Multilateral Token Trade Protocol (MTTP)
v0.6

daniel@mttp.io
jay@mttp.io
alex@mttp.io

MTTP Foundation
http://mttp.io
foundation@mttp.io

June 10, 2017

Abstract

Multi-lateral token exchange protocol(MTTP) is an open protocol for decentralized exchange on the Ethereum blokchcian. MTTP is intended to serve as an open standard and common building block, driving interoperability among decentralised applications(dAPPs) that incorporate exchange functionality.Trades are executed by a system of Ethereum smart contracts that are publicly accessible, free to use, and that any dApp can hook into for taken exchanging.

Contents

1 Background

Blockchain[1][2] technology was created to facilitate the cryptocurrency Bitcoin[3]. It is originally a decentralized system to enforce the financial agreements[4][5]. The technology that underlies them could spread into other transactions: trading stock, IP, buying and selling real estate, purchasing music and much more. Despite both consortium blockchain and private blockchain have been developed and implemented in few years, however the value only exists among the closed set of entities or internal entity. While fully public blockchain operates by having a large number of participants, resulting in trust by numbers. According to coinmarketcap.com stats, the total cryptocurrency market cap value has reached to 79 billions USD, including 17 billions USD from Ethereum[6].

Blockchain has massive influnce on the many areas, particular in finance area. It is strongly believed that tokenization[7][5][2] is a new solution. Asset tokenization can reduce the cost, globalize the asset and increase the liquidation. We will see more dApps that require the use of these different tokens. As a result, an open standard for exchange is critical to supporting this open economy.

A traditional exchange platform is based on peer-to-peer IOUs and blockchain technology. Firstly, users need to deposit thier money or tokens into exchanges wallet or bank account, the their account will be credited some IOU. Thus, users actually are trading the IOU in the exchange. Users have to file a ticket when they want to withdraw or sell the tokens. In February 2014, World largest bitcoin exchange Mt. Gox suspended trading, closed its website and exchange service, and filed forbankruptcy protectionfrom creditors[8]. Mt. Gox announced that approximately 850, 000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $ 450 million at the time. Research showed less than 1We describe a protocol that facilitates decentralized exchange machanism of ERC20 tokens on the Ethereum blockchain to slove above issues. One of the strength for decentralization is not holding by any party, thus stolen becomes impossible, which can build up the trust bewteen customers and exchange at a very low cost. In addition, this machanism has no time and region limits, but highly transparent and traceable features. All those features make trasaction more liquidatable and minimize the price difference.

2 Market and Industry

There are some decentralized exchanges on blockchain technolegy like Ripple, BitShares, Openledger in open sourced community. Ripple[9]is areal-time gross settlementsystem, currency exchangeandremittancenetwork operated byRipple. Also called theRipple Transaction Protocol (RTXP)orRipple protocol, it is built upon adistributedopen sourceInternetprotocol, consensus ledger. Ripples solution is built around an open, neutral protocol (Interledger Protocol or ILP[10]) to power payments across different ledgers and networks globally. It offers a cryptographically secure end-to-end payment flow with transaction immutability and information redundancy. Architected to fit within a banks existing infrastructure, Ripple is designed to comply with risk, privacy and compliance requirements. BitShares[11][12] is an industrial-grade financial blockchain smart contracts platform. TheBitSharesdecentralized exchange - also known as The DEX is a next-generation cryptocurrency trading platform. The DEXis inherently decentralized, enabling you to trade the BitShares core token (BTS) and a range of trustless price-stable, market-pegged assets such as bitUSD, bitCNY, bitBTC, bitGold and more. These assets can all be traded withzerocounter-party risk, putting you in total control of your funds. However, Bitshares project has many limitations on itself. The OpenLedger Dex[13] is a cryptocurrency exchange. It allows users to exchange bitcoin into SmartCoins and then withdraw the smartcoins and convert them into cash through PayPal, Ripple or NanoCard. Additionally, openledger highly relys on BitShares 2.0 platform and Graphene Toolkits operation. The Bancor[14][15] protocol enables built-in price discovery and a liquidity mechanism for tokens on smart contract blockchains. These smart tokens hold one or more other tokens in reserve and enable any party to instantly purchase or liquidate the smart token in exchange for any of its reserve tokens, directly through the smart

