Allbit

2018. 8. 10.

ozys
koon

Cryptocurreny exchange

CEX vs DEX

Centralized exchange

- traders money is under CEX controlled
- trades in CEX databases

Decentralized exchange

- Assets is under owners controlled , anyone have permission to controll asset
- Each trade asset trade wallet to wallet on blockchain

Decentralized exchange

Asset Escrow exchange

Onchain P2P matching smart contract

Offchain P2P matching smart contract

Exchange FIAT asset on blockchain

Instant Exchange based on reserver

Limitation of DEX

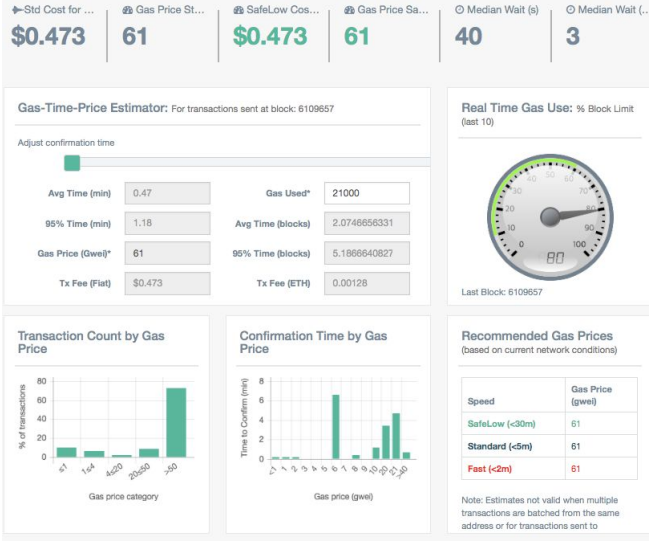
Ethereum unstable gas

- 5862 ether on transaction fee in one day (because of FCoin)

Long waiting time for transaction

Frequent regorg

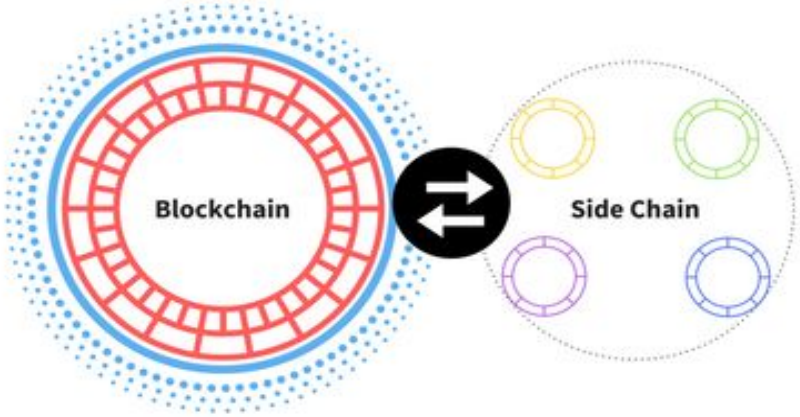
Block Height	UncleNumber	Age	Miner	Reward
6108173	6108170	53 secs ago	miningpoolhub_1	1.875 Ether
6108169	6108168	1 min ago	Ethpool_2	2.625 Ether
6108168	6108167	2 mins ago	Nanopool	2.625 Ether



