DSS: A Decentralized Stablecoins and Peer-to-Peer Trading System

Takeshi Tanaka
i@dsss.io www.dsss.io
August 26, 2018

Abstract: In this whitepaper, we will introduce DSS system. It achieved the decentralization of the stablecoins. Stablecoin USDi in DSS will become the main currency in the blockchain network and in daily life. Peer-to-peer trading system in DSS can achieve secure transactions between strangers.

The system will ultimately achieve cryptocurrency price stability, peer-to-peer secure trading, free transfers, real-time confirmation, and millions of TPS.

DSS system will apply the technology of Bitcoin, Ethereum and Graphene.

1.Background

The emergence of bitcoin and other cryptocurrencies have significant influence, but there are still large disadvantages: Price fluctuations are too huge. It cannot realize the function of value exchange. We believe this is the main reason why cryptocurrencies have not been widely used. The volatility of the cryptocurrency price makes the funds with risk aversion preference not involved, and this part of the money is the highest proportion in the financial market. There are no ultra-low-risk, value-stable cryptocurrencies, It is also one of the main reasons why traditional financial institutions have not been chosen to enter the cryptocurrency market. Although many blockchain platforms have been working hard to support the development of stablecoins, they all adopt the method of credit issuance and asset mortgage, and the risk is very high.

2. Goal

2.1Price stability

This is the most basic requirement for stablecoins.

2.2Free transfer

DSS and USDi transfers should be free. High transfer fees reduce the frequency of people using cryptocurrencies.

2.3Real-time confirmation

A transfer should be in real time. Waiting longer will make users feel worried, and it will make the stablecoins lose its advantage over traditional payment methods.

2.4Millions of TPS

The goal of DSS is to become a widely used stablecoins payment system all over the world.

3.Multi-token mechanism

DSS contains multiple tokens. There are DSS and USDi at this stage.

DSS ERC20 TOKEN is obtained by crowdfunding. After the DSS main network pop up online, ERC20 TOKEN will be mapped to the DSS main network. Selling DSS to the virtual exchange can obtain USDi and this is the only way to get USDi.

4.Decentralized stablecoins realization

4.1Consensus mechanism

We introduce a new concept: Proof Of Index (POI). The DSS price index is an index based on certain rules for the price of DSS against legal currencies and other cryptocurrencies is a consensus. Similar to the NASDAQ Composite Index includes timestamp, price and volume. The investors will obtain the same DSS price index at the same time. If a BP (Block Producer) entered into a different index, then the block produced by this BP is illegal. The index is so natural as the timestamp that we all ignore its existence. The DSS price index reflects the decisions made by people all around the world and they don't know what other people are doing and thinking when they make these decisions. DSS takes on the function of price discovery, also indicates that free market is the price determinant.

