A block chain based decentralized exchange

Harsh Patel

Harsh.patel54@gmail.com

Abstract. A pure peer to peer version of the exchange system would allow all parties access to the market without relying on any central organization for market access. Paper proposes a solution for the problem of maintain an order book and determine the execution rate in the peer to peer network. Like crypto-currencies the network relies on blockchain of transaction. Digital signature system would be the core of the decentralized market place. The paper defines basic ground rules for the working of decentralized exchange. The major components of the decentralized exchange are issuing process, co-existence of blockchain and order books and functions of the miner. Unlike other crypto currencies de-centralized exchange would have a trust based issuing process which in long run would be a sum zero game. The decentralized
Exchange would have 3 types of entities namely – Issuer, Trader and Miner.

Keywords: Crypto-currencies, decentralized exchange, Payment system.

1 Introduction

Traditionally exchanges have been a place where buyers and sellers of a commodity meet to decide on a specific price for the commodity based on demand and supply. Initially exchange was a common marketplace, later it evolved into an organized market place regulated by defined rules. The decentralized exchange which can facilitate the functions of exchange without relying on central point of authority embedding all the basic principles of exchange in an autonomous technical protocol by the extending the capabilities of blockchain.

2 Functions of exchange

The exchange by very definition is an organized market place where various commodities, currencies, Financial Securities and derivatives are traded. The basic Components of any exchange are the entities (buyer and seller), A pair of Financial Instrument [FI] (Commodity, Security, Currency or derivatives), Quantity in trade and Price for the Financial Instrument against another Financial instrument. For this paper, Currency has been considered as a financial instrument. Each Financial instrument has a finite unit of exchange. (I.e. 1oz of gold is basic unit of exchange or 1 unit of share is basic unit for exchange.). In an exchange the entities bring in their respective financial instrument for trade with other financial instrument and based on demand and supply between two financial instruments the price is determined.

3 Need for A completely decentralized exchange

The each financial instrument is subject to speed of transfer. Speed of transfer is time taken by each financial instrument to exchange hands from I^{th} owner to N^{th} owner. Speed of transfer is a limited of different Financial instrument is different. (i.e. Time taken by simple cash purchase transaction is not same time that has been taken for a transfer of real estate.). The decentralized exchange standardizes the speed of transaction across all financial instrument there by reducing loss due to speed of transfer. One of the main function of exchanges is fair price determination between two financial instruments. In centralized exchange the price determination mechanism is a blackbox raising a ethical question over price. Keeping the entire exchange function over blockchain would ensure transparency in the entire system.

4 Block-chain based Decentralized exchange

The decentralize exchange relies on the fundamentals of block chain for storing a transactions over a peer to peer network. Unlike crypto currencies the decentralized exchange have three type of entities (i.e. Issuer, Trader [User] and Miner). The network relies on issuing process (FI Definition, FI issue and FI withdrawal), orders (Open order and execution order) and blockchain . The miner would verify the transaction for validity as well as match the execution orders and upon successful conformation would generate a block using proof of work as followed by the Bitcoin protocol.

Issuer. Issuer is the entity who is the initial starting point for the decentralized exchange. Issuer has Private Key [I_{Pv}], Public Key [I_{Pu}] and Issuing Token [I_n]. Only Issuers can generate financial instruments in the decentralized exchange and can delegate the right of being an issuer to another entity by generating new issuing token. The Issuer defines / issues / withdraws FI, which facilitates the entry and exit point for the market there by making a sum zero game among Issuers and Trader. By definition, issuer is a custodian for all the FI's Issued within the marketplace. (I.e. amount of a FI^x held by issuer in custody should be amount of a FI^x in circulation inside the decentralized marketplace.) The Issuer is entitled for an issuing cost via discounting methods.

Trader. Trader is the entity that places the order to either buy / sell a defined quantity of FI^x in lieu defined quantity of FI^y upon finding a successful match (i.e. countering order) an execution order is broadcasted by trading entity which determines the price and is subject to verification by mining entity. Trader has private key [T_{Pv}] and Public Key[T_{Pu}]. The Trader places open order on the network as a broadcast to all the nodes. Each order has an exactly opposite countering order which would result in an execution order. The trading entity constantly monitors the network for countering order for the orders placed by itself to generate the execution order. The execution order determines the notional price for a specific market (i.e. market between Fi^x and FI^y.). The trading entity can cancel the order which has been issued by itself. The trading entity has the option to select the market it wills to be active on (I.e. Pair of FI market where trader wills to be active on), so that only open orders relating to a particular market are only being accessed by that node.

