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

DSS：一個實現去中心化穩定幣和點對點交易的系統

Takeshi Tanaka

i@DSSs.io www.DSSs.io

August 26, 2018

摘要：在這份白皮書中，我們將介紹 DSS，它實現了穩定幣的去中心化。DSS 中的穩定幣 USDi，將成為區塊鏈網路和生活中的主要貨幣。DSS 中的點對點交易系統（PPTS），實現了陌生人之間的安全交易。該系統最終可以實現加密貨幣價格穩定，點對點安全交易，免費轉帳，即時確認，每秒數百萬次交易的目標。

DSS 使用了 Bitcoin，Ethereum 和 Graphene 的技術。

背景

比特幣和其他加密貨幣的產生有著非凡的意義，但是依然存在極大的缺陷：價格波動太大，無法行使價值交換的功能。我們相信，這是加密貨幣沒有得到大量應用的主要原因。加密貨幣價格的劇烈波動使風險厭惡偏好的資金不會參與其中，而這部分資金是金融市場中占比最高的。沒有低風險的、價值穩定的加密貨幣，也是傳統金融機構沒有選擇進入加密貨幣市場的主要原因之一。

雖然許多區塊鏈平臺一直在努力支持穩定幣的發展，但是都採用了信用發行、資產抵押的方式，風險非常高。

目標

1.價格穩定

這是穩定幣最基本的需求。

2.免費轉帳

DSS 和 USDi 的轉帳應該是免費的，高額的轉帳費用減少了人們使用加密貨幣的頻率。

3.即時確認

一筆轉帳應該是即時到賬的，更長時間的等待會使用戶感到擔憂，並使穩定幣與傳統支付手段相比失去優勢。

4.百萬級 TPS

DSS 的目標是成為全球廣泛使用的穩定幣支付系統，每秒數百萬次交易顯得尤為重要。

去中心化穩定幣的實現

多代幣機制

DSS 包含多個代幣，現階段有 DSS 和 USDi。

DSS 的 ERC20 TOKEN 由眾籌獲得。在 DSS 主網上線後，ERC20 TOKEN 會轉移到 DSS 主網，把 DSS 出售給虛擬交易所可以獲得 USDi，這是獲取 USDi 唯一方式。

共識機制（POI + BFT-DPoS）

我們引入一個全新的概念：指數證明（Proof Of Index）。DSS 價格指數是以 DSS 對法幣和其它加密貨幣的價格，按照一定規則制定的指數，是一種共識，就像 NASDAQ Composite Index 一樣，包含時間戳記、價格和交易量。同一時間所有人獲得的 DSS 價格指數都是一樣的。如果某個生產者中輸入的指數是不同的，那麼這個生產者此時產生的區塊是不合法的。指數就像時間戳記一樣自然，以至於我們都忽略了它的存在。DSS 價格指數反映了世界各地的人所作出的無數個決定，而這些人在做決定的時候並不知道其他人在做什麼。DSS 承擔了價格發現的功能，也表明，自由市場才是價格的決定者。