tokens contract, at a continuously calculated price, according to a formula which balances buy and sell volumes. 0x[16] is a protocol that facilitates low friction peer-to-peer exchange of ERC20[17] tokens on the Ethereum blockchain. The protocol is intended to serve as an open standard and common building block, driving interoperability among decentralized applications (dApps) that incorporate exchange functionality. Trades are executed by a system of Ethereum smart contracts that are publicly accessible, free to use and that any dApp can hook into. DApps built on top of the protocol can access public liquidity pools or create their own liquidity pool and charge transaction fees on the resulting volume. While, 0x protocol has many limitations including, only accept simple OTC order; unclear competing mechanism among each exchanges; lack of protection mechanism for miners. Due to above reasons and limitation, centralized exchange is now still playing an important role in cryptocurrency market. Nevertheless, Our team has inspired by both 0x protocol and payment channel and brought up a new solution for decentralized exchange protocol.

3 Design Protocol

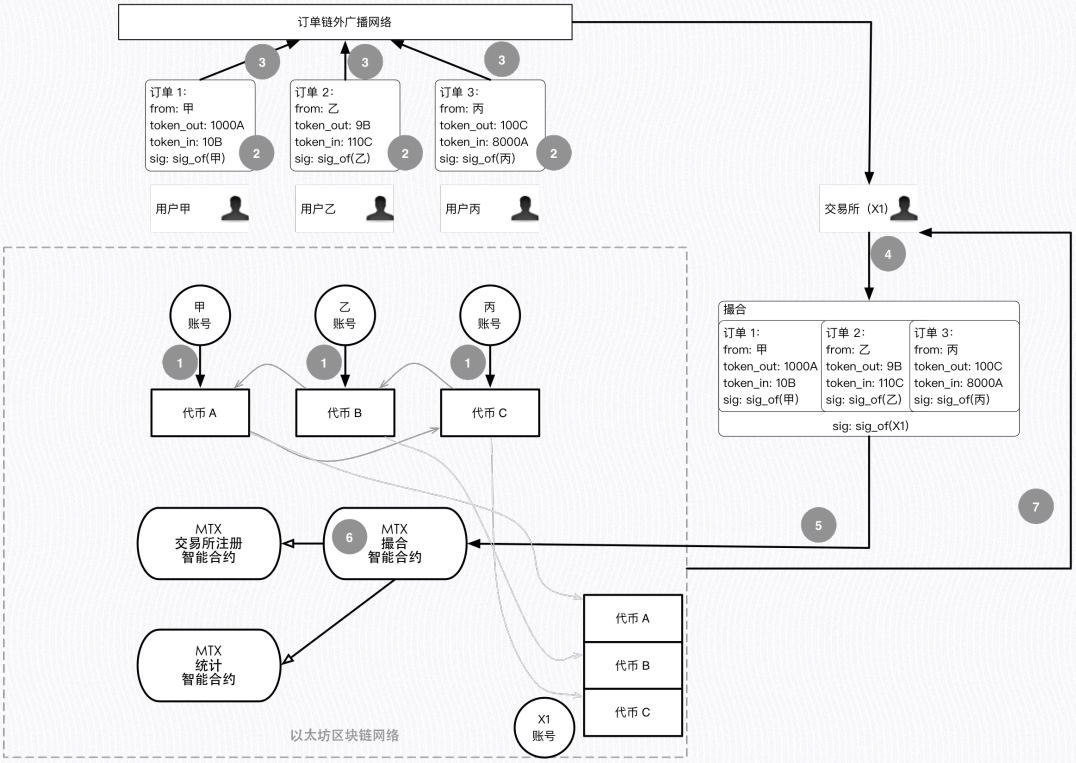

Figure 1: MTTPFigure shows mix and match 3 orders

Figure 1 presents the general sequence of steps used for three parties transaction under MTTP:

1. User A, B and C authorize MTTP matching smart contract to manipulate their account for token trading and exchanging. From figure, Contract will transfer out 1000 token A from User As account, and transfer out 9 token B from User Bs account, 100 token C from User Cs account;