Miner. Miners are entities who constantly listen to the network for successful transaction broadcasted by the nodes. The transactions monitored are issue token transfer transaction, FI Definition transaction, FI issue transaction, Execution orders and FI withdrawal Transaction. The mining nodes have the function of validating all the transactions. By validating issue related transaction (Token transfer Tx, FI definition Tx, FI issue Tx and FI withdrawal Tx) miner brings trust into the marketplace. By validating execution order the miner determines actual price between two FI's. The validates all the transaction's by using proof of work and generates a block which is stored sequentially in block chain upon consensus by other nodes. The transaction cost associated to all transaction is accumulated by the miner and is the incentive point for miner. The mining node must listen to all events happening across markets (i.e. All Pair of Financial instrument). Fig 1 explains the macro level functioning of the entire system.

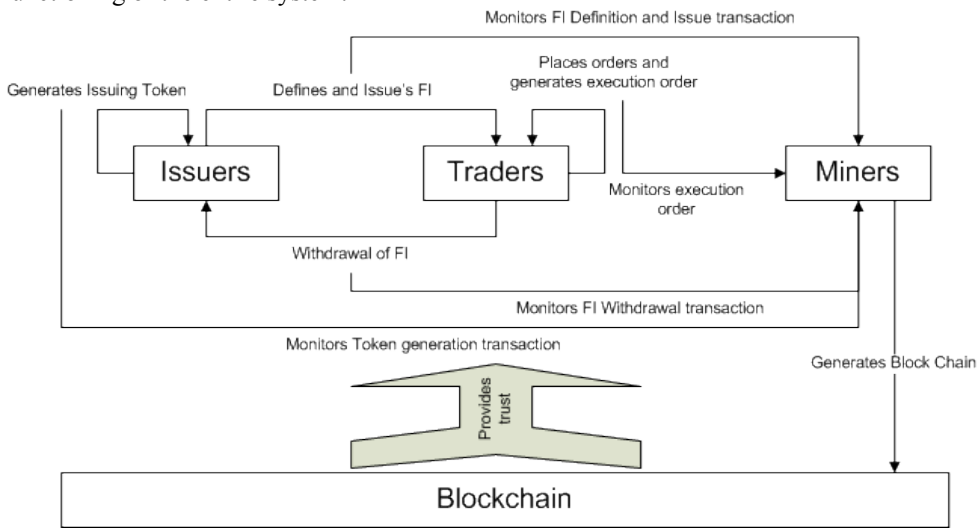

Fig. 1. Overview of interaction between entities in the decentralized exchange.

5 Transactions in the decentralized exchange.

The Transaction in decentralized exchange are of many types but all of the transactions are linked to genesis transaction.

Token transfer Tx. All issuers have token which serves the function of limiting the number of FI's being floated in the decentralized exchange. Only the Issuer can generate an Issuing token which can be passed down to another issuer using a token transfer transaction. Issuing token is the hash of the new token owner's public key and previous token which is signed by previous token owner's private key, forming a block chain of issuing token there by providing the trust relationship amongst issuers. Fig 2 Describes the entire block chain of issuing tokens.

