# Crodex

A Cross-chain wallet for Hybrid Decentralized Exchange

# Table of Contents

# Abstract

There are several exchanges suffered by hackers in recent years, which makes users notice the security issue about their crypto assets. Therefore, decentralized exchanges become more and more popular. However, when we want to trade bitcoin with ethereum or digital-fiat money, which is the major trading pair in cryptocurrency market, we found none of current decentralized exchanges support. So, we propose Crodex, A cross-chain wallet for hybrid decentralized exchange, to solve this problem.

# Chanllenges of Exchanges

## Centralized Exchange

Cryptocurrency markets have a dramatic growth in recent years. The daily trade volume of cryptocurrency market has exceeded $10 billion nowaday. Cryptocurrency, which is mostly based on blockchain technology, is secured by cryptography and decentralized technology. But most  trades of cryptocurrency are happened in a centralized way. You need to deposit your cryptocurrency to a centralized exchange before trading. Which makes exchanges become a honeyspot to hackers because they hold all cryptocurrency from every trader. For a recent instance, $534 million worth cryptocurrency were stolen by hackers from Coincheck in Jan 2018.

## Decentralized Exchange

Decentralized exchanges aim to solve the security problem of centralized exchanges. But even through centralized exchanges get hacked over and over again, the trading volume of decentralized exchanges still much smaller than centralized exchange (IDEX trades less than $5 million a day, while Binance trades more than $1 billion). What makes user reluctant to use decentralized exchange? Please read the figures below.

## Binance

| # | Currency | Pair | Volume (24h) | Price | Volume (%) |
|---|---|---|---|---|---|
| 1 | Bitcoin | BTC/USDT | $482,768,000 | $8,381.42 | 27.67% |
| 2 | Ethereum | ETH/USDT | $129,045,000 | $556.46 | 7.40% |
| 3 | Ethereum | ETH/BTC | $93,581,600 | $555.87 | 5.36% |
| 4 | NEO | NEO/USDT | $83,610,200 | $67.58 | 4.79% |
| 5 | TRON | TRX/BTC | $50,273,400 | $0.030202 | 2.88% |
| 6 | NEO | NEO/BTC | $44,100,800 | $67.47 | 2.53% |
| 7 | Ripple | XRP/BTC | $40,757,500 | $0.676917 | 2.34% |
| 8 | Binance Coin | BNB/BTC | $39,632,200 | $9.20 | 2.27% |
| 9 | Litecoin | LTC/USDT | $37,137,300 | $156.38 | 2.13% |
| 10 | IOTA | IOTA/BTC | $36,792,600 | $1.23 | 2.11% |

Figure 1. 24 hour top 10 trading volume of Binance from coinmarketcap.

## Bitfinex

| # | Currency | Pair | Volume (24h) | Price | Volume (%) |
|---|---|---|---|---|---|
| 1 | Bitcoin | BTC/USD | $780,985,000 | $8,369.00 | 48.13% |
| 2 | Ethereum | ETH/USD | $366,801,000 | $554.60 | 22.61% |
| 3 | Ripple | XRP/USD | $76,870,600 | $0.675430 | 4.74% |
| 4 | Litecoin | LTC/USD | $54,240,100 | $155.95 | 3.34% |
| 5 | EOS | EOS/USD | $51,122,800 | $4.77 | 3.15% |
| 6 | Ethereum | ETH/BTC | $39,776,400 | $555.62 | 2.45% |
| 7 | Bitcoin | BTC/EUR | $36,071,000 | $8,380.36 | 2.22% |
| 8 | IOTA | MIOTA/USD | $35,576,500 | $1.22 | 2.19% |
| 9 | NEO | NEO/USD | $35,157,000 | $67.62 | 2.17% |
| 10 | Bitcoin Cash | BCH/USD | $28,617,900 | $952.97 | 1.76% |

Figure 2. 24 hour top 10 trading volume of Bitfinex from coinmarketcap.