Side Chain

Sidechains

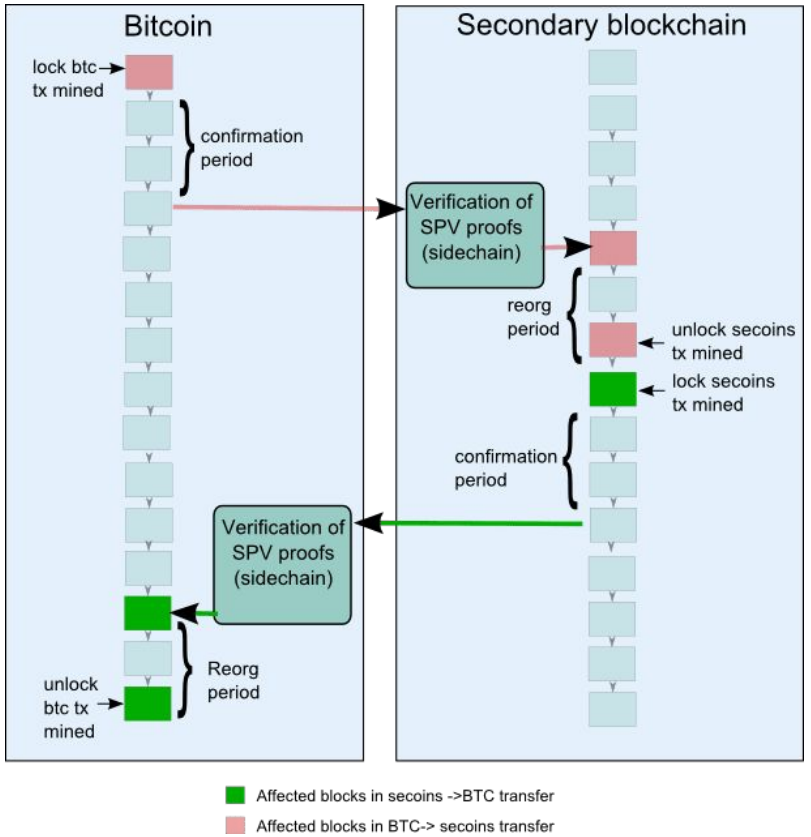
- Scalable solution for main chain / pegging main chain asset to sidechain
- 2-way pegged / lightning network