2. User A, B and C place their own orders with signature on their private keys. Thus, all the orders go into a medium and ready to exchange - Order A is selling no more than 100 token A and purchase no less than 10 token B; if the order is partially matched, then exchange rate between A to B should be no less than 1000/10=100.00 (Selling

tokens divided by purchasing tokens). We will illustrate other involved parameters in chapter 3.7;

3. User A, B and C continue to send their order one of multiple exchanges;
4. After the exchange received three separate orders, they will replace them into corresponding orderbook, while update new block and calculate each orders status in order to match the set order - since we call it circulation exchange or matching exchange. Once all the orders are confirmed and successfully mix-matched;
5. Exchange will send out a signature to MTTP matched smart contract address;
6. Matching smart contract to verify quadruple signatures in order to verify three orders closing. If closing is failed, then terminate the conract(exchange still cost certain gas); vice verse, smart contract needs to calculate the proceed and cost for each users, then complete the token exchange. During the each steps, matching smart contract will use MTTP Registration Contract to calculate all the fees and discount; discount; before closing, system will also need to use MTTP Stats Contract to update database.
7. Exchange starts receiving new block and new data from the chain in order to upgrade the orderbook then to mix-match the orders.

3.1 Definition of Symbol

First we would introduce the definition of each symbol.

C_i: i is set of token.
$O_{i\to j}$: stands for selling a token, $C_j$stands for purchasing a token.
$s_{i\to j}$: number of token sold C_i.
$b_{i\to j}$: number of token purchased C_j.
$r_{i\to j}$: exchange rate, $s_{i\to j}/b_{i\to j}$.

We underlined the symbols to emphasis on their original numbers. For example $\overline{s}_{i\to j}$ and $\overline{b}_{i\to j}$ stands for number of token from the original order

3.2 Fixed order exchange rate

For instance, if the order is fully completed, $s_{i\to j} = 0$. Otherwise numbers will be showed as $s_{i\to j}/b_{i\to j} = \overline{s}_{i\to j}/\overline{b}_{i\to j}$, after MTTP updated: $r_{i\to j} = \overline{r}_{i\to j}$.

3.3 Agreement

We can use token C_j to connect two orders ($O_{i\to j}$ and $O_{j\to k}$), regard as a order for selling token Ci, other is purchasing order C_k. we use $O_{i\to j\to k}$ to display this order. Thus mix and match with order $O_{i\to k}$

$$s_{i\to j\to k} = min(b_{i\to j}, s_{j\to k}) \cdot r_{i\to j} \tag{1}$$

$$b_{i\to j\to k} = min(b_{i\to j}, s_{j\to k})/r_{j\to k} \tag{2}$$

$$r_{i\to j\to k} = r_{i\to j} \cdot r_{j\to k} \tag{3}$$

We will introduce a concept of ordering-chain. It contains two or more orders. Both two orders exchange same type of token except the last order. Additionally, final orders purchasing token should be differ from initial orders selling token (it will become a circulation if its same type of token).

$$s_{0\to\ldots\to n} = \begin{cases} s_{0\to 1} & \text{as } n = 1 \\ min(b_{0\to\ldots\to n-1}, s_{n-1\to n}) \cdot r_{0\to\ldots\to n-1} & \text{as } n > 1 \end{cases}$$

$$b_{0\to\ldots\to n} = \begin{cases} b_{0\to 1} & \text{as } n = 1 \\ min(b_{0\to\ldots\to n-1}, s_{n-1\to n})/r_{n-1\to n} & \text{as } n > 1 \end{cases}$$

$$r_{0\to\ldots\to n} = \prod_{i=0}^{n-1} r_{i\to i+1}$$

3.4 Mix and Match Trading

Centralized exchange happens between two kinds of tokens/currencies; However, MTTP exchange involves multiple tokens/currencies through connecting each orders to complete the exchange.

Definition 3.1 (Circular Trading) *Let C_0, C_1, $\cdots$, C_{n-1} be n different kinds of token, $O_{0\to 1}$, $\cdots$, $O_{i\to i\oplus 1}$, $\cdots$, $O_{n-1\to 0}$ be n orders. Those orders can mix and match with different kind of tokens for trading:*

$$O_{0\to 1} \to \cdots \to O_{i\to i\oplus 1} \to \cdots \to O_{n-1\to 0},$$

where n is the length of the circulation, and $i \oplus 1 \equiv i + 1 \mod n$.

