

Stakenet: 点对点的连锁经济

X9 开发者

2019 年 6 月

摘要: Stakenet 是一个分散的平台，提供了一个去信任的链间经济。它是由一个桩证明区块链与闪电网络，主节点，和分布式应用/去中心化应用组成的，用来为加密货币提供一个高度安全的跨链平台，在这个平台上，个人只需使用 Stakenet 及其本地货币 XSN 就可以轻松地操作任何区块链。

1 介绍

在过去几年里，加密货币社区稳步增长。现在有数百种加密货币可供选择，而且每天都有更多的加密货币出现。重要的是要了解哪些技术，社区和分散的分类帐技术将与其他技术分开，推动持续进入密码领域的噪音。我们相信，未来将会形成一个全球性的后端-----一个由迄今为止创建的每个链、技术和服务组成的区块链网络，而不是单一的链式规则。一个由不同的链路组成的联合网络，所有的链路都通过不同的接口相互通信。这种对话对于终端用户来说是完全不知道的，因为不同链之间的交换将在后端逐个进行---从未见过，实现过，甚至被用户选择过。

1.1 Stakenet 的目的

尽管大多数人把“股份”这个词与“押注”联系在一起，但“股份”的根源在于企业管理经济学，它远远不止代表被动收入。Stakenet 不仅仅是押注;它是利益相关者的网络。为达成共识，我们需要定义网络这个术语，并将其与利益和利益相关者的适当定义联系起来。

- 网络被定义为一个由许多相似的连接部分组成的系统。
- 股份是企业或其活动的重要利益。
- 利益相关者是指在企业的愿景和使命中拥有内部或外部利害关系的任何个人或社会。

因此，任何积极或消极地受加密货币活动影响的人都将成为区块链经济的利益相关者。这包括货币的所有权和持有权、财产和法律利益、经济和社会依赖性、开发者和社区活动，以及任何其他与加密相关的工作或利益。这样，加密货币的利益相关者:

- 影响区块链经济。
- 受区块链经济的影响。
- 既受区块链经济影响又影响区块链经济。

综上所述，我们可以看到 Stakenet 正在追求的愿景。将区块链经济的所有利益相关者连接到一个巨大网络的技术架构——Stakenet。

1.1 行动计划

为了给区块链经济创建一个成功的链间解决方案，我们需要确定其大多数利益相关者，并找到连接他们的方法，并确保我们的方法不会损害他们的完整性。因此，下列三个分项目对我们的行动计划特别重要。

- 1) **识别大多数:**在区块链经济中, 最常见的利益相关者是比特币本身, 它是一种对等版本的电子现金, 日益强大。最引人注目的是在过去的几年里获得了巨大的吸引力和广泛的受众。如今, 无数人受到比特币的影响, 作为回报, 由于他们的工作和活动, 也会影响比特币。这包括采矿业、金融产品、不同的钱包解决方案, 以及许多其他与比特币相关的工作。除了比特币, 具有智能合约功能的区块链也特别出名。其区块链体系结构的美妙之处在于, 它们支持创建侧链和子链。这允许开发分散的应用程序(dApps)。最著名的智能合约区块链是 **Ethereum**, 它为不同的区块链相关业务提供很多令牌。另一个具有类似用例的著名区块链是 **EOS**, 它是当前加密货币领域中使用最多的区块链。这两个区块链也分别受到内部和外部利益的影响。没有一个区块链不使用利益相关者方法。
- 2) **联系大多数人:**在确定了我们的利益相关者是谁之后, 我们需要找到一种方法来联系他们。如果两个区块链都使用兼容的接口(如第二层协议), 或者支持相同的加密哈希函数, 那么就有可能弥合区块链之间的鸿沟。因此, 可以在不同区块链之间执行不可信的事务。在比特币的情况下, 我们可以利用闪电网络作为默认接口来窥视两个不同的链, 就像我们已经对比特币、莱特币和 **Stakenet** 所做的那样。其他区块链, 如 **Ethereum** 或 **EOS**, 可以通过他们自己的智能合约语言集成到我们的利益相关者网络中。我们将开发 XSN_{ETH} 和 XSN_{EOS} 令牌, 利用哈希时间锁定契约(hash time locked contracts, 简称 HTLCs)在本地链和相反的链之间进行无信任的交换。hashlocks 和 timelocks 的使用为我们提供了一种解决方案, 在本地链上锁定 XSN , 同时在智能合约链上解锁相应的 XSN 令牌, 并在相反的一端交换这些令牌, 然后子链与其他加密货币啮合。除了交换货币和代币, 连接区块链的利益相关者也意味着你需要整合这些区块链的外围产业。因此, 我们为分散式挖掘池, 交叉链放置以及托管其他链条应用程序的接口提供了解决方案。
- 3) **保护完整性:**如果我们只是开发另一个集中式解决方案, 那么所有这些想法都将是空话。我们通过将不同区块链的优势结合到一个链间管理架构中来保护每个人的完整性。关键的支柱是我们自己的不可信的股权证明共识, 升级的主节点层与瞭望塔功能, 升级的闪电网络层与专门的交换解析器。除了一些产品, 其中一个是我们的硬件设备 **XSN Viper** --用于存储, 交换和利用不同的链原生资产和工具。