$$Token\ Transfer\ _{Tx} = Sign_{I_{Pv}^{n-1}}(Hash(I_{Pu}^{n}, I^{n-1}))$$

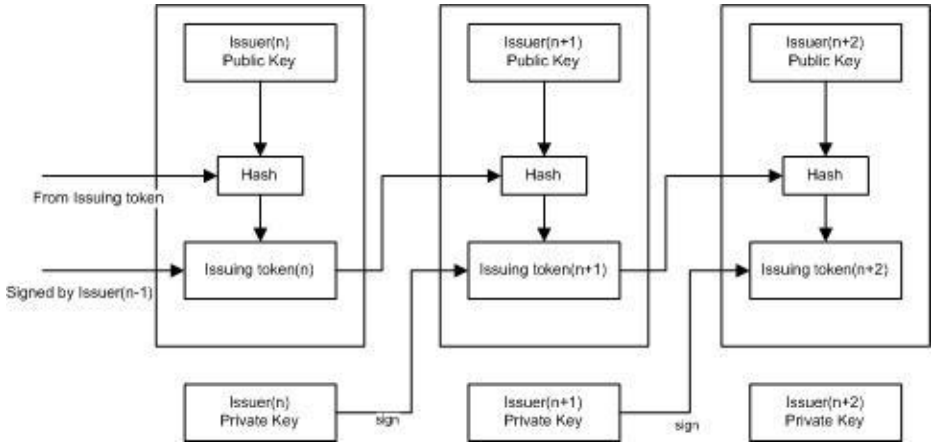

Fig. 2. Block Chains of issuing tokens

FI Definition/inception Tx. All issuers are capable of issuing FI's. A Financial instrument (FI) can be a currency, commodity, Stock, Bonds or even a product. While issuing the issuer specifies certain basic properties of FI's which are as follows.

1- Name of FI
2- Basic unit of exchange
3- Time stamp of the inception date of FI

When a FI is defined / incepted a transaction(FI Definition Tx) is broadcasted by the Issuer using the issuing token which server as a reference point for all issue and withdrawal transaction done by the issuer. One issuer can generate multiple FI's. The FI Definition Tx consists of signed hash of Issuing token and FI definition's by Issuer's Private Key [I_{pv}]. . Fig 3 Describes the FI Definition transaction in details.

$$FI\ Definition\ _{Tx} = Sign_{I_{P_v}^n}(Hash(I^n, FIdef))$$

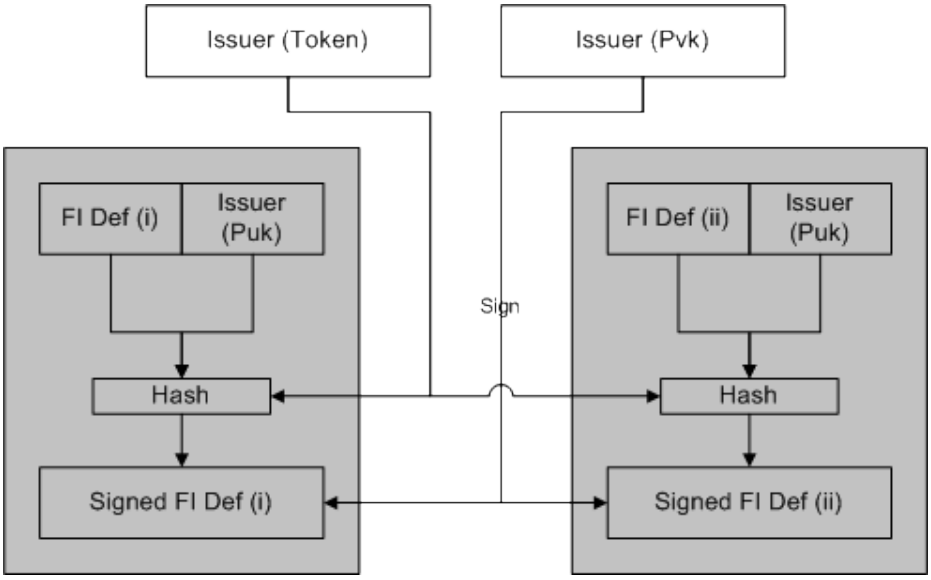

Fig. 3. Diagrammatic representation of FI Def Tx.

FI's issue Tx. Once the FI's are defined / incepted the issuing process starts where in each physical /virtual FI's are kept in custody of the issuer and are allotted to the trading entities. The issuer for issuing the FI in the system can levy an issuing charge on the trader by the virtue of discounting. FI Issue Tx consist of hash of Issuing

Token, Traders Public key, FI Definition transacation and quantity issued which is signed Issuers Private key. Fig 4 describes the overall structure of the FI issue Tx.

$$FI\ Issue_{Tx} = Sign_{I_{Pv}^{n}}(Hash(I^{n}, FIdef_{Tx}, T_{puk}^{x}, Qty))$$