Figure 1, and 2 show the top 10 trading volume of Binance and Bitfinex, the top 2 cryptocurrency exchanges in the world. We can find that most of those asset are pair with BTC or USD(USDT). But current decentralized exchanges only allow us to trade ETH and ERC20 asset. When we want to trade BTC with USDT or other cryptocurrency listed above, None of current decentralized exchanges support. We think this is the reason why user are not willing to use decentralized exchange. The real pain point of decentralized exchange.

# Introduction to Crodex

We propose Crodex, wallet for cross-chain hybrid decentralized exchange on ethereum to address those challenges above. We makes ethereum smart contracts interoperable with Bitcoin or other blockchains by using Crodex wallet. Which means we can trade coins from several blockchains without trusting a specific third party.

In the next section, we will talk about how Crodex works.

# Crodex

## Crodex Cross-chain Wallet

The basic concept of Crodex cross-chain wallet is to build a Lightning Network(LN) channel between Crodex wallet service provider(CWSP) and each user. Then we combine trade invocation in Ethereum smart contract with Hash Timelock contract(HTLC) in LN channel. Now, we will explain how to use Crodex  wallet to trade BTC on Ethereum network.

As we mention before, Crodex wallet is designed for decentralized exchange. So, the operation of wallet can be classified into three parts: deposit to wallet, trading in decentralized exchange and withdraw from wallet. We will talk about those part respectively.

### Deposit

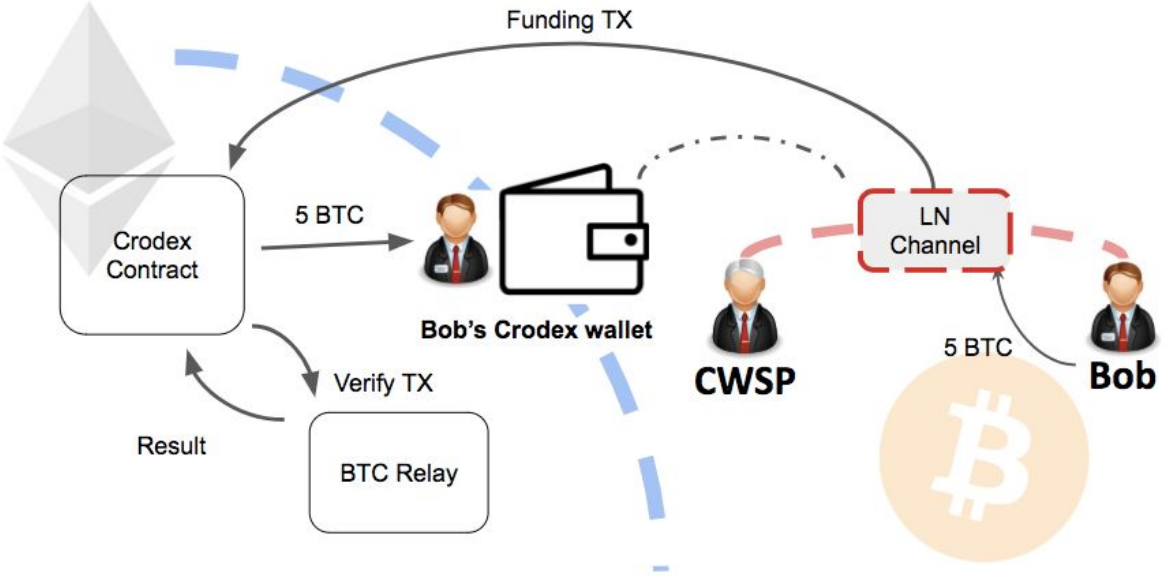



Figure 3, Process of deposit

Figure 3 shows how Bob deposits 5 BTC to Crodex wallet. First, Bob create a LN channel between CWSP and himself with depositing 5 BTC therefore Bob own 5 BTC in this channel.

Then, CWSP or Bob call Crodex contract with BTC-relay to generate 5 BTC(Ethereum) to Bob's wallet. Bob deposit successfully.