简而言之, **Stakenet** 将最大的分布式网络开发连接到一个分散的位置, 个人可以使用 **Stakenet** 作为默认接口来操作任何区块链。

2 区块链体系结构

Stakenet 是一个股权证明区块链, 它为区块链经济提供了一个真正分散, 高度安全且专业的链接网络。它由其原生硬币 XSN 提供支持, 同时由其自己的主节点和闪电网络节点网络管理。**Stakenet** 有 1 秒的转换时间, 每秒最多有 240 个链上事务。它基于 1-4 兆字节的块大小和 60 秒的块生成时间。此外, **Stakenet** 区块链还可以通过使用闪电网络, 以几乎零费用的方式实现 O 链的初始规模扩展。

2.1 学分

Stakenet 是一个由比特币、Dash 和 Peercoin 组成的修改代码。它使用了与比特币相同的核心, 改进了 Dash Masternode 架构, 并基于 Peercoin 的货币使用情况, 以及基于 Peercoin 的造币利用率的调整后的铸造共识证明。

2.2 共识

分散数字货币的共识用于验证新生成的区块链块。简单地说，它是一个软件组件，验证器使用它来投票关于过去的故事是否真实。为了证明这一点，Stakenet 使用了一种股份共识的生成证明，它通过一种称为股份不可信证明的非正式的押注解决方案进行了扩展。

2.2.1 铸造桩的证明

与工作证明不同的是，工人使用硬件的哈希能力来解决密码难题，铸造股权证明的工人使用他们的硬币(最多 24 小时)和财富来建议新的块。在这里，货币被定义为时间，因为 staker 的货币没有移动，而货币财富只是一个 staker 拥有的货币数量。。新生成的块的证明是通过一个名为 `coinstake` 的特殊事务完成的。在这个事务中，`rst` 输入被命名为 `kernel`。为了确保新块的创建者是由随机进程选择的，内核输入必须满足特定的散列目标协议。这个散列目标被定义为每个单位货币的目标，在随后在内核中使用它之前需要达到这个目标。其技术后果是，所选的 staker 必须向自己支付一定数量的货币，从而使用货币造币来获得为网络生成新块的特权。由于货币的消耗，一个 staker 连续验证几个块的机会大大降低，因为他们的投票权在每次成功投票后都会重置。

2.2.2 股权去可信证明

对证明协议押注的一个主要批评是，当所有硬币都在线并且避免权威的押注节点时，它只是最安全的。以前的在线和离线押注解决方案都不能满足这些条件。通常，stakers 需要将他们的全节点钱包连接到区块链以建议新的块。有了我们自己的共识升级(不可信的股份证明)，Stakenet stakers 可以验证、移动和保护区块链，而他们的货币仍然在一个钱包里，如 Trezor 或 Ledger Nano。与其他离线股份解决方案不同，我们的验证器节点的数量不仅限于一些专制代表，称为委托证明代理。此外，我们的解决方案不支持旧的网络节点随着时间的推移而得到更多的影响，就像在租赁证明制度中仅仅是造币者的造币和财富才是至关重要的。

不可信的证明协议押注本质上允许 stakers 使用任何其他节点来为他们做押注，而不必与节点共享任何可使用的余额或私钥。这是一个特殊的协议，我们的区块链，它允许一个给定地址的所有者给一个单独的商户地址的立桩许可。该商户地址的运营商无权在该地址中移动资金，仅有权将该地址的余额作为押注。业主可随时将其资金移出该地址，使业主在本合同执行期间和整个过程中完全控制其资金。押注契约由一个特殊事务签署，该事务具有 `OP-RETURN`，该事务保存指定术语的数据，并由向自己发送 1 个 XSN 的用户创建。要取消合同，用户只需将所有资金转移到一个新地址，或者解锁并移动包含所有合同信息的 1 XSN。

