USDX: A Decentralized Monetary Policy System

Richard Tiutiun

Lucas Porco

Michael Gord

Dennis S. Lee

White Paper version 4.0.12 （February 18, 2018）

Draft for open review and subject to change.

Contents

Abstract

USDX is committed to developing the third generation stablecoin ecosystem, and is committed to becoming the infrastructure of the future blockchain economy, making the blockchain economy more simple, convenient and warm.

Bitcoin and other cryptocurrencies have attracted the attention of speculators because of volatile prices. However, cryptocurrency is difficult to be widely used because of the price fluctuations and will never become a popular medium of exchange, and it is difficult to build a financial and ecological system based on it.

The first generation of stablecoins, such as Tether, was widely used in the early days, relying on centralised companies to charge dollar mortgages and issue stablecoin. But the regulatory risk of moral hazard makes this model unsustainable.

The second generation of stablecoins, such as Havven, relied on a centralised mortgage network to encourage participants to mortgage cryptocurrencies and gain stablecoins, solving moral hazard, but creating new problems with insufficient collateral.

The third generation stabilization program adjusts market exchange rate stability through 「Seigniorage Shares」 to issue or contract the supply of tokens. The implementation of monetary policy depends only on the exchange rate data obtained by decentralization, not the governance of the centralized subject.

Compared with other third-generation stablecoin schemes, USDX relies on excellent technical strategies and economic research implementation:

1. Based on Proof of Stake, it has high speed and convenient transaction efficiency and strong ductility.
2. Infrastructure compatible with existing cryptocurrencies (such as exchanges, wallets, miners)
3. A comprehensive and systematic regulation mechanism provides strong support for stablecoin fluctuations.
4. Focusing financial ecological strategies, we will build up a financial system based on cryptocurrency together with third-party developers.

Keywords: price stability, stablecoin, monetary policy, decentralization

1 Introduction: The rise of stablecoins

Price volatility has long been a big problem for cryptocurrency users, and a lot of people have already taken double-digit intraday percentage fluctuations as an

investment price. As a matter of fact, the price of Bitcoin surged from about $7,000 to $20,000 in the last two months of 2017[1]. Today's cryptocurrency is more like digital gold for speculation than a daily medium of exchange. Although the market has always been so volatile, the key to the problem is not to make money or lose money, but the users of the encrypted money can't get rid of the price fluctuation until the stable coin appears.

Users who send bitcoins, whether to exchanges or individuals, have to accept the delays caused by distributed bookkeeping. It usually takes hours to fully confirm the bitcoin transaction, but the price has changed dramatically during the same period. This not only for the average trader at risk, and makes it challenging to do any business with bitcoin - What kind of business owners pay suppliers in an currency with extremely volatility? Because most exchanges refuse to use the fiat currency, the fluctuations of cryptocurrency are indeed a nuisance.

Stablecoin provides a smart solution for the market: a cryptocurrency that is always worth $1. There is also a stablecoin pegges to the euro, but the concept is the same: a way of protecting people from volatility in the world of cryptocurrency.

Tether is currently the largest stablecoin by market value, with private ownership of the dollar and the right to control the new issue of Tether, ensuring Tether's value is linked to the dollar, and to be converted back and forth depending on the market. However, Tether has recently been subjected to intense scrutiny for its transparency and legitimacy.

Supporters of stablecoin want to find an alternative mechanism to control the stability of the exchange rate by decentralizing monetary policy to release and contract the liquidity of the entire stablecoin system. This approach, which does not rely on the principal credit of any institution, avoids moral hazard and regulatory risk and opens new possibilities for stablecoin in the coming months.

2 Why we need stablecoin?

2.1 Cash

Stablecoins are usually pegged to the dollar and can be used as a medium of exchange, a value scale and a store of value in the blockchain world.

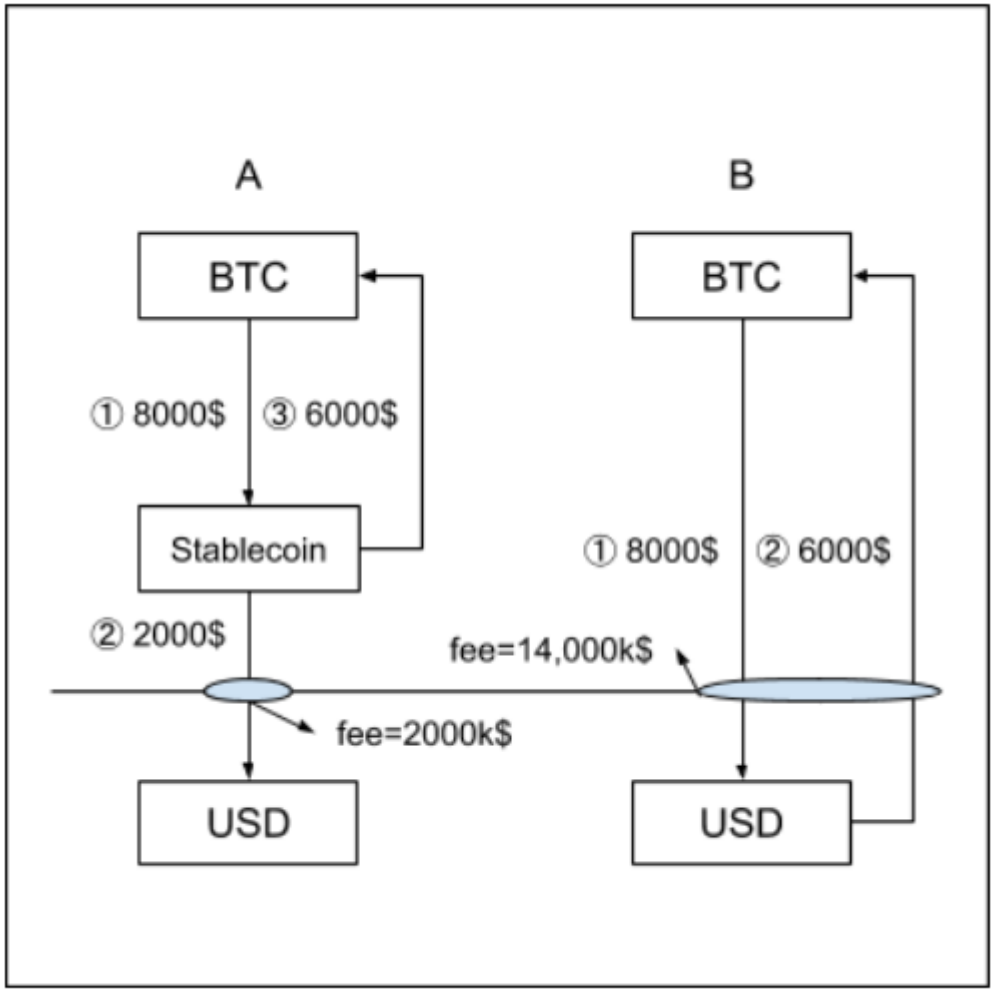
The cost of moving legal currencies in and out of the cryptosystem is very high, so when investors do not want to hold any encryption currency, they prefer to "park" their investments in an cryptocurrency as stable as cash., namely a stablecoin.