## Trade

We will use an example to explain the trading process between Bob and Alice that Bob want to pay 5 BTC for 10 usdt(ERC20 usd Tether) and Alice want to pay 10 usdt for 5 BTC. We assume the LN channel between both them and CWSP were build, which means Bob and Alice already deposit to Crodex wallet.

**Method 1**

**Step 1** : Bob create order: $Bob(5BTC \rightarrow 10usdt)$ with hash of a secret number $H(B)$ and CWSP create a HTLC in LN channel between Bob and CWSP with $H(B)$ like:

$$HTLC(Cond(H(B)),\ Update(Bob(-5),\ CWSP(+5)))$$

And Alice create order: $Alice(10usdt \rightarrow 5BTC)$ with hash of a secret number $H(A)$.

**Step 2** : Order match

**Step 3** : CWSP create a HTLC in LN channel between Alice and CWSP with $H(B)$ like:

$$HTLC(Cond(H(B)),\ Update(Alice(+5),\ CWSP(-5)))$$

Then, Alice reveal $A$.

**Step 4** : Bob reveal $B$. Then CWSP invoke settlement function likes:

$$Settle(\ Bob(5BTC \rightarrow 10usdt,\ H(B)),\ Alice(10usdt \rightarrow 5BTC,\ H(A)),\ B,\ A)$$

**Step 5** : Update both LN channel.

With method 1, we can trade ether or ERC20 token with BTC without trusting any third party. And benefit from LN and speed of trade doesn't limit by Bitcoin network. But it's kind of over the counter (OTC) trading because user still need to do some work after order matched. Therefore, the user experience of this method is not smooth as other exchange. To solve this problem. We propose another method which improved from method 1 below.

**Method 2**

**Step 1** : Bob create order: $Bob(5BTC \rightarrow 10usdt)$ with hash of a secret number of CWSP $H(C_1)$ and EM create a HTLC in LN channel between Bob and CWSP with $H(C_1)$ like:

$$HTLC(Cond(H(E_1)),\ Update(Bob(-5),\ CWSP(+5)))$$

Alice create order: $Alice(10usdt \rightarrow 5BTC)$ with hash of a secret number of CWSP $H(C_2)$ and CWSP create a HTLC in LN channel between Alice and CWSP with $H(C_2)$ like:

$$HTLC(Cond(H(C_2)),\ Update(Alice(+5),\ CWSP(-5)))$$

**Step 2** : Order match

**Step 3** : CWSP invokes settlement function and reveals $C_1,\ C_2$ likes:

$$Settle(\ Bob(5BTC \rightarrow 10usdt,\ H(C_1)),\ Alice(10usdt \rightarrow 5BTC,\ H(C_2)),\ C_1,\ C_2)$$

**Step 4** : Update both LN channel.

**Cond. 1** : If CWSP reveal $C_2$ without settlement of Alice's order, Alice will earn 5 BTC from CWSP for free.

**Cond. 2** : If CWSP reveal $C_1$ without settlement of Bob's order, Bob can report to contract with order and $C_1$ like :

$$Report(\ Bob(5BTC \rightarrow 10usdt,\ H(C_1)),\ C_1)$$

Contract will give Bob 10 usdt from CWSP's account when report verified.

We can trade without trusting any third party with method 2 as long as CWSP can afford this order. The user experience of trading become very smooth compared to method 1 because the trading process of user can be fully abstracted to a single step(step 1). Just like trading in normal exchange, all you have to do is setting an order. Any other process can be handled by CWSP.

## Withdraw

Bob just need to close the LN channel between exchange and himself when he want to withdraw BTC from exchange. And after the settlement transaction of LN channel confirm, Exchange manager will call exchange contract with BTC-relay to burn the BTC balance of Bob in contract.

It's OK for Bob if he don't want to withdraw all BTC from exchange. We just need to create or reset a new LN channel between Bob and exchange manager again with remain BTC as long as the channel closed.

## Summary of Crodex Wallet

Crodex provide a new way to trade out-chain coin on ethereum. You can trade BTC, ZEC… on ethereum network directly and efficiently without depositing your coin to exchange or gateway service provider at first. The out-chain coin is still under your control so you don't need to worry that exchange or gateway service provider may abscond with your coin. Furthermore, every operation on Crodex wallet will effect on both ethereum and original blockchain network simultaneously by cooperation between Crodex and Lightning network. Which make a trustless cross-chain exchange possible.