本合同所需资料如下：

- `tposAddress`: 合同创建者拥有的地址(此余额将作为股份)。
- 商人地址: 这个地址的所有者将有能力在它的平衡押注。
- 委员会: 告诉协议如何分割股份奖励从 `tposAddress` 创造。
- 签名: 合同创建者的 65 字节签名，以证明他们是 `tposAddress` 的所有者。

样品合同：

```
Out 0: { tposAddress : 1 XSN } (deposit)
Out 1: { OP_RETURN tposAddress merchantAddress commission signature }
Out 2: { changeAddress: changeAmount }
```

RPC 调用创建 TPOS 契约并将其提交到网络：

```
- tposcontract create [tposAddress] [merchantAddress] [comission]
- sendrawtransaction [hex encoded contract]
```

一旦用户启用 TPoS 后端堆栈，执行以下步骤：

- 1、为所有者生成新的 tposAddress。
- 2、使用输入的商品地址生成 TPoS 合同。
- 3、向网络广播合同。
- 4、将 XSN 的数量发送到所有者的 tposAddress 以进行押注。

此外，我们将结合我们的一些独特的主节点任务，为潜在的交叉链桩奠定基础。通过合并我们的区块奖励支付与我们的 XSN Dex 技术，用户可以将他们的硬币和其他货币的奖励直接存入冷库。例如，您可以将 XSN 放在一个硬件钱包中，并将其作为块奖励直接接收比特币或莱特币。

2.3 加密算法

区块链中的每个信息位都经历了一个称为密码散列的过程。为此，Stakenet 使用 X11 算法。这是一种密码算法，它使用 11 个哈希函数的链式组合，根据它们的输出大小迪尔。这种链式哈希解决方案的复杂性增强，为数字货币的价值存储提供了更高的安全性和持久性；与其他单哈希解相比，所有 11 种算法都需要同时被破坏才能对网络构成威胁。

X11 由以下算法组成:Keccak, 它是 NIST 哈希函数竞赛的获胜者，进一步称为 SHA-3。BLAKE, Grstl, JH(吴洪军)和 SKEIN, 他们都是 NIST 哈希函数竞赛的 NIST 成员。最后, Blue Midnight Wish (BMW)、Lua、CubeHash、SHAvite、SIMD 和 Echo 都未能进入决赛，但值得注意的是，它们无一明显被破解。”

因此，X11 具有合理的安全边际，因为所有使用的算法都经过了彻底的分析，一些最好的密码学家参与了这些算法的设计。注意，量子计算据说很快就能打破已知的哈希算法。然而，如果你考虑到量子计算的可用信息，并且根据最近的研究，SHA-3 256 是量子抗性的，因为它需要 1032 年才能打破它。因此，我们可以安全地假设在 SHA-3 256 量子计算机的生命周期内不会对 Stakenet 构成真正的危险。

2.4 供应

Stakenet 的初始供应是由于从 POSW 到 XSN 的交换。因此，在初始块中创建了 7600 000 个 XSN。交换结束后，350 万枚未交换的 XSN 硬币被发送到以下燃烧地址：
XmPe9BHRsmZeThtYF34YYjdnrjmcAUn8bC

2.4.1 硬币发射

Stakenet 区块链在第一个 10 天(分别是第一个 10 天和第一个 2 万块)内公平地推出了空块奖励，以避免收益不对称，并让每个人都有公平的机会交换货币和设置节点。当块生成时间为 60 秒时，块奖励每 63 个块逐步减少 5 个 XSN，降至 20 XSN。

Phase 1:	[0	—	20 000]	0 XSN
Phase 2:	[20 001	—	63 200]	50 XSN
Phase 3:	[63 201	—	106 400]	45 XSN
Phase 4:	[106 401	—	149 600]	40 XSN
Phase 5:	[149 601	—	192 800]	35 XSN
Phase 6:	[192 801	—	236 000]	30 XSN
Phase 7:	[236 001	—	279 200]	25 XSN
Phase 8:	[279 201	—	infinity]	20 XSN

