STASH

藏匿白皮书 V1

2017/6/27

藏下一代 Cryptocurrency

介绍

藏匿是开放源码的加密货币，结合从比特币、 短划线和 Zcash 的许多创新协议功能同时解决目前遇到的各种数字货币的众多问题。虽然不同的 cryptocurrencies 具有多样和宝贵每个属性也有他们自己的问题。这些问题包括慢交易速度，交易成本高、 扩展性差、 公平的发射、 强烈的隐私、 实际治理框架、 连续的筹资结构和正确的用户奖励。藏匿的目标是要在一起的许多最前沿的 cryptocurrency 功能和在证明块生成链技术来解决或消除这些问题。这反过来应该创建是越来越有用的和需要为最终用户和长期持有相似的 cryptocurrency.

这被设想，随着时间的推移新功能会被内部开发，以及在逃来自加密的社区，以及新的创新成为可用储备网络决定可以实现这样的功能，来提高储备数字货币的效用。

而不是静态和刚性藏匿的想法是虽然有机演变及其社会的帮助下，数字货币。为此，藏匿发起了令牌销售以收集资源，帮助人们提高认识作为吸引人才和志同道合开发者从全球各地去帮助发展和创新的数字货币。

虽然已经取得了很大的进步从藏匿令牌销售增加的资源，将有助于加快和改善藏匿 Cryptocurrency 隐私通过零知识安全层 (ZSL) 一体化的发展。ZSL 藏匿在将旨在在 blockchain 上匿名结算的交易记录。隐藏标记所有者将能够使用其藏匿令牌来购买 1 1 基础藏匿 Cryptocurrency 一旦 ZSL 一体化已定稿。一旦他们被用于购买藏匿 Cryptocurrency， 藏匿的所有令牌将被烧都死。

虽然令牌销售资金将提供初始资本集成所需的 ZSL， 预算编制系统和财政部，将每月从块奖励资助了藏匿将意味着该项目继续有足够的资源发布令牌出售 基金正在利用。

藏匿将永远努力进化和适应的灵活的、 开放的、 灵活到可能出现的新机会。为此目的藏匿治理系统已设置为快速采用并利用新的机会，作为他们变得明显而无需处理一些分散的决策问题，明显与其他加密的货币。藏匿的终极目标是简单，为每一天，国际交易成为最有用的和方便用户的加密货币给最终用户。

Incentivizednode 网络

数字货币操作，全部节点是必需的。这些节点操作在 P2P 网络上，并将更新发送到网络发生的事件后的同龄人。然而，为了向 是有效的此类节点需要高容量，以及支持从额外的资源，要付出重大代价。

这可以导致的全部节点，不断减少如目睹比特币网络上。对这样的结果是一大败笔性能，与块传播时间超过 40 秒。

藏 cryptocurrency 打击这通过 2nd 层网络层作为一种安全网，保证长时间的高性能。这是服务的 Incentivizednode 网络的高可用性并必须提供一定水平，如果他们有资格获得激励 Incentivizednode 奖励计划节点。

Incentivizednodes 奖励？

Incentivizednode 奖励计划有助于激励网络，越来越多的任何一次都是业务的全部节点。如果没有这种程序，网络运营商必须支付的全部节点作为交通跨网络的增加，可以是不可持续。

Incentivizednode 网络是服务的不同的因为单个节点被捆绑进特定水平，这服务的有抵押保障的。该担保物仍然受保护的而 Incentivizednode 仍在运作，鼓励跨网络的稳定性和给 Incentivizednode 运营商赚取额外储备数字货币的机会。

这些款项来自块奖励累积在网络上，与共 Incentivizednodes 人秉承自己的服务水平在股息付给的 45%左右。然而，有一些波动，总的金额支付每一天，Incentivizednode 奖励计划百分比固定的和节点的数目却变量。广交; 计算每日的 Incentivizednode 操作付款

$n * r * s / t$

在其中

n = 块每一天

r = 块奖励

s = Incentivizednode 共享的每个块奖励

t = Incentivizednodes 总数

计算奖励费在 Incentivizednode 上的，将使用以下公式，基于相同定义以上;