虛擬交易所（Virtual Exchange）

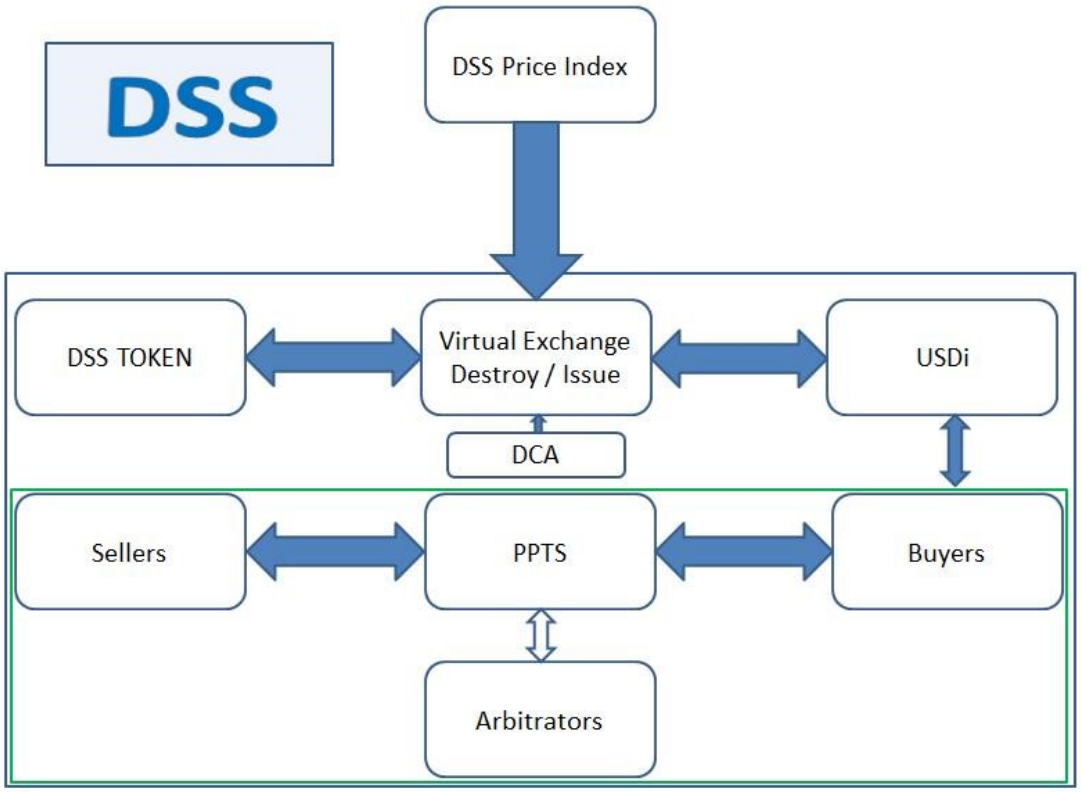
虛擬交易所是 DSS 的核心所在，是系統內置帳戶。USDi 買入過程中，DSS 持幣者將一定數量的 DSS 發送到虛擬交易所，並約定價格，虛擬交易所根據收到的包含數量和價格的訂單，與同一區塊的時間段內其它的訂單，計算出應獲取的 USDi 數量。並扣除少量的手續費後，將 USDi 發送給 DSS 持幣者。

虛擬交易所通過深度曲線演算法（Depth Curves Algorithm DCA）計算出虛擬訂單薄。參數包括交易量，交易價格，價格變化的速率和 DSS 價格指數。USDi 賣出過程則與買入過程相反。DSS 從 Ethereum 中的合約設計和 Bancor 演算法中得出靈感，在此基礎上進行了革命性的改進。其中最重要的是加入了 POI 和 DCA。DCA 有效的決定了訂單簿（orderbook）和滑點（Slippage）程度。用戶在虛擬交易所中大量買賣時，就會得到相對應的滑點。

虛擬交易所綜合了交易價格，資金的反應時間，價格心理關口，價格變化的速率，成交量，深度，這些因素之間的相關性。虛擬交易所在一個時間段，將收到的買單和賣單金額相等的部分以中間價[(買一價+賣一價)/2]計算，訂單的差額部分，會沿著虛擬交易所的訂單薄成交，這些成交訂單的最高價或最低價，會成為最新的價格。所有人的交易對手方都是虛擬交易所，差額部分為"副本式"成交：每個訂單都是獨立和訂單薄成交的。低的交易成本對於 USDi 的價格穩定有促進作用，虛擬交易所收取 2%%--20%%的費用。高於賣一價的賣單、低於買一價的買單，這些限價單會放在鏈下。限定了價格的訂單，未成交的部分退回系統會收取 1%%的費用。虛擬交易所會根據接收的訂單金額和數量，動態調整最低訂單限額。所有的設計保證了流動性，規避了性能的瓶頸。虛擬交易所實現了跨時間，跨空間的價值交換。人們向虛擬交易所出售 DSS 獲取 USDi，使用 USDi 向虛擬交易所購買 DSS。虛擬交易銷毀所有收到的 DSS 和 USDi，同時發行成交訂單對應數量的 DSS 和 USDi。虛擬交易所沒有資產和負債。

