USDX: A Decentralized Monetary Policy System

White Paper version 4.3 (February 28, 2018)

Richard Tiutiun
Lucas Porco
Michael Gord
Dennis S. Lee

Abstract

USDX is committed to developing the third generation Stablecoin ecosystem, to make the blockchain economy simpler and more convenient and to become the backbone infrastructure of the future blockchain economy.

Cryptocurrencies' rapid rise and promising future has attracted great attention from speculators and, increasingly, from Wall Street. There are rising expectations among academics and investors that virtual currencies will revolutionize the current financial system. However, the high volatility associated with traditional cryptocurrencies like bitcoin has crippled their adoption as a public medium of exchange.

Stablecoin was invented to solve the high volatility problem of traditional cryptocurrencies. It is a special type of cryptocurrency that has its valued pegged to an index-most typically, the equivalent of one US dollar.

The first generation of Stablecoin, represented by Tether, relies on a centralized and collateral-based model where, in theory, one Stablecoin is issued only when one US dollar is deposited at the Stablecoin issuer. However, regulatory risk and moral hazard have rendered this model unsustainable.

The second generation of Stablecoin, such as Havven, also employs a collateral based model, where virtual currency instead of fiat is mortgaged on a decentralized blockchain network for the issuance of Stablecoin. While solving the regulatory and moral hazard problems, this model has created new issues with fluctuant collaterals and more complicated mechanisms.

The third generation of Stablecoin relies on an 'algorithmic central bank' to automatically adjust the total quantity and velocity of Stablecoin to achieve a stable exchange rate. The implementation of elastic monetary policy is strictly data dependent and will not subject to the governance of any centralized party.

USDX is a third generation Stablecoin. Compared to other third generation Stablecoins, USDX differentiates itself in terms of its cutting-edge technology and robust algorithmic logics derived from economic principles. Specifically, USDX possesses the following 4 unique features:

1. USDX is a public blockchain based on 'Proof of Stake' with high transaction speed

2. USDX is compatible with existing blockchain infrastructures, such as cryptocurrency exchanges, wallets, and miners

3. USDX has a sophisticated and systematic adjustment mechanism that can efficiently regulate price fluctuations

4. USDX's infrastructure was built with a goal in mind to serve as the center of the next generation blockchain-based financial system. We will build up a crypto-based financial system together with third-party developers

Keywords:price stability, stablecoin, monetary policy, decentralization

Contents

1 Introduction:
The rise of stablecoins 4
2 Why do we need stablecoin? 4
2.1 Cash 4
2.2 Freedom 5
2.3 Ecosystem 6
3 The evolution of stablecoin in three generations 7
3.1 Collateral-backed IOU 7
3.2 Collateral on blockchain 8
3.3 Elastic monetary policy based 8
4 What is USDX? 9
4.1 Phase 1: Genesis 9
4.2 Phase 2: Stable 9
5 USDY's self-rebalancing mechanism 11
5.1 The economics of price stability 12
5.1.1 The theory of purchasing-power parity (PPP) 12
5.1.2 The quantitative theory of money (QTM) . . . 13
5.2 The mechanisms to adjust M and V 14
5.2.1 Mechanism 1: Variable Block Reward 14
5.2.2 Mechanism 2: Lock in Mining 15
5.2.3 Mechanism 3: Variable Transaction Fee 15
5.2.4 Adjustment Accuracy Improved by Negative Feedback Mechanism 16
5.2.5 Mechanisms' Efficiency Improved by the Free Market 18
6 Infrastructure 18
6.1 POS Consensus Mechanism 18
6.2 Decentralized Oracle Data Source 19
7 What are the problems with other stablecoins? 20

Reference **23**

1. Introduction: The rise of stablecoins

Volatility has almost been a synonym of cryptocurrency and market participants have become accustomed to the double-digit intraday percentage fluctuation. For example, the price of Bitcoin surged from about $7,000 to $20,000 in the last two months of 2017[1] . Cryptocurrencies today are treated more like 'digital gold' for speculation rather than as a medium of exchange. It's not just about making or losing money in the market-users of cryptocurrencies must endure large price swings even when they do not wish to take an exposure.

When exchanges or individuals make a transaction in Bitcoin, they must accept the delays caused by distributed bookkeeping. It usually takes hours to fully confirm the transaction and the price will typically change dramatically during the same period. This makes it challenging to conduct any business with Bitcoin. After all: what kind of business would pay suppliers in a currency with such volatility?

Stablecoin provides an intelligent solution for the volatility problem: a type of cryptocurrency that is always worth 1 US dollar or Euro. It is a way of protecting people from volatility in the world of cryptocurrency.

USDT is the largest Stablecoin by market cap today. The issuer of USDT, Tether, takes dollar deposits and controls the new issue of USDT. It ensures USDT's value is always linked to the dollar and that it will be converted back and forth depending on the market condition. However, Tether's transparency and legitimacy have recently come under intense scrutiny.

Supporters of Stablecoin want to find an alternative mechanism to achieve stability in the exchange rate, by releasing and contracting the liquidity of the entire Stablecoin system through decentralized monetary policy. This approach, which does not rely on any individual institution, avoids moral hazard and regulatory risk and opens up new possibilities for Stablecoin in the coming months.