每 Incentivizednode 收益率 $= (n * r * s) / t * 365.25 / 10000$

其中 10,000 = Incentivizednode 操作所需的储备 cryptocurrency 担保的数额。

有可用的只有数量有限的藏匿处 cryptocurrency，涉及与运行 Incentivizednode 有一限制，在多少 Incentivizednodes 可以在网络上运行在任何给定的时间成本。此限制基于藏匿在令牌销售中生成加任何储备，储备 blockchain 启动以来已开采 500 m。

Incentivizednode 安排

伪随机的确定性方法用于订购 Incentivizednodes 采矿块哈希算法。挖掘网络通过对于每个块使用的哈希值从工作证明提供此功能的安全。

担保制度

它是任何一个个人或机构获得的整个网络的 Incentivizednodes 控制系统的安全性的关键。要实现这一目标后，提到担保制度已，其中任何人想要控制活动的 Incentivizednode 必须放下 10,000 藏匿作为押金。供应意味着藏匿 cryptocurrency 有限的藏匿的价格直接、 迅速地对需求作出反应。要获得在网络上的一个重大部分的 Incentivizednodes 控制，个人需要购买大量的储备单位从公开市场，抬高价格，使得他们能够实现他们的目标。

这使得整体的藏匿处网络，利用 2nd 层 Incentivizednode 网络进行敏感任务。没有信任或整体责任颁发给任何一个节点或组节点，，所以谁也不能控制他们自己的网络结束因为 Incentivizednodes 随意挑选的同时执行相同的任务。

网络监督制衡

Incentivizednodes 的作用并不限于继电保护及验证交易。还有其他，非常重要的这些节点可以提供的好处。因此，网络必须能够评估这 Incentivizednodes 是在线、 哪些积极响应，和哪些行为符合他们已同意的服务守则至关重要。

这就需要证明的服务。它不是服务的简单地评估哪些 Incentivizednodes 仍在运作，也必须达到一定水平。为了确保这种服务水平，Incentivizednode 网络使用 Quoroms;对于每个块，选择两个仲裁，仲裁 A 评估服务水平的法定人数 B.仲裁 A 由接近当前块的哈希值的节点。仲裁 B，另一方面，是组成的节点最大限度地远离此哈希。

以这种方式的系统保持不可靠通过随机选择通过仲裁制度使得网络节点自访问。

Incentivizednode 程序

Incentivizednode 的基本功能很简单来转播及验证交易记录，如节点要求只有两个协议消息变得活跃藏匿网络上。这两个消息是 Incentivizednode 宣布消息和 Incentivizednode ping 消息。

宣布消息协议用于宣布的网络上的节点的存在，它最初启动时。在此之后，ping 消息协议将会每隔 15 分钟，作为的一部分发送服务程序的证明。如果这不令人满意的速度进行的该节点将最终被停用。此外，该节点必须随时准备接受 ping，其端口如果不是，它被认定为非活动状态。

然而，在实践中，它们的功能都较为复杂，并且依靠附加议定书，包括 PrivateSend 和 InstantSend，两个用于确定服务的证明。

当用户发送 10000 个藏匿 cryptocurrency 单位到指定的地址，在网络上的指定钱包时，Incentivizednode 将被激活。一旦确认了这一行动，该节点将能够使用公布和 ping 协议消息通过网络传播本身。

该网络包括内置的安全措施中使用冷模式以防止在系统上的恶意活动。例如，如果 Incentivizednode 将私钥发送激活后的消息中，这一台机器上使用，系统将停用原来的节点，10000 个藏匿单位免受盗窃。

10,000 藏匿 Cryptocurrency 抵押品不需要存储在实际 Incentivizednode 钱包，但宁愿可以被远程存储在安全的位置，防止被盗藏匿 Cryptocurrency 抵押品。

寻找积极 Incentivizednodes

如果隐藏网络是要取得成功，新用户必须能够快速、 轻松地理解 Incentivizednodes 当前处于活动状态。要实现这一目标，只要他们加入网络，已知的 Incentivizednodes 及其状态的列表发送用户。收到后的此列表中，用户的缓存列表中，当他们重新启动时他们可以只查找目录，而不必再要求整个列表。

交易的速度和可扩展性

通过实施 150 第二挡次和第二层 Incentivizednode 网络层的是能够支持起到 20 兆字节块，藏匿提供 80 x Bitcoin 交易能力，因此确保了交易费用保持在低。这也意味着储备将有没有近期的产能问题使藏匿团队研究和进一步改善能力随着时间的推移。