虛擬交易所裡的中間價會每小時同步更改為 DSS 價格指數最後十分鐘的算術平均價。市場中，中間價與 DSS 價格指數互相影響。既能反映資金對價格的衝擊，又使 USDi 完美的成為穩定幣。

深度曲線演算法的優點在於不依賴於流動性，並且一切操作透明，由系統計算完成。



理論依據

DSS 的建立依據是一價定律和套利定價理論

套利者為了獲取真實利潤，尋找並發現 DSS-USD 和 DSS-USDi 交易對的價格差異，購買並等待 DSS 中間價與 DSS 價格指數同步時出售

這些資產。一價定律被套利過程強行驅動，套利保證了 USDi 始終錨定 USD。套利是自發行動的力量，這是人類的本能，無法阻擋。USDi 屬於貨幣市場，DSS 屬於加密貨幣市場。實際上在資訊嚴重不對稱的情況下，暫時的折價和溢價是正常的，只要有充足的流動性，折溢價可以很快消除。

我們用例子來說明，這裡的資料是假設的，並且忽略了交易成本。Carl 擁有 200 個 DSS，現在 DSS 的價格指數是 20，虛擬交易所中，DSS 中間價是 20 USDi。Carl 想將 DSS 出售給虛擬交易所換取 USDi，並願意最低以 19.8USDi 的價格出售。於是 Carl 將訂單發送到虛擬交易所的帳戶地址。在相同的時間，Linda 擁有 2000USDi，她想向虛擬交易所購買 DSS。虛擬交易所在收到 Carl 和 Linda 的訂單後，計算得出 100 個 DSS 的淨賣量，Linda 將會收到 100 個 DSS。而 Carl 的 100 個 DSS 淨賣單，將會沿著深度圖以 19.9USDi 成交 50 個，以 19.8USDi 的價格成交 50 個，最終 Carl 獲得 3985USDi。虛擬交易所在這兩筆交易中，會銷毀 200 個 DSS、2000USDi，並發行 100 個 DSS，和 3985USDi。

特徵

生產者（Block Producer）激勵

虛擬交易所收取的費用會獎勵給生產者。為了防止資源的濫用，系統會對一些必要的項目收取一定的費用。這些收益會發放給生產者用作激勵。

技術

DSS 使用 Graphene 技術構建並做了大的改變。通過投票產生 21 個生產者和 100 個觀察者，而且生產者需要抵押 DSS，時間為 5 年。用戶不能創建合約和 DAPP，不需要購買資源，沒有每年 5%的通脹，帳戶競價只需要抵押 DSS 。DSS 遵循最重要的比特幣精神：透明，不可篡改，去中心化，安全。DSS 沒有憲法，無法凍結帳戶，私密金鑰丟失無法恢復。除修復 BUG 外，生產者對 DSS 任何規則、資料和代碼的改動，都會直接失去生產者身份。

當面臨惡意攻擊時，除非控制了所有的生產者，否則無法使惡意區塊進入不可逆狀態。多個生產者被攻擊者控制時，100 個觀察者和其他節點會發現這些惡意攻擊，投票讓其出局，並從 100 個觀察者中選出新的生產者。

在廣播時間平均 0.25 秒後，可以認為交易具有 99.9%的確定性，在 1 秒內提供 100%的不可逆性確認。DSS 和 USDi 轉帳只需要 1 秒鐘就可以確認，這可以被認為是即時的。

如果 Graphene 技術被證明是不安全的，DSS 會採用 Ripple 技術並加以改進：將出塊時間縮短，禁止用戶創建合約，產生新的區塊不會增發 DSS。這樣會降低性能，但是可以提高安全性。

以上技術可以完全實現 DSS 的構建。

易用

DSS 會簡化 USDi 使用方式,使用者可以在任何終端方便的使用 USDi。一次典型的 USDi 移動端二維碼支付,花費的時間在 10 秒鐘以內,這其中包括了打開 APP 和確認的時間。這是非常重要的。人們只需要使用 USDi 即可，不用關心其中的價值轉換過程。

資金容量

當 USDi 被廣泛使用，而需要更多的 USDi 時，DSS 通過市值增長來滿足人們對 USDi 的需求。這是由經濟學最基本的供給與需求原理決定的。對 USDi 的需求,直接、快速、準確的反應到 DSS 價格指數上。DSS 承載的資金容量是沒有上限的。