# Others

## Hybrid Decentralized Exchange

Hybrid decentralized exchange is combination of centralized order matching and decentralized settlement improved from decentralized exchange. The hybrid architecture take advantage of efficiency from centralized exchange and security/transparency from decentralized exchange. The cross-chain exchange of Crodex wallet is also a hybrid architecture. Therefore, we will support hybrid decentralized exchanges like 0x protocol.

## BTC Relay

BTC Relay is an Ethereum contract that stores Bitcoin block headers. BTC Relay uses these block headers to build a mini-version of the Bitcoin blockchain: a method used by Bitcoin SPV light wallets. With the help of this SPV wallet, We can verify a Bitcoin transaction in ethereum network.

## Lightning Network (LN)

The Lightning Network is a "second layer" payment protocol that operates on top of a blockchain. It features a peer-to-peer system for making micropayments of digital cryptocurrency through a network of bidirectional payment channels without delegating custody of funds and minimizing trust of third parties.

The LN also support trustless routing payment by HTLC. Routing payment is very suitable for implement of exchange because the role of exchange is really like a medium route between 2 trader. That’s why we use the concept of LN to implement Crodex.

However, we don’t need a complete Lightning Network solution, we only need some component of it. So, we will rewrite it and only implement the function we need to optimize our service.

# Competitor

## ERC20 (Hybrid)DEX

There are many project of hybrid decentralized exchange base on ethereum. Although most of them only support trade between ether and ERC20, we focus on propose a cross-chain service for exchanges. Therefore we can work together and we are not actual competitor to each other.

## Stellar Dencentralized Exchange(SDEX)

SDEX is a decentralized exhcange on stellar network. They support trading between most major coin and digital-fiat money. Although all trade in STDX is decentralized, but you need to trust a third party gateway to deposit and withdraw.

For example, if you want to trade ETH on SDEX, you need to find a gateway service provider like apay.io. You deposit ETH to wallet of apay.io and you will receive a $ETH_{apay.io}$ IOU. Then, you can trade this IOU on SDEX.

## OpenLedger

OpenLedger are a gateway service, holding coins and providing IOU tokens that can be easily traded on the bitshares distributed exchange. Like SDEX, trade in open ledger exchange is decentralized but you need to trust OpenLedger as gateway when deposit and withdraw.

## Blocknet

Blocknet is a OTC trading platform. They match order first and then start a atomic cross chain transfer(ACCT) by using check lock time verify. The benefit is the whole process is trustless. But the signing process of ACCT is complicated to user and hard to abstract away. So, the user experience of it is not as smooth as other exchange.

## KyberNetwork

KyberNetwork is a cross-chain DEX project on Ethereum. They use 2-way relay technology to handle the cross-chain deposit and withdraw. However, it doesn't work for blockchains without smart contract protocol like Bitcoin. To solve this problem, they design a contract to allow third party to be a gateway between Ethereum and Bitcoin with stake. This contract will guarantee user will receive their BTC when they withdraw it. Otherwise, they will get more ETH from contract as compensation by reporting to contract.

Taking BTC as example. The major difference between KyberNetwork and Crodex is you need to put your BTC to someone's wallet when deposit to KyberNetwork while Crodex doesn't. All of your BTC is still under your control because you don't actually deposit your BTC to someone's wallet. You can withdraw it anytime you want without trusting a third party.