采矿

隐藏网络上, 有复杂的加密问题必须解决，以便安全上 blockchain 的一个街区。此过程称为采矿，和隐藏网络将奖励从事采矿活动与藏匿 cryptocurrency 的用户。

为了确保上藏匿 blockchain 块，我们建议矿工将需要找到解决办法的 X11 算法。这可以实现对各种不同的硬件设备，包括基本的 CPU，在标准的桌面和膝上型电脑中被发现。

现代 CPU 都相当强大，但他们也为了与许多不同的应用程序，在脑海中。这种多功能性其实是一个障碍挖掘，而需要大量的向量，同时计算的时候。

一个标准的 CPU 可以进一步使用 AES 或 AVX，使它更适合于采矿作业。GPU 的提供改进的性能，由于开采所需的可预测计算他们众多的输油管道。然而，ASIC，这专为高性能决议的特定类型是算法的远远优于 CPU 和 GPU 的

薪酬和执行

隐藏网络设置以确保每个 Incentivizednode 接收块奖励其应得的份额。这就要求网络执行块问题和正确的 Incentivizednode，而这反过来要求自觉行为和实践从矿工之间的付款。如果不能维护这些标准的矿工，他们处理的块将被拒绝通过网络，为了防止作弊。

但这必须强制执行。要实现这种强制措施，Incentivizednodes 创建仲裁，然后广播他们选择正确的 Incentivizednode （其中必须支付）。过程完全分散和不可靠的所以有没有办法，Incentivizednodes 可以勾结对这件事和欺骗系统。一旦收到了一定数量的消息，投票可以达成共识，此区块就会有义务支付所选 Incentivizednode。

矿工使用池软件可以获得关于如何通过 RPC API 使用的块的信息。当访问 API，用户扩展窗体，并在 GetBlockTemplate 中添加次要收件人。如果成功地开采块，付款是拆分矿工和 Incentivizednodes 之间。

治理和供资

治理的难题是一个棘手的一个开发商的 cryptocurrency 网络来解决。一方面，网络需要迅速作出的决定是有效的并有效地确保在短期和长期的积极发展。另一方面，cryptocurrency 的分散的性质应受到保护。
这就需要一个结构化的治理系统;隐藏网络实现通过一个系统的自我治理的东西。

自我管理是什么？

自我管理是藏匿使用允许一个分散的网络快速决策的治理解决方案。而不是辩论选择和决定可能性自我治理提供了快速的决议允许的规则。以比特币作为一个例子，关于个别的块的大小此网络上的争论已年才可以解决，对储备网络，这样的问题可以付诸表决和放在短短几小时内休息。其结果是一个更高效的网络。

自治系统需要建议，提出了网络的整体，然后付诸表决。在实践中，这意味着 Incentivizednodes 是能够投到系统或网络的重要变化，因为没有人可以承担太多的 Incentivizednodes 控制，支配地位的选票是不可能。

什么自筹资金？

包括在自治系统中是块奖励利用提供不断向网络提供资金的方式。对于每个块这种开采，矿工接收 45%的奖励，而 Incentivizednode 接收另一个 45%，叶剩余的 10%。这 10%不是直到在本月底之前创建的。在一个月内，任何人都可以使预算提案，由网络投票决定。月底月财政部块创建，如果 10% incetivizednodes 投票赞成任何比该提案的提案被批准。如果没有建议批准或 10%奖励金额是那更多被用来覆盖成本比奖励归财政部，可供未来拨款的建议。此系统允许网络基金本身，还提供机会，建立资产藏匿 cryptocurrency 用于基金未来以及可能更大的建议的形式。

可互换性问题

与比特币，它已成为明显的交易并不是完全私人。这导致一个可互换性问题。可互换性只是意味着我比特币值得和你的一样的数量完全相同，因为他们是完美的替代品。然而，通过分析公共会计科目第三方都能够将比特币交易链接到人们的身份。这会导致比特币被污染由于其不利过去的历史。藏匿将整合零知识安全层 (ZSL) 在藏匿网络，为用户提供卓越的交易隐私和解决可互换性问题。

零知识安全层基于 zk 虫子为网络上的用户提供交易隐私零知识加密的一种形式。隐私被通过完全事务上启用加密的 blockchain，但以协商一致方式网络保留可验证性。本节讨论如何这是可能的和好处它提供给用户和整个网络。

