

VSS 白皮书

White Paper



V1.0

打造全球顶级数字货币交易平台

摘要

随着区块链技术的进步以及项目应用逐步落地，通证经济从技术复杂度、内容深度和广度都有极大地提升，其所代表的全新投融资模式和商业经济形态正呈现出旺盛的生命力。

VSS 是一个去中心化交易所，旨在打造更透明、更安全、流动性更强的数字资产交易平台。与市面上现有交易所不同，VSS 将以自身对区块链行业的深刻理解，重新解读市场、改变市场，为用户提供极致的服务。

文档用途

本文档的用途是初步介绍 VSS 的系统模式，具有相当的技术性，适读人员是对于区块链行业有一定了解的相关从事人员、投资人或消费者，以及对比特币、以太坊等加密货币有一定了解的人员。

文档范围

本文档描述了 VSS 平台系统架构的重要的组成元素和细节，开发团队会对现有产品的架构设计及功能进行优化和升级，因此，实际产品可能会出现和此文档介绍的有所不同。

目 录

一、数字资产服务行业现状.....	1
二、数字资产服务行业痛点分析.....	2
2.1 技术架构有待提升.....	2
2.2 产品体验较差.....	2
2.3 安全稳定性低.....	3
2.4 新项目审核机制不完善.....	3
2.5 平台优化差.....	3
三、VSS——全球顶级数字货币交易平台.....	4
3.1 VSS 品牌释义.....	4
3.2 VSS 团队介绍.....	4
3.3 VSS 愿景.....	5
3.4 VSS 核心功能简介.....	5
3.5 VSS 盈利模式.....	6
3.6 VSS 优势.....	6
四、VSS 技术解析.....	8
4.1 VSS 系统的技术支持.....	8
4.2 VSS 系统架构.....	8
4.3 VSS 系统核心业务背书.....	9
4.4 分配 ID 并避免哈希计算.....	11
4.5 从业务逻辑处理器中去除签名校验.....	11
4.6 智能合约.....	12
五、平台币 VSS 介绍.....	14
5.1 什么是 VSS?	14
5.2 VSS 分配方式.....	14
5.3 VSS 权益机制.....	15
5.4 VSS 获取途径.....	15
5.5 VSS 升值逻辑.....	15

六、团队介绍.....	16
七、免责声明及风险提示.....	20
7.1 免责声明.....	20
7.2 风险提示.....	21

一、数字资产服务行业现状

近几年来，基于区块链技术的数字资产种类不断丰富，规模迅猛增长。截至2019年7月，全球区块链数字资产种类超过3000种，资产规模约3000亿美元，区块链数字资产钱包用户约2000万人，明显看出，当前区块链数字资产投资还处于萌芽期，市场拓展空间极大。在当今行业发展中，最迅猛的无疑是交易平台。

交易平台作为数字资产流通集散地，不仅连接着一二级市场，也连接项目方和投资者。遗憾的是，在以去中心化理念的区块链世界，绝大多数交易平台却是高度中心化的。这里的中心化不单单指底层的交易撮合方式，更多是指平台的理念和价值观，包括通证经济模型、平台治理机制、利益分配。

绝大多数中心化交易平台都存在资产不透明、利益分配不公平、暗箱操作等弊病，受制于既得利益，中心化交易所没有能力，也没有动力去主动改变现状。区块链创业者和数字资产投资者需要更加公平、透明、开放、民主的交易平台。