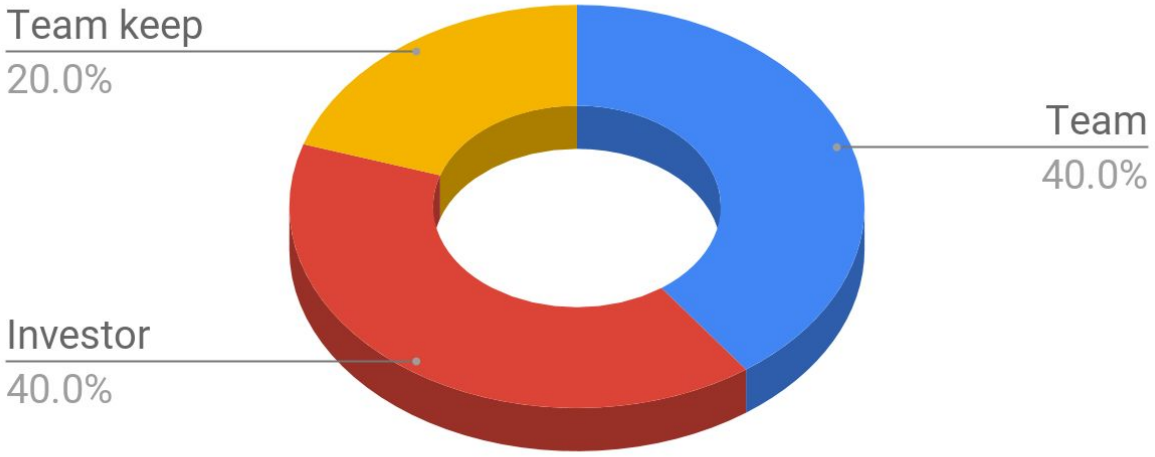
Another difference is compensation mechanism. Although you can get some ETH as compensation if you fail to redeem your BTC from KyberNetwork, but it is still not what you expect to receive. However in Crodex, compensation is depend on user's order. It's just like trading with CWSP from perspective of users because users can still get what they expect according to their order. Therefore, there is no risk to trade via Crodex as long as CWSP can afford your order.

# Token Economy

## CRD Token

We will issue 100,000,000 CRD in initial stage. Other CRD will be generated and given to trader (user) of as reimbursing of trading fee. Trader will receive RCDs equivalent to 40% to 90% of trading fee they paid. We will define formular later. .

Then, let's talk about distribution of CRD. Our team will hold 40% of CRD, and 40% of CRD will airdrop to investors. Remains will keep by our team as backup for usage like marketing and operating.




Figue 1. Token distribution of CRD.

## Usage of CRD

### Voting

The CRD holder will have the right to vote on various governance and operational issues raised by Crodex, such like which tokens are listed on the exchange or which coin of cross-chain trading should be support at first.

### Revenue sharing

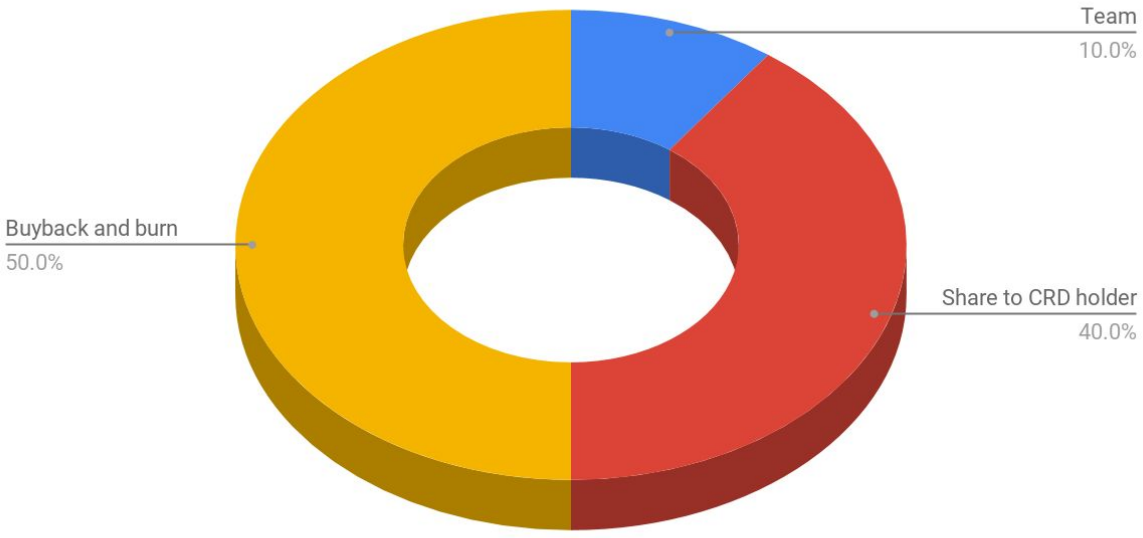
Crodex will distribute 40% of total revenue to all CRD holder on schedule.

