DSS：一个实现去中心化稳定币和点对点交易的系统

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

Takeshi Tanaka

i@dsss.io www.dsss.io

August 26, 2018

摘要：在这份白皮书中，我们将介绍 DSS，它实现了稳定币的去中心化。DSS 中的稳定币 USDi ,将成为区块链网络和生活中的主要货币。DSS 中的点对点交易系统（PPTS），实现了陌生人之间的安全交易。该系统最终可以实现加密货币价格稳定 ,点对点安全交易 ,免费转账，实时确认，每秒数百万次交易的目标。

DSS 使用了 Bitcoin，Ethereum 和 Graphene 的技术。

背景

比特币和其他加密货币的产生有着非凡的意义 ,但是依然存在极大的缺陷：价格波动太大，无法行使价值交换的功能。我们相信，这是加密货币没有得到大量应用的主要原因。加密货币价格的剧烈波动使风险厌恶偏好的资金不会参与其中 ,而这部分资金是金融市场中占比最高的。没有低风险的、价值稳定的加密货币，也是传统金融机构没有选择进入加密货币市场的主要原因之一。

虽然许多区块链平台一直在努力支持稳定币的发展，但是都采用了信用发行、资产抵押的方式，风险非常高。

目标

1.价格稳定

这是稳定币最基本的需求。

2.免费转账

DSS 和 USDi 的转账应该是免费的，高额的转账费用减少了人们使用加密货币的频率。

3.实时确认

一笔转账应该是实时到账的，更长时间的等待会使用户感到担忧，并使稳定币与传统支付手段相比失去优势。

4.百万级 TPS

DSS 的目标是成为全球广泛使用的稳定币支付系统，每秒数百万次交易显得尤为重要。

去中心化稳定币的实现

多代币机制

DSS 包含多个代币，现阶段有 DSS 和 USDi。

DSS 的 ERC20 TOKEN 由众筹获得。在 DSS 主网上线后，ERC20 TOKEN 会转移到 DSS 主网 ,把 DSS 出售给虚拟交易所可以获得 USDi，这是获取 USDi 唯一方式。

共识机制

我们引入一个全新的概念：指数证明（Proof Of Index）。DSS 价格指数是以 DSS 对法币和其它加密货币的价格，按照一定规则制定的指数，是一种共识，就像 NASDAQ Composite Index 一样，包含时间戳、价格和交易量。同一时间所有人获得的 DSS 价格指数都是一样的。如果某个生产者中输入的指数是不同的，那么这个生产者此时产生的区块是不合法的。指数就像时间戳一样自然，以至于我们都忽略了它的存在。DSS 价格指数反映了世界各地的人所作出的无数个决定，而这些人在做决定的时候并不知道其他人在做什么。DSS 承担了价格发现的功能，也表明，自由市场才是价格的决定者。

虚拟交易所

虚拟交易所是 DSS 的核心所在 ,是系统内置账户。USDi 买入过程中，DSS 持币者将一定数量的 DSS 发送到虚拟交易所，并约定价格，虚拟交易所根据收到的包含数量和价格的订单 ,与同一区块的时间段内其它的订单，计算出应获取的 USDi 数量。并扣除少量的手续费后，将 USDi 发送给 DSS 持币者。