如今全球数字货币交易平台有数千家，市场增量极大，当今交易平台的比拼，不再只是技术层面的较量，而是通证经济、治理机制、生态建设全方位的竞争。

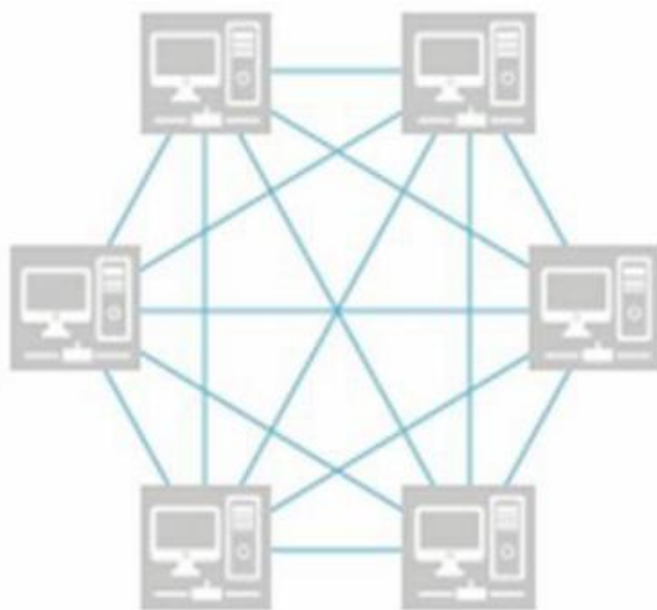
基于区块链技术的数字资产服务平台目前主要分两类：一类涉及各国国家法定货币，提供数字资产与法定货币兑换业务的服务平台；另一类则是我们涉足并专注的领域，纯数字资产之间交易服务的平台。从目前的市场整体状况来看，纯数字资产间交易业务的需求和交易总量的增长已经成功超越国家法定币兑换数字资产服务的规模。目前数字资产服务市场普遍存在缺乏创新性和用户流通成本过高的问题，很大程度限制了数字资产服务平台行业的发展。

二、数字资产服务行业痛点分析

2.1 技术架构有待提升

当前，市面上大部分主流交易所在技术架构方面仍然存在较大提升空间，他们只是非常简单地各种功能拼凑搭建出一个服务平台。这种做法在之前极为常见，但区块链行业的发展需要更为专业的技术团队来支撑。为了保证快速稳定地处理高并发交易请求，服务平台必须从底层提升系统的效率及容错能力，从而保障用户的资产安全。

迄今为止，已有大量新闻爆出各个交易所因技术构架低级带来了各种安全问题，这令人十分遗憾，同时，这种现象也是当前市场上极为常见普遍的现象。



2.2 产品体验较差

作为一项处于整个科技产业链前沿的产业，当今不少区块链交易所在产品体验方面表现一般，甚至可以说非常原始且简陋。

2.3 安全稳定性低

对于平台来说，安全是重中之重。事实上，因黑客攻击而导致关闭的服务平台已经多达几百家，这为数字货币交易所和热爱区块链技术的用户带来了巨大的损失。哪怕以当前顶级头部交易所币安而言，也在近期内发生了被盗 7000 余个比特币的丑闻，头部交易所尚且如此，其他被盗事件，更是屡见不鲜：

2014 年 2 月，日本 Mt.Gox（门头沟）交易所 85 万枚比特币被盗；

2015 年 1 月，意大利 bitstamp 交易所 19000 枚比特币被盗；

2016 年 8 月，bitfinex 交易所 12 万枚比特币被盗；

2017 年 4 月，韩国 youbit 交易所 17% 的数字资产被盗；

2018 年 1 月，日本 Coincheck 交易所 5.23 亿个数字货币被盗；

2018 年 5 月，韩国最大，全球排行第五的交易所 UPbit 被调查，涉嫌转移顾客账号资金给公司账号……

2.4 新项目审核机制不完善

目前行业内的数字货币交易所在处理新项目加入的审核流程存在严重的机制不合理。具有安全审查技术实力的大型平台收费过高，导致大量优质合规的新项目无法加入平台，而往往不合规的项目方更愿意支付大额审查费用来通过审查，然后通过损害普通用户的利益短时间获取大量数字资产。另外大量中小型服务平台又不具备合格的安全审查技术，优质项目被大量的劣质项目淹没。整个市场目前处于“劣币驱逐良币”的恶性循环中。

2.5 平台优化差

由于当前行业发展过快，许多数字货币交易所在优化层面问题极大，看似外表光鲜，然而内部优化问题极为严重，这其中不乏许多知名交易所。动辄掉线、黑屏、卡顿竟是常见情况，这给用户带来了非常不好的体验，甚至会导致用户对于整个交易所实力产生怀疑。