2. Why do we need stablecoin?

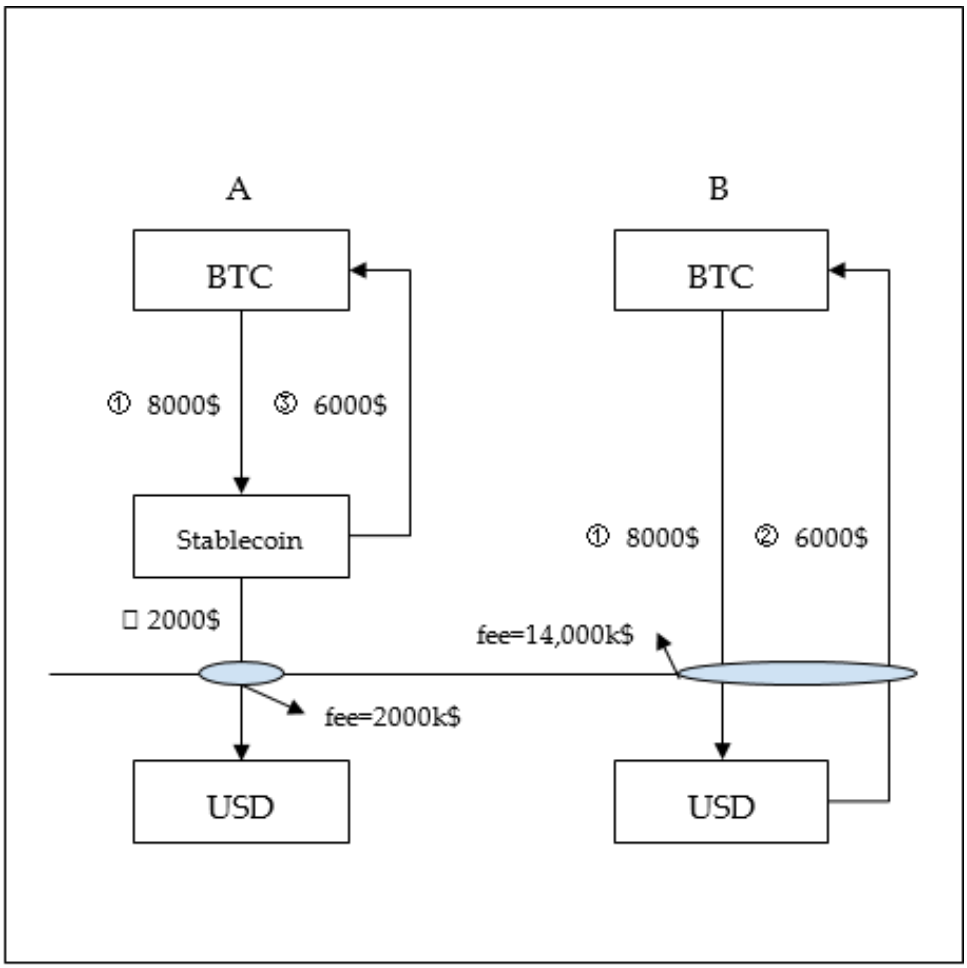
2.1. Cash

Stablecoin is usually pegged to the dollar and can be used as a medium of exchange and a store of value in the blockchain world. The cost of transferring fiat currencies in and out of the cryptosystem is very high, so when investors do not want to have an exposure to traditional cryptocurrencies like bitcoin, they can 'park' their assets in a cryptocurrency as stable as cash, like Stablecoin.

For example, as shown in the diagram below, assuming user A wants to sell the equivalent of $8,000 worth of bitcoins for dollars, $2,000 is withdrawn for cash and the remaining $6,000 will re-enter the market in a few days to buy back the bitcoins in the hope of a better price. Assume the transaction handling

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

fee between crypto and fiat currency is k, and the handling fee between two cryptocurrencies is negligible. In the first case, with the help of Stablecoin, user pays a 2,000*k handling fee. In the second case, without Stablecoin, the user will have to pay a handling fee of 14,000*k, which is seven times worse. K can reach 5% in some Asian countries due to tight regulations.



Stablecoin is also an ideal candidate for the payment of various decentralized applications. The token issued by a decentralized application is similar to the stock of a company with price fluctuation dependent on the decentralized application/company's success and popularity, therefore meaning it is not suitable for general purpose payment. For users, having a token that can be used for different applications is much more convenient than having one token for each application. Stablecoin can be used as a medium of exchange to meet the payment needs of any decentralized application.

2.2. Freedom

We believe there are two groups of people who buy cryptocurrency today. The first group of people has an equity investment mentality — they want to make capital gains in the crypto-market through either speculation or value investment. The second group is more concerned with the actual application

of coins and tokens, and one of the most important applications is that cryptocurrency helps them to exchange and store their wealth with great freedom.

In a country with foreign exchange control, the government manages both the flow of capital and the flow of information. The flow of capital is easy to manage in a country with capital control because even sophisticated hedge funds cannot move money in and out of the country at their will. However, governments often lack an efficient method to regulate the flow of information; more than a third of the employees in the financial and internet sectors acquire information through the use of VPNs, despite government warnings against the move.

Cryptocurrency effectively reduces the difficulty of capital movement to the same level as movement of information.
Enabling wealth to circulate as easily as information is one of the major missions of cryptocurrency. And ultimately, cryptocurrency will depend on people who value its applications rather than just speculators. However, for those who value its applications, the associated volatility is the number one concern. Any secured and stable cryptocurrency will easily gather huge popularities among this group.