As an example, as shown in the figure below, assuming that the bitcoin fell, the user needs to sell the equivalent of $8,000 worth of bitcoins for fiat currency, $2,000 of

[1] https://coinmarketcap.com/currencies/bitcoin/

which may be withdraw for cash, and the remaining $6,000 will eventually enter the market and be used to buy the cryptocurrency. We assume that the handling fee between the cryptocurrency and the fiat currency is k, and the handling fee between two cryptocurrencies transaction is negligible. In the first case, the total amount of fees that the user needs to pay is 2000k; In the second case, the user pays a fee of 14000k, which is seven times worse.

As countries become more tightly regulated in terms of cryptocurrency, for example, k can reach 5% in some countries in Asia.



With the rise of decentralized application, stablecoin is also very suitable for the payment of decentralized application. Decentralization is more like a stock, with purchasing power unstable and the popularity of the price greatly influenced by the application itself so it is not suitable for payment in general use. In addition, a token that can be used for different applications is much more convenient than having a token for each application. The stablecoin can be used as a medium of exchange to meet the payment needs of the central application.

2.2 Freedom

We believe there are two types of people who buy cryptocurrency today.

The first group of people with similar equity investment mentality, some for speculation, some for value investment, but in any case is to make gains through the surge of cryptocurrency. The second group is more concerned with the use of value, and the cryptocurrency can help them achieve the free exchange of wealth and the value of freedom.

In a country with foreign exchange control, the government manages the free flow of wealth while managing the free flow of information. In the former case if the government manages well, even very clever hedge funds can't get their money out of the country; But in the latter case if the government lacks effective management, even if it has already sent some VPN developers into jail, it will not be able to prevent more than a third of employees in the financial and Internet industries from “get over the wall”.

In fact, cryptocurrency effectively reduces the difficulty of free circulation of wealth to the difficulty of free circulation of information.

Making wealth as free as information is the mission of cryptocurrency. Ultimately, users of the cryptocurrency must be those who value its value in use, not the financial investors. But for those who value its value in use, the volatility of cryptocurrencies, such as bitcoin, is the biggest hurdle. If there is a secure currency at this time, there is no doubt that they will win.

fiat currency	Not Free	Stable
BTC/ETH	Freedom	Unstable
Stablecoin	Freedom	Stable

2.3 Ecosystem

Count how much of your wealth is spent on consumption, and how much is invested -- and there is no doubt that investing is the most important use of wealth. For holders of cryptocurrency, the biggest difficulty in investing in financial products is not knowing how to price them. If A uses 1 BTC to invest in a fiat currency based bond fund managed by B today, the yield of the fund will be 10% after 1 year, but the BTC has jumped 100%, and A can only buy back 1.1/2=0.55 BTC. If the BTC plunges 50 percent, A will eventually buy back 1.1/0.5=2.2 bitcoins.

The volatility of bitcoin makes it almost impossible to use it to invest in any asset denominated in fiat currency, and it turns any asset into a derivative combining two kinds of volatility. Stablecoin can reduce the friction cost in the transaction, making the whole financial system more efficient.

In the ecosystem of the stablecoin, there will emerge a series of companies that move fiat currency based investments to blockchain world. Maybe in the near future,

you can use the stablecoin to buy U.S. stocks, A-shares, bonds, gold, real estate, even to buy equity in Space X, or to invest in some VC funds.

With stablecoin being widely used, many users and data will be accumulated, which will lead to exciting new business models. Because the community is open to all, it will inspire the imagination and creativity of teams around the world. To accelerate this process, we will incubate, invest and collaborate on different projects, develop various virtual assets, and create a truly decentralized, virtual world with enormous economic value.

3 The evolution of stablecoin in three generations

After studying the history and current situation of stablecoin, we first put forward the evolution logic of three generations of stablecoin. History tells us that the third generation stablecoin is the final form of stablecoin.

Collateral-backed IOU	Tether/Sweetbridge/Arccy
Collateral-backed on-chain	Maker/Havven/Augmint/BitShares
Seigniorage Shares	Basecoin/Fragments/Carbon/Kowala

3.1 Collateral-backed IOU

The first stablecoin is Tether, which is the same company as Bitfinex, and the issued token is called USDT. Take an "inappropriate" analogy, just like when you enter a casino and you need to change your chips, the USDT is what you need to use when you enter an exchange to buy and sell a cryptocurrency.

Why do people trust USDT? If you pay the Tether company 1USD, they will print 1USDT notes for you, Tether said. If you find Tether with 1USDT, he will give you another 1USD. That is to say, Tether promised to exchange, investors and partners that the USDT exchange rate would always be pegged to USD, through a private company commitment.

In the early days, Tether did what he said, in a bank account in Taiwan, where he kept the equivalent of the dollar reserves in place. This is the first stablecoin in the history of cryptocurrency, fulfilling its promise to traders and helping all participants operate more easily and efficiently. The USDT became the medium of exchange between fiat currency and cryptocurrency, helping to invest money in the young cryptocurrency market. However, some dubious events have affected the credibility of Tether. There are two big inevitable questions during Tether's development: moral hazard and regulatory risk.

Moral hazard refers to the fact that Tether's account is not regulated, and it is likely that Tether release the USDT without any collateral. As with the Bretton Woods

System, the dollar eventually decoupled from gold. So who can guarantee that one day the USDT and USD will not be decoupled? All the people who use and hold USDT are betting their money on the credibility of Tether. Once Tether oversupplies USDT, all the holders will suffer from it.