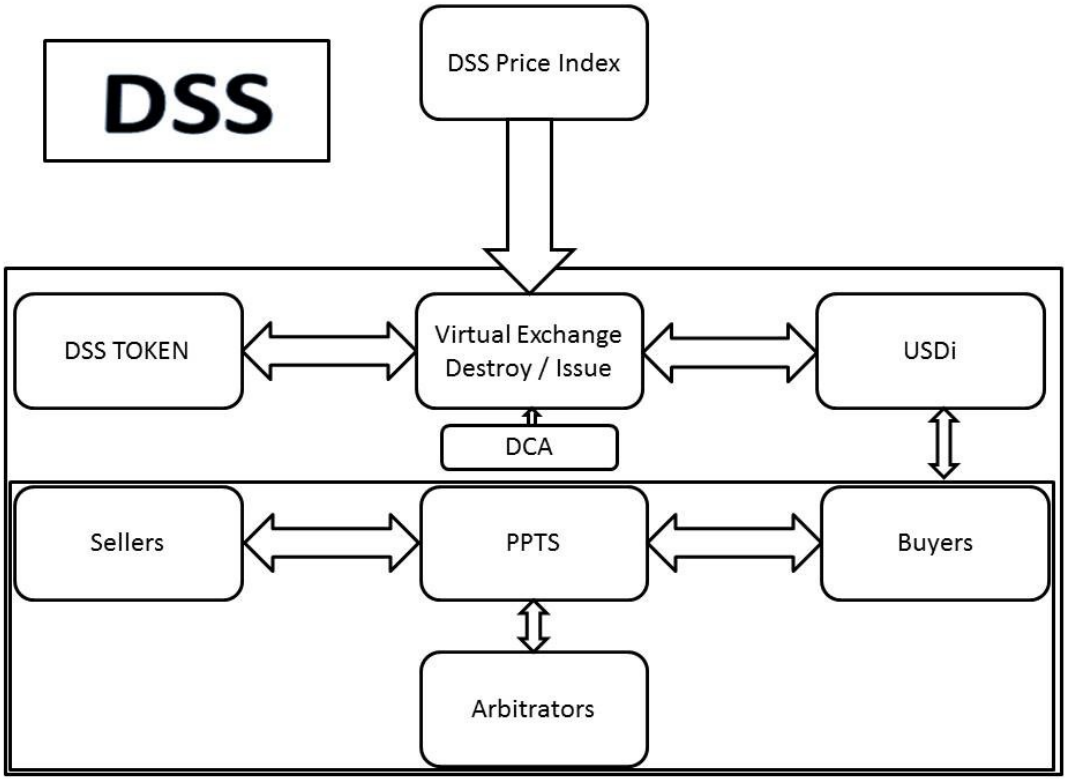
4.2Virtual exchange

Virtual exchange is the core of DSS. It is a systematic built-in account. In the buying process of USDi, DSS holders send a certain number of DSS to the virtual exchange, and agreed price. The virtual exchange receives orders based on the quantity and price received, and other orders within the time period of the same block, then calculating the number of USDi that should be obtained. After deducting a small amount of transaction fees, the virtual exchange will send USDi to DSS holders.

Virtual exchange calculates the virtual order book out through the Depth Curve Algorithm (DCA) method. Parameters include trading volume, trading price, change rate of price and DSS price index. The USDi selling process is the opposite to the buying process. DSS was inspired by the contract design in Ethereum and the Bancor algorithm, revolutionized improvement on this basis. The most important of these is the adding of POI and DCA. The DCA effectively determines the order book and the degree of slippage. When users buy and sell in a large amount in the virtual exchange, they will get the corresponding slippage.

The virtual exchange will take the transaction price, the reaction time of the fund, the price psychological barrier, the rate of price change, the volume of the transaction, the depth into consideration, and the correlation among these factors. At a time, the virtual exchange will calculate the middle price [(BID + ASK)/2] amount by making the purchase order and the sell order equal. The spread of the order will be traded along the order book in the virtual exchange. The highest or lowest price of these trade orders will become the latest price. Every investor's counterparty is the virtual exchange. The spread is a "duplicated" deal: each order was executed separately and the counterparty is virtual exchange. Low transaction fees attribute to the price stability of USDi. The virtual exchange fees are 2%%- 20%%. Limit orders are sent to the virtual exchange only if the price is triggered. For an order with a fixed price, the uncompleted portion of the transaction will be refunded and the transaction cost is at 1%%. The virtual exchange dynamically adjusts the minimum order limit based on the amount and quantity of orders received. All designs ensure fluidity and avoid performance bottlenecks. The virtual exchange has realized the value exchange across time and space.

People sell DSS to the virtual exchange, obtained USDi and used USDi to buy DSS from the virtual exchange. The virtual exchange destroys all received DSS and USDi. At the same time, issue the corresponding quantity of DSS and USDi. The virtual exchange has no assets and liabilities.
The middle price in the virtual exchange will be changed hourly to the arithmetic average price of the last ten minutes of the DSS price index. In the market, the middle price and the DSS price index affect each other. It can reflect the influence of funds on prices, which can make USDi a perfect stablecoin.
The advantage of the DCA is that it does not depend on fluidity; all operations are transparent and are calculated by the system.



4.3Theoretical Basis

DSS system is based on The Law of One Price and the Arbitrage Pricing Theory. In order to obtain real profit, Arbitrageurs will discover and find out the spread of price between DSS-USD and DSS-USDi trading. They will purchase and wait for the DSS middle price to synchronization with the DSS price index to sell these assets. The Law of One Price is forcedly driven by the arbitrage process, arbitrage guarantees USDi always fixed on USD. Arbitrage is a spontaneous action which come from human's instinct and cannot be stopped. USDi belongs to the money market and DSS belongs to the cryptocurrency market. In fact, under the situation of severe information asymmetry, temporary discount and premium are normal, and as long as there is sufficient liquidity, the discount and premium can be quickly eliminated.