Fiat currency	Limited freedom	Stable
BTC/ETH	Complete freedom	Unstable
Stablecoin	Complete freedom	Stable

2.3. Ecosystem

Statistics show that, on average, the percentage of wealth invested is much larger than the percentage spent on consumption. For holders of cryptocurrency, the biggest challenge in investing their wealth in traditional financial products through cryptocurrency is in not knowing how to price different assets. For example, A uses 1 BTC to invest in a fiat-currency-based bond fund managed by B and the yield of the fund is 10% after one year. If BTC's price jumps by 100%, A's net worth measured by BTC decreases to 1.1/2=0.55 BTC. If the price of BTC plunges by 50 percent, A's net worth measured by BTC increases to 1.1/0.5=2.2 BTC.

An investment in a traditional financial product with Bitcoin is a derivative with two kinds of volatility; the volatility of the financial product and the volatility of Bitcoin. The high volatility of Bitcoin disqualifies it as a candidate to link the crypto and traditional financial system. Stablecoin, on the other hand, does not have a volatility of its own. It eliminates the volatility problem in this type of transaction, making the whole financial system more efficient.

In the ecosystem of Stablecoins, there will emerge companies whose business models are to move fiat-currency based investment products to the blockchain world. Maybe in the near future, one can use Stablecoin to invest in U.S. stocks, A-shares, bonds, gold, real estate and VC funds, or even to buy

equity in Space X.

As Stablecoin gains momentum, the user base will broaden and a large amount of data will be collected, 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 with other companies 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 present and the past of Stablecoin, we put forward the evolution logic of 'three generations'. History suggests that the third generation Stablecoin will be the final form of Stablecoin.

Collateral-backed IOU	Tether/Sweetbridge/Arccy
Collateral-backed on blockchain	Maker/Havven/Augmint/BitShares
Elastic monetary supply based	Basecoin/Fragments/Carbon/Kowala

3.1. Collateral-backed IOU

The first Stablecoin is Tether, which shares the same parent company, Tether, with Bitfinex exchange. USDT is what one needs to buy and sell cryptocurrencies on a crypto-exchange similar to the chips purchased in a casino for gaming.

Why do people trust USDT? Tether promised the blockchain community to exchange USDT back to the US dollar anytime at an target exchange rate of 1:1.

In the early days, Tether strictly honored its commitment by keeping its USD reserve equivalent to total circulating USDT in a Taiwanese bank. This was the first Stablecoin in the history of cryptocurrency, fulfilling its promise to traders and helping all participants operate more easily and efficiently. USDT soon became the medium of exchange between fiat and virtual currency, helping people to invest money in the young cryptocurrency market. However, some dubious events affected the credibility of Tether and two big questions emerged regarding moral hazard and regulatory risk.

Violation of moral hazard refers to the fact that Tether's bank account was not audited, and it is likely that Tether had been releasing USDT without sufficient collaterals. Not unlike the Bretton Woods System, the dollar eventually decoupled from gold, and many blockchain community members fear that one day the value of USDT will divorce from USD. All the people who use and hold USDT are essentially betting their money on the credibility of Tether.

If Tether oversupplies USDT, all the holders will suffer the dire consequences.

Regulatory risk refers to the fact that, since any legal currency Tether collects can only be placed in a bank account, Tether's bank account could be frozen at any time by regulators for reasons such as Anti-Money Laundering (AML)[2].

Tether refused to cooperate with accountants and did not provide sufficient data for annual auditing, which led to the accounting firm cutting off all ties with the company, and the market's confidence in USDT was shaken. In addition, some analysts pointed out that when the price of Bitcoin falls, a large quantity of USDT is usually issued, questioning whether they are simply 'printed' without collateral. Regulatory risk has emerged and, according to Tether officials, a Taiwanese account has been frozen.

As these events have demonstrated, the root cause of all Tether's controversies is 'centralization', since it is the only entity overseeing the supply of USDT. Tether is too opaque to play an important role in crypto-money markets. As things stand now, if a credible auditing firm proves Tether's behavior to be fraudulent, it will pave the way for the 'judgment day' of USDT. The entire blockchain community will realize that the value of their Stablecoin is artificially inflated and they will likely rush to sell USDT. As the name suggests, the most important characteristic of Stablecoin must be 'stability'-therefore this level of black swan risk is absolutely unacceptable.

3.2. Collateral on blockchain

The second generation of Stablecoin solves these problems by issuing Stablecoins against a distributed collateral pool that consists of assets like Bitcoin and Ethereum. 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 prevent the emergence of any moral hazard. And because there is no need for a bank account to hold collateral, it also avoids the regulatory risk that surrounds the first generation of Stablecoin.

But the second generation of Stablecoin created new issues while it was solving old problems. Because the price of Bitcoin and Ethereum are so volatile, the value of collateral can easily become less than the value of Stablecoins. If that scenario occurs, the entire system could collapse before the Stablecoin has had a chance to be widely used and accepted.

3.3. Elastic monetary policy based

The first two generations of Stablecoin rely on collateral-based models, and they will share a common destiny. Initially, when the market cap is small enough to ignore systematic risk, their business models can be easily tolerated, but as the amount of money in the Stablecoin system grows they are in danger of being abandoned because of the inherent defects in their mechanisms.

In contrast, the third generation Stablecoin adjusts market exchange rate

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

through an 'Algorithmic central bank' that automatically expands and contracts the supply of tokens. In the early days, it might have taken some time for people to comprehend the complexity of the mechanism and fluctuation of exchange rate, similar to people's reaction to Bitcoin's value proposition in 2010, but when market liquidity reaches a certain threshold, the algorithm-based decision-making principles will be perceived as ultra-effective. Most importantly, there is no systematic risk like moral hazard or volatile collateral value that comes with a collateral-based system, so once the critical point of market liquidity has been reached, the Stablecoin will become just as well recognized as BTC and possess eternal legitimacy.