高级隐私通过零知识 Cryptopgraphy

不同于其他方法依靠遮蔽之间交易的联系 cryptocurrency 隐私，隐藏加密 blockchain 的交易记录。这允许额，起源和

支付目的地保持隐藏，同时仍在核实下网络的协商一致规则使用 zk 斯纳克证明资金的转移。

认识 Zk-虫子吗？

Zk-斯纳克 —— 或零知识简洁的知识 —— 证明非交互式参数已经推出一段时间，但它首先部署在 ZCash cryptocurrency 内广泛的规模上。

通过 zk-敌情动向，和个人可以证明他有一定的信息，没有透露有关信息，并与他自己和另一个用户; 没有相互作用谁被定义为证明者和验证者。

零知识证明是能够说服验证某些声明是真实，只透露信息，证明了该语句，但是不是语句本身的有效性。举个例子，可以证明一个随机数的哈希存在没有透露这一数字什么。

零知识的知识证明' 进一步迈出这一步。不仅这种大量存在，但没有透露任何信息关于这个数字，他们知道什么那号码是证明可以说服验证程序。

它是可能确认简洁零知识证明只有几百字节，在几毫秒之内，甚至对于大型的语句。而早零知识证明系统需要无数次的沟通，非交互式结构只需要单个消息证明和验证程序之间发送。在这一点上是足够短，在 blockchain 上发布只有零知识证明包括创建一个相互引用字符串，它证明和验证程序之间共享的安装阶段。这些共享的引用字符串可以称为公共参数。

如果有人能够访问用于创建公共参数的秘密随机性，他们可以产生虚假的证明，并反过来，创建假藏匿硬币，这将是真正的没有什么区别。然而，在其中创建参数的方式，使得这种恶意的活动采取的地方。公共参数生成在一个复杂的事件，涉及多个不同的用户;这被称为仪式的事件。每个用户参与仪式的然后被迫销毁参数的小片。即使只有一个用户破坏他们的片断，参数是不可用的这些**参数可能存在和落入坏人之手的可能性很小。藏匿将在**仪式上我们的网站上提供更多的信息。

隐藏分层网络

Cryptocurrency 网络正常工作，必须有一个结构到位;**交易必**须经过一定的证明，才可以验证。
在比特币交易将进行验证后证实了以下三个项目;

1.**正在使用比特**币不花了发件人以前。发件人不需要采取任何行动，表明这是个案，这是确定只需通过检查分类帐。

2.发件人拥有必要的授权，将发送到价值的硬币商定在事务中。这被验证通过与的地址发送硬币至从何处是关乎的密钥签署交易。

3.这种交易平衡输入的硬币，硬币取出来。**本**应该是明显的交易记录，正在传输量众所周知的所有当事**方**

藏匿将使用一种称为 zk **虫子的零知**识证明的形式证明以上各点，而不必透露任何额外的信息。每个交易记录验证时，也存在 zk **斯**纳克可以用来表明藏匿硬币存在和不花了，发件人有权发送藏匿硬币，硬币送等于藏匿硬币收到大量的储备量。

在此过程中，所需支出藏匿硬币的信息附加到交易记录通过创建新的 zk **斯**纳克和使用收件人的公钥，只可由交易收件人进行加密。

这会导致新的分布式分类帐，被称为零知识安全层。

瞬时交易

隐藏网络交易需要安全和私人的但是也要快。隐藏用户 Incentivizednodes 仲裁提供的能力来发送和接收不可逆交易瞬间。

时有足够法定人数输入的交易记录锁定为支出。这把锁需要大约 4 秒内完成。如果 Incentivizednode 网络能达成共识，将从此拒绝任何冲突的事务或块。只有精确匹配的事务 id 将被接受。

这个想法是与现实世界的用法，例如，通过在销售终端的移动设备连接藏匿 cryptocurrency。如果用户能够解决商业交易与零延迟，使用数字加密的 cryptocurrency， 然后隐藏数字货币可能成为严重媲美传统现金，信用卡或者借记卡卡形式的支付。

隐藏标记和藏 Cryptocurrency 供应

共 5 亿藏匿令牌将在令牌销售中分配。出售的收益将用于进藏匿 Cryptocurrency 层零知识密码学中，创建一个藏匿钱包。一旦此隐私功能已定稿藏匿令牌业主将能够用来购买上一件为藏 Cryptocurrency 的一个基础。最多 997.8million 藏匿 Cryptocurrency 将创建其中包括将随购买的藏匿处 Cryptocurrency 藏令牌，以及将在大约未来 100 年的开采产生的藏匿处 Cryptocurrency。