2-way pegged

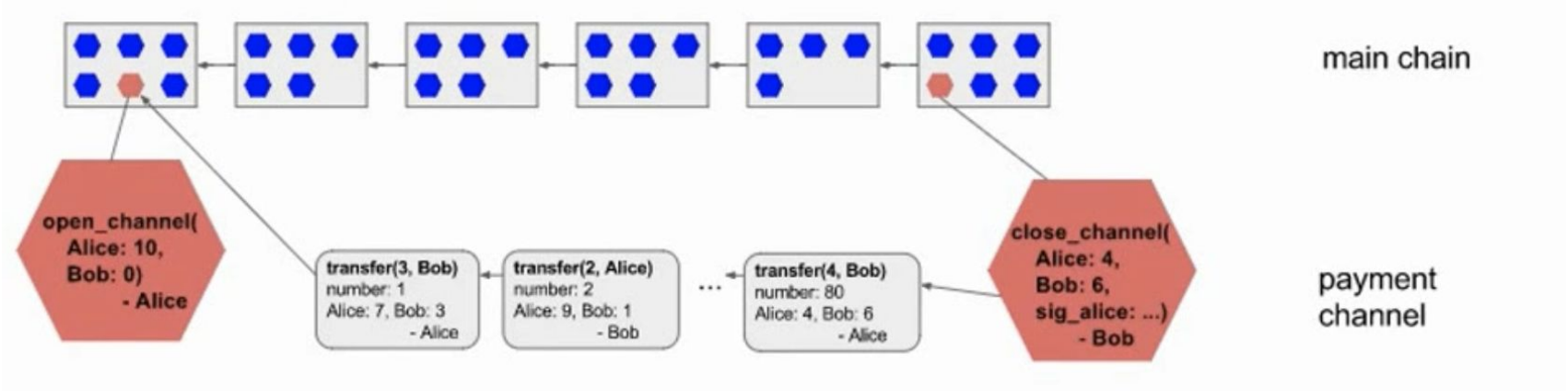
SPV proof / atomic swap

- based of bitcoin , 2-way pegged



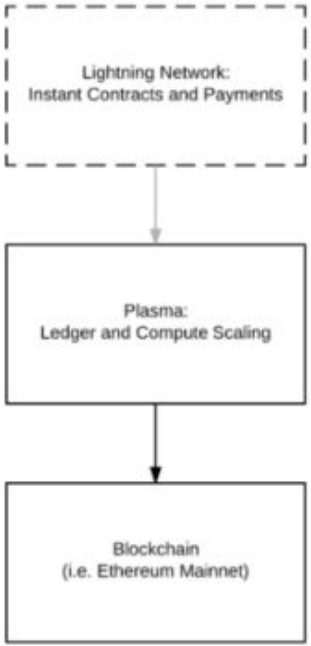
Lightning network

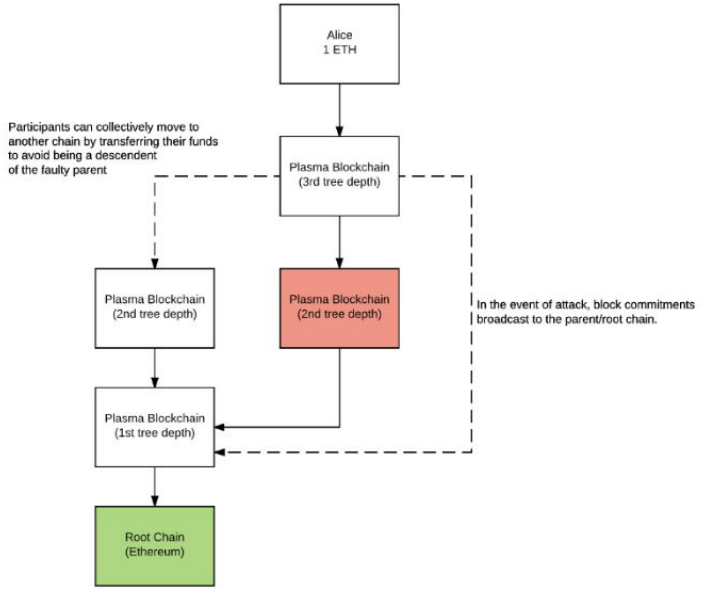
payment channel in bitcoin



Plasma

Plasma: Scalability solution by Joseph poon, Vitalik Buterin, 2017