三、VSS——全球顶级数字货币交易平台

3.1 VSS 品牌释义

当今市场存在诸多乱象，作为顶级的去中心化交易所，VSS 将打造更透明、更安全、流动性更强的数字资产交易平台。与市面上现有交易所不同，VSS 将以自身对区块链行业的深刻理解，重新解读市场、改变市场，为用户提供极致的服务。

最终，VSS 将用实际行动重新解读区块链行业，创建一个安全、稳定、便捷、全面的区块链产业生态体系。

3.2 VSS 团队介绍

VSS 团队高层拥有 10 年以上的金融风控和大型互联网平台运营经验，团队成员包含骨灰级币圈大佬、原华尔街量化交易团队成员、原顶级市值管理团队人员、顶级电子交易系统架构师、千万用户级别高并发互联网社区高管等。

VSS 总团队成员超过 100 人，其中约 30% 为专业运营人员，他们是有创意、有想法的运营团队，能够实时了解科技发展动态、进行精准的市场推广、有效的市场维护指导，并建立全方位的社群维护体系。

同时，VSS 其余技术人员均拥有多年技术开发经验，在所从事的本专业工作领域里曾有不凡的业绩，具有非凡的创新能力，并具有对最新技术执拗的探索精神。

3.3 VSS 愿景

VSS 致力于打造极速、安全、自由、自治、高效、稳定、透明的全球化数字货币交易平台，交易用户和投资者可以在 VSS 上极速安全的交易，VSS 会创建公正、透明、安全的交易环境，并利用高并发系统保证撮合交易的稳定性。

同时，VSS 创新地提出了数字资产交易平台社区化的规划，VSS 社区是一个基于 Token 经济模型打造的新形式的组织，每个 VSS（平台币）持有者都有权利参与社区的业务决策、团队选举等社区活动。

VSS 是一个所有 VSS 持有者共有、共治、共享的数字资产交易平台，我们将打造成一个具有良性生态循环的交易平台。

未来，VSS 将会利用自身优势，打造自有公链，它将会逐渐进化为一种生态系统。由此，未来 VSS 将不断寻求拓展区块链应用技术创新，为所有通过互联网提供服务的行业提供基础支持。

3.4 VSS 核心功能简介

VSS 核心平台将覆盖 PC，MAC，IOS，Android，H5，功能上包含现货交易，合约交易，货币理财，OTC，全球行情，最新资讯，社区等各大特色模块。

现货交易：币币之间的自由交易，满足用户数字货币资产交易兑换的要求。

合约交易：用户可添加杠杆进行合约交易，最多可使用 20 倍杠杆。

货币理财：通过平台提供的理财功能，用户可投入数字货币获得资产增值。

OTC：用户在完成 KYC 验证后，可在平台撮合下完成场外交易。

全球行情：平台内将显示当前主流货币行情，助于用户快速了解行情。

最新资讯：用户可在平台内查看最新行业资讯。

社区：为给用户带来更好的体验，平台内将牵头搭建资讯交流社区，为用户提供更多的服务。

平台币 VSS，支持 BTC、VSSH、USDT、VSS 四种交易区。所谓的 BTC 交易区就是指使用 BTC 和其它币种之间的买卖。在 VSS 上，BTC、VSSH、USDT、VSS 两两直接也可进行交易。

3.5 VSS 盈利模式

VSS 数字货币交易平台的主要收入及利润来自平台的良好运行，与此同时，平台在获取利润后，将会回馈用户，提供更加优质的服务体验。

VSS 盈利方式包含：

1. 交易手续费：用户在进行数字货币交易时，需向平台支付一定比例的手续费。后期会根据运营需要及用户历史交易级别，设置不同手续费比例。
2. 提现手续费：数字货币进行提现时，需要支付平台一定数额的提现手续费。
3. 会员服务费：用户购买平台会员服务获得交易手续费折扣优惠、增值服务，以此作为运营手段锁定用户。
4. 上币费：平台会不定期上线一些优质数字货币作为交易标的，并收取一定数额的上币费。
5. 杠杆手续费：平台会上线期货交易功能，支持杠杆交易，并向用户收取一定比例的手续费。
6. 理财板块：平台将会推出数字资产的理财与借贷服务。
7. 其他收入：其他通过各类平台生态资源输出获得的收入。