Regulatory risk refers to that since any legal currency that Tether collects can only be placed in one bank account., Tether's account could be frozen at any time for fear of cryptocurrency or for other reasons, such as Anti-Money Laundering (AML).[2]

Tether did not provide the data for auditing even after the deadline, which led to the accounting firm cutting off all ties with the company, and the market's confidence in Tether was shaken. In addition, astute analysts have found that when the price of bitcoin falls, a lot of USDT is produced, most likely being released out of thin air without collateral. Policy risks have emerged and, according to Tether officials, a Taiwanese account has been frozen.

As these events have demonstrated, the biggest problem with Tether is its centralization. Since there is only one entity authorizing the currency, Tether is opaque and cannot afford to play an important role in money markets.
If the audit proves the fraud behavior of Tether, it will pave the way for the world's end of cryptocurrency. Users will immediately realize that the value of the stablecoin they hold is artificially inflated and eager to sell. It is certainly not acceptable for users to take a certain risk when they use a stablecoin, which is not likely to gain the benefits of inflation.

3.2 Collateral-backed on-chain

Collateral-backed on-chain solves these problems by issuing a price-stabilised token against a distributed collateral pool which derives its value from the utility of the system. Fees are levied on transactions, and they are dispersed proportionally among collateral holders.

Because the collateral is a cryptocurrency rather than a fiat currency, it can be mortgaged with a smart contract to circumvent the moral hazard of the first generation of stablecoin. By the way, because there is no need for a bank account to hold collateral, it also avoids the regulatory risk of the first stablecoin.

But the second generation of stablecoin bring new problems. As collateral, cryptocurrencies are extremely volatile. If the value of the collateral becomes less than the value of the stablcoin, system immediately becomes unstable.

Volatility can easily destroy the market before the stablecoin is widely used and influential.

[2] https://tether.to/announcement/

3.3 Seigniorage Shares

The first two generation of stablecoin schemes are based on mortgage, and their common features are: When the current amount of money is too small to ignore moral hazard, the model of their stablecoin can be easily trusted.

But when the amount of money is large enough, they will be abandoned by the people because of the insuperable mechanism.

In contrast, the third generation stablecoin scheme adjusts market exchange rate stability through 「Seigniorage Shares」 issuance or contraction of the supply of tokens. In the early days, because of the complexity of the mechanism and the volatility of exchange rates, it was hard to be trusted by most people (like bitcoin in 2010); But when market liquidity reaches a certain level, the algorithms based on the exchange rate will be very effective. More importantly, there is no centralised moral hazard in the third generation of stablecoin until the end, which means that, Once the critical point of a certain market liquidity is reached, the stablecoin will become more and more recognized such as BTC, which will have eternal vitality.

Many in the industry are trying to create a third generation of stablecoin, but the most viable is USDX.

Our vision is to create a stablecoin with fast trading speed, low transaction costs and price stability to be widely used in daily transactions. The price of a stablecoin can be pegged to any particular value index through flexible supply of intelligent adjustments. We believe that the stablecoin represents the next generation of cryptocurrency, the general trend towards decentralization and diversification.

4 What is USDX?

USDX defines a decentralized monetary policy system by anchoring certain asset prices and enabling a self-balancing mechanism to ensure stablecoin prices. The specific self-balancing mechanism will be introduced in the next chapter.

The following is a detailed description of the two phases of USDX development:

4.1 Phase 1: Genesis Phase

The first stage is called the Genesis Phase. It will produce a token based on Ethereum ERC 2.0, called USDX. USDX is not a stablecoin, but represents the holder's interest in USDX ecosystem. USDX is limited in number and does not have the self-balancing mechanism of stablecoin. USDX trades on the open market, the price will be free to rise and fall and reflect market expectations of USDX, and the

rise in the price of the token will indicate the market is full of hope for the future of USDX.

In addition, during the Genesis Phase, our specialized community management team will do all it can to expand the foreign exchange and cooperation relationship of USDX as well as continue to promote the listing of USDX tokens on all major exchanges around the world. By actively disseminating knowledge and building a strong and active community with users and developers; And support the development of USDX infrastructure by using funds raised during the Genesis Phase.

4.2 Phase 2: Stable Phase

The second stage is called the Stable Phase. Along with the completion of the development work and the establishment of the exchanges and developer cooperation, an independent public chain will be created, called USDY, the time of which is called the pegging day. USDY is a stablecoin anchored to the dollar, with a self-balancing mechanism of stablecoin, and the price always fluctuates around one dollar. In the future, decentralised monetary policy will dominate the expansion and contraction of USDY, which will depend only on changes in the price of USDY/USD rather than any human operation. As a public chain, it has its own token, mining network and smart contracts.

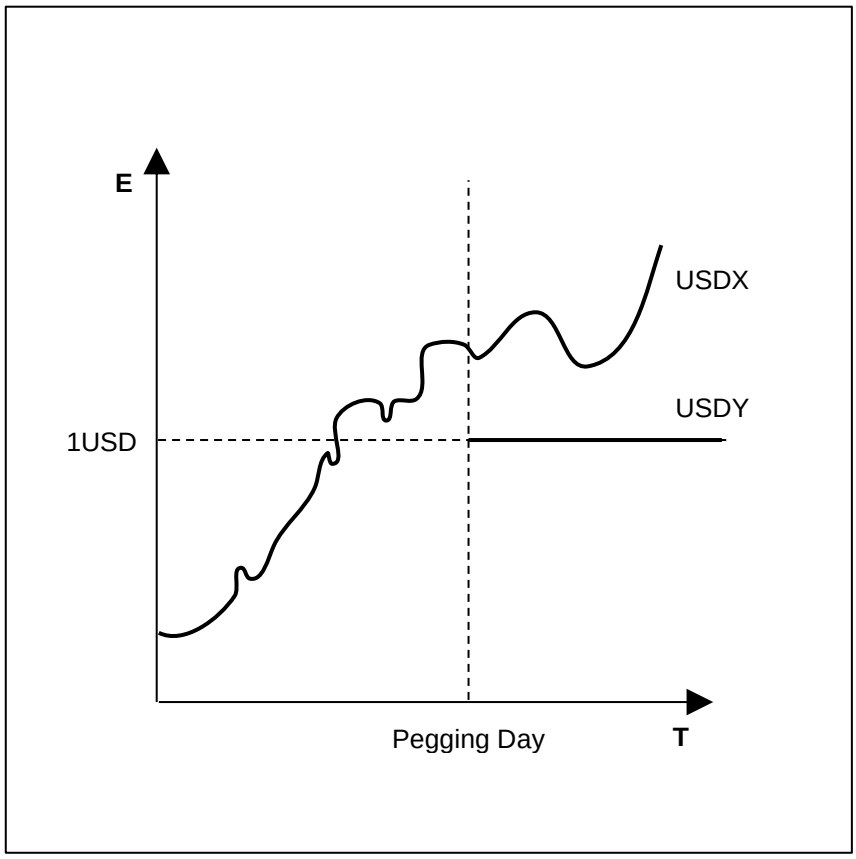
USDY's public chain is based on the Proof of Stake (POS) mechanism. The advantages of POS are fast transaction speed and low transaction cost. Users can mine the POS on a dedicated wallet, mining it through laptops, mobile phones and even cloud services, without the need for a lot of electricity and expensive equipment.