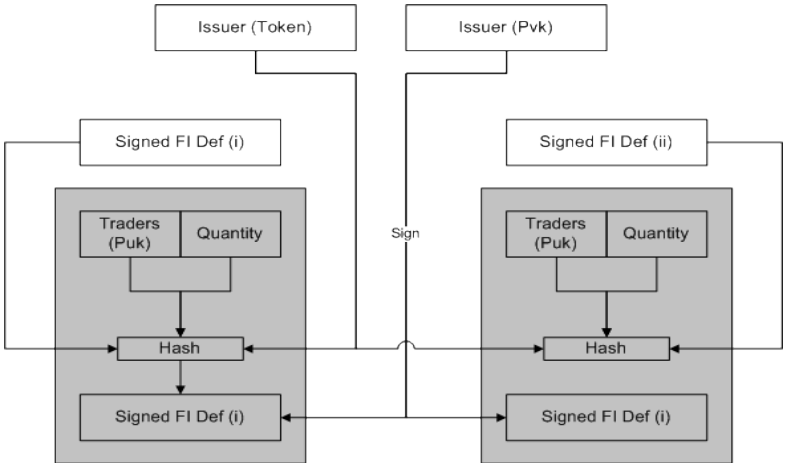

Fig. 4. Diagrammatic representation of FI Issue Transaction

Open Order transaction. Open order transactions are broadcast over the network stating expression or willingness of the trader to trade one FI for another FI. Trader can gain FI by virtue of Issuing transaction or by virtue of Execution order from pervious trades. Technically open order transaction is signed hash of following information Trader Public key, FI_1 and FI_2 definition transaction, Quantity of FI_1 and FI_2 pledge and previous issuing transaction or previous execution transaction where in the trader claims the ownership of FI_1. The Open orders are not recorded in the block chain and miner entity holds no interest in open orders. Open orders are subject to execution order. In active market open orders make up the order books(i.e. Buy and sell orders). By the very nature of the decentralized exchange number of markets are in combination of two with the number of FI definitions present in the market. The trader specifies the markets where he wills to be active on, and open orders of those markets are only accessible to his node by this virtue. Open order are stored in the buffer / temporary storage space of the active nodes. An open order can be cancelled by the trader by sending a broadcast of cancel order to network. Upon receiving the cancel order the open order is removed from the buffer of the node. Cancel order contains signed hash of all details of open order transaction along cancelation flag. Cancel order is signed by the Trader's private key. Nodes verify the cancelation orders as public key of trader is specified in the open order only. Fig 5 Describes the overall structure of Open orders.

$$Open\ Order_{Tx} = Sign_{T_{Pv}^{n}}(Hash(T_{Puk}^{2}, Ex_{Tx} | FI\ Issue_{Tx}, FI\ Def_{Tx}^{1}, FI\ Def_{Tx}^{2}, FI_{QTY}^{1}, FI_{QTY}^{2}))$$