第一阶段展会开幕日期：2018年3月6日。

第八阶段开始日期：2018年9月20日。

由于 XSN 的总块报酬率将稳定在 20 XSN，因此理论上的供应是无限的。因此，Stakenet 燃烧网络内的每一笔交易费用，作为供应增加的对应，并增加额外的业务，为 XSN 提供更多的价值。要么烧掉它们的支柱，从而减少 XSN 硬币的供应，要么把它们收益捐给财政部，为更多的项目和产品提供资金。因此，确保 Stakenet 生态系统中的所有项目最终都会使所有 XSN 硬币所有者受益。

2.4.2 货币分布

我们认为，网络安全和网络服务与拥有强健和强大的基础设施同等重要。由于 Stakenet 区块链由两种类型的节点提供支持：Staking 节点和 Masternode，我们不区分它们的工作。这就是为什么押注节点和 Masternode 同样得到奖励，每个节点和奖励都有 45% 的奖励。最后，10% 的大额奖金被送往财政部。国库是一个加密的公共地址，持有网络分配给它的资金。它被用来资助 Stakenet 进一步的硬币发展和新项目。还有一个长期发展基金，用于更大的项目、伙伴关系和关键发展。

2.5 第二层

Stakenet 区块链为链上、o 链和跨链特性使用了几个第二层解决方案。其中最重要的是它自己的主节点和闪电网络层，以及其他区块链的令牌化层。

2.5.1 Masternodes

主节点是区块链的专用全节点，驻留在世界各地的服务器上，以确保分散和冗余。虽然押注节点负责区块链的验证，但 Masternode 为网络提供了多种服务。要操作一个主节点，每个主节点需要有效的附带输出 15000 个货币。这样做是为了对抗节点的疯狂生长，并避免异常节点。除了 Masternode 默认功能，如即时发送和分散民主，我们的 Masternodes 旨在成为加密行业中最强大的站之一，并将根据他们提供的服务获得被动收入。他们将：

- 主持并运行 XSN Dex。
- 主机都需要区块链探险家，确保真正的权力下放。
- 主机需要保持 XSN Dex 分散和轻量化的区块链。
- 处理不同区块链之间的 Lightning Swaps 和 Tokenized Swaps。
- 被用作了望塔来托管和监控闪电频道。
- 使用他们的抵押品提供闪电网络的流动性。
- 授权并确保在不同区块链之间转移标记化硬币。
- 方便即时和私人链上交易。
- 提供洋葱路由并确保网络的安全出口点。
- 主机 dApps Stakenet 和其他区块链。
- 用于网络的分散民主。
- 为 Stakenet 网格中的每个人卸载 CPU 和数据库容量。

由于主节点的存在，Stakenet 区块链变成了一个生态系统，在这个生态系统中，没有一个实体能够管理和服务整个网络。

2.5.2 闪电网络

闪电网络是第二层解决方案，它支持区块链内或不同区块链之间的对等 o 链事务。它要求供应商将硬币锁在通道中，以确保流动性，并在不同节点之间路由支付。为了了解闪电网络的工作原理，需要了解单向和双向支付渠道的知识。

单向支付渠道：没有闪电，经典的支付渠道只存在于双方或对等方之间。该技术使用多签名(MultiSig)特性和所谓的锁时。使用 MultiSig 机制，您可以生成需要多个私钥来签署此事务的事务。这意味着与交易相关的硬币需要双方的批准才能发送。锁定时间确保在一定时期内多重团体内的硬币是不可转让的。

双向支付渠道：上述机制称为单向渠道，因为只有一方可以向另一方发送货币。如果双方想要相互交换支付，他们需要一个双向的渠道。这就导致了一个两难的境地:为什么一方要等待整个锁定时间，而不是立即要求全部股权?为了防止这种情况，闪电使用了一种相互保护的机制。在这里，在设置通道之前，每一方都要考虑一个单独的安全号码，并相互发送该号码的散列。与单向支付通道一样，支付合作伙伴生成一个 MultiSig 地址。在向网络广播其 MultiSig 地址之前，每一方生成一个称为承诺事务的事务。在此承诺交易中，资金被分割：一部分流向承诺交易的创建者，另一部分流向一个锁定的地址，交易对手可以在指定的时间之后访问该地址。因此，两家公司都制定了防止欺诈的合同。