	Token/Public Chain	Price Stability	Initial Acquisition	Quantity
USDX	Token	No	ICO	Limited Supply
USDY	Public Chain	Yes	Assigned to USDX's holder	Elastic Supply

At the beginning of the creation of USDY, the initial USDY will be generated, which quantity is equal to the market value of USDX in dollar terms at that time. Each USDX holder will obtain the initial USDY by the proportion holding USDX, for example:

1. Tom bought 100 USDX at $0.2 / a price for $20.
2. On the pegging day, the price of one USDX is $4. Tom will receive 100*4=400 USDY. USDY is widely used with excellent self-balancing mechanism and trading speed. The price is stable at 1USD and has good liquidity. Tom has 400 USDY dollars worth $400.

3. While receiving USDY, Tom will continue to hold USDX. Tom can sell each USDX for $4 with total price of $400, or hold for long term, and in the future receive other stablecoins based on USDX currency policy .



Since the dollar is the most widely accepted fiat currency in the market for a certain period of time, the strategy of pegging the dollar was adopted at the beginning of the model design. Once USDY is widely used and support, according to the voting of the community, the foundation will launch stablecoins pegging on other legal currencies (such as JPYY, EURY), and allocate to the holders of USDX in accordance with the above method. Our ultimate aim is hoping to build a SDRY (Special Drawing Rights is the currency combination defined by IMF, representing the basket of reserve currencies including dollar, euro, yuan, yen and pound), to provide a simple, convenient and warm currency scheme for people of the countries such as venezuela, Nigeria who lack of stablecoin as a medium of exchange.

5 USDY’s self-rebalancing mechanism

5.1 The only goal of monetary policy is price stability

In real economies around the world, monetary policy is conducted by central bank and therefore centralized. This centralization, while effective, could still cause problems.

Monetary policy is controlled by central bank officials. Although there are various guiding principles, but it is impossible to eliminate human discretion. A discretionary policy is subject to time inconsistency, which may lead to shortsightedness (local optimal) rather than global best. This is the tendency to deviate from long-term planning when making short-term decisions. In addition to price stability, maximum employment is also an important objective of the real world monetary policy. Policy makers are always advocating an expansionary monetary policy, which increases output in the short term and reduces unemployment in order to make them more likely to win the next election. But in the long run, it comes at the expense of inflation. Moreover, centralized monetary policy is prone to single failure.

Therefore, monetary policy must be decentralized and supervised by the whole community. The only goal of USDY's monetary policy is price stability, eliminating the trade-off in dual mandates. Here is how the USDY agreement implements decentralized monetary policy:

5.2 The economics of price stability

5.2.1 The theory of purchasing-power parity (PPP)

The mechanism of USDY's exchange rate with the dollar is consistent with the fiat currency, based on the theory of purchasing-power parity. The exchange of two currencies is essentially the exchange of purchasing power represented by two currencies: the exchange rate is the purchasing power of the two currencies in their respective countries.

Under free trade, the same goods are equivalent in each market.

Because the unit of money is different, the price of the same commodity in different currencies has been converted at the equilibrium exchange rate, and eventually it is equal. For example, the price of gold in New York is $1,250 an ounce, while London's price is 823 pounds per ounce, and E stands for the pound against the dollar. So based on purchasing power parity: $1225 =E * 823.

In the theory of absolute purchasing-power parity, P represents the general price level of the local currency market, P* represents the general price level of the foreign currency market, and E represents the exchange rate of local currency to foreign currency. You can get: P* is equal to E x P.

So under the absolute purchasing-power parity theory we can express the exchange rate as:

$E = (p*)/p$

P* as the general price level in the fiat currency market is an input value which cannot be regulated, so the adjustment of the exchange rate can only be adjusted by P.

But many markets usually report only price indices, not absolute prices in their own currencies. If the price index does not have any units, absolute purchasing-power parity cannot be used. While relative purchasing-power parity agrees that the exchange rate reflects the change of the purchasing power of each countries' currency, and the exchange rate changes in proportion to the relative changes in the price level of the two countries in the same period.

It's expressed as this formula. : $E_1 = \frac{P_1/P_0}{P_1^*/P_0^*} \times E_0$

E1: current exchange rate level.

E0: base exchange rate.

P1: current market price index of A currency.

P0: base period A currency market price index.

P1: current B currency market price index.*

P_0: base period B currency market price index.*

If the price of a piece of cloth in the UK rose from 1 pound to 2 pounds, but in the United States rose from $2 to $6, then the exchange rate between the pound and the dollar's will be from £ 1 = $2, to £ 1 = $3.

It's expressed as this formula. : $E_1 = \frac{6/2}{2/1} \times 2 = 3$

For a market, all the values have been produced during the base period, cannot be controlled, and the price index of the foreign currency market is not regulated, so it can only control the price index of the local currency market. The price index comes from the comparison between the current price level and the base price level, and the price level of the base period has been fixed, so the adjustment of the price index is still back to the adjustment of the general price level in the current period.

From the above theory, it can be concluded that the key to regulating E is to adjust the general price level P.

5.2.2 The quantitative theory of money

The quantitative theory of money is the cornerstone of monetarism. It shows the direct relationship between the amount of money in the economy and the price level, and can be the basis of the elastic supply of our stablecoin.The equation is illustrated by John Stuart Mill, who expands on David Hume's idea. The algebraic formulation comes from Irving Fisher, 1911.

$$M \times V = P \times T$$

M: total quantity of money in the economy

V: the velocity of money

P: the price level

T: aggregate output]

This approach can be rewritten as follows:

$$P = \frac{MV}{T}$$

When we consider the impact of monetary policy on cryptocurrency prices, we assume that T is generally stable as output. The adjustment of P is only affected by M and V, and E is affected by P. To sum up, when we need to adjust the size of E, we can do it by adjusting M and V.