Due to the superior properties of third generation Stablecoin, numerous companies are trying to create their version of third generation Stablecoin, and the most outstanding of all is USDX.

Our vision is to create a Stablecoin that has fast transaction speed, low transaction cost, and unshakable price stability to be widely used in day to day transactions in both the crypto and the fiat world. We believe that Stablecoin represents the next generation cryptocurrency which is trending towards decentralization and diversification.

4. What is USDX?

USDX creates a decentralized monetary policy system by anchoring certain asset prices and enabling a self-balancing mechanism to ensure the Stablecoin's stability against anchoring assets. The specific self-balancing mechanism will be introduced in the next chapter. The following is a detailed description of the two phases of USDX's development:

4.1. Phase 1: Genesis

The first phase is called the Genesis Phase, in which USDX, a token based on Ethereum ERC20, is produced. Instead of being a Stablecoin, the token represents the holder's concessions in the USDX ecosystem, which might include the initial Stablecoin offering, a low transaction fee or low mining difficulty level. USDX is finite and does not have the self-balancing mechanism of a Stablecoin. USDX will be traded on the open market and the price will be free to rise and fall to reflect market expectations.

In addition, during the Genesis Phase our specialized community management team will strive to disseminate knowledge and build a strong community by cooperating with third-party developers, listing USDX on all major exchanges in the world and educating people on the benefits of Stablecoin in general.

4.2. Phase 2: Stable

The second phase is called the Stable Phase. On the first day of this phase, USDY, (a coin that is based on an independent public chain) goes live. USDY is a third generation, self-balancing Stablecoin anchored to some kind of asset (like the US dollar). It benefits and leverages the development work that we

conducted in the Genesis Phase (like the formation of partnerships with major exchanges and the creation of a large, active user community). The expansion and contraction of USDY is dominated by a decentralized monetary policy that relates solely to changes in the price of USDY/USD, rather than other subjective operations. As a public chain, it has its own tokens, 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 servers, without the need for an industrial electricity supply or expensive equipment.

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

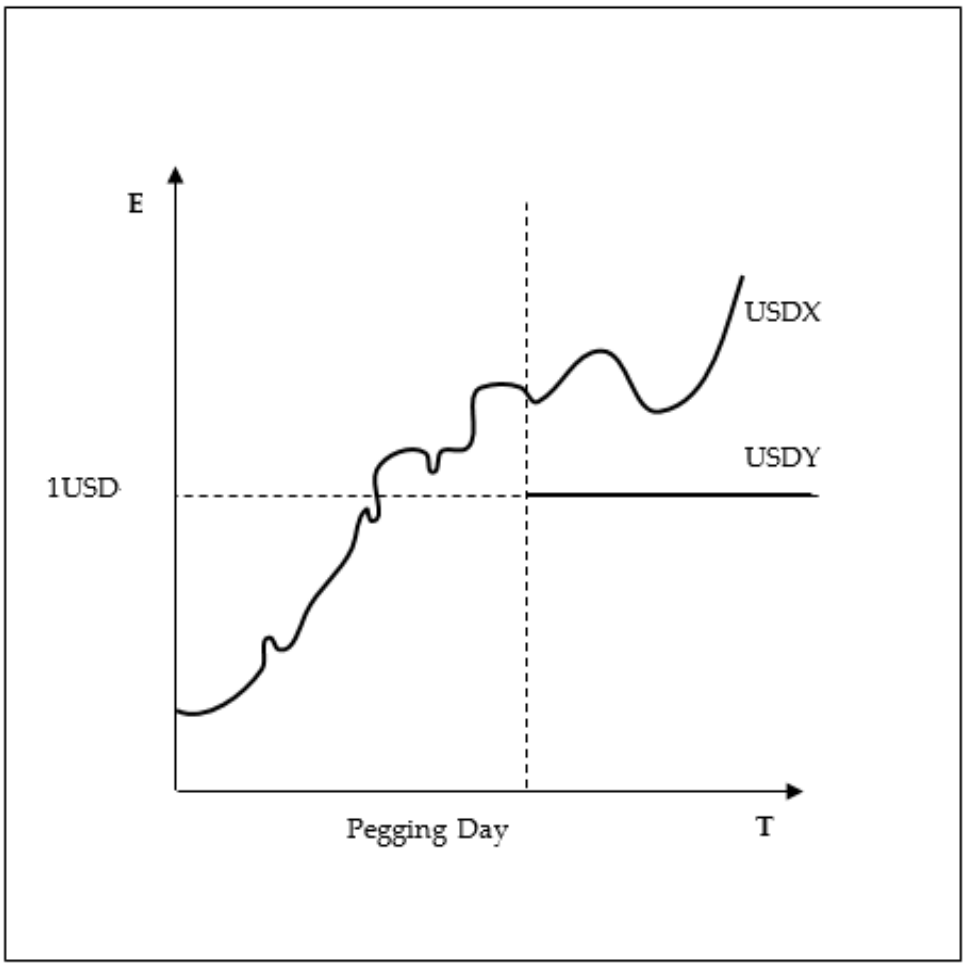
On pegging day, each USDX holder can obtain the equivalent value of USDY of his/her USDX holdings. For example:

1. Tom bought 100 USDX at $0.2/USDX during Genesis Phase for a total price of $20

2. On the pegging day, the price of one USDX is $4. Tom will receive 100*4=400 USDY

3. After receiving USDY, Tom will continue to hold USDX. Tom can sell each USDX for $4 for a total of $400, or he can hold for long-term and obtain other Stablecoins based on universal USDX monetary policy, while enjoying the concession of USDX holders