3.6 VSS 优势

顶级技术

世界级金融交易架构，通过先进的内存撮合算法、异步非阻塞读写、分布式实时消息框架等先进技术实现系统的高可靠性、高性能、强安全性、可扩展性以及易维护性。预计我们的系统能达到 20 万笔/秒的处理速度，同时证券级别的 API 接口支持高频、GTT、GTC、FOK、ICO 等专业交易指令。为专业技术基金提供交易支持。

公开透明

面向所有人实时公开透明的交易平台，建立实时的资产与交易数据查询验证机制。做到完全公开透明，让用户安心，提升用户归属感与凝聚力。

自治生态

VSS 迈出了数字资产交易平台社区化的构想和运营模型，未来会成为交易平台的典范。

VSS 将建立一个所有 VSS 持有者共有、共治、共享的社区型组织。

顶级安全

立体安全防护体系，与世界级的安全公司合作，上线前对全站代码进行代码审计。架设多级防火墙，实时监控数据异常。在用户资产上，采用多重签名及冷热隔离的钱包方案，最大程度保障用户资产安全。

专业团队

团队核心成员主要包括技术、运营、产品、商务等，均有着丰富的行业经验与能力，依靠传统金融交易行业的专业服务经验结合顶级的系统研发实力。整个团队将为打造一个开放、公平、共享、自由的区块链资产交易平台而努力。

四、VSS 技术解析

4.1 VSS 系统的技术支持

高效且可扩展性能：

高性能的区块链技术对加密货币和智能合约平台来说是必须的，VSS 从底层开始重新设计。通过股份授权证明机制，VSS 网络可以在平均一秒的时间内确认超 20 万次转账交易。

安全有保障：

作为顶级的去中心化数字货币交易平台，安全问题是重中之重，VSS 在通过技术手段保证系统安全的同时，还准备了相应的安全储备金存放在区块链上，为用户提供保障。

开源且完全透明：

VSS 源代码已在全球最大第三方开源站点 github.com 公开。整个交流是开源的，由一个非常开放的社区支持。没有任何地方会做到 VSS 一样的透明。

4.2 VSS 系统架构

VSS 系统构架技术的关键点如下：

在内存中存储数据

以单一线程存放核心的业务逻辑

在核心业务逻辑以外存放加密算法操作

将校验的操作已经状态独立和状态依赖检查

使用一种面向对象的数据模型

通过遵守这些简单的规则，VSS 在未进行颠覆式优化工作的情况下，实现了每秒处理 20 万次转账的高效性能。如果有进一步的优化工作的话，会让 VSS 处理速度获得进一步提升。

需要注意到，VSS 达到这样的性能表现是高度依赖其中的一个兼容交易协议。如果想用业务逻辑运行在一个进行加密算法操作和用哈希识别器去调用所有对象的虚拟机上的话，不可能达到同样层级的性能表现。区块链天生就是单线程

的，而单核的 CPU 的性能是各种资源中最短缺的、最难扩展的一个方面。VSS 的技术逻辑能够让这个单线程的执行达到极可能的高效。

4.3 VSS 系统核心业务背书

区块链是一个下达关于确定去修改一个共享的全局状态交易的全球账本。这些交易中包含的命令可以改变其他交易的有效性。例如，你不能在你的支票存入生效前，从你的银行账户里支取金额。在能够影响一个特定的账户的所有先前交易都被处理之前，你不可能知道一个交易是否有效。