Take USDY as an example, M stands for the total amount of USDY in the market, and V represents the number of times each USDY changes hands every year, USDY/USD=E, namely:

1. If E is greater than 1, we need to increase M or increase V, so that E goes down to 1.
2. If E is less than 1, we need to decrease M or decrease V, so that E goes up to 1.

From the actual operation, the biggest risk is that the users do not trust USDY and start the run, which is the case when E is less than 1, so it needs to decrease M or decrease V. This is a challenge that needs to be addressed in the following Seigniorage Shares. A large number of third generation stablecoin policies in the market have a good effect in adjusting the situation of E > 1, but the effect is very poor when the adjustment of E is less than 1. We're going to talk about how we reduce M or V in the following chapters.

5.3 The mechanisms to adjust M and V

In the beginning, we set 3 mechanisms to adjust M and V. Mechanism 1 is Variable Block Reward, which adjusts block reward to increase M. Mechanism 2 is Mining locking, which sets time of lock in the mining process to reduce M. Mechanism 3 is

Variable Transaction Fee, which changes the rate of transaction fee to reduce V. We may adopt decentralized governance of community and introduce new mechanisms to increase robustness of stablecoins.

	M	V
Increase	Mechanism 1	×
Decrease	Mechanism 2，Mechanism 3	Mechanism 3

5.3.1 Mechanism 1: Variable Block Reward

Since USDY is based on POS mining mechanism, most of the holders will participate in POS verification and earn block rewards. Mechanism 1 can increase the total amount of currency in circulation (M) by regulating block rewards, thus affecting the price of USDY/USD.To illustrate variable block reward, we need to clarify the following concepts:

InitialReward: initial block reward, set as 30.
M: the growth rate of block reward, set at 1%.
cap(b): the upper limit of block b
minReward: the lower limit of block reward
E(b) : the market exchange rate corresponding to block b.

E(b) represents the price of USDY/USD, which is monitored and provided by Oracle Please refer to the following section about Oracle.

The calculation of variable block reward is as follows:

$$\text{reward}(b) = \begin{cases} \text{initialReward}, & \text{b} = 1 \\ \max\left((1+m)reward(b-1), cap(b)\right), & \text{b} > 1, \text{E(b)} > \text{E(b}-1) > 1 \\ \min\left(\frac{1}{1+\text{m}}\text{reward(b}-1), \text{minReward}\right), & \text{b} > 1, \text{E(b)} < \text{E(b}-1) < 1 \\ \text{reward}(b-1), & \text{otherwise} \end{cases}$$

We divided the rewards into four stages according to E(b):

- Initial stage: the reward of the creation block is equal to the initialReward.
- Rising stage: during this stage, Oracle monitored the E(b) >1 and showed a rising trend, and the stablecoin was in short supply. Therefore, the block award is needed to be increased to increase the stablecoin supply. In this case, the block award is increased by m times compared to the previous block, and the block reward does not exceed cap(b). By increasing the reward(b) of the block, the total amount of money in circulation can be increased by M, so that E(b) decreases and approaches 1.
- Decline stage: during this stage, Oracle monitors E(b)<1 and presents a decreasing trend, stablecoin supply exceeds demand, so it is necessary to reduce the block award to reduce stable money supply. In this case, the block award is reduced by m times compared with the previous block

reward, and the block reward is not less than minReward. By reducing the reward reward(b) of the block, the growth rate of the total amount of money in circulation can be reduced, so that E(b) rises and approaches 1.

- Convergence stage: if E (b) does not meet the requirements for the above three stages of judgement, this indicates that the previous block award has made the change direction of E(b) consistent with the target, so the block reward is consistent with the previous block.

5.3.2 Mechanism 2: Mining locking

In most cases, however, contraction is much more difficult than expansion, as can be seen in the experience of the fiat currency market and in the study of central bank monetary policy. During the declining stage, E(b)<1, even the block reward approaches 0, it is difficult to make E(b) rise and return to 1.

To solve this dilemma, we introduced another mechanism called mining locking. When E(b)<1, in the descending stage, the variable block reward of mechanism 1 has been reduced to the lowest value, but the decline of E(b) has not slowed down. At this point, mechanism 2 will be activated, and users can choose to take part of the funds in the wallet to participate in the mining locking project. The funds involved in the mining locking will be frozen (possibly 7 days) and also into the POS mining status. The frozen funds are not free to circulate, reduce M, effectively help E(b) rise and approach 1.

Miners who are not involved in mining locking and miners who are involved will work simultaneously to ensure a steady flow of blocks. In order to encourage the holders to participate in the mining locking, a series of mechanism designs will increase the probability of the miners who participate in mining locking. In addition, the newly generated blocks will also generate special block rewards (different from variable block rewards) to attract the holder to take part in mining locking.

The lock is not continuous but divided in to 3 situations according to the following judgement:

$$\text{lockintime}\ (b) = \begin{cases} 7\text{days}, & count.c(b,1440) \geq 200, count.t(b,1440) \geq 800 \\ 30\text{days}, & count.c(b,10080) \geq 1500, count.t(b,10080) \geq 5500 \\ 180\text{days}, & count.c(b,43200) \geq 4000, count.t(b,43200) \geq 20000 \end{cases}$$

Count. c (b,d) refers to the number of contiguous E(b)<1 blocks which is d blocks prior to block b; Count. t (b,d) is the total number of E(b)<1 blocks which d blocks prior to block b.

If E(b) enters the above convergence stage, it is indicated that mechanism 2 works well and the policy of mining locking will cease.

5.3.3 Mechanism 3: Variable Transaction Fee

In order to control the supply of USDY more effectively, we introduced variable transaction fees, which are used to change the velocity of currency (V) and the total amount of USDY in circulation (M).

The transaction fee is a special fee charged to the sender of each transaction. According to the following formula:

$$Transaction\ fee\ =\ Gas\ +\ Circulation\ Cost$$

Here, Gas costs are calculated by USDY and will be paid to the miners. Because USDY uses the POS mechanism and will run on its own chain based on its own Gas measurement, Gas costs will be much lower than ETH and BTC.