由于我们现在了解了双向支付渠道的工作原理，我们需要找到一种方法将它们连接到网络中。在闪电网络之前，各方必须为每个新的支付活动创建一个新的通道。因此，如果甲方想与丙方开展业务，无论甲丙双方是否已经在与乙方进行交易，双方都必须建立一个支付渠道。那么为什么 A 和 C 要使用一个新的通道，而 B 可以在两者之间架起桥梁。唯一的问题是，B 是否可信?如果 B 是欺诈性的，索赔了钱，却不把钱转过去怎么办? 因此，考虑到这一点，我们如何确保 B 不关闭他的 Lightning 节点或者是否存在迫使他将其节点设置为脱机的技术问题? 作为这些问题的解决方案，闪电网络使用散列时间锁合同 (HTLC) 来保证不会发生这些问题。一个例子：C 想出一个秘密，这是一个特殊的随机数使用密码证明。C 把这个秘密的散列给了 A。这个散列现在变成了一个押注。B 只有在知道这个秘密的情况下才会收到付款。甲方可以使用散列来检查。如果收件人也知道秘密散列，则 B 再次传递散列并承诺付款。原则上，A 和 C 之间的路径可以包含其他参与者，所有参与者都使用散列作为押注。使用 HTLCs，可以在各方之间链接支付渠道。正如您所看到的，网络中的参与者作为节点在 A 和 C 之间架起桥梁，构成了闪电网络的主干。它们的重要性可以与常规区块链上的矿工或小型企业的重要性进行比较。

Stakenet 在缺省情况下使用主节点的附属品为其闪电通道提供资金，并使用主节点作为各方之间的桥梁节点，从而升级了当前的闪电解决方案。您可以将其想象为一个池，其中不同主节点以特定的多签名地址分配资金，同时还提供了随机钱包加入这些通道的可能性。现在在这个主通道内，所有各方可以同时打开许多 2x2 通道，并且由于闪电互换甚至在不同的区块链之间。这个解决方案不仅有利于 Stakenet，而且它也是闪电网络中每个区块链的升级，因为 Stakenet 的货币 XSN 也可以用作比特币和莱特币交易的载体货币。因此，Stakenet 消除了低资金渠道的风险，并提供了一个解决方案，将不同的闪电网络合并到一个链间解决方案。

2.5.3 标记

标记化是将资产的权限转换为数字标记的过程。因此，每个令牌表示基础资产。为此目的使用区块链可以确保所有权信息是不可变的。目前，我们正在开发 Ethereum 和 EOS 区块链上的 XSN 令牌，它们代表原生的 XSN 币，可以在 Stakenet、Ethereum 和 EOS 之间通过桥接协议进行转换。通过专门的多重签名地址，哈希锁和时间锁，我们可以在我们的本地链地址上锁定 XSN，同时解锁对方智能合约链上的 XSNETH 和 XSNEOS 令牌。Stakenet 用户无需手动将其货币转换为代币，因为所有货币都由网络上的智能合约执行，并由我们的 Masternodes 层控制。

注意本地 XSN 货币的数量不会增加，这一点很重要。所有可移动的货币和令牌的现有数量等于 XSN 的总供应量，并且是可加密审计的。一旦使用桥接协议将 XSN 货币发送到 Ethereum 或 EOS 网络，它们就被锁定并存储在一个特殊的智能合约地址中。因此，发送方没有访问本机货币的权限，但可以获得相反令牌的权限。通过标记化将 Stakenet 区块链连接到以太坊和 EOS 区块链，我们可以将这些区块链的每个已知标记集成到我们的链间网络中。通过这种方式，我们将能够提供一种可互操作的技术，用于跨越不同的网络交换资产，以允许每个人使用区块链网络中的任何货币和令牌自由操作。另一个优点是该工作与支持标记化的任何其他区块链兼容。这意味着 Stakenet 链间网络可以轻松地日益增长，其他开发人员的新成就也可以在我们的网络中受益。