## Buyback / Burn Policy

Crodex will spend 50% of total revenue to buyback and burn CRD from market on schedule. Because the amount of new generating CRD is depend on trade fee, or our revenue in other word. So the total supply token in network will be well control by this policy.

# Distribution of Income Revenue

Crodex will earn revenue from fee of each trade. Crodex team will keep 10% of total income to cover our operating cost at early stage. Then, as we mention above. We will distribute 40% of total income as revenue sharing to every CRD holder. The last 50% of income will be used to support burn policy to control the total supply of CRD in network.




Figue 2. Usage of  income revenue.

## Reimbursing Formula

As we mention above, new CRD will be generated from each trade as reimbursing for trading fee. In order to control the inflation rate of CRD, we also spend 50% of revenue (or trading fee) to burn CRD. So, how to make the inflation rate of CRD well control? We will use a formula to define the reimbursing rate below.

Variable define :

$R$ : *Reimbursing rate.*

$B$ : *Rate of revenue we use to buyback and burn CRD.*

$D$ : *Daily trade volume.*

$f$ : *Trade fee rate.*

$V$ : *Total maket value of CRD.*

$I$ : *Expect inflation rate per day.*

$P$ : $D/V$

We assume our schedule of revenue sharing and burning plan is once every 24 hour, and we hope daily inflation rate is not great than expectation. So,

$$D \cdot f \cdot R - D \cdot f \cdot B \leq I \cdot V$$
$$\Rightarrow R \leq B + \frac{I}{P \cdot f}$$

We want to set up bound of reimbursing rate to 0.8. So,

$$R = 0.8, if\ B + \frac{I}{P \cdot f} > 0.8$$
$$R = B + \frac{I}{P \cdot f}, otherwise.$$

For example, let B = 0.5, daily trade volume is 20% of total CRD value which means P = 0.2, expect inflation rate per day I = 0.026% (about 10% per year) , and trading fee f = 1%. Then the Reimbursing rate will be 63%. With this formula, we can set appropriate reimbursing rate according to trade volume and current CRD price or market value.

## Summary of CRD

We will issue token CRD to build decentralized governance with community. CRD can be used to vote for roadmap of Crodex, reimburse to trader's fee cost and join revenue sharing of Crodex. In order to control the inflation rate of CRD, we will spend parts of our revenue to buyback and burn CRD from market. Furthermore, all of those policy are planned to define and execute with smart contract to realize decentralized governance with Crodex community.

# Conclusion

There are many project about decentralized exchange. Due to lack of support about exchange between BTC, USDT and other coins, which take major market share of cryptocurrency(As figure 4 below). It's not widely accepted by users. To address this problem, we propose Crodex, a cross-chain wallet for hybrid decentralized exchange to improve interoperability between blockchains. Therefore, a cross-chain decentralized exchange become possible.