Circulation Cost = the amount of USDY during transaction *circulation cost rate (ranging from 0.001% and 2%, and it is just a small part of the total amount of transaction)

The following is how we calculate circulation cost:

When USDY price is equal to 1 usd 1, the system will automatically calculate a circulation cost rate, as a %, and according to the value of the volatile prices of USDY automatically adjust a. Thus by changing the cost of circulation to change the velocity of USDY circulation. (the upper limit of this value is 2%, and the lower limit is 0.001%)

The following is how USDY changes a%:

We define b as the block with serial number b, c(b) is the circulation cost rate of USDY in block b, and p(b) is the price of USDY in block b, and p '(b) is the price change rate of USDY in block b.

$$a\% = \begin{Bmatrix} \min(1.034c(b-1), 0.02), p(b) \preccurlyeq 1, P`(b) \preccurlyeq 0 \\ max(1/1.034c(b-1), 0.00001), p(b) \succ 1, P`(b) \succ 0 \end{Bmatrix}$$

Here, 1.034 is the constant that we have calculated through the existing data modeling, and then we will continue to optimize our model.

P'(b) is defined by the following equation:

$$p`(b) = \frac{\sum_{i=b-n}^{b} p(i)(i - b + 0.5n)}{\sum_{i=b-n}^{b} i^2 - (b - 0.5n)(n + 1)}$$

The generation of each block takes 1 minute, and we calculate every n block.

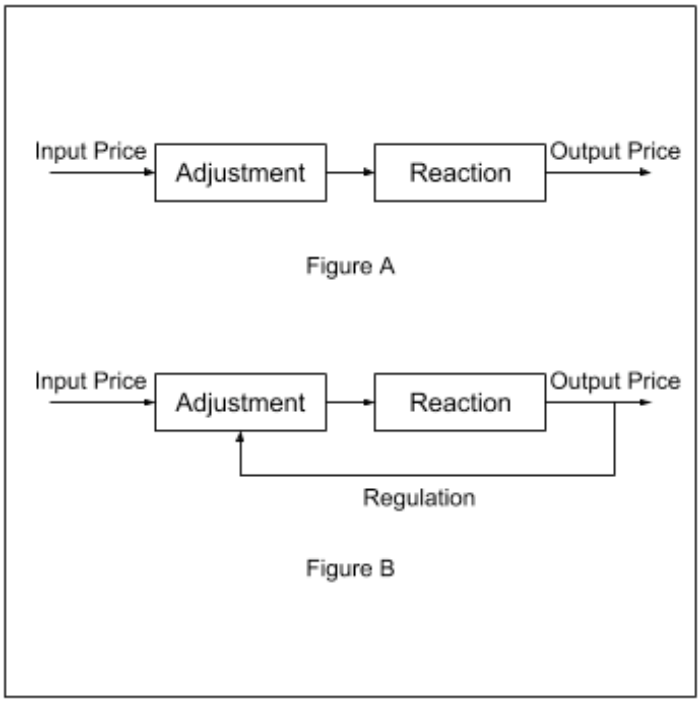
The mechanism of variable transaction costs regulates the frequency of market participants' trading activities, thus regulating the velocity of USDY. At the same time, the system pays the miners the part of Gas in the transaction cost, puts the part of the circulation cost into the dead end address, adjusts the M and V at the same time, and finally realizes the adjustment of the price of USDY/USD. When M and V need to

increase, circulation costs will be reduced; When M and V need to be reduced, circulation costs will increase.

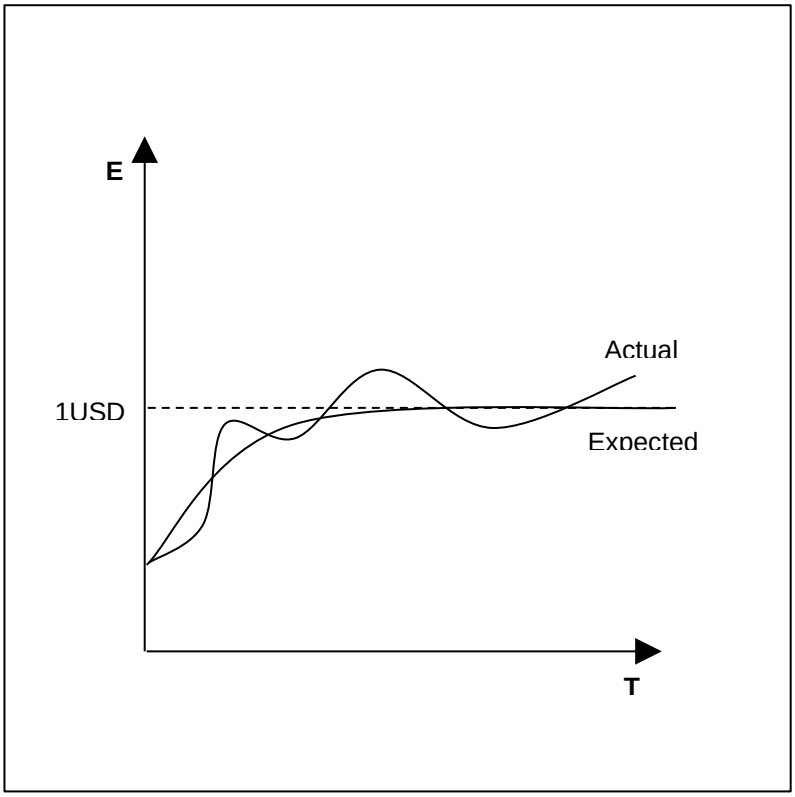
5.3.4 Negative Feedback Mechanism Improves the Accuracy

Since different monetary policies have different effects under different conditions, the impact of different monetary policies is also complicated, and it is impossible to control the amount of regulation precisely. Fortunately, we can reduce the requirement for accuracy in the initial design by means of negative feedback. The system changes the adjustment quantity through the feedback on the price adjustment of USDY/USD continuously, and finally achieves a high precision.

We think there is a causal relationship between monetary policy and stablecoin prices, in figure A, the input-output relationship represents the causality of the process, but there is no feedback mechanism in the open loop system. In figure B, the introduction of the feedback enable us to control the system and get the expected output. It also improves the precision of the monetary policy, but it also requires us to give enough attention to the stability of the system response.



The following diagram shows a price response curve of stablecoin. Even if the initial control is biased, it can be corrected by the negative feedback system in real time, so that the price can change to the correct degree, and finally ensure the accuracy of the regulation.



5.3.5 Free Market Improves the Efficiency of Mechanisms

In a free market, we are less demanding of the efficiency of the mechanism. Therefore, by implementing these three mechanisms and taking some time, the price of the dollar will return to the parity level, which means that USDY's exchange rate of USD, labled as E, is equal to 1. We believe that this is the primary impact of the return of the USDY price. In addition, if the primary impact has been recognized by the market participants, we think there will be several implications.