Once the prices match the orders under circumstance, we could start to complete trading in this circle.

3.4.1 Price

We will introduce an example for a better understanding of price mechanism. Assume three kinds of token are C_0, C_1 and C_2, three separate orders$O_{0\to 1}$, $O_{1\to 2}$ and $O_{2\to 0}$. Easy to approve, as if $r_{0\to 1} \cdot r_{1\to 2} \cdot r_{2\to 0} = 1$, when three orders could complete the exchange. As $r_{O\to 1} \cdot r_{1\to 2} \cdot r_{2\to 0} > 1$. We named the first situation as `original matching`, Second as `discount matching`.

According to MTTP protocol, each order in the circulation would share the same price. For instance, if discount rate is γ, then price for each order will be: $r_{0\to 1}\cdot(1-\gamma)$, $r_{1\to 2}\cdot(1-\gamma)$, $r_{2\to 0} \cdot (1-\gamma)$, and satisfied

$$r_{0\to 1} \cdot (1-\gamma) \cdot r_{1\to 2} \cdot (1-\gamma) \cdot r_{2\to 0} \cdot (1-\gamma) = 1 \tag{4}$$

We can find out

$$\gamma = 1 - \frac{1}{\sqrt[3]{r_{0\to 1} \cdot r_{1\to 2} \cdot r_{2\to 0}}}.$$

In the other circumstance, if transaction cross n orders, `discount rate`

$$\gamma = 1 - \frac{1}{\sqrt[n]{\prod_{i=0}^{n-1} r^i}},$$

where r^i is the order turnover rate of i-th order.Obviously, only when the discount rate is $\gamma \geq 0$, transaction can be completed; and i order's O^i actual exchange rate $\hat{r^i} = r^i \cdot (1-\gamma)$, $\hat{r^i} \leq r^i$.

3.4.2 Volume

To find out the lowest value order can help to figure out the total volume. For instance, i is the lowest value order, then number of token sold from each order $\hat{s}$ and number of token brought $\hat{b}$ from each order can be find:

$$\begin{aligned}
&\hat{s}^i = \overline{s}_i,\ \hat{b}^i = \hat{s}^i/\hat{r}^i,\ ;\\
&\hat{s}^{i\oplus 1} = \hat{b}^i,\ \hat{b}^{i\oplus 1} = \hat{s}^{i\oplus 1}/\hat{r}^{i\oplus 1};\\
&\hat{s}^{i\oplus 2} = \hat{b}^{i\oplus 2},\ \hat{b}^{i\oplus 2} = \hat{s}^{i\oplus 2}/\hat{r}^{i\oplus 2};\\
&...
\end{aligned}$$

where $\overline{s}_i$ is the the balance left after order partially traded.

3.4.3 Cost and Fee

Exchanges normally charge transaction fee. For instance, we assume fee will be calculated in MTTP token MTC, order ID is i and total fee for completing the transaction is m^i

$$f^i = b^i \cdot m^i/\overline{b^i}$$

In order to encourage exchange to offer best rate for the users, MTTP would distribute profit from `cost saving` to the exchange. as an order O^i, if price for purchasing is b^i($b^i \leq \overline{b^i}$), then we define the from saving cost

$$\Delta^i = b^i \cdot r^i \cdot \gamma$$

If MTTP requires every order to set up a saving cost distributing rate θ^i, and minimum distributing ratio is Θ. Then order O^i should pay to exchange

$$f^i = \Delta^i \cdot \Theta = b^i \cdot r^i \cdot \gamma \cdot \Theta$$

Since the income from cost saving among each matching trade:

$$F = \sum_{i=0}^{n-1} b^i \cdot r^i \cdot \gamma \cdot \Theta$$

In order to encourage MTC usage, if the order has no preset token fee m^i, or $m^i = 0$, then the actual ratio is 100%, regardless of the relevant hash in this order. As if none of the order has set up this rate $\Theta = 100\%$, then all proceeds from the saving will go into exchange.

