Final Project Proposal

The Design of Bitcoin Exchange Application

Pengfei Wang
Jiahua Li
Shujun Lei
2018/3/27

Problem Overview

Bitcoin (₿) is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain.

Bitcoins can be bought on digital currency exchanges. Digital currency exchanges (DCE) are businesses that allow customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or different digital currencies. They can be market makers that typically take the bid/ask spreads as transaction commissions for their services or simply charge fees as a matching platform.

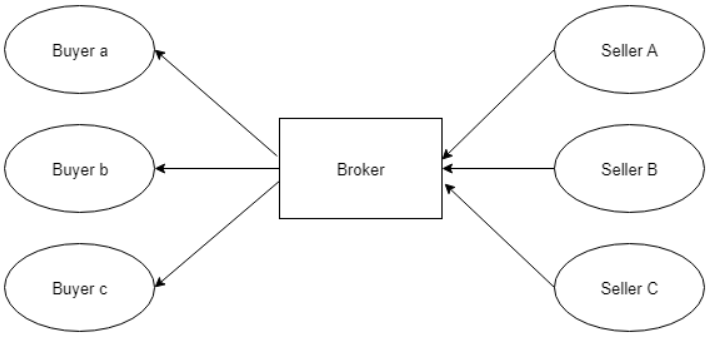
In one type of system, digital currency providers (DCP), are businesses that keep and administer accounts for their customers, but generally do not issue digital currency to those customers directly. Customers buy or sell digital currency from DCEs, who transfer the digital currency into or out of the customer's DCP account. Some DCEs are subsidiaries of DCP, but many are legally independent businesses. The denomination of funds kept in DCP accounts may be of a real or fictitious currency.[1]

Our goal is to design an application to fulfill the bitcoin exchange. This application can create a platform with high security achieved by full trace verification, which can be used by buyers and sellers.

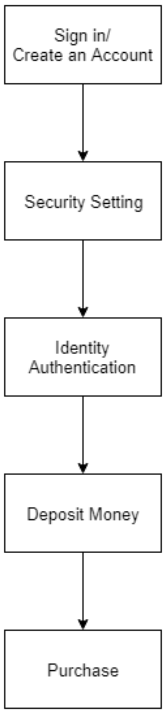
Application Key Functionalities

The trading can be performed in two ways: 1. Bitcoin Exchange 2. Over-The-Counter (OTC) Trading

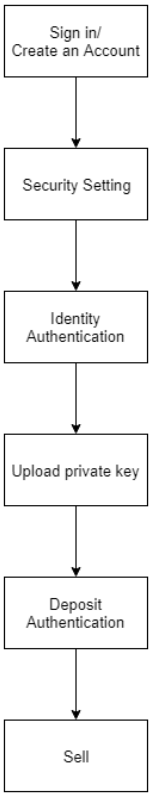
1. Bitcoin Exchange



For a Buyer, it needs to sign in/create an account, do the security set, and identity authentication by platform. Next, it will deposit money in Broker to complete the purchasing process.



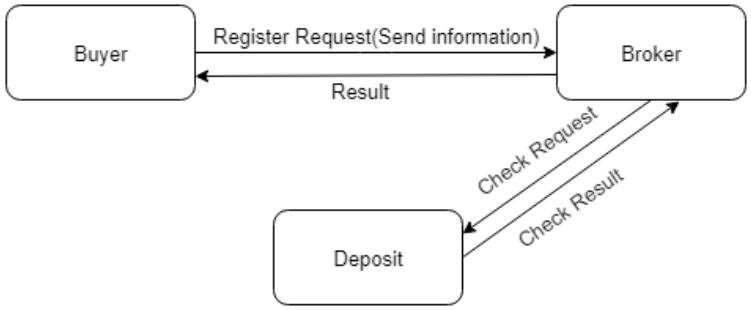
For a seller, it needs to sign in/create an account, do the security set, and identity authentication. Next, it will upload the private key to platform which needs to be



authenticated by deposit. If the information is correct, it can sell the bitcoin.

a) Registration

For a buyer, it needs to create an account in Broker, Broker will send the account information to Deposit for authentication. If the request has been approved, the account will be created.



b) Trading

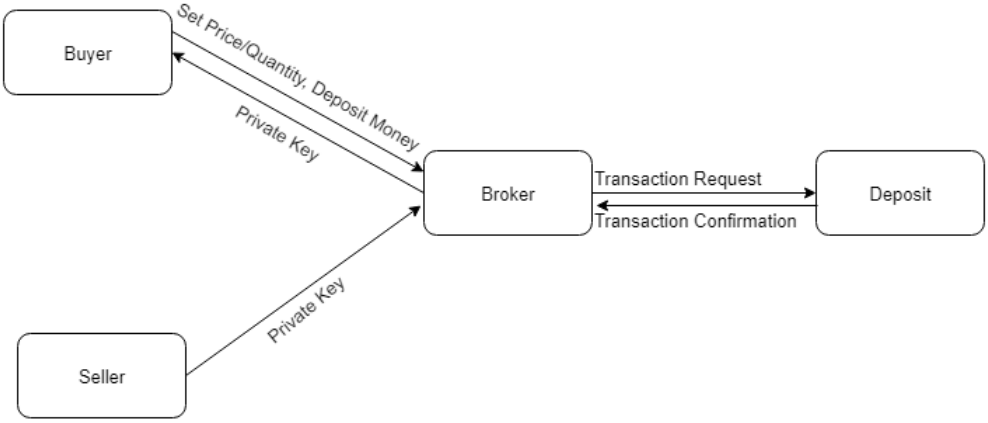
Bitcoins are stored in the Bitcoin Wallets. If someone wants to sell the bitcoin, it needs to upload the private key to the platform. If someone has successfully bought the bitcoin, the private key will be stored in its account in Broker unless it will trade into flat money.