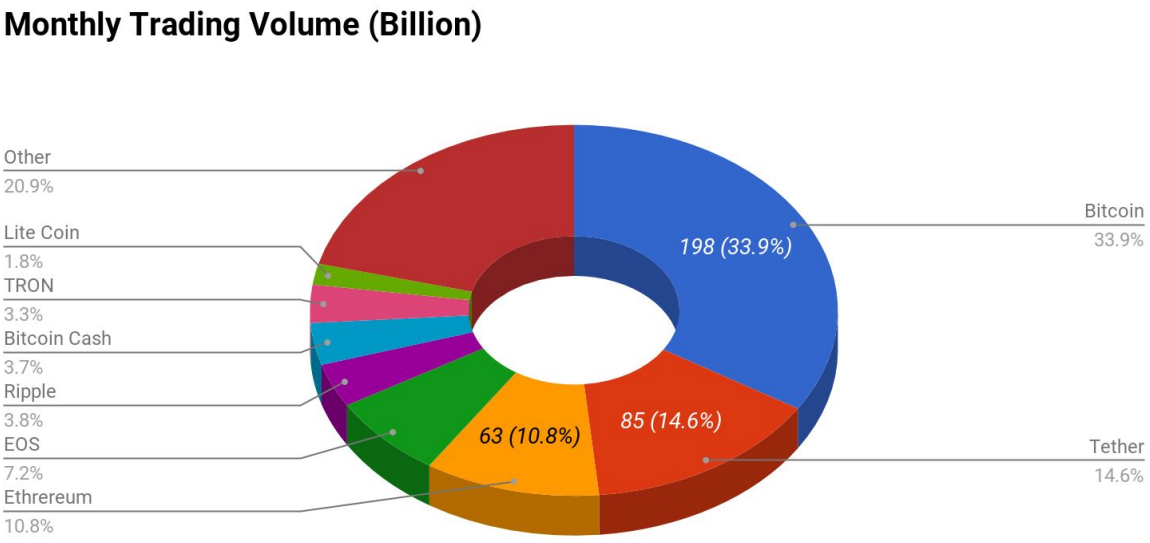



Figure 4 Monthly Trading Volume (Billion USD) of Cryptocurrency Market

Crodex reach interoperability by Crodex wallet, a interface of other blockchains on ethereum network. Every operation through Crodex wallet will effect on both network simultaneously. Which means we can trade out-chain coin like BTC on ethereum network directly with Crodex wallet.

# Roadmap

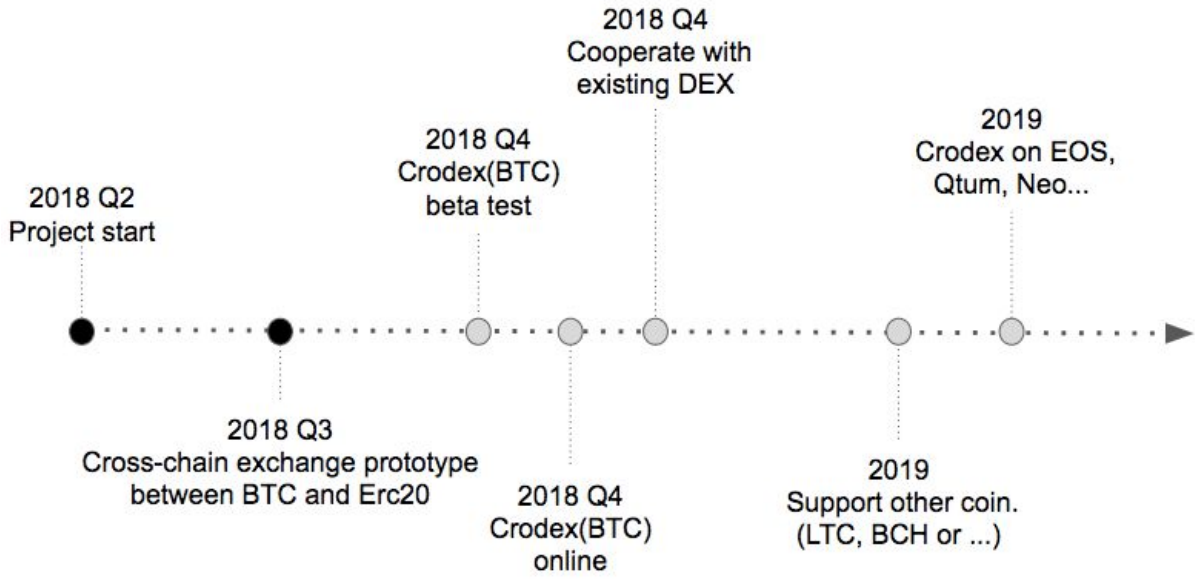



Figure 5 Roadmap of Crodex