In next chapter, we will introduce a token pledge policy, smart contract will list out each exchanges depositing tokens and rank them up. Secondly calculate a `mandatory discount cost` for each exchange, λ, this figure will affect the total cost. Meanwhile, exchange can also offer some discount, η. Total cost for completion a full trading

$$F = (1-\lambda)\cdot(1-\eta)\cdot\sum_{i=0}^{n-1}(b^i \cdot r^i \cdot \gamma \cdot \Theta + b^i \cdot m^i/\overline{b^i})$$

3.4.4 Discount

MTTP requires exchange platform offering discount for each transaction, discount fee depends on the number of deposit token MTC. The higher the rank, the lower fee will charge; For example Rank n's cost will be:

$$\lambda_n = 0.05 \cdot (\ln(n + e - 1) - 1).$$

Details below:

Deposit Ranking n	cost for discount λ
1	0%
2	1.57%
10	7.31%
20	10.39%
99	18.06%
100	18.11%
1000	29.55%
1001	30.00%*

Table 1: Deposit MTC Ranking and cost for discount

For those exchanges ranked under 1001 and those undeposited exchanges, 30% cost will apply.

Figure 2 shows, $\lambda_2 - \lambda_1 \gg \lambda_{100} - \lambda_{99}$.

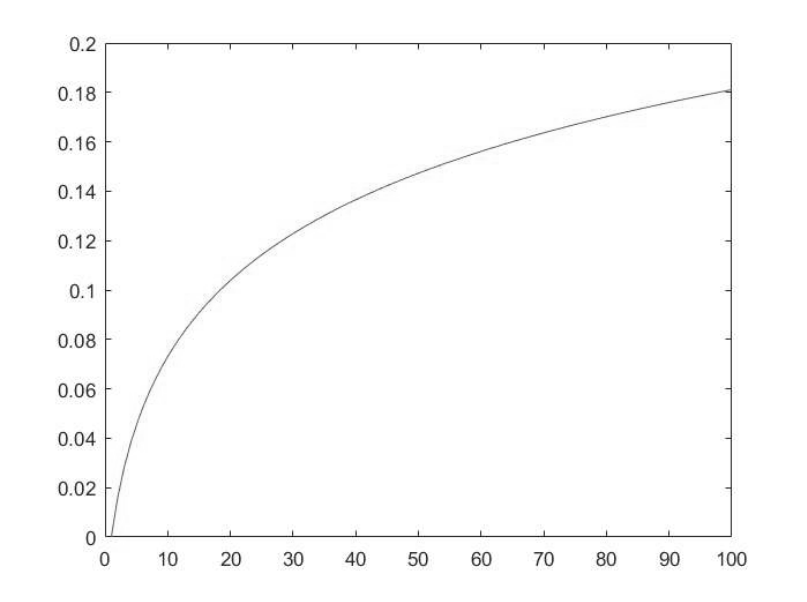

Figure 2: MTC token deposit rank and cost for discount

3.5 Fraud and Attach Protection

3.5.1 Exchange Covered Interest Arbitrage

MTTP is trying create a fair ecosystem and find a balance between customers and exchanges. Firstly, we will explain how exchange could archive a zero risk covered interest arbitrage.

Assume there are two orders $O_{a\to b}$, $O_{b\to a}$, form a loop, $r_{a\to b} \cdot r_{b\to a} > 1$. Exchange can input three new orders between those two. $O_{b\to c}$, $O_{c\to d}$, $O_{d\to b}$, to create a five orders-loop, $r_{a\to b} \cdot r_{b\to c} \cdot r_{c\to d} \cdot r_{d\to b} \cdot r_{b\to a} = 1$. Exchange could make all the possible cost down to zero, once the transaction completed, it's like zero risk covered interest arbitrage and $O_{b\to c} \to O_{c\to d} \to O_{d\to b}$. In order to stop those matter, MTTP requires**verified loop must not be able to create more sub-loop to trade**.

3.5.2 Rejection Service

MTTP allows exchange to select the order. Order can be sort by token, quantity, number and others. Condition can be modified, hidden or public.

3.5.3 Mass Small Order

User can send out mass small orders to attach the exchange. Due to tiny profit from those orders, exchange would reject most of them.

Few exchanges can use same method to attack other exchanges. However this would not work in MTTP ecosystem.

3.5.4 Insufficient Balance

Multiple order can be sent out at one time, while the account balance is actual zero. Thus, even those orders been sent to exchange. Exchange would detect the zero balance account and pause the transaction. This action could increase large time cost. In conclusion, set up regulation to block those suspicious account in the future.