There are two kinds of trading methods on the platform: 1. Limit trading 2. Market trading.

In the process, Buyers don't know the exact seller, and Broker performs as an agent. Broker helps the Buyers and Sellers to do the matching, bitcoin trade and flat money trade.

In Limit trading, Buyers will set the bid price, Broker will find out the match result, then finish the trading part.

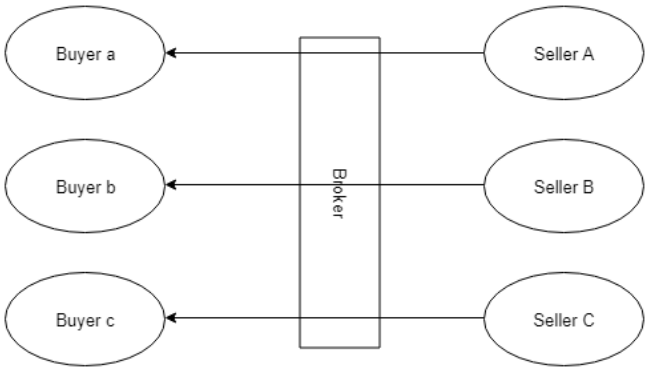
In Market trading, Buyers will set the quantity of bitcoins, Broker will find the suitable Seller who trade Bitcoins in market price.

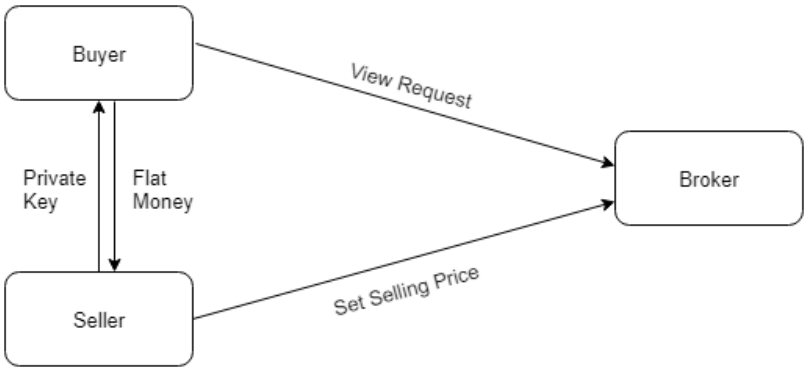


2. Over-The-Counter (OTC) Trading

The other way to trade has significant difference with bitcoin exchange.

They trade the bitcoin more directly without much security guarantee. The Seller can set one selling price in the platform. The Buyer can view the sellers price list to find the most suitable seller in their own way. Next, Buyer will trade with Seller directly.





Proposed Entities

Ecosystems: a singleton class.

Network: it contains a set of enterprises.

Enterprise: Bitcoin exchange platform, Person to Person community platform, Deposit.

Organizations:

1. Bitcoin exchange platform
    a) Administrator: Manage the registration of users, and basic authentication.
    b) Account: the management of currency flow
    c) Agency: Help the users to trade

    d) Analysis: Provide related analysis report
2. OTC platform
    a) Administrator: Manage the registration of users, and basic authentication.
    b) Account: the management of currency flow
    c) Analysis: Provide related analysis report
3. Deposit
    a) Authentication: Authenticate the trading records and information of users
    b) Records: Keep the records of all trading information

Employee: Accountant, Broker, Analyst, Record Keeper, Examiner

User: Investor, Seller

WorkQueue: a series of WorkRequest

Additional features

1. The summary of Live Traders: Amount, Price, UTC Time.
2. The summary of Live Order Book(Bid): Bid, Amount, Value
3. The summary of Live Order Book(Ask): Ask, Amount, Value
4. The statistical information: Last Price, Daily Price, 24-hour Low, 24-hour High, Today's Open, 24-hour Volume.
5. The prediction of Market Price in the future.

References

[1] T. Simonite, "What Bitcoin Is, and Why It Matters," MIT Technology Review, 26-Mar-2018. [Online]. Available: https://www.technologyreview.com/s/424091/what-bitcoin-is-and-why-it-matters/. [Accessed: 28-Mar-2018].

[2] J. Ryan, "Coinbase Bitcoin Exchange Review & Tutorial," BitcoinBestBuy, 18-Jan-2018. [Online]. Available: https://bitcoinbestbuy.com/exchanges/review-coinbase-bitcoin-exchange/. [Accessed: 28-Mar-2018].

[3] J. Kroll and I. Davey, "Mining," Understanding Bitcoin, pp. 143–158, 2014.