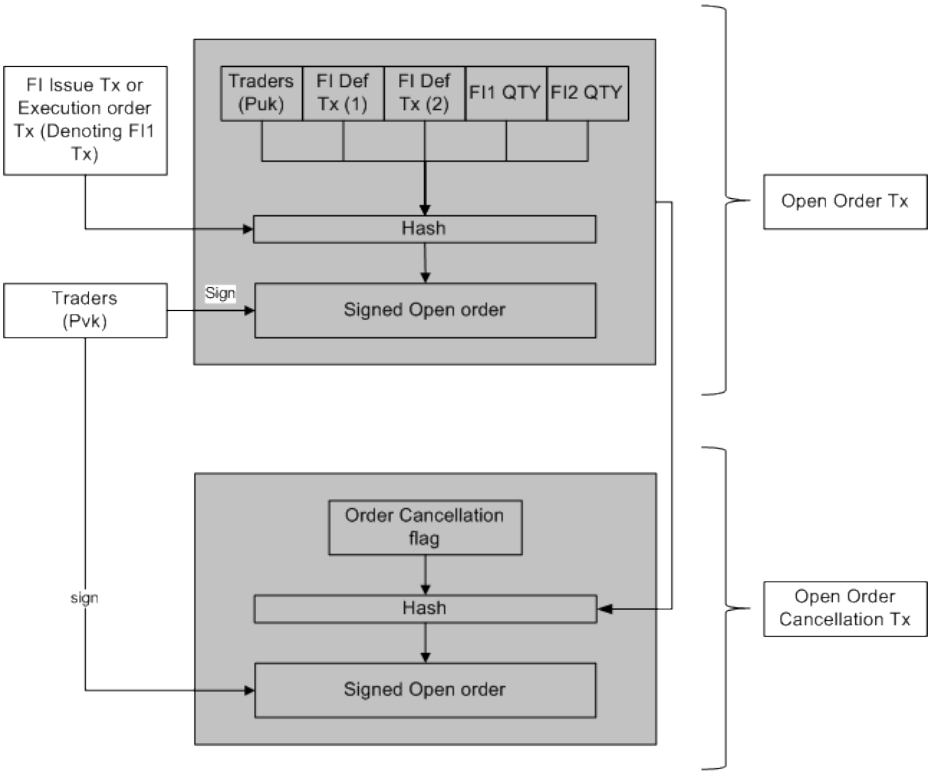

Fig. 4. Diagrammatic representation of Open order Transaction

Execution transaction. Each and every open order has an equal and opposite open order which makes the exchange transaction between two parties complete. Theoretically execution order is a collision point for two opposite orders and is recorded in the block chain. Execution order can only broadcasted by the nodes who broadcasted initial open orders. Execution order is subject to split transactions (i.e. – Large open order can be fulfilled by multiple smaller countering open orders.), thereby making a partial execution of the order. Technically execution order include the both countering open order signed by issuer of the either of the order. For any open order there can be minimum two execution order. At node level the execution order are broadcasted only if they meet the execution conditions. Following are the execution conditions.

If the countering open order matches the specification of broadcasted open order Then

Broadcast the entire amount as execution order.

Else

Calculate the difference between the orders and broadcast the execution order of appropriate measure leaving the rest as open order.

Execution transaction confirms the transfer of ownership of one FI to another. Figure 4 Describes the overall structure of the execution transaction.

$$Execution\ order^{i} = Sign_{T_{Pv}^{i}}(Hash(Open\ Det_{Tx}^{1}, Open\ Det_{Tx,}^{2},))$$

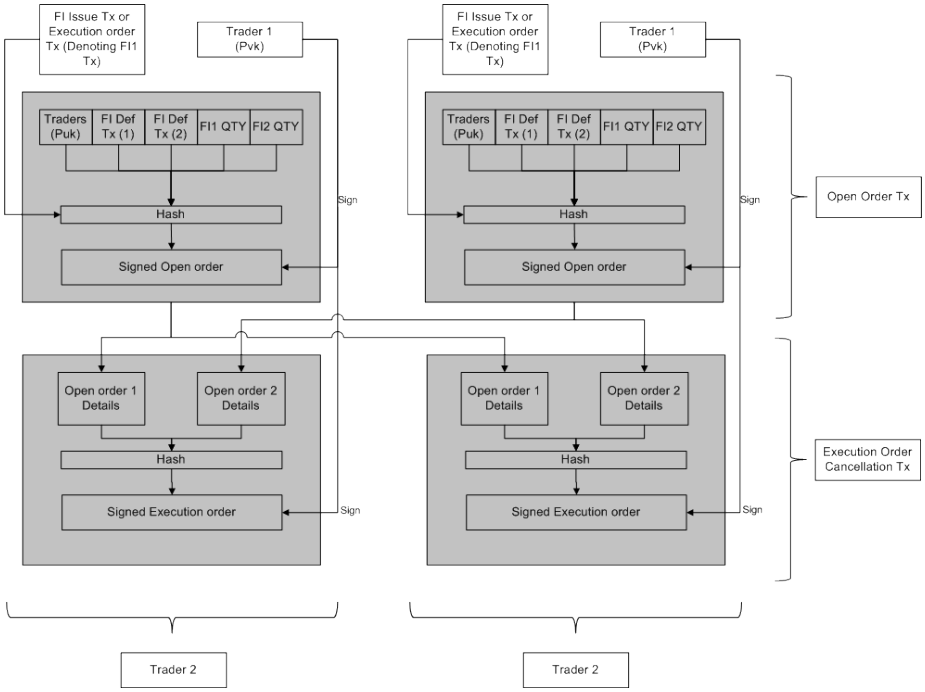

Fig. 4. Diagrammatic representation of Execution order Transaction

FI withdrawal transaction. All FI issued within the ecosystem are subject to withdrawal transaction, since the role of the issuer is as a custodian. The FI Withdrawal transaction serves as an exit point from the decentralized ecosystem. Withdrawal transaction is broadcasted by the trader and is the liability of issuer to withdraw the FI's. Technically FI withdrawal transaction is hash of Issuing token used to Issue the FI, Execution order transaction / FI Issue transaction denoting respective FI ownership, Quantity to withdraw, FI Definition transaction and Public key of issuer signed by Private key of Trader. Fig. 5 describes the overall structure of the FI Withdrawal transaction.