抵押

DSS 中的所有資源都是通過抵押獲得的,消耗的是資金的時間價值。除了使用帳戶,其他的抵押需要指定時間,最長為 5 年。除競選和競價外，所有需要抵押的 DSS 數量都是根據網路狀態自動計算的。

穩定的系統

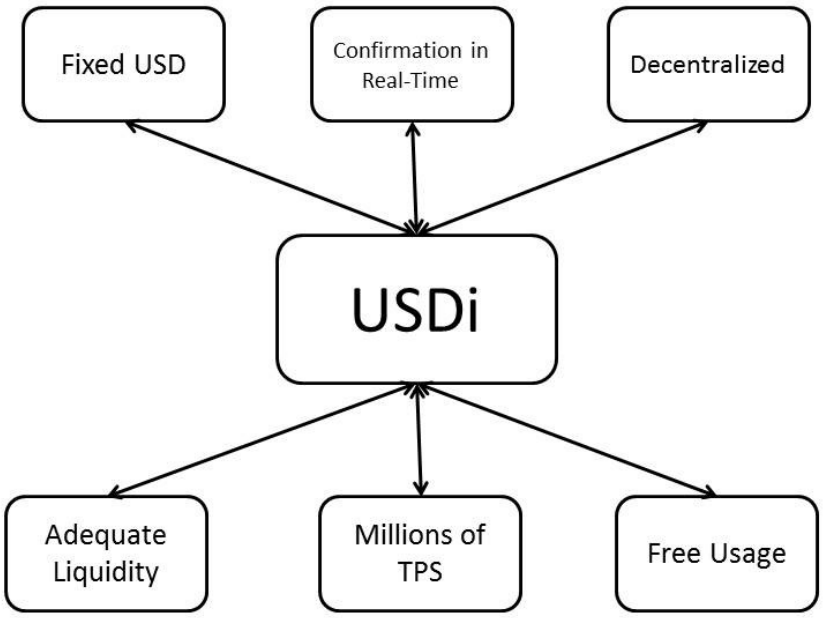
使用者不能創建合約和 DAPP，這樣使系統更透明，效率更高，更穩定，BUG 更少，更安全，更簡單。

移動支付

DSS 將提供 USDi 的支付介面，二維碼支付、NFC 支付，社交支付等解決方案。

全球 USDi 支付

USDi 將成為全球通行的網站和 APP 使用的支付方式。讓人們在生活和商業活動中直接使用 USDi，這是我們重要的目標。



點對點交易系統

PPTS 是系統內置帳戶。PPTS 保證了買賣雙方資金的安全，是一個資金中轉站。買家先付款到 PPTS，在確認收到貨物後，PPTS 才會將 USDi 轉帳到賣家帳戶。PPTS 現階段只能使用 USDi。

櫃檯

賣家通過抵押 DSS 獲取資源，使用櫃檯功能。

櫃檯包括識別標識，用以輸入多媒體內容的資訊介面，存放交易資訊，雙方留言和評分的存儲空間，和其它所必備的功能。

賣家出售商品需要交付 10%的保證金給 PPTS。

仲裁者 Arbitrators

如果買賣雙方出現貿易糾紛，可以申請仲裁。仲裁者隨機介入，最少需要 9 個仲裁者投票，票數多者獲勝 。申請仲裁需支付 1-5%的費用，由失敗的一方支付，收益由票數多的仲裁者和生產者獲得。

仲裁者實行積分和等級制度。

通過抵押 DDS 獲得見習仲裁者身份。在成為正式仲裁者之前，只能投票，無法獲得收益，投票不計分，10 次多數方投票後成為正式的仲裁者。主網上線時的第一批仲裁者直接獲得正式身份。買賣雙方和仲裁者的身份始終都是不可見的，投票資訊在結果出現之前是隱藏的。仲裁者通過成為多數方的投票者獲取積分，更高的積分可以處理更高

金額的交易糾紛，少數方的投票會被扣分，分值由處理的交易金額決定。

以上即是一個實現去中心化的穩定幣和點對點交易系統所需要的方法和理論。

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.