3.5.5 Trade Matching Filch

A dodgy exchange could monitor those unclosed deal from the internet. In order to protect us from cyber-fraud. We require exchanges to complete two steps in order to submit the order

- A transaction has saved on blockchain, and update the record,
- Data has been recorded on blockchain, exchange provide detailed info.

Hash rate:

$$h = H(r, nonce),$$

where $H()$ is a one-way hash function, r is order record. Hash Hash function contains a random number *nonce*.

3.6 Market Insights

Exchange no need to offer market depth data. Under this ecosystem, both single organization and corporation can possibly pool all the un-closed orders into one market depth data. We can find out trading data between any two ERC20 tokens according to the argreement in chapter 3.3.

3.7 Database Formula

All the orders can be illustrated into one module due to adopting OTC module. This module contains both digital signature and all parameters. Before the signature, connect the parameter data from the orders into a set data, calculate the orders hash by using Keccak SHA3 methodolgy, then sign on this accounts private keys with ECDSA.

```
message Order {
 address protocol;
 address owner;
 address outToken;
 address inToken;
 uint256 outAmount;
 uint256 inAmount;
 unit256 expiration
 unit256 fee;
 uint8 savingShare;
 bytes signature;
}
```

Though theres no indicated price from the order, but we are still able to find out through the formula: $outAmount/inAmount$ to get exchange rate r. All the actual exchange rate must be less than r. A user-friendly exchange should allow user to input $outAmount$, $inAmount$, selling and asking price and use any two of those numers in order to calculate the missing $outAmount$ $outAmount$ figure.

Actual orders can be defined in two different ways: Definition A - transaction can be completed once number of token sold reaches $outAmount$; Definition B - transaction can be completed once number of token purchased reaches $inAmount$; Therefore, we can setup a quote for exchange and mix-matching contract to help to define the trade. At our initial version, we would pre-set Definition A method.

Exchange could create a circular trading from below date:

```
message Match {
  Order[] orders;
  address fee Recipient;
  unit256 additional Discount; // eta
  bytes signature;
}
```

3.8 Order Status

Order cannot be modified since its been signed and announced. Data will be updated on the blockchain once smart contract find the matched order. Thus $inAmount$ and $outAmount$ will modified in corresponding with updated price. If $inAmount/outAmount$ shows 0, it means the order has been fully closed. For example, if the user wants to cancel the order, a special request will be filed, $inAmount/outAmount$ will be 0 to close the order. An expired order will not be updated on the blockchain - it can be tracked through the final cutting time. Hence, we expect most of the orders will be expired or invalided.

3.9 Smart Contract

MTTP consists of many smart contracts, including:

- **Mix-Matched Contract**is responsible for ensuring each order status in the loop, calculating the price and volume, transferring and interactionwith other smart contracts, API for MTTP;
- **Order Contract**update order database and support cancelling policy;
- **Registration Contract**maintain and upgrade service for exchanges who accepted MTTP, support the token deposit from exchange and defaulted parameters backup;
- **Stats Contact**calculate the exchange volume and price between two tokens.

4 Token MTC

We will issue a token base on ERC20 Ethereum Token Standard called MTC(display in italics).

4.1 Token Application

MTC will be use in below areas

- **Gas Fees** — MTC can be used for transaction fee for exchange. It will be easy and productive for the exchange to calculate all the cost in MTC. Same as request sender and receiver. We have mention this from previous chapter3.4.3.

- **Deposit for Exchange Registration** —Decentralized exchange mechanism has no limits on location or time. Thus, those high turnover exchange would receive more orders and get more users. Hence, we have setup a policy for those exchange that allow them to use MTC to deposit into smart contract in order to increase exchange's credibility. Moreover, it can also protect user from certain circumstance.

4.2 Decentralization Mechanism

Regulation has been updated as well as exchange's mechanism. Any MTC holders have the voting power S, and number of the pledging N and pledging time $CoinAge$

$$S = f(N, CoinAge),$$

where $CoinAge = H_c - H_s$. Joining CoinAge is to protect customers from speculations.