Allbit Decentralized exchange

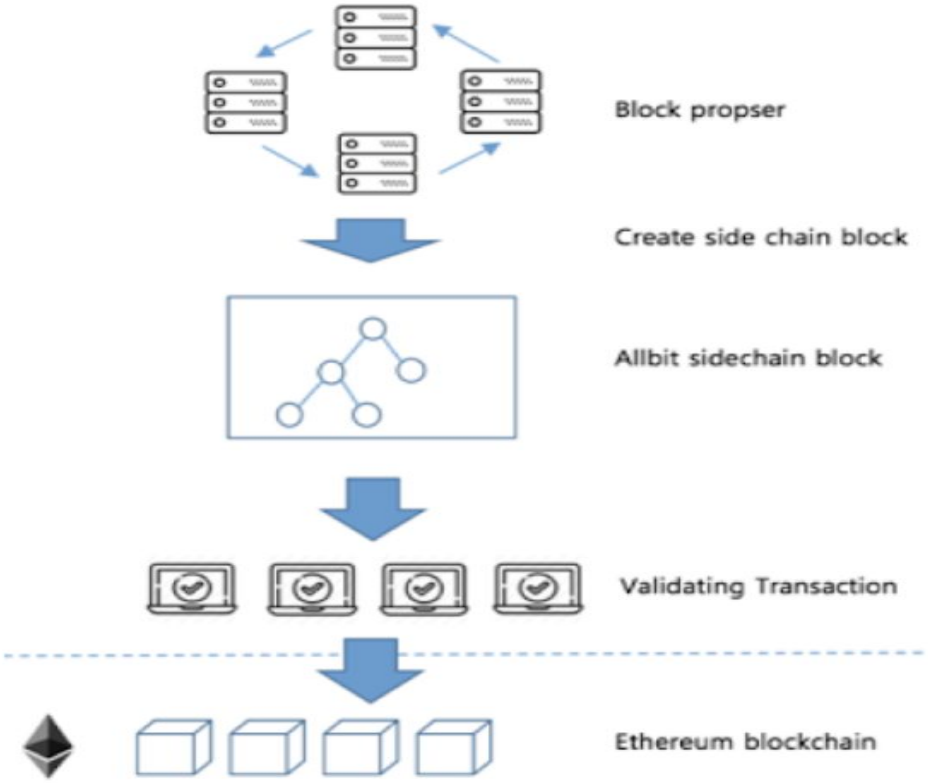
Consensus

- PoA ethereum sidechain
- Based on AuthorityRound with no reorg
- Zero transaction fee

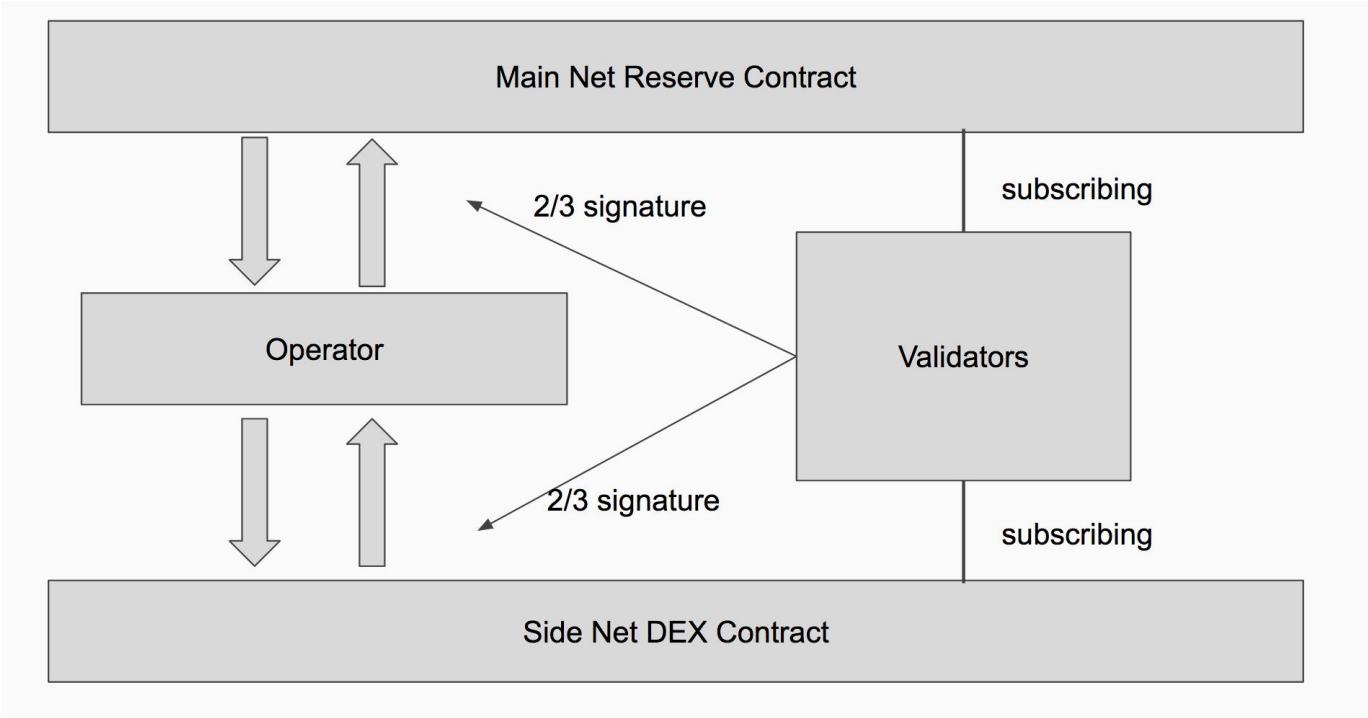
Performance

- 4 block time / 500 tps (1 block time 1000tps 2018 Q4)