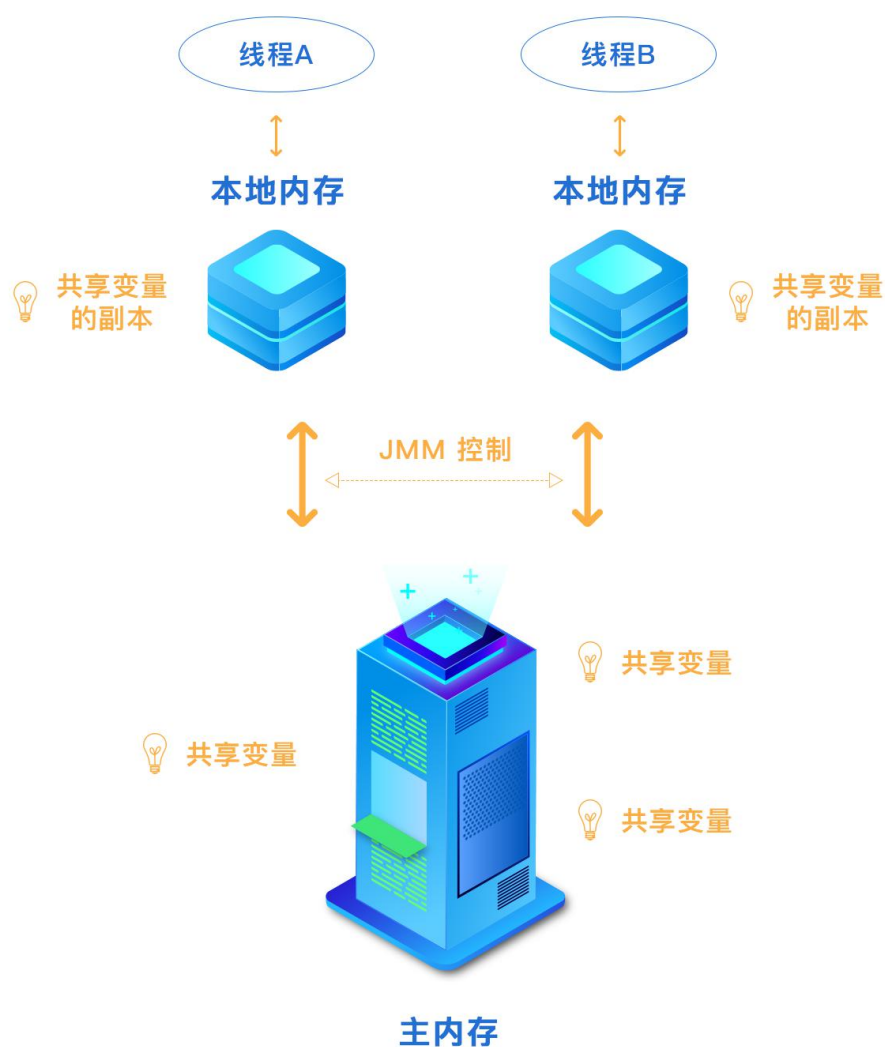
如果两个无关联的账号没有共享任何通用的依赖关系的话，理论上这两个账号的交易可以是在同一时间进行处理的。实际上，在一个由具备仲裁条件的智能合约驱动的账本上识别哪些交易是真正独立存在的耗费是很棘手的。唯一的保证两个交易是真正独立存在的方法，是通过维护完全分离的账本，然后定期在它们之间传输价值。如果要用这种性能表现的权衡关系去打比方的话，可以像是非一致内存访问架构 (Non-Uniform Memory Access, NUMA) 和一致内存访问架构 (Uniform Memory Access, UMA) 之间的关系。

实际上，一致内存访问架构对开发者来说是更容易去设计的，而且耗费更低。非一致内存访问架构通常是在建造超级计算机和大型计算机集群时作为不得已的方法去采用的。计算机产业逐渐意识到通过平行计算去实现性能的扩张并没有早期那么容易，毕竟那时候最需要做的事情只是提高处理器的频率而已。就是因为这个原因，处理器的设计者们在尝试去采用多线程去提高性能之前都在拼命去提高单线程的性能。当多线程还不够的话，而且只有这样的话，集群计算这个方案才会被考虑。

很多加密货币产业的人在探索过在技术上一台电脑的单个核心能实现什么之前，就尝试通过用集群计算的方案去解决可扩展性的问题。

业务逻辑处理器是所有顺序交易和订单匹配发生的地方。它是一个可以每秒处理百万级别订单的单线程。这个架构可以很容易地用在加密货币和区块链设计的领域。输入分解器扮演的角色是从很多来自不同源头的用户里面收集订单，然后分配给它们一个确定的顺序。当给它们分配好顺序后，它们会被复制、记录然后广播到很多冗余的业务逻辑处理器。输入分解器是高度并行的，而且容易分包