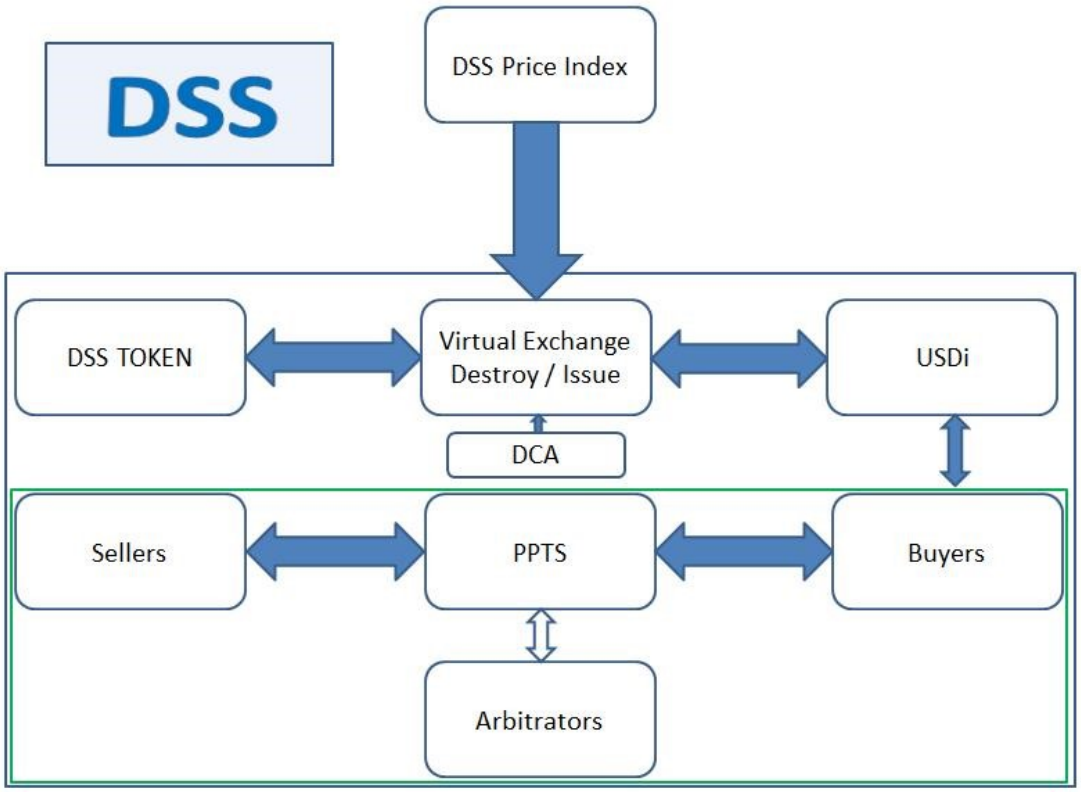
虚拟交易所通过深度曲线算法（Depth Curves Algorithm DCA）计算出虚拟订单薄。参数包括交易量，交易价格，价格变化的速率和 DSS 价格指数。USDi 卖出过程则与买入过程相反。DSS 从 Ethereum 中的合约设计和 Bancor 算法中得出灵感，在此基础上进行了革命性的改进。其中最重要的是加入了 POI 和 DCA。DCA 有效的决定了订单簿（orderbook）和滑点（Slippage）程度。用户在虚拟交易所中大量买卖时，就会得到相对应的滑点。

虚拟交易所综合了交易价格，资金的反应时间，价格心理关口，价格变化的速率，成交量，深度，这些因素之间的相关性。虚拟交易所在一个时间段，将收到的买单和卖单金额相等的部分以中间价[(买一价+卖一价)/2]计算，订单的差额部分，会沿着虚拟交易所的订单薄成交，这些成交订单的最高价或最低价，会成为最新的价格。所有人的交易对手方都是虚拟交易所，差额部分为"副本式"成交：每个订单都独立和订单薄成交的。低的交易成本对于 USDi 的价格稳定有促进作用，虚拟交易所收取 2%%--20%%的费用。高于卖一价、低于买一价的限价单会放在链下。限定了价格的订单，未成交的部分退回会收取 1%%的费用。虚拟交易所会根据接收的订单金额和数量，动态调整最低订单限额。所有的设计保证了流动性，规避了性能的瓶颈。虚拟交易所实现了跨时间，跨空间的价值交换。

人们向虚拟交易所出售 DSS 获取 USDi，使用 USDi 向虚拟交易所购买 DSS。虚拟交易销毁所有收到的 DSS 和 USDi，同时发行成交订单对应数量的 DSS 和 USDi。虚拟交易所没有资产和负债。

虚拟交易所里的中间价会每小时同步更改为 DSS 价格指数最后十分钟的算术平均价。市场中，中间价与 DSS 价格指数互相影响。既能反映资金对价格的冲击，又使 USDi 完美的成为稳定币。