In the beginning, because the price of USDY itself tended to be 1 USD, the parity level was the focus of the game. In this case, the USDY is highly likely to remain at parity (1USDY=1USD) because of the lack of adequate communication and trust among the participants at the parity.

In addition, professional arbitrageurs can actively help push prices back to parity and make profits when prices and parity are skewed. Such opportunities are created by the patience and wait of professional arbitrageurs, while the average users will worry about the price deviation in the short term. Although professional arbitrageurs are operating for their own profits, their trading helps improve the efficiency of the return to parity.

Last but not least, participants' confidence in the price self-balancing mechanism will push prices back to parity with the history of the return of market prices to parity.

Because the free market has the perfect USDY/USD trading market system, the implied self-regulation effect will be stimulated, and the self-interest behavior of market participants such as miners, users and USDY changers will accelerate USDY back to parity.

5.4 Decentralized Oracle Data Source

In order for the system to function properly, it needs to obtain the exchange rate of stablecoin to the fiat currency, and the data is outside the blockchain. We have designed a decentralized Schelling point oracle system that is fully integrated with the DPoS consensus to provide these key data. It is safer than existing methods and introduces less overhead and complexity to the blockchain system.

Problems with existing solutions:

Single Trusted Data Source: this is the first attempt to introduce external data onto the blockchain. Typically, a single trusted party is responsible for collecting external data and supplying the blockchain application. This is a fully centralized service. Although the changes in the encryption trace are required, and the authenticity of Oraclize is provided (for example, https://docs.oraclize.it/#security-deepdive-authenticity-proofs-types) to ensure data integrity, verification can only be conducted under the chain and after the event. In addition, there is no way to prevent data providers from cheating by delaying data sources or not providing data sources at all.

Delegated Decentralized Data Source: One example is the distributed data source in BitShares, where each DPoS node provides the data source and the BTS token holder needs to monitor the data source provided by each node. Once a bad person is found, the token holder should actively switch to other honest nodes so that the bad person can be removed. This process is theoretically valid, but in practice most users are not capable or interested in constantly monitoring node behavior, and there is no immediate incentive.

Schelling Point Mechanism: First of all, Vitalik is introduced in his concept of SchellingCoin https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/. The basic idea is to design a decentralized incentive scheme to motivate participants to provide accurate data. It allows anyone to submit data to the blockchain and rewards data that provides within the middle range (for example, between 25% and 75%). Providing reliable data sources in a completely decentralized manner is a good idea, and the only drawback is that the design adds extra overhead and complexity to the system.

Considering the problem of the above solution, we propose a hybrid design combining the concept of Delegated Decentralized Data Source and the Schelling Point Mechanism. In this system, each node participating in DPoS has the obligation to provide data source, and only nodes that provide data in the center can be eligible to receive mining rewards. Details of the design will be announced later, after a more thorough experiment.

6 What’s the problems with Other stablecoins?

In order to solve the problem of price fluctuation, many stablecoins were born, such as USDT, SmartCoin, and Dai. However, these stablecoins do not really achieve price stability and decentralization.

Tether

Tether is based on the parity of the fiat currency, which means that every new USDT will have one USD to be stored in Tether's bank account as a reserve. This guarantees Tether's ability to redeem the legal currency at any time. Yet because the company is in full control of the money supply and reserves, the model is essentially centralized. Company itself is not trustworthy, and reports have pointed out that due to a lack of verification, there are millions of tokens that don't have a legal currency. Tether was also subject to a hacking attack that resulted in the theft of $30 million in tokens. Moreover, because its mortgage reserves are in regulated bank accounts, it will be subject to government regulation.

BitShares

There are two tokens in the BitShares system, BTS and SmartCoin, which can be traded in BitShares internal exchanges. SmartCoin is a kind of stablecoin, which can peg various assets and circulate with BTS as collateral. The SmartCoin pegged to USD is called BitUSD. However, if the price of the BTS as a result of the black swan event is relative to the collapse of the pegged asset, then the mortgage backed system will be very fragile.

Maker DAO

The token for MakerDAO is called Dai and is based on mortgage. Anyone can get Dai on the Maker platform with a mortgage value of twice Dai's Pooled Ether (PETH). For the same reason, Dai's mortgage mechanism is also very vulnerable, and Dai's market value will be limited by collateral.

Basecoin

Basecoin uses a three-token model which includes Base Share, Basecoin and Base Bond. The supply of Basecoin is elastic while the supply of Base Share is fixed. When the supply of Basecoin contracts, it triggers the Base Bonds to recycle and destroy the Basecoin; When the Basecoin supply expands, the new Basecoin will first repay the Base Bonds, and the rest will be assigned to the Base Shareholders. The three-token model may work in theory, but they expose complex problems when traded on exchanges.

In addition, Basecoin does not have a network effect, and the only way to increase revenue for Basecoin holders who do not have Base Share is to buy Base Bonds when supply contracts, which could limit Basecoin medium and long-term

development. Since the Base Shares represent a permanent distribution rights for newly-generated Basecoin, the Base Share market is likely to be much more popular than Basecoin, which will weaken the stablecoin, the Basecoin status.

Carbon

Carbon claims that it can achieve instantaneous callbacks by freezing part of the 「wrapped coins」, and the participants themselves choose whether to「package」their currency and by how much. If the total amount of the「wrapped coins」does not meet the instantaneous correction, the Carbon reserve will start to buy back the coin and「package」it. Let's not talk about the effect of the Carbon reserve buyback, but the reserve itself is like a centralised part, which goes against the principle of decentralization.

In addition, Carbon does not take into account the velocity of money, which can make Carbon more reliable and stable.

		Tether	MakerDAO	BitShares	Basecoin	Carbon	USDX
Generation		1st	2nd	2nd	3rd	3rd	3rd
Token or Public Chain Coin		Token	Token	Token	Token	Token	Public Chain
Economic Machanism	Add M	/	×	×	√	√	√
	Reduce M	/	×	×	√	√	√
	Add V	/	×	×	×	×	√
	Reduce V	/	×	×	×	×	√
Technology (1-3stars)	Effectiveness	★★★	★	★	★	★	★★★
	Simplicity	★★★	★★	★★	★	★★	★★
	Scalability	★	★	★	★	★	★★★

*M represents total supply of money, V represents velocity of money.