Decentralized mechanism include token registration, exchange registration, stat hash, deposit scale, maximum length, discount hash, subcontract address.

- **token registration** MTTP would adjust token, low trading volume will be eliminated and new popular token will be replaced. however all the adjustment have to be recorded on smart contract.
- **exchange registration** Only those exchanges accept MTTP would allow to start trading.
- **stat hash** Data will increase to certain amount after a long period operating. The more data exchanges have, the more accurate system computation ability has.
- **deposit scale** Deposit for each exchange should be scalable. if the amount is huge, the liquidation gets worse; verse vice.
- **maximum length** Technically, more orders can create more profit, however the risk of failure also increase. As well as the trading cost.
- **discount hash** Discount hash will be adjust with the market. Below figure shows, blue line represents normal market, yellow line represents supply market, red line represents demand market.

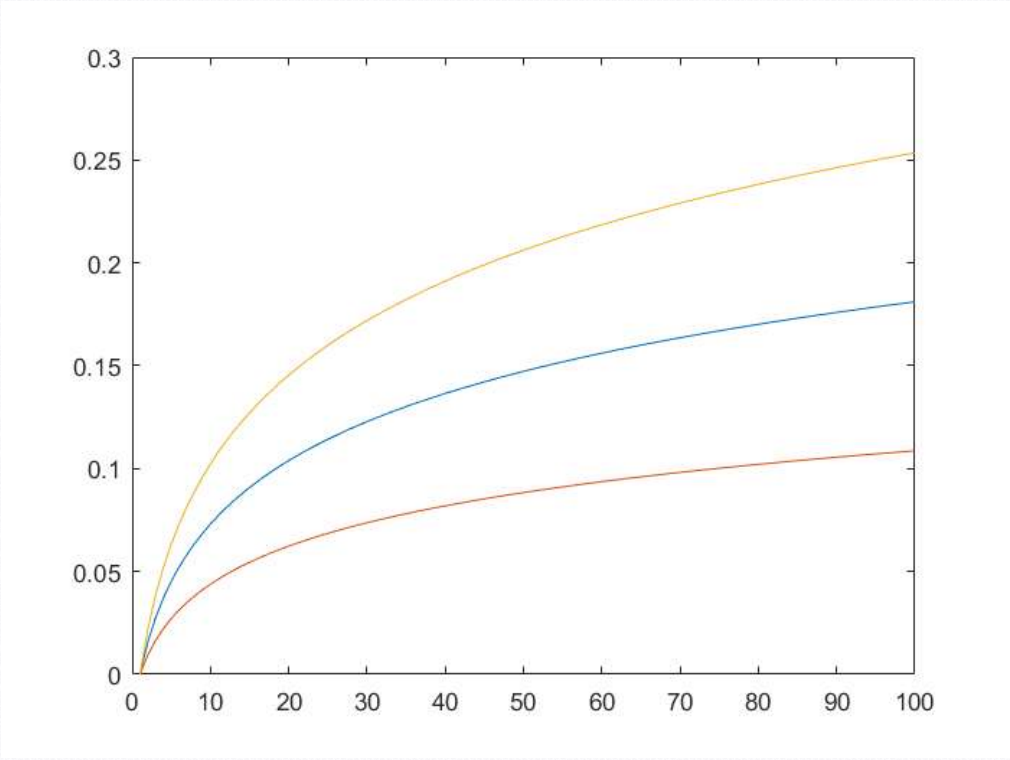

Figure 3: discount rate after adjustment

- **subcontract address** If MTTP exchange based on Ethereum ecosystem, then smart contract cannot be modified. Therefore, update MTTP's subcontract in order to modify subcontract address.

4.3 Tokens Liquidation

MTTPs token is based on ERC20 Ethereum Token Standard and it can be liquidated through MTTP smart contract. It means MTC trading can be made out of centralized exchange. All the ERC20 Ethereum tokens can be exchanged to MTC token(assume pre-order is MTC, with zero fee) by adopting MTTPs decentralized mechanism.