深度曲线算法的优点在于不依赖于流动性，并且一切操作透明，由系统计算完成。



理论依据

DSS 的建立依据是一价定律和套利定价理论

套利者为了获取真实利润，寻找并发现 DSS-USD 和 DSS-USDi 交易对的价格差异，购买并等待 DSS 中间价与 DSS 价格指数同步时出售

这些资产。一价定律被套利过程强行驱动，套利保证了 USDi 始终锚定 USD。套利是自发行动的力量，这是人类的本能，无法阻挡。USDi 属于货币市场，DSS 属于加密货币市场。实际上在信息严重不对称的情况下，暂时的折价和溢价是正常的，只要有充足的流动性，折溢价可以很快消除。

我们用例子来说明，这里的数据是假设的，并且忽略了交易成本。Carl 拥有 200 个 DSS，现在 DSS 的价格指数是 20，虚拟交易所中，DSS 中间价是 20 USDi。Carl 想将 DSS 出售给虚拟交易所换取 USDi，并愿意最低以 19.8USDi 的价格出售。于是 Carl 将订单发送到虚拟交易所的账户地址。在相同的时间，Linda 拥有 2000USDi，她想向虚拟交易所购买 DSS。虚拟交易所在收到 Carl 和 Linda 的订单后，计算得出 100 个 DSS 的净卖量，Linda 将会收到 100 个 DSS。而 Carl 的 100 个 DSS 净卖单，将会沿着深度图以 19.9USDi 成交 50 个，以 19.8USDi 的价格成交 50 个，最终 Carl 获得 3985USDi。虚拟交易所在这两笔交易中，会销毁 200 个 DSS、2000USDi，并发行 100 个 DSS，和 3985USDi。

特征

生产者（Block Producer）激励

虚拟交易所收取的费用会奖励给生产者。为了防止资源的滥用，系统会对一些必要的项目收取一定的费用。这些收益会发放给生产者用作激励。

技术

DSS 使用 Graphene 技术构建并做了大的改变。通过投票产生 21 个生产者和 100 个观察者，而且生产者需要抵押 DSS，时间为 5 年。用户不能创建合约和 DAPP，不需要购买资源，没有每年 5%的通胀，账户竞价只需要抵押 DSS。DSS 遵循最重要的比特币精神：透明，不可篡改，去中心化，安全。DSS 没有宪法，无法冻结账户，私钥丢失无法恢复。除修复 BUG 外，生产者对 DSS 任何规则、数据和代码的改动，都会直接失去生产者身份。

当面临恶意攻击时，除非控制了所有的生产者，否则无法使恶意区块进入不可逆状态。多个生产者被攻击者控制时，100 个观察者和其他节点会发现这些恶意攻击，投票让其出局，并从 100 个观察者中选出新的生产者。

在广播时间平均 0.25 秒后，可以认为交易具有 99.9%的确定性，在 1 秒内提供 100%的不可逆性确认。DSS 和 USDi 转账只需要 1 秒钟就可以确认，这可以被认为是实时的。

如果 Graphene 技术被证明是不安全的，DSS 会采用 Ripple 技术并加以改进：将出块时间缩短，禁止用户创建合约，产生新的区块不会增发 DSS。这样会降低性能，但是可以提高安全性。

以上技术可以完全实现 DSS 的构建。

易用

DSS 会简化 USDi 使用方式 ,用户可以在任何终端方便的使用 USDi。一次典型的 USDi 移动端二维码支付，花费的时间在 10 秒钟以内，这其中包括了打开 APP 和确认的时间。这是非常重要的。人们只需要使用 USDi 即可，不用关心其中的价值转换过程。

资金容量

当 USDi 被广泛使用，而需要更多的 USDi 时，DSS 通过市值增长来满足人们对 USDi 的需求。这是由经济学最基本的供给与需求原理决定的。对 USDi 的需求 ,直接、快速、准确的反应到 DSS 价格指数上。DSS 承载的资金容量是没有上限的。