到一个计算机集群系统中。当业务逻辑处理器处理完输入后，一个输出分解器负责通知那些关心结果的人。



4.4 分配 ID 并避免哈希计算

在单线程系统的系统里面，处理器周期是需要被保留的稀缺资源。传统的区块链设计使用加密算法基础上的哈希计算去生成一个全球独特的 ID 系统，以实现统计学上不会有碰撞的保证。进行这些哈希计算的问题是，它会耗用越来越多的内存和处理器周期。与一个直接的数组索引相比，这种方式会显著地占用更多处理器的时间去查找一个账户的记录。

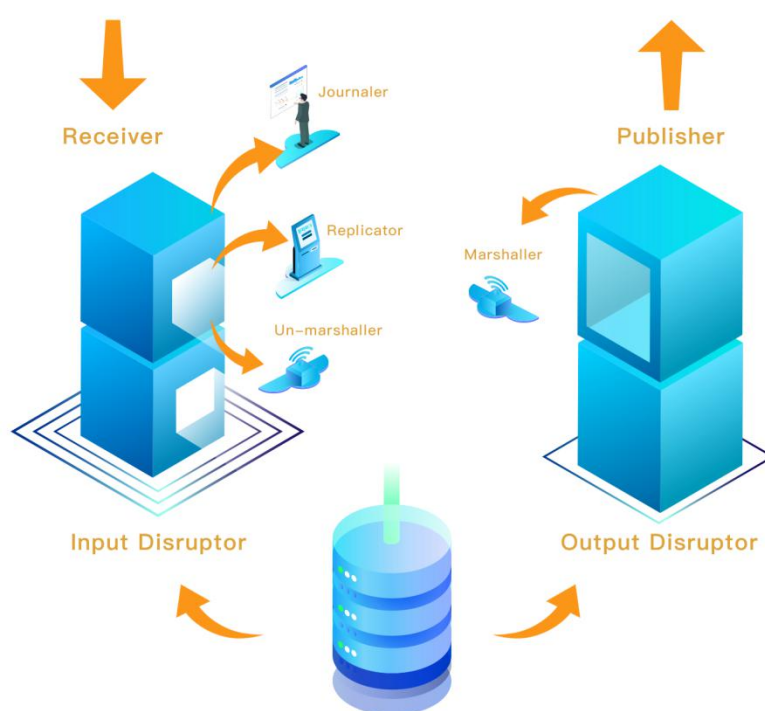
例如，64 位的整数对比和操作起来都要比 160 位以上的 ID 更简单。更大的哈希 ID 机制意味着 CPU 缓存里面的空间更少了，而需要更多的内存。在现代的操作系统里不常访问的随机存储器是会被压缩的，不过哈希识别器是随机数，这是没法压缩的。型号区块链给了我们一个在全球内分配独特的 ID 的方法，这些 ID 互相之间不会起冲突，因此完全避免使用像比特币地址那样的哈希算法为基础的识别器去引用一个账号、余额或者许可。

4.5 从业务逻辑处理器中去除签名校验

所有在加密货币网络的交易依赖于用加密算法签名去校验权限。大部分情况下，请求的权限可以由其他交易的结果改变。这意味着在业务逻辑处理器里面，权限需要被定义成与加密算法计算无关的情况。

要达到这个目的，所有的公钥需要分配一个独特的和不可代替的 ID。当 ID 被分配后，输入分解器可以校验提供的签名与指定的 ID 是否匹配。当交易到达业务逻辑处理器后，只需要去检查 ID 就可以了。这个同样的技术可以在拥有不可代替的静态 ID 的对象上实现去除前提条件检查。

对交易来说，有很多特性是可以进行静态检查的，而不需要引用当前的全局状态。这些检查包括参数的范围检查、输入的去冗余和数组排序等。通常来说，有很多检查是可以被进行的，如果交易包含它“假设”是全局状态的数据的话。在这些检查被执行后，业务逻辑处理器必须要做的事情就只有去确保这些假设还是正确的，这个过程总结下来就是检查一个涉及交易签名时间的对象引用的修改时间戳。