]

7 Team

Our team includes experienced entrepreneurs, developers, and experienced blockchain industry and financial industry consultants.

USDX team

Richard Tiutiun

Richard is a fanatical blockchain tech genius and hacker born in Ukraine. He specializes in languages such as Android, JavaScript, Java, iOS, jQuery, and Python. After dropping out of the UC Berkeley, he designed and developed the XOR project and the stablecoin laboratory, focusing on the next generation of money.

Lucas Porco

Lucas is an experienced lawyer focusing on the compliance of blockchain and cryptocurrency. He is a Ph.D. candidate in Law at the University of Toronto and is deeply involved in the legal framework of several virtual currency projects. He is now in charge of the USDX's economic model, legal framework and compliance.

Michael Gord

Michael is an entrepreneur and an expert on blockchain and smart contract technology. He is the founder of Bitcoin Canada and the McGill Cryptocurrency Club. He has a degree in entrepreneurship, marketing and information systems at McGill university's Desautels Faculty. At McGill university, Michael organized Bitcoin Airdrop events, where he got hundreds of students to get their first Bitcoin. In the USDX project, he is responsible for strategic planning, business development and cooperation with regulators, Banks and other institutional sectors.

Dennis S. Lee

Dennis s. Lee is a serial entrepreneur and cryptography evangelist. He is a developer of INK Business and has a flair for marketing and branding. He has a lot of experience in Business development and is an outstanding planner.

7.1 USDX R&D Support Team

Hash Hao (Researcher)

Hash Hao, graduated from Columbia University, is a serial entrepreneur and Fintech expert. He succeeded in starting and running a series of projects. He has worked in investment Banks and hedge funds in New York and Beijing.

Steven Li (Researcher)

Steven Li, graduated from the university of Toronto, is a serial entrepreneur and angel investor who founded and managed three VC funds. He was the chief investment officer of Qihu360.

Connor Huang (Researcher)

Connor Huang is a fintech expert focusing on risk management and monetary policy. He used to work at China Renaissance and Alibaba and has accumulated rich experience in investment banking and Internet marketing.

Chen Nie (Development)

Chen nie, graduated from the university of Toronto, is the chief engineer at BCG Digital Ventures and an expert in trading strategies, investment analysis and engineering.

7.2 Advisors

Hon. Ernie Eves

Mr. Eves, founder and chairman of the GIC group, has a distinguished career in both the public and private sectors. Mr. Eves has a very rich experience in investment and management, and has a very unique understanding of foreign exchange market, international trade and monetary policy. Mr. Eves was called to Ontario after graduating from Osgoode Hall Law School in 1972, and in 1983 he was appointed to Queens Counsel, and in 2015 he was awarded an honorary doctor of Law degree by the University of Windsor.

Jim De Wilde

Dr. Jim de Wilde is a famous venture capitalist and management educator and has managed and invested over $5 billion. He has been working on the commercialization of early-stage technologies through JdW Strategic Venture since 1993. He has a Ph.D. in political science and is a tenured professor at McGill University with a dissertation focusing on the Canadian public policy process and competitiveness in technology sectors.

Motoko Eio

Mr. Motoko Eio, graduated from Tokyo university, was an economic adviser to the Japanese central bank and was involved in the formulation of Japan's monetary policy.

Alan Wunsche

Alan is CEO & Chief Token Officer of TokenFunder, a regulatory-compliant blockchain venture funding platform with Ontario's first regulated Initial Token Offering. He is also Chair & Co-Founder of Blockchain Canada, a Canadian federal not-for-profit corporation with a mission to connect Canadian Blockchain Innovators and to help Canada be a leader in blockchain technology. Alan is a finance technologist focused on new blockchain business models and the disruptive impacts of blockchain on global wealth distribution. He brings hands-on technology experience as a finance and risk transformation executive at a global bank (Scotiabank), management consulting (Deloitte, PwC), and startups.

Alex Mashinsky

Mr. Mashinsky is one of the main evangelists on the web exchange and is considered one of the early developers of VoIP, currently the CEO of Celsius. He is a famous entrepreneur who has founded many companies including GroundLink, Transit Wireless, Elematics and Arbinet for many years. As an entrepreneur, Alex's

success is rooted in his ability to identify successful trends and the formation of world-class teams. Two of his companies, Arbinet and Transit Wireless, have become monopolies in their respective fields, becoming pioneers in new business models and technology applications.

Xiahong Lin

Xiahong, graduated from purdue university's statistical machine learning direction, is the founder of Bodhi's prediction market and has developed the android version of Twitter.

Patrick Dai

Patrick, founder of the Qtum, has abundant experience in blockchain technology and has been active since 2012 in blockchain industry. He is so fascinated by cryptographic software at the bottom of bitcoin and other digital currencies that he has abandoned his PhD in communications and information systems that have not been completed in the Chinese Academy of Sciences. Patrick's influence helped Qtum get the support of the most prominent people in the blockchain community.

Jason Fang

Jason, the founding partner of Sora Ventures, is the soul of silicon valley's Alchemist Accelerator and Startupbootcamp. He worked for distributed capital and matrix finance.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Sams, R. (2015). A Note on Cryptocurrency Stabilisation: Seigniorage Shares. Working paper.

[3] Fisher, I. (2006). The Purchasing Power of Money: Its' Determination and Relation to Credit Interest And Crises. Cosimo, Inc..

[4] Mishkin, F. S. (2014). The economics of money, banking and financial markets (11th ed.). Pearson.

[5] Qtum's Decentralized Governance Protocol [Blog Post] (2017, June 6). Retrieved January 25, 2018, from Qtum: https://qtum.org/en/blog/qtum-s-decentralized-governance-protocol

[6] Al-Naji, N., Chen, J., & Diao, L. (2018). Basecoin: A price-stable cryptocurrency with an algorithmic central bank [Whitepaper]. Retrieved January 25, 2018, from Basecoin: http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf

[7] Kuo, E., & Iles, B. (n.d.). Fragments: A platform for stable consumer tokens. Retrieved January 25, 2018, from Fragments: https://www.frgcoin.com/about/

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

[9] Paul Tak Shing Liu (2016). Medical record system using blockchain, big data and tokenization. In Information and Communications Security, pages 252–264. Springer.

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

[11] Smart contracts: https://en.bitcoin.it/wiki/Contracts

[12] Reusable proofs of work: http://www.finney.org/~hal/rpow/

[13] Ben-Sasson, Chiesa, Garman, Green, Miers, Troma and Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014.

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