2.6 指标概述

名字：Stakenet。

股票：XSN。

货币类型：货币。

共识：出具股权证明，去信任股权证明。

货币：启用，24 小时。

加密算法：X11。

块生成时间：60 秒。

块大小：1-4 MB。

最后一个方块奖励：20XSN。

方块奖励分配：45%母节点，45%押注，10%金库。

主节点抵押品：15000 XSN。

治理：分散的民主。

资金：权力下放的财政部，没有初始资金

闪电网络：在主网上激活。

链上可伸缩性：240 tx/s。

链上交易成本：~0.00001 XSN/kB。

链上可伸缩性：理论上是无限的 tx / s。

链上交易成本：几乎为零。

交叉链接口：闪电互换，令牌互换。

3 XSN 产品

XSN 产品提供与 Stakenet 日常交互的软件和硬件解决方案，以确保用户友好和安全的地方，让人们处理不同的区块链。

3.1 Stakenet 钱包

Stakenet 钱包是一个非托管的多加密货币轻钱包，是加密货币世界的主要交互接口。从本质上讲，它是一切一站式的地方-在移动和桌面版本。它是 Stakenet 的主要产品，因而得名。钱包本身是加密货币世界的重要组成部分。它是一个安全的数字钱包，可以帮助存储和交易比特币和以太坊等数字货币。大多数货币和代币都有它们的社交核心和轻便钱包，但问题来了：对于用户所持有的每一种加密货币，他也需要一个钱包来存储它，因此让持有者拥有这么多钱包变得很麻烦。

Stakenet 提供了解决此问题的方法，因为它的 Masternode 网络将保存数据库并运行多个区块链的完整节点，允许 Stakenet 创建一个钱包，可以在单独的区块链上安全地发送，

接收和确认交易。把这些区块链放在第二层，我们就有可能开发出真正轻便的 **Stakenet** 钱包，没有任何限制。与其他轻钱包相比，**Stakenet** 钱包将不局限于基本的区块链交互，如存储、发送和接收。与其他 XSN 产品(如 XSN Viper)相结合，**Stakenet** 链间经济中的所有用户都可以将其用作访问其他功能的界面，例如从硬件设备离线放置，设置 **Masternode** 或运行闪电网络的集线器。此外，**Stakenet** 钱包将拥有一个内部的场外交易引擎，该引擎将与 **XSN Dex** 相连，用户可以在不同区块链之间交换资产，而无需透露自己的私人密钥。

为了确保安全访问我们的链间网络，**Stakenet** 钱包提供了全面的支持。这将由我们的主节点层管理。**TOR** 本身是一种 IP 混淆服务，支持在基于分层电路的网络上进行匿名通信。每个 **Stakenet** 主节点将在数千个中继之间引导我们网络的区块链流量，以隐藏用户的位置。简单地说，当用户将他们的钱包连接到 **TOR** 网络时，他们的流量将通过多个全局主节点服务器，每个全局主节点服务器都删除前一个服务器的信息，因此，最后一个退出节点服务器不会获得网络来自何处的信息。

3.2 XSN 货币

XSN 是一种允许对等支付方法的最先进的加密货币。由于 **XSN** 是开放的、无许可的、分散的、不可信的、抗审查的、不可变的、智能的、可互操作的、可替换的、安全的，并且具有固定的排放速率，因此它具有任何中央发行的货币都无法实现的独特属性。因此，它是一个用于全球范围内真实事务的交换媒介，包括 **Stakenet** 生态系统中发生的交易活动。每个产生费用的服务都需要以 **XSN** 的方式支付---在某些情况下，用户甚至不会意识到他们已经用 **XSN** 支付了，因为所有这些都将在后台通过闪电交换来处理。总而言之，**XSN** 是 **Stakenet** 的货币，天然气和基础，因为一切都在它上面运行，这是生态系统运行所必需的。

3.3 XSN 核心

XSN Core 是一个开源软件组件，用于在 **Stakenet** 区块链中运行一个 **fullnode** 来接收、存储和发送 **XSN**。它作为使用 **Stakenet** 网络的所有功能的核心接口，为了操作一个押注节点、商人节点、闪电节点和主节点，它是必需的。这些节点是我们区块链的核心支柱，因为它们允许在对等网络中连接计算机，从而在共享数据上达成协议。**XSN Core** 兼容最流行的操作系统，如 **Linux**、**macOS**、**Windows**，可以通过命令行界面或图形用户界面访问。

3.4 XSN Excalibur

XSN Excalibur 是我们的开源私钥管理和存储系统，可供公众审核。它基于 **Trezor** 的信誉良好的代码，并使用助记词短语，它只是一个单词列表，也称为种子，为 **Stakenet** 链间生态系统中的每个区块链钱包生成私钥。感谢 **XSN Excalibur**，**Stakenet** 用户只需知道一个短语即可备份和访问所有加密货币。