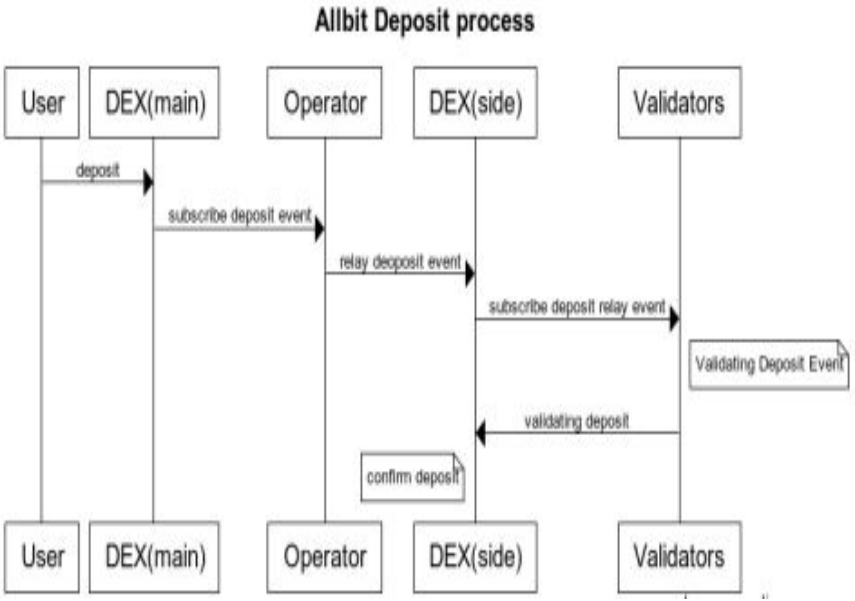
PoA Shared validation

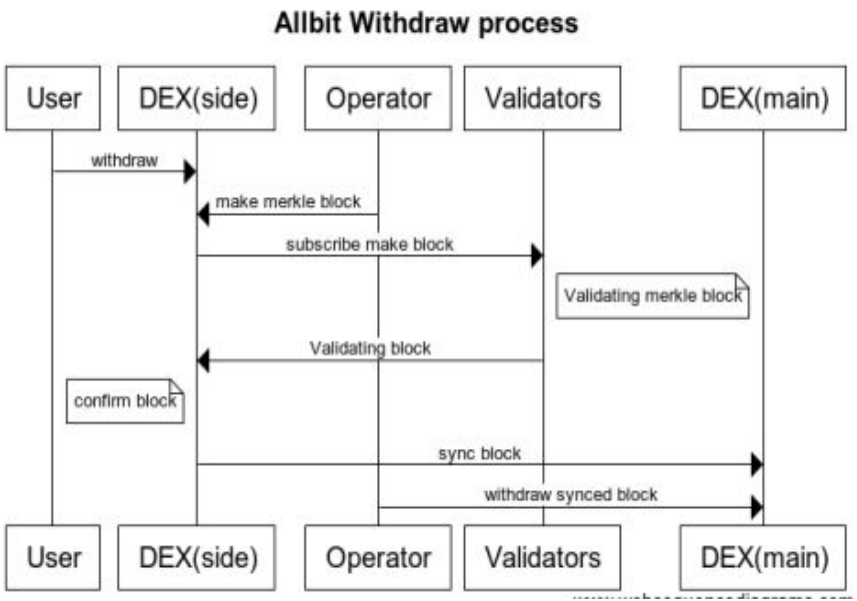


PoA Shared validation



PoA Shared validation





PoA Shared validation

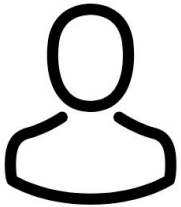
Operator

- operated by allbit

Validator / Block proposer

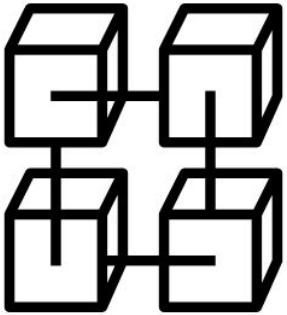
- Related to performance : start at 6 , increase 30% per year, max validator 100
- Reward DEX transaction fee
- Instant penalty
  - Fault signing , Violating protocol rule
  - lose their reserve
- Partial penalty
  - Timeout penalty
  - Absent penalty

All process in on-chain



User

requestOrder(coin, amount, is_sell)