We use an example to illustrate that the data here is hypothetical which ignores transaction costs.
Carl has 200 DSS. Now the DSS price index is 20.In the virtual exchange, the middle price of DSS is 20 USDi. Carl wants to sell DSS to the virtual exchange for USDi and is willing to sell at a minimum

of 19.8USDi.So Carl sends the order to the account address of the virtual exchange. At the same time, Linda has 2000USDi. She wants to buy DSS from The virtual exchange. After the virtual exchange received the order from Carl and Linda, it calculated the net sales of 100 DSS. Linda will receive 100 DSS. While Carl's 100 DSS net orders will be sold along the depth chart for 50 at 19.9USDi and 50 at 19.8USDi, resulting in Carl's 3985USDi.The virtual exchange will destroy 200 DSS, 2000USDi, and issue 100 DSS, and 3985USDi in both transactions.

5.Feature

5.1BP(Block Producer) incentive

The fees charged by the virtual exchange will be awarded to the BP. To prevent abuse of resource, some fees will be charged as necessary for their service.These benefits will be used as incentives for BP.

5.2Technology

DSS was built using Graphene technology and have made great changes. 21 BP and 100 observers will be voted and Block Producers need to mortgage DSS for 5 years. Users cannot create contracts and DAPP. There is no need to buy resources. And the system will not be affected by 5% inflation per year. Account bidding only needs to mortgage DSS. DSS follows the most important bitcoin spirit: transparent, unchangeable, decentralized and secure. DSS has no constitution, cannot freeze accounts, and private key loss cannot be recovered. In addition to fixing the bug, the BP's changes of any rules, data, and code of the DSS will directly lose the BP identity.

When faced with a malicious attack, the malicious block cannot be brought into an irreversible state unless all BP are controlled. When multiple BP are controlled by an attacker,100 observers and others will find these malicious attacks to vote it out, and select new BP from 100 observers.
After averaging 0.25 seconds of broadcast, this transaction can be considered a certainty of 99.9%, provided 100% irreversibility confirmation within 1 second. DSS and USDi transfers can be confirmed in just 1 second, which can be considered as real-time.

If Graphene technology proves to be unsafe, DSS will apply Ripple technology. DSS will adopt Ripple technology and improve it. It will shorten the time it takes to get out of blocks; Users cannot create contracts and DAPP, and create new blocks without adding additional DSS. This will reduce its performance but improve security.

The above technology can fully realize the construction of DSS.

5.3Ease of Use

DSS simplifies the usage of USDi. Users can easily use USDi at any terminal. It takes less than 10 seconds by using typical USDi mobile QR code payment. This includes the time to open the app and the confirmation of it. This is very important. People just need to use USDi and don't need to care about the value conversion process.

5.4Capital capacity

When USDi is widely used and more USDi is needed, DSS meets people's demand for USDi through market capitalization growth. This is determined by the most basic principles of supply and demand in economics. The demand for USDi is directly, quickly and accurately reflected on the DSS price index. There is no limit to the amount of funds that DSS can afford.

5.5Mortgage

All resources in DSS are obtained through mortgage. It consumes the time value of money. In addition to using the account, other mortgages need to specify the time, which is up to 5 years. In addition to campaign and bidding, the amount of DSS required to be mortgaged is automatically calculated based on the network status.