4.6 智能合约

很多区块链正在整合一种通用的脚本语言去定义所有的操作。这些设计最终将业务逻辑处理器定义为一个虚拟机，而所有的交易被定义为由这个虚拟机运行的脚本。这个方案有一个在真实处理器上的单线程性能极限，并且由于将所有东西强制通过一个虚拟处理器去执行，让问题更严重了。一个虚拟处理器即使用上了实施编译技术(JIT)也总会比一个真正的处理器要慢，不过计算速度并不是这种“任何东西都是一个脚本”方案的唯一问题。当交易被定义在这么低的层次上，意味着静态检查和加密算法操作还是会被包含到业务逻辑处理的环节里，这也让会让整体的吞吐量降低。一个脚本引擎永远不应该要求执行一个加密算法签名检查的请求，即使这个请求是通过原生的机制实现的。

区块链设计的虚拟机应该考虑到单线程表现。这意味着在一开始就要为实施编译优化，而且最常用的智能合约应该通过区块链原生支持，而只有那些不常用的、定制的合约会运行在一个虚拟机上。这些定制的合约设计的时候要考虑性能，

这意味着虚拟机应该将可以访问的内存范围限制到可以放在处理器缓存上的级别。

在内存中保存所有东西的其中一个好处是，软件可以设计成模仿现实世界中数据的关系。这意味着业务逻辑处理器可以迅速根据内存内的指针去找到数据，而不是被迫去进行耗费高的数据库查询任务。这意味着数据不需要复制就能访问了，而且可以当场就被修改。这个优化提供了比任何数据库为基础的方案高一个数量级的性能表现。

VSSVSS 系统的高效性能的成功创建，是建立在核心业务逻辑上去除与关键性、订单依赖性和评估无关的计算任务，并且设计一个可以帮助优化这些事项的协议。这就是 VSS 做的事情。

五、平台币 VSS 介绍

5.1 什么是 VSS?