cancel(orderId)



Allbit chain

- Balance check
- lock balance
- maintain orderlist
- matching order
- trade and exchange

….

Road map

2018 Q4

- BTC and other currency market support
- Improve chain performance (1sec block time , 1000 tps)

2019 Q1

- Support and linked with micro payment services providers

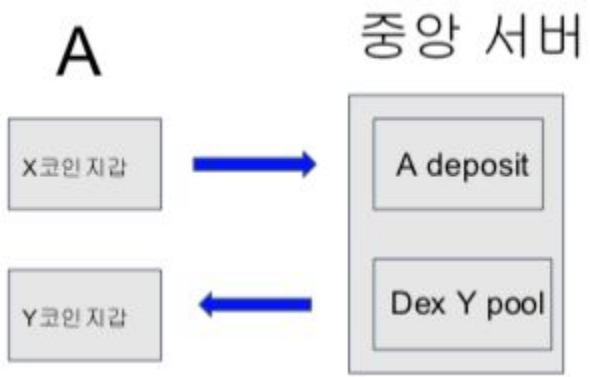
2019 Q2

- Open chain to public or dex service providers can join
- Shared liquidity

Appendix

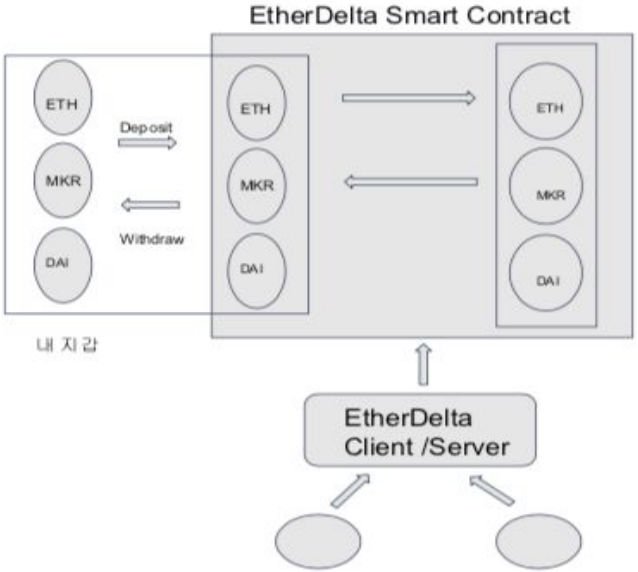
중앙 분산 거래소

- 가상 계좌 발급을 통한 자산 에스크로 형태의 분산 교환소
  - 장점
    - 손쉬운 거래 프로세스 / 빠른 교환 속도 / 모든 토큰 거래 가능
  - 단점
    - 거래 비율을 중앙 서버가 직접 판단 / 시세에 대한 불신 / 에스크로에 따른 자산 위험성