5.6Stable system

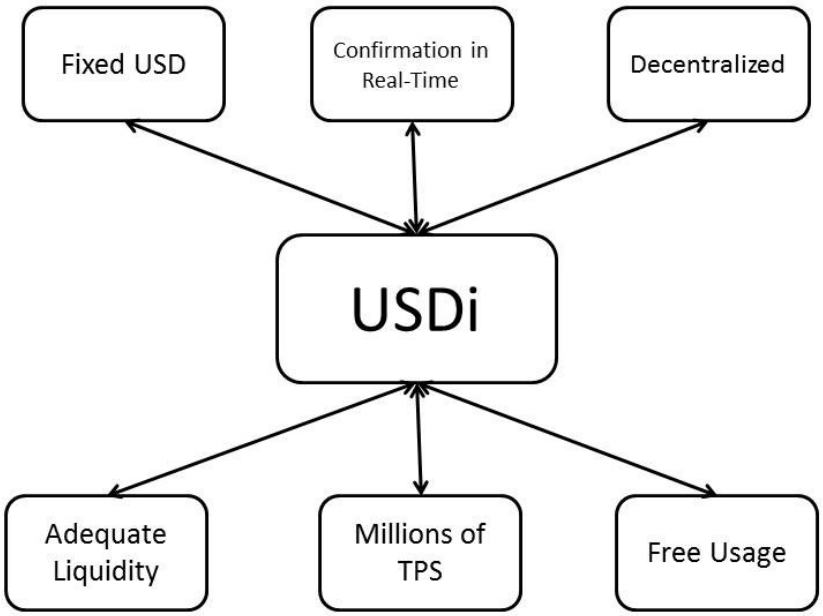
No other contracts and DAPPs make the system more transparent, more efficient, more stable, safer, simpler and less buggy.

5.7Mobile payment

DSS will provide USDi payment interface, QR code payment, NFC payment, social payment and other solutions.

5.8Global USDi payments

USDi will become a payment method that used by websites and apps all around the world. Let people use USDi directly in their daily lives and business practices. This is our important goal.



6.Peer-to-peer trading system

Peer-to-peer trading system is a system built-in account. PPTS guarantees the security of the buyers' and sellers' funds and is a fund transfer station. Buyers pay first to PPTS, and it will transfer USDi to the seller's account after confirming receipt of the goods. PPTS can only use USDi at this stage.

6.1Counter

The seller gets resources by mortgaging the DSS and using the counter function.

The counter includes an identification tag for inputting information interfaces for multimedia contents, for storing transaction information, small storage space for both buyers and sellers to leave messages and ratings, and other necessary functions.

Sellers need to pay a 10 % margin to PPTS to sell goods.

If the buyer and seller have a trade dispute, they can apply for arbitration. The arbitrators were randomly got involved, requiring at least 9 arbitrators to vote, with the majority to win. The applicants of the arbitration need to pay 1%-5% of the fee, which is paid by the losing part. The benefit will be obtained by the majority and BP.

6.2The arbitrators practice points and hierarchies

In order to obtain the identity of the trainee arbitrator, they have to mortgage DSS. Before becoming a formal arbitrator, one can only vote but receive no gains and the voting will not be scored. The first batch of arbitrators on the main line directly obtained official status. The identity of buyers, sellers and arbitrators are always invisible on the internet, and voting information is hidden before the results release. Arbitrators earn points by voting correctly (the majority party), they can handle with larger transaction disputes if they get more points. A failure vote (the minority) will reduce the points and it determined by the amount of the transaction proceed.

The above is a method and theory needed to implement a decentralized stablecoins and peer-to-peer trading system.

References

[1] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamoto

[2] *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Vitalik Buterin

[3] *EOS.IO Technical White Paper*. Block. One

[4] *An Inquiry into the Nature and Causes of the Wealth of Nations*. Adam Smith

[5] *The General Theory of Employment, Interest, and Money*. John Maynard Keynes

[6] *Denationalization of money*. Friedrich von Hayek

[7] *Efficient Markets Hypothesis*. Eugene F. Fama

[8] *Arbitrage pricing theory*. Stephen Ross

[9] *Finance and the Good Society*. Robert James Shiller

[10] *Free to Choose: A Personal Statement*. Milton Friedman and Rose Friedman

[11] *Financial Economics*. Zvi Bodie, Robert C. Merton and David L. Cleeton

[12] *Principles of Economics*. N. Gregory Mankiw

[13] *Behavioural Finance*. William Forbes

[14] *The Economics of Money,Banking,and Financial Markets*. Frederic S.Mishkin
[15] *Bancor protocol whitepaper*. Eyal Hertzog, Guy Benartzi and Galia Benartzi
[16] *Executive Summary for Financial Institutions Ripple: Internet protocol for interbank payments.* Ripple Labs Inc.