藏采矿设备

藏的 Cryptocurrency 挖掘将创建新的 cryptocurrency 单位，并因此导致通货膨胀的藏匿处 Cryptocurrency。为了抵消这种膨胀，新的供应将减少每 7.1 年 %的速度每年。

这项措施，以及藏匿在网络上实现了对每个块的供应和矿工活动数目之间的直接连接。如果矿工数目减少，从每个收到奖励相应批准块增加和 vis 反之亦然。

Cryptocurrency 正在进行生产预计将继续直到关于下个世纪的中途，此时块奖励将接近零和矿工和 Incentivizednodes 将盈利的交易费用。

藏匿路线图

ZSL 一体化和藏匿钱包 Q2，2018

藏匿将使用人群销售所得来帮助整合 ZSL、 零知识安全层设计为匿名，安全上同时保持原籍国、 目的地和付款金额私人 blockchain 结算的交易记录。藏还将开发用于存储藏匿 cryptocurrency GUI 钱包。

藏 Cryptocurrency 发射第 2 季度 2018年

一旦 ZSL 已经一体化，藏匿令牌 (STT) 业主将能够利用自己的代币来购买，1 对 1 的基础上，对藏匿 Cryptocurrency，将开放给挖掘。业主将能够设置 Incentivizednodes，以提供对网络资源的储备 cryptocurrency 会得到报酬藏匿 Cryptocurrency 从块奖励的一部分。

藏治理和供资系统 Q3 2018

藏匿处将开放社会资金和治理的建议，这将使储备来开始实施任何新的功能，由 Incentivizednodes 投票选出。藏匿治理和供资系统将帮助藏匿开放分散自主网络 （一个），高效运作，并同时利用藏匿社区的集体智慧有机进化。

藏匿移动应用程序第 3 季度 2018

藏匿将开发的移动应用程序将允许隐藏用户存储和匿名发送和接收藏匿 cryptocurrency 给任何人。藏匿手机应用程序将允许您轻松地使用您的手机的日常交易。此外，您将能够监视你藏匿 cryptocurrency 奖励支付从运行 Incentivizednodes。

私人消息第 4 季度 2018

点对点私人消息传递系统集成 (StashChat)，允许所有藏匿用户发送屏蔽的消息使用零知识加密。StashChat 将是一个完全匿名通信网络，没有第三方中介机构将允许用户进行私下交流这两个人和集体。

分散的 API Q1 2019

藏匿处将推出一个分散的 API，将利用随机群体的 Incentivizednodes，将消除对软件开发人员能够存储、验证和仍然证明他们与安全和隐私的 Incentivizednode 同时下载整个藏 blockchain 的需要。

藏借记卡卡 Q2 2019

创建一个将允许藏匿业主安全支付与他们藏匿的人，在网上或通过电话接受法定货币的任何商家的藏匿处借记卡卡。因此，这将允许藏匿业主购买几乎任何产品或服务他们希望与他们的积蓄，将增加的藏匿处 Cryptocurrency 实用程序。

直接藏匿到菲亚特货币转换第 3 季度 2019 年

创建一个允许用户直接交换他们藏匿菲亚特货币和 vis 反之亦然的直接支付设施。藏匿的谈话网关将纳入藏匿的钱包和手机应用程序。它将允许用户无缝地和直接转移之间美元、 欧元、 ￥ 元、 澳元和藏匿而不需通过交易所或第三方提供。

令牌发射所涉法律问题

藏匿令牌不是证券。藏匿令牌是不退还的。隐藏标记不是投机性的投资。所有隐藏文档、 设计和来源都是在研究、 开发和概念阶段和变更。 没有承诺的未来业绩或价值或将作出藏匿令牌或藏匿 Cryptocurrency, 包括内在价值没有承诺，没有承诺的继续付款，并不能保证藏 令牌或藏匿 Cryptocurrency 将举行任何特定的值。隐藏标记和藏匿 Cryptocurrency 并不是参与公司藏匿令牌和藏匿 Cryptocurrency 持有说公司没有权利。隐藏标记销作为一个功能良好和公司所得的所有收益也许都花费自由的公司没有任何条件。藏匿令牌和藏匿 Cryptocurrency 用于处理加密令牌和基于 blockchain 的软件系统的专家。