$$FI\ Withdraw_{Tx} = Sign_{T_{Pv}^{n}}(Hash(I^{n}, FI\ Issue_{Tx} |\ Ex_{Tx}, I_{puk}^{n}, Qty))$$

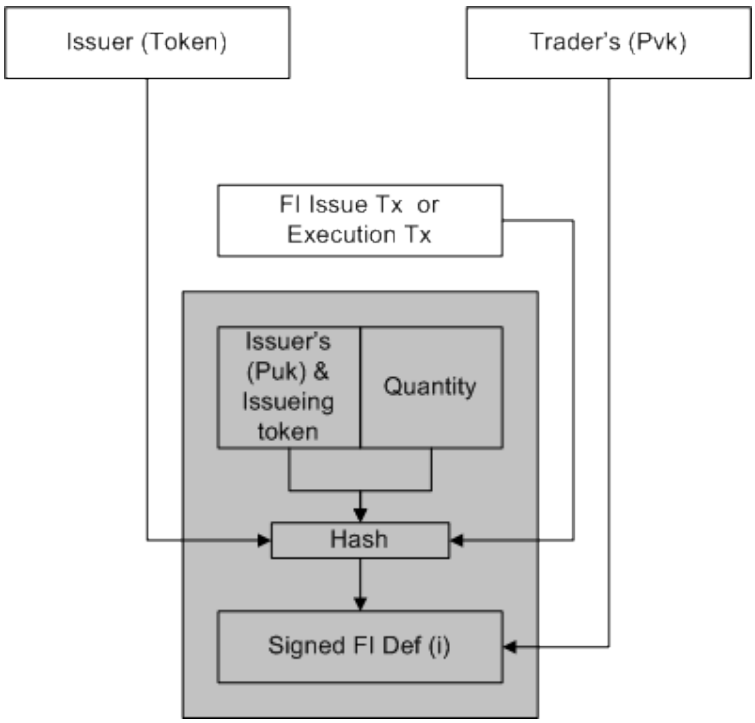

Fig. 5. Diagrammatic representation of FI Withdrawal Transaction

6 Price Discovery using the blockchain and mining

Notional Price. In the decentralized exchange price is determined by execution orders. Notional price is determined when a node in the network broadcast's an execution order. However the notional price of exchange for two FI's is subject to validation by miner since it can include bogus transaction (i.e. Double Spend transaction etc). Notional price is the real time price of a commodity but not the real / actual price of exchange for two FI's.

Actual Price. Actual Price of exchange for two FI's is determined by successful conformation of execution order in the block. Actual price is calculated on the basis of the valid execution transaction in block broadcasted in the network by the miner. Actual price is the real price of exchange prevalent in the market. All nodes update their open order books/ buffer upon receiving the new block.

Mining. The purely decentralized exchange is coinage independent, but dependent more on network for optimal functionality. Decentralized exchange can be implemented in either of the methods. (i.e Proof of stake or Proof of work). Proof of stake would be Ideal implementation for a completely decentralized exchange, however the method of implementation is subject to debate. The ideal block generation rate would be 1-60 seconds for a decentralized exchange.

7 Incentivization in the block chain.

For Issuer. Issuer is entitled for issuing / withdrawal fee and is directly allotted to the issuer as a direct percent of Transaction and is at the discretion of the issuer.

For Miner. The decentralized exchange is coinage free there by not depending on any specific coin for its stability but issuer generate various FI's which act as coins. Each transaction in the decentralized exchange is subject to transaction fee except for token transfer transaction and FI definition transactions. The transaction fee is mandatory for all the parties in the decentralized exchange.

8 Future work.

The application of decentralized exchange to other normal business functions like online ticketing or commoditizing of various daily products using decentralised exchange is a matter of debate for the future as well as definition of time driven and other such complex financial instruments are a matter of research for the future. Further more research is required in the mining process and execution process in order to strengthen the security of the entire system.

9 References

A, B. (2002). *Hashcash - a denial of service counter-measure,*. http://www.hashcash.org/papers/hashcash.pdf.

Merkle, R. (April 1980). Protocols for public key cryptosystems. *Symposium on Security and Privacy, IEEE Computer Society,* , 122-133.

Nakamoto, S. (2011). Bitcoin: A Peer-to-Peer Electronic Cash System.

Project, N. (2011). Retrieved from https://github.com/namecoin/namecoin.

S. H., & W. S. (1991). How to time-stamp a digital document,. *Journal of Cryptology vol 3 no 2* , 99-111.