum blockchain is possible. There is a three-step minting process: locking ETC in an ETC contract; minting an ETC token by sending the locking transaction and its proof to the token contract running on Ethereum; and verifying, via the token contract, that the locking transaction with ETC Relay occurred, before minting the corresponding amount of ETC tokens. The claim process for withdrawing ETC from its corresponding ETC token occurs in a similar manner.

ALTTEX RELAY

Alttex relay is two-way peg interchain communication between the Ethereum blockchain and any other blockchain (e.g., Bitcoin, dogecoin). With Alttex relay, a Bitcoin submitter can claim a BTC token in the Ethereum blockchain by depositing Bitcoin to the ClaimManager contract. In this case, the BTC of the claimant will be locked by the Alttex relay contract, and a new BTC token will be created on the Ethereum blockchain. After the creation of the BTC token, the BTC proof of work of the BTC block will be check by the NIPOPOW contract. With this contract, a copy of the entire blockchain is not required as only the Proof of Proof of Work is enough to check the integrity of the Bitcoin block. This method is superior to BTCRelay and PeacRelay because the blocks do not need to be saved. Afterwards, the BTC token is tradeable via the TradeManager contract with the 0x protocol API.



REFERENCES

[1] Atomic Swap. https://en.wikipedia.org/wiki/Atomic_swap, 2018

[2] Ethereum Blockchain. https://www.ethereum.org/, 2015

[3] 0x protocol. https://0xproject.com/pdfs/0x_white_paper.pdf, 2017

[4] Dogethereum.
https://www.reddit.com/r/dogecoin/comments/61vg5k/dogethereum_we_can_do_this_dogether/, 2017

[5] Non-Interactive Proofs of Proof-of-Work, https://eprint.iacr.org/2017/963.pdf, 2017

[6] Chain relay,
https://medium.com/@loiluu/peacerelay-connecting-the-many-ethereum-blockchains-22605c300ad3, 2017