스마트 컨트랙트 기반 분산 거래소

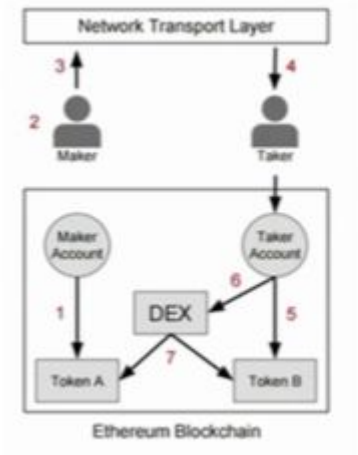
- Etherdelta 초기 모델
- ERC20 Token 들은 ERC20을 따르기에 동일한 규격 가지고 있음
- 스마트 컨트랙트를 통해 토큰들을 교환

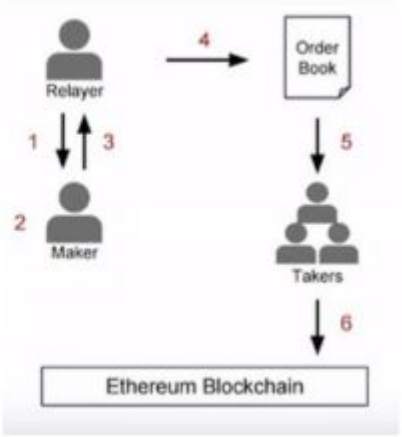


오프 체인 방식의 분산 거래소

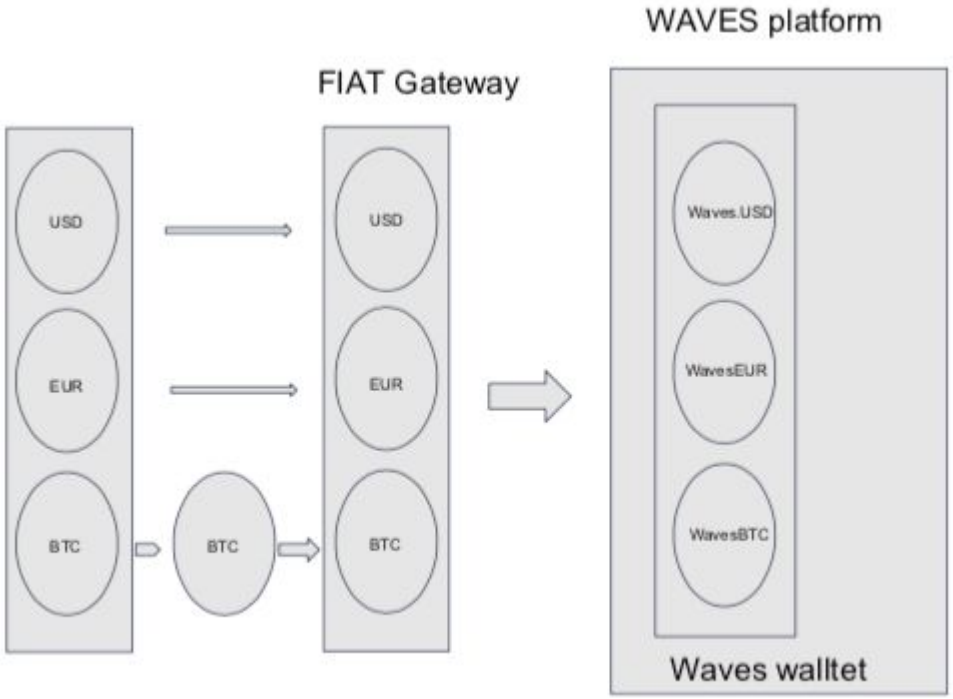
0x protocol

- 기존의 이더델타 모델 대비 낮은 수수료와 높은 유동성 확보
- 거래 프로세스와 매칭 프로세스를 분리
- 외부 네트워크를 통해 주문 정보를 공유 / Relayer 를 통한 주문 매칭





플랫폼 체인을 통한 피아트 형태 분산 거래소



Atomic-swap

- 아토믹 스왑을 활용한 이종체인간의 교환
- HTLC (Hash Time Lock Contract) 활용

리저브를 통한 인스턴트 분산 거래소