Since the dollar is the most widely accepted fiat currency worldwide, the strategy of pegging USDY to the dollar was adopted at the beginning of the model design. Once USDY is widely circulated and accepted, the foundation will launch Stablecoins pegged to other legal currencies (such as JPYY, EURY) according to the voting of the community. Holders of USDX will receive any Stablecoin we decide to release in accordance with the same method as USDY. Our ultimate aim is to build a crypto-version of SDR (Special Drawing Rights, a term defined by IMF, representing the basket of reserve currencies including dollar, euro, yuan, yen and pound). The anchored indexes of the USDY will also be adjusted according to the consistent decision of the community. Our final vision is to provide a simple, convenient and robust currency regime for people from countries such as Venezuela and Nigeria who are constantly under the threat of high inflation, capital controls and wealth erosion.



5. USDY's self-rebalancing mechanism

The only goal of monetary policy is price stability.

In today's world, monetary policy is a decision conducted by each country's central bank. But centralization, while effective, can still cause problems. Usually, a committee of central bank officials sets a country's monetary policy. Although there are various guiding principles, monetary policy is still inevitably affected by human judgement. The process of policy-making always suffers time inconsistency, leading to shortsightedness and lagging reactions. There is a tendency to deviate from long-term planning and best global interest by focusing on short-term objectives.

In addition to price stability, employment maximization is also an important objective of monetary policy. Policymakers always prefer an expansionary monetary policy, which increases output and reduces unemployment in the short term. A growing economy helps policymakers' next elections, but a growing economy stimulated by monetary steroids comes at the expense of inflation and reduced economic potential in the long run. No matter how smart and thorough a regulator is, human beings make mistakes and errors in monetary policy can dramatically traumatize one country or even the world's

economy.

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 works:

5.1. The economics of price stability

5.1.1. The theory of purchasing-power parity (PPP)

USDY's exchange rate against the dollar is governed by the theory of purchasing power parity. Since the value of a currency depends on what it can purchase, the exchange rate between two currencies is essentially the exchange rate of purchasing power represented by those two currencies.

If we assume free trade and zero transportation cost, the exchange rate adjusted price of the same goods must be the same in any market. For example, assume the price of gold is 1,250 US dollars in New York and 823 Pounds in London and E stands for the exchange rate of Pound against Dollar. Based on purchasing power parity, we know 1225 USD = E * 823 Pound.
We can, therefore, generalize this as follows: Assume 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. From purchasing power parity, we have p^*=E * p. We can therefore express the exchange rate as:

$$E = \frac{p^*}{p}$$

As the general price level in the fiat currency market, p^* is an input value which cannot be regulated, so the exchange rate can only be adjusted by p.

However, many markets 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 country's currency, the exchange rate between two countries changes in proportion to the changes in the price levels of the two countries in the same period.

$$E_1 = \frac{P_1 / P_0}{P_1^* / P_0^*} * E_0$$

E_1: current exchange rate level.
E_0: base exchange rate.
P_1: current market price level of A currency.
P_0: base period A currency market price level.
P_1^*: current B currency market price level.
P_0^*: base period B currency market price level.

If the price of a piece of cloth rose from 1 Pound to 2 Pounds in the UK and from 2 US dollars to 6 US dollars in the US, then the exchange rate between the Pound and the Dollar will change from £1: $2, to £1: $3.

$$E_1 = \frac{6/2}{2/1} * 2 = 3$$

For a given market, all the values have been produced during the base period and 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 comparing the current price level with the base price level, and the price level of the base period has been fixed, so the adjustment of the price index still can rebase to the adjustment of the general price level in the current period.

As we have shown above, the key to regulate E is to adjust the general price level P.

5.1.2. The quantitative theory of money (QTM)

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 of goods and can form the basis of the elastic supply of our Stablecoin. The equation is illustrated by John Stuart Mill, who expanded on David Hume's idea and the algebraic formulation comes from Irving Fisher, 1911.

$$M * V = P * T$$

M: total quantity of money in the economy
V: the velocity of money
P: the price level

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 an output. The adjustment of P is only affected by M and V, and E is affected by P. In other words, 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, so: USDY/USD=E. From this we can draw the following two conclusions:

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

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

When E is greater than 1, the adjustment mechanism is relatively straightforward. The biggest risk to the stability of USDY is when E is less than 1 for an extended period of time. In this case, investors' confidence in USDY's ability to serve as a Stablecoin might be shaken. How to effectively decrease M or V is the biggest challenge facing all third generation Stablecoin developers. We will demonstrate how we reduce M or V in the following chapters.

5.2. 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 the mortgage time of USDX in the mining process to reduce M. Mechanism 3 is variable transaction fee, which changes the rate of the transaction fee to reduce V. We reserve the right to adopt decentralized governance of community and introduce new mechanisms to enforce the stability of USDY.

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

5.2.1. Mechanism 1: Variable Block Reward

USDY is based on POS mining mechanism and most of the holders will participate in POS verification and earn block rewards. Mechanism 1 increases the total amount of currency in circulation (M) by regulating block rewards, thus affecting the price of USDY/USD.