5 Exchange

Exchange is unable to guarantee all the transaction could make profit after adopted MTTP. First reason is high operating cost. Secondly, high expectation cannot match the actual outcome. There are few other reasons would cause this sutuation. Overall, both exchange platform and other parties have reciprocal relationship: exchange looks for profitable order; while order senders look for exchange with lowest fee. Exchange is not responsible for users ERC20 token after accepting MTTP. The workload has move from money despit, withdraw, internal virtual account management to mix-matched order service. Meanwhile, for the users, MTTP does not require customer to deposit or lock any asset, that means asset have zero risk to get stolen, at same time single order can mix and match multiple trades. For Non ERC20 asset, exchange can offer asset tokenization service.

5.1 Comparing Regular and MTTP Exchange

In a regular exchange, Maker send a order and Taker receive order. The exchange price highly depends on senders end. Under MTTP circumstance, it has adopted Over-The-Counter (OTC) module. In current market, there is considerably high risk for users to trade

in those platform, no law to regulate the exchange if they vanish. But with MTTP, users do not to deposit money to the exchange anymore. All the transactions will be made among users coin address. Another feature for MTTP is that it has change the Trading Pairconcept. Transaction can be completed with multiple paries instead of 2 parties in current exchange.

	Centralized Exchange	MTTP Exchange
Deposit for the order	Yes	No [1]
Frozen Account	Yes	No [2]
Deposit/Withdraw	Yes	No [3]
Internal Trading Risk	Yes	No[4]
Customer loss from exchange closing	Yes	No[5]
Transaction is the main income	Yes	No[6]
Accept Legal Currency	Yes	Yes[7]
Can be traded among multiple exchanges	No	Yes [8]
Fairness for Maker and Taker	No	Yes [9]
Mix and Match Trading	No	Yes[10]
Supervision	Strong	Weak[11]

Table 2: Contrast between centralized exchange and MTTP exchange

6 Summary

We describe a protocol that facilitates decentrazlized exchange of ERC20 tokens on the Ethereum blockchain. MTTP allows multi token transaction exchnage, as well as it accepts exchange liquidation on blockchain; This whitepaper has explained how the mechanism work under different circumstance. In additional, the benefit that MTTP has brought to current exchange mechanism. MTTP protocol fits any ERC20 and smart contract blockchain platform. After many discussion, our team will develop MTTP on the Ethereum blockchain. We also plan to create a non profit foundation for MTTP through crawdsale and issue ICO.

7 Acknowledgements

We would like to express our gratitude to our mentors, advisors and to the many people in the community that have been so welcoming and generous with their knowledge. In particular, we would like to thank Xing, Jiang; Xiaochuan Wu; Zhen, Wang and Jun, Ma for reviewing and providing feedback on this work. We are also welcoming more feedbacks from community.

[1]MTTP — , ..
[2]MTTP — , .
[3]MTTPMTTP, .
[4]MTTP, , .
[5]MTTP, — ., ..
[6]MTTP, , .
[7]MTTP, ERC20.
[8]MTTPMTTP, .
[9]MTTP, Maker.
[10]MTTP, .
[11]MTTP, ., .

References

[1] Economist Staff. Blockchains: The great chain of being sure about things. *The Economist. Retrieved*, 18, 2016.

[2] Melanie Swan. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[4] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[5] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[6] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151, 2014.

[7] Paul Tak Shing Liu. Medical record system using blockchain, big data and tokenization. In *Information and Communications Security*, pages 254–261. Springer, 2016.

[8] Robert McMillan. The inside story of mt. gox, bitcoins 460 dollar million disaster. 2014.

[9] David Schwartz, Noah Youngs, and Arthur Britto. The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5, 2014.

[10] Stefan Thomas and Evan Schwartz. A protocol for interledger payments. *URL https://interledger. org/interledger. pdf*, 2015.

[11] Fabian Schuh and Daniel Larimer. Bitshares 2.0: Financial smart contract platform.

[12] Fabian Schuh and Daniel Larimer. Bitshares 2.0: General overview, 2015.

[13] Open ledger. *URL https://openledger.info/*, 2017.

[14] Bancor protocol. *URL https://bancor.network/*, 2017.

[15] Robin Hanson. Logarithmic markets coring rules for modular combinatorial information aggregation. *The Journal of Prediction Markets*, 1(1):3–15, 2012.

[16] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain, 2017.

[17] Fabian Vogelsteller. Erc: Token standard. *URL https://github.com /ethereum /EIPs /issues /20*, 2015.