VSS 致力于成为领先的基于社区共识的全球化数字资产交易平台。VSS 平台推行的代币 VSS，发行总量恒定发行 1 亿个，且保证永不增发。



VSS 将作为整个平台的血液，流通运转于整个平台之中，未来，VSS 将会参与更多平台生态建设，为平台的良性发展贡献力量。

5.2 VSS 分配方式

1% 空投

3% 市场宣发

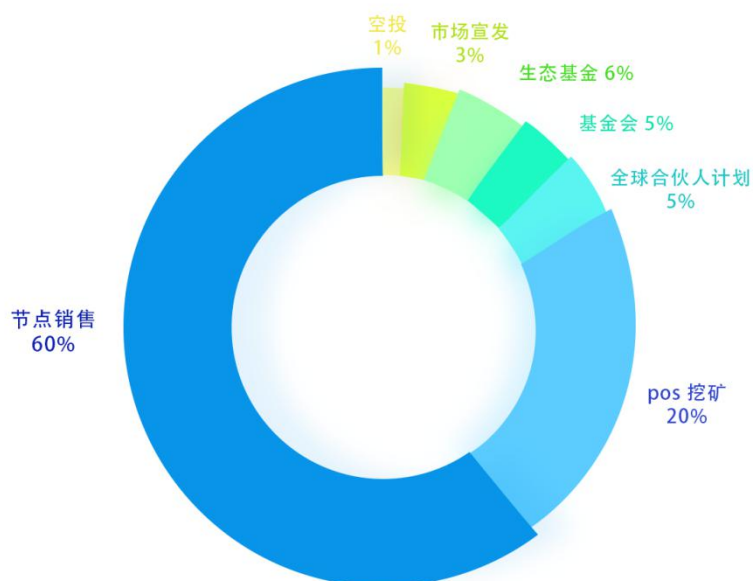
6% 生态基金

5% 基金会

5% 全球合伙人计划

20% pos 挖矿

60% 节点销售



5.3 VSS 权益机制

拥有 VSS 的用户，可参与投票、手续费服务抵扣、优先领取糖果、项目推荐优先上市等权益。

VSS 作为可协商加密数字权益证明，将成为未来数字经济时代的基本要素。VSS 代表 VSS 社区的权益，是 VSS 社区治理的基石。

5.4 VSS 获取途径

※购买 VSS

通过币币交易，OTC 交易，购买 VSS。

※贡献奖励 VSS

邀请新用户，社区内容贡献，产品体验建议。

※市场活动获得 VSS

糖果派送，抽奖，空投等方式获赠 VSS。

※参与节点销售获得 VSS

用户可利用手中其他数字货币获得 VSS。

5.5 VSS 升值逻辑

为提升 VSS 的价值，我们设计了一套完整的 token 销毁模式，平台每月将拿出各类获取收入用于回购并销毁 VSS，以此提升 VSS 的稀缺性，促使 VSS 不断升值，当 VSS 总数下降至 2100 万枚时将停止销毁。我们坚信，完善的 token 体系将吸引更多的投资者进入，形成良性循环，具体细则如下：

※每月收取交易手续费的 50%将用于回购并销毁 VSS

※每月收取上市费的 60%将用于回购并销毁 VSS

※每月收取节点销售费用的 3%将用于回购并销毁 VSS

未来，VSS 会全力寻找更广泛的盈利点以及更多商业伙伴！为 VSS 减少至 2100 万的流通量不懈努力！

六、团队介绍



최광수

CEO

毕业于首尔大学金融系，有着超过 10 年金融行业从业经验，7 年以上区块链从业经验。



안무현

CMO

毕业于延世大学新闻系，有着丰富的市场运营经验，对整个区块链行业有着极深的看法与理解。



Mike

CTO

毕业于伦敦大学并获得了计算机科学硕士学位。他在系统构架方面取得了很大的成就。目前负责 VSS 整体技术开发工作。



Bill

COO

毕业于斯坦福大学金融专业，曾在华尔街任职多年，目前负责 VSS 整体运营工作。



Glen

核心技术人员

毕业于斯坦福大学，拥有服务端丰富的开发经验，现负责 VSS 服务器高并发系统开发。



Edwin

核心技术人员

毕业于芝加哥大学，参与过数个知名区块链项目研发，现负责 VSS 前端功能开发。



Tom

安全顾问

毕业于弗吉尼亚大学，拥有超过 10 年以上的网络安全经验，现在负责 VSS 网络安全工作。

七、免责声明及风险提示

7.1 免责声明

该文档只用于传达信息之用途，并不构成买卖 VSS 股份或证券的相关意见。任何类似的提议或征询将在一个可信任的条款下并在可应用的证券法和其他相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。

本文档不构成关于证券形式的投资建议、投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。VSS 明确表示相关意向用户明确了解 VSS 的风险，投资者一旦参与投资即了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。VSS 明确表示不承担任何参与 VSS 项目造成的直接或间接的损失，

包括：

- 1、因为用户交易操作带来的经济损失；
- 2、由个人理解产生的任何错误、疏忽或者不准确信息；
- 3、个人交易各类区块链资产带来的损失及由此导致的任何行为；

4、VSS 不是一种投资。我们无法保证 VSS 会增值，在某种情况下也有价值下降的可能，没有正确使用其 VSS 的人有可能失去使用 VSS 的权利，甚至会可能失去他们的 VSS。

5、VSS 不是一种所有权或控制权。控制 VSS 并不代表对 VSS 或 VSS 应用的所有权，

6、VSS 并不授予任何个人任何参与、控制，或任何关于 VSS 及 VSS 应用决策的权利。

7.2 风险提示

安全：

许多数字资产交易平台因为安全性问题而停止运营。我们非常重视安全，但世界上不存在绝对意义上的 100%安全，例如：由于不可抗力导致的各种损失。我们承诺尽一切可能确保您的交易安全。

竞争：

我们知道交易平台是一个竞争异常激烈的领域，有数千个团队正在计划并着手开发交易平台，竞争将是残酷的，但在这个时代，任何好的概念，创业公司，甚至是成熟的公司都会面临这种竞争的风险。但对我们来讲，这些竞争都是发展过程中的动力。