To illustrate the dynamic block reward algorithm, we first need to clarify the following concepts:

InitialReward: initial block reward, set as 30
M: the growth rate of block reward, set at 1%
maxReward: the upper limit of block reward
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:

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

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 monitors that E(b) >1 and shows a rising trend, implying that the Stablecoin is in short supply. Therefore, the block reward needs to be increased to expand USDY's supply. Then, the block reward is increased by m times compared to the previous block, but the block reward will not exceed maxReward. By increasing the reward 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, implying USDY's supply exceeds demand, so it is necessary to reduce the block reward to reduce Stablecoin's supply. In this case, the block reward is reduced by m times compared with the previous one under the constraint that the block reward will not be less than minReward. By reducing the reward of the block, reward(b), the growth rate of the total amount of money in circulation is decreased, so that E(b) rises and approaches 1.
• Convergence stage: if E (b) does not meet the criteria of the above three stages, it suggests that the previous block reward has moved E(b) to the desired direction, so the block reward remains the same.

5.2.2. Mechanism 2: Lock in Mining

In most cases, contraction is much more difficult to regulate than expansion. This is easily observed in a short study on the history of monetary policy. During the declining stage, E(b)<1, even the block reward approaches 0, and it might still be difficult to make E(b) rise and return to 1.

To solve this dilemma, we will introduce another mechanism called 'lock in mining'. This mechanism will only be activated when E(b)<1 and the variable block reward of mechanism 1 has been reduced to the lowest value, but the decline of E(b) has not slowed down. In this scenario, users can choose to take part of the USDY in their wallets to participate in the 'lock in mining' project. The funds involved in this process will be frozen (possibly for 7 days) and recorded as 'POS mining status'. The frozen funds are not free to circulate, therefore reducing M on the market, effectively helps E(b) rises to 1.

Miners who are not involved in lock in mining and miners who are involved will work together to ensure a steady flow of blocks. In order to encourage the holders to participate in the lock in mining, a step-wise solution might be developed. 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 lock in mining.

The lock is not continuous but divided into 3 steps as shown below:

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

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

If E(b) enters the above convergence stage, it indicates that mechanism 2 is working and the policy of lock in mining will cease to operate.

5.2.3. Mechanism 3: Variable Transaction Fee

In order to control the supply of USDY more effectively, we will introduce variable transaction fees, to change the velocity of money (V) and the total

amount of USDY in circulation (M).

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

Transaction fee = Gas + Circulation Cost

Gas is paid to the miners and circulation cost is put into a dead-end address, which is an address that only allows for coin inflow.

Circulation Cost = the value of USDY in a transaction * circulation cost rate

Define c(b) as the circulation cost rate of the block with serial number b. And the fluctuation range of c(b) is from 0.001% to 3%. The system will automatically calculate c(b) according to the price fluctuations of USDY. Specifically, this is how c(b) is calculated:

$$c(b)\% = \begin{cases} 0.00001 & b = 1 \\ min(1.034c(b-1), 0.03), & p(b) \leq 1, p^{'}(b) \leq 0 \\ max(\frac{1}{1.034c(b-1)}, 0.00001), & p(b) > 1, p^{'}(b) > 0 \\ c(b-1) & otherwise \end{cases}$$

1.034 is the constant that we have derived from modeling on existing data. We will continue to optimize the model as we gather more information. E'(b) is the change rate of exchange rate E(b). It is calculated every every n blocks and is defined by the following equation:

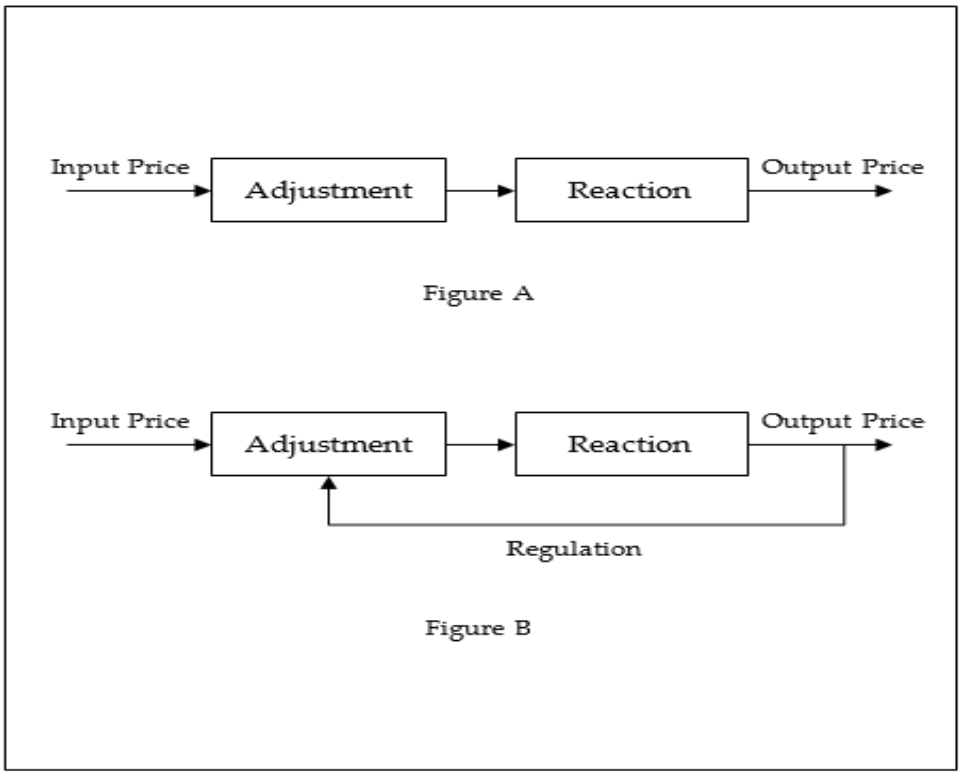
$$E^{'}(b) = \frac{\sum_{i=b-n}^{b} E(i)(i - b + 0.5n)}{\sum_{i=b-n}^{b}(i^2 - (b - 0.5n)(n+1))}$$

The mechanism of variable transaction costs adjusts the frequency of market participants' trading activities, thus adjusting the velocity and quantity of USDY in circulation, which can lead to effective control of the USDY/USD exchange rate.