抵押

DSS 中的所有资源都是通过抵押获得的，消耗的是资金的时间价值。除了使用账户，其他的抵押需要指定时间，最长为 5 年。除竞选和竞价外，所有需要抵押的 DSS 数量都是根据网络状态自动计算的。

稳定的系统

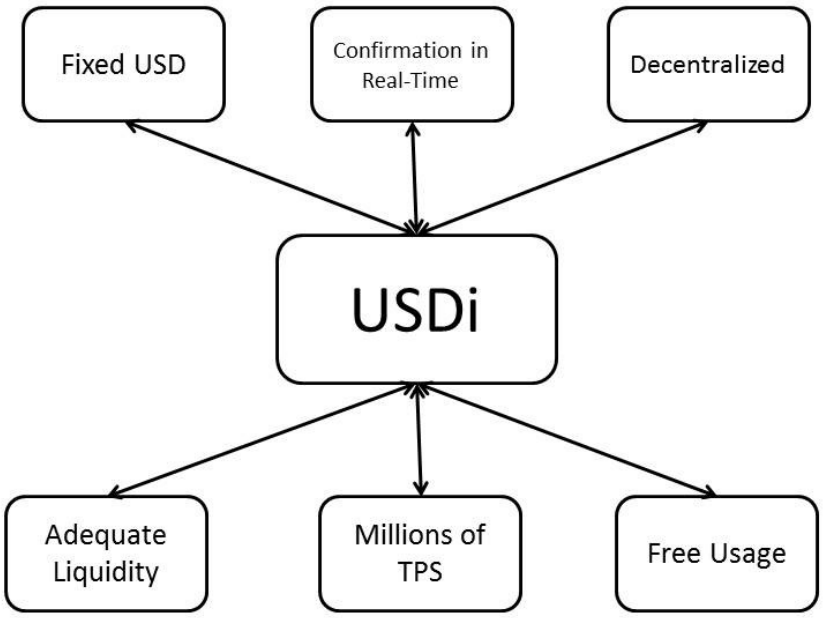
用户不能创建合约和 DAPP ,这样使系统更透明 ,效率更高 ,更稳定，BUG 更少，更安全，更简单。

移动支付

DSS 将提供 USDi 的支付接口，二维码支付、NFC 支付，社交支付等解决方案。

全球 USDi 支付

USDi 将成为全球通行的网站和 APP 使用的支付方式。让人们在生活和商业活动中直接使用 USDi，这是我们重要的目标。



点对点交易系统

PPTS 是系统内置账户。PPTS 保证了买卖双方资金的安全，是一个资金中转站。买家先付款到 PPTS，在确认收到货物后，PPTS 才会将 USDi 转账到卖家账户。PPTS 现阶段只能使用 USDi。

柜台

卖家通过抵押 DSS 获取资源，使用柜台功能。

柜台包括识别标识 ,用以输入多媒体内容的信息接口 ,存放交易信息，双方留言和评分的存储空间，和其它所必备的功能。

卖家出售商品需要交付 10%的保证金给 PPTS。

仲裁者 Arbitrators

如果买卖双方出现贸易纠纷，可以申请仲裁。仲裁者随机介入，最少需要 9 个仲裁者投票 ,票数多者获胜。申请仲裁需支付 1-5%的费用，由失败的一方支付，收益由票数多的仲裁者和生产者获得。

仲裁者实行积分和等级制度。

通过抵押 DDS 获得见习仲裁者身份。在成为正式仲裁者之前，只能投票，无法获得收益，投票不计分，10 次多数方投票后成为正式的仲裁者。主网上线时的第一批仲裁者直接获得正式身份。买卖双方和仲裁者的身份始终都是不可见的 ,投票信息在结果出现之前是隐藏的。仲裁者通过多数方的投票者获取积分 ,更高的积分可以处理更高金额的交易纠纷，少数方的投票会被扣分，分值由处理的交易金额决定。

以上即是一个实现去中心化的稳定币和点对点交易系统所需要的方法和理论。

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.