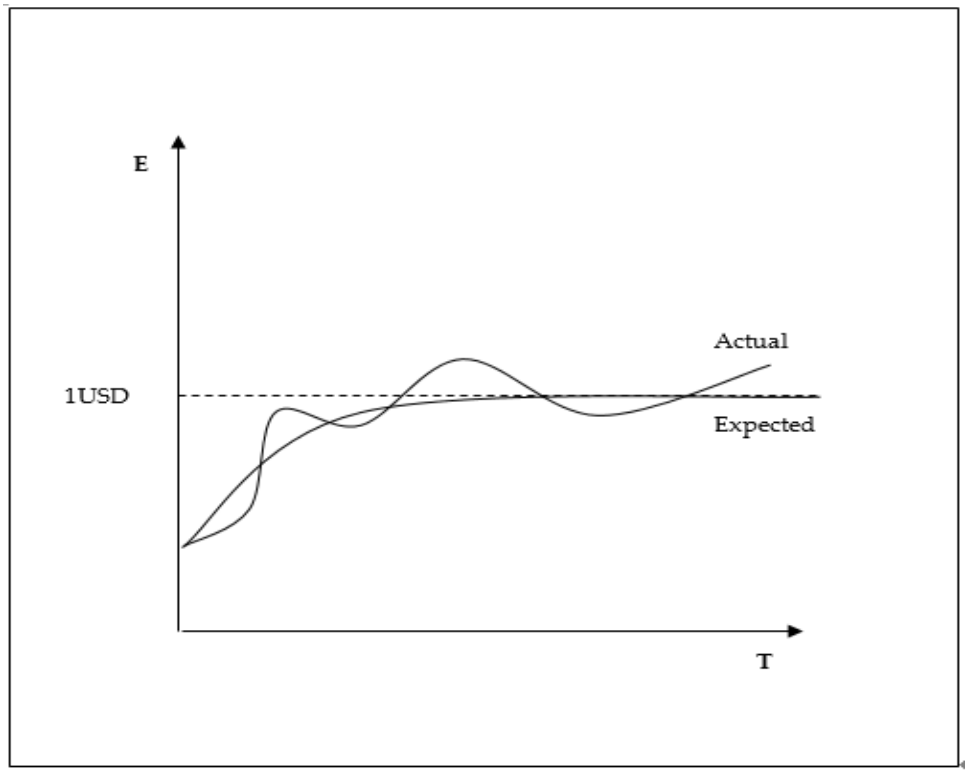
5.2.4. Adjustment Accuracy Improved by Negative Feedback Mechanism

Feedback Mechanism Different monetary policies have different effects under different conditions and the actual results are often a mixture of several complicated scenarios, thus one can never expect 100% accuracy. However, we have reduced the requirement on accuracy of output price in the design process by incorporating a negative feedback mechanism.

We consider there is a causal relationship between monetary policy and Stablecoin price. Figure A represents an open loop causal process, which is unstable and requires a highly accurate price adjustment to effectively control the system. Figure B represents a causal system with negative feedback, which enables us to control the system with a lower requirement of price adjustment accuracy.



The following diagram shows a price response curve of Stablecoin. Even if the initial control is biased and inaccurate, with the help of negative feedback loop, the fluctuation against the expected price is gradually reduced over time and will eventually reach an equilibrium.



5.2.5. Mechanisms' Efficiency Improved by the Free Market

In a free market, we are less demanding on the mechanisms' efficiency . With the help of the three mechanisms introduced above and some time, the USDY/USD exchange rate E will eventually stabilize to 1. If our regulating mechanisms are recognized by market participants, we believe there will be several important implications.

In the beginning, because the price of USDY is likely to be 1 USD, the parity level will be the focus of the game. USDY price is highly likely to remain at this parity because of the lack of adequate communication and trust among the participants at this level.

Speculative arbitrage traders will actively help to push prices back to parity and make profits when the gap between price and parity is closed. Although arbitragers are solely profit-driven, their actions help to improve the efficiency of the system.

People gain their confidence from historical precedents, and as time goes by and the USDY self-balancing mechanism proves its effectiveness, even non-speculative market participants will actively push the price back to parity when it deviates from $1.

In a free market, miners, users, exchanges, and speculators are all motivated to maximize their self-interest and together, their behavior will stimulate and enhance USDY's self-balancing mechanism and accelerate USDY's path back to parity when needed.

6. Infrastructure

6.1. POS Consensus Mechanism

Consensus mechanism has been discussed for a long time. The two mechanisms most widely discussed and applied are Proof of Work(PoW), adopted by BTC and ETH, and Proof of Stake(PoS), adopted by Qtum and ETH Casper. Compared with PoW, PoS is safer, more decentralized and more efficient in terms of computation power.

Discussion on the techniques of PoS is well known and we will not further elaborate. We will focus on introducing the application of PoS mechanism on the USDX network and how it works together with economic principles to adjust the amount of coins in circulation. There are two types of rewards in mining as we mentioned above; variable block reward and special block reward.

Block reward is not a fixed value but varies by the exchange rate of USDY against USD. Miners need to take out USDX they owned as collateral in exchange for block reward opportunities. The block is obtained by the first miner who provides the hash of the block that meets the following requirement:

$$BlockHash < coin \times coinage \times target$$

Target is a constant that is set by the system rules and defines the difficulty of creating a block at the current period. At regular intervals, the system

adjusts the difficulty and target of the next period according to the average time of the previous period, in order to stabilize the time required for creating a block.

Coin represents the quantity of USDX mortgaged by miners. Coin age represents the time of USDX has been mortgaged. It can be seen from the formula that the probability of getting block rewards is proportional to the product of the stake of the mortgage and the time of the mortgage. The more USDX mortgaged, the more time of USDX has been mortgaged, the higher the probability of getting block reward.
Special block reward is provided to the miners involved when mechanism 2 (mining locking) is triggered. Miners involved in mining locking are obligated to provide the hash that meets the following requirement to obtain special block reward.

$$LockHash < lockage \times locktarget$$

The quantity of special block reward is determined when miners are involved in mining locking. Each block can contain several hashes of mining locking but only one hash of the block.

6.2. 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 PoS consensus to provide this key data. It is safer than existing methods and introduces less overheads and complexity to the blockchain system.

There are three main solutions currently:

Single Trusted Data Source: this is the first attempt to introduce external data to the blockchain. Typically, a single trusted party is responsible for collecting external data and supplying this information to the blockchain application. This is a completely centralized service. Although changes in the encryption traces are required, and the authenticity of Oraclize is provided[3] 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: This is an updated method compared to the Single Trusted Data Source solution. 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 fraudulent individual is found, the token holder should actively switch to other honest nodes so that the fraudulent individual 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: Vitalik was the first person to introduce the concept of SchellingCoin[4] . His idea was to design a decentralized incentive

[3]https://docs.oraclize.it/security-deepdive-authenticity-proofs-types

[4]https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

scheme to motivate participants to provide accurate data. The model allows anyone to submit data to the blockchain and rewards data that falls within the middle range of it (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 overheads and more complexity to the system.
Built on Vitalik's great wisdom, 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 feed, 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.

7. What are the problems with other stablecoins?

Many Stablecoins were born in an attempt to solve the problem of price fluctuation, including USDT, SmartCoin and Dai. However, these Stablecoins do not really achieve price stability and decentralization.

USDT

In theory, every USDT has one USD as reserve stored in Tether's bank account. This guarantees Tether's ability to redeem the legal currency at any time. Yet the model is 100% centralized because the company is in full control of the money supply and reserves. Tether is not trustworthy, and reports have pointed out that due to a lack of verification, there are millions of tokens that don't have adequate USD reserves. Tether was the target of a hacking attack that resulted in the theft of $30 million in tokens. Last but not least, because its US dollar reserve must be stored in regulated bank accounts, it is subject to government regulations.

Bitshares

There are two types of tokens in the BitShares system, BTS and SmartCoin. The two tokens can be exchanged in BitShares internal exchanges. SmartCoin is a Stablecoin, which can peg various assets by holding BTS as collateral. The SmartCoin that is pegged to USD is called BitUSD. If the price of BTS declines dramatically against pegging assets due to a black swan event, then the collateral based model will instantly become ultra-fragile.

Maker DAO

The token for MakerDAO is called Dai and is based on collateral. Anyone can generate Dai on the Maker platform with a collateral value of twice Dai's

Pooled Ether (PETH). Like Bitshares, Dai's mortgage mechanism is also very vulnerable, and Dai's market value is limited by available collaterals.

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 repays the Base Bonds and the rest is assigned to the Base Shareholders. Three-token models may work in theory, but they present 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's medium and long-term development. Since Base Share represents a permanent distribution right for newly-generated Basecoin, the Base Share market is likely to be much more popular than Basecoin, which will weaken the status of Basecoin.

Technology implementation was not mentioned in Basecoin's whitepaper. Let's assume it will be implemented as a Ethereum ERC20 Token Smart Contract. According to the current block gas limit of 8,000,000 and each SSTORE operation cost 5,000 gas, and assume the most optimistic scenario where there is only one transaction in the current block, Basecoin can only support a maximum of 1600 Share and Bond owners. This is not scalable at all.

Carbon

Carbon claims that it can achieve instantaneous callbacks by freezing part of the 'wrapped coins', and market participants are free to choose whether or not to 'package' their coins and by how much. If the total amount of 'wrapped coins' does not meet the instantaneous correction, the Carbon reserve will start to buy back the coins and 'package' them. Without discussing the effect of the Carbon reserve buyback, the very word 'reserve' means centralization, which goes against the number one principle of blockchain-decentralization. In addition, Carbon does not take advantage of the velocity of money, which should have helped Carbon become more reliable and stable.

		Tether	MakerDAO	BitShares	Basecoin	Carbon	USDX
Generation		1st	2nd	2nd	3rd	3rd	3rd
Token or PCC		Token	Token	Token	Token	Token	Public Chain
EM	Add M	/	✗	✗	✓	✓	✓
	Reduce M	/	✗	✗	✓	✓	✓
	Add V	/	✗	✗	✗	✗	✓
	Reduce V	/	✗	✗	✗	✗	✓
T (1-3 stars)	Effectiveness	★★★	★	★	★	★	★★★
	Simplicity	★★★	★★	★★	★	★★	★★
	Scalability	★	★	★	★	★	★★★

M represents total supply of money, V represents velocity of money, PCC represents Public Chain Coin, EM represents Economic Mechanism, T represents Technology.

Reference

[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 Hanson2012. 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. URL http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

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