3.5 XSN Dex

加密交换是加密货币市场的主要支撑，因为它们允许交易货币，从而为生态系统提供流动性。即使在成为加密市场的重要组成部分之后，大多数交换机都是集中式的，并且由少数服务器运行。这使得它们依赖于有限的基础设施并且易受黑客攻击。一旦用户与集中交换进行交易，他们的货币就会离开他们的所有物并与交换机一起存储，从而使用户失去从这些货币接收的效用和好处。这些是 **Stakenet** 在通过其提议的 **XSN Dex** 来解决的一些潜在风险。

借助 **Stakenet** 钱包，闪电互传和标记化的互换等重要组件，我们距离创建此解决方案只有几步之遥。目前有一些分散的交易所正在运营，但它们都有一些集中化的漏洞。**Stakenet** 将是第一个运行完全分散的解决方案，该解决方案完全由 **Masternodes** 运行，而不是由集中式实体支持。

除非交易完成，否则用户在 XSN Dex 中持有的硬币永远不会离开，允许无限制访问。将这些硬币放在自己的钱包中，用户也可以从硬币的所有实用程序，功能和股份中获益。此外，用户保持匿名，因为他们无需向任何人提供任何“了解您的客户”（KYC）详细信息，从而提供完全匿名和自由、无需担心的交易。所有交易都是在点对点的基础上完成的，没有中央机构的参与，因为费用较低，交易更安全，更便宜。

XSN Dex 的另一个关键点是它能够聚合其他 Dex 解决方案。只要对立的 Dex 真正分散，就有可能将它们的验证节点添加到 Stakenet 链间经济中，并在不同的订单之间架起桥梁。聚合 Dex 和本地 XSN Dex 之间的交易可能比内部 XSN Dex 交易花费几秒钟。这是因为桥接协议需要在两个交换之间交换标记化资产。但最终所有 Stakenet 用户都可以通过一个界面与任何其他兼容的 Dex 进行交易。

3.6 XSN Viper

XSN Viper 是一款专用硬件钱包，具有集成的基本闪电网络路由功能，可以为闪电网络运行集线器并为 Stakenet，比特币和莱特币生成费用。即将推出的版本将提高性能，并允许在一台设备上运行多个集线器和 Masternode。这样我们就可以让用户安全地执行各种链的更高级功能。XSN Viper 通过使用一个独立的微控制器将用户的硬币安全地存储在冷藏库中，该微控制器可以保存私钥并保持不动，所有这些都由我们的开源固件 XSN Excalibur 提供支持。这允许 Stakenet 用户使用来自一个硬件钱包的所有支持的硬币功能。

3.7 XSN Cloud

XSN Cloud 是一个集中式应用程序，提供区块链服务，旨在为 XSN 用户提供更好，更轻松的体验，从而有助于采用。注意 XSN Cloud 不是基于 Stakenet 区块链，而是与其分散的生态系统和 DApp 无关。简而言之，<https://stakenet.io> 是一个托管 XSN Cloud 应用程序的信息网站，而 Stakenet 是基于区块链的分散式网络。XSN Cloud 具有以下功能：

- **Staking-as-a-Service**（在线押注钱包）：自动投注的钱包。存入的用户的货币被发送到一个主要地址（称为池），该地址定期接收许多押注，然后实时分发。
- **Masternodes-as-a-Service**（主持人）：我们自己的无信任 Masternode 托管解决方案。它是无风险的，因为您可以随时在本地钱包中控制您的货币。
- **监控服务**：Masternodes 的实时监控服务和无信任的合同证明合同。如果出现任何问题，客户将立即收到电子邮件警报。
- **ROI 计算器**：放样节点和 Masternode 之间的关系每天都在变化，因此每个节点可用性也会发生变化。ROI 计算器是一个工具，可以为您提供最佳选择。

XSN Cloud 从用户处收取使用其中一些服务的费用。然后将费用发送到 XSN Cloud 财务部以支付费用和进一步开发。注意，您丢失了存入 XSN Clouds 钱包的硬币的所有权，因为您无法控制私钥。请不要存入大量货币，而是通过去信任的股权证明或常见的押注解决方案自行投注。XSN Cloud 钱包仅适用于没有经验和小货币余额的新手，否则几个月都不会获得任何押注奖励。其余的 XSN Cloud 服务是可供所有人使用的去信任解决方案，因为您不会失去货币的所有权。

4 总结

Stakenet 是一个激励利益相关者的分布式网络，提供去信任的链间经济。它基于增强的证据桩区块链证书，具有多个第二层解决方案，如闪电网络，Masternodes 和 dApps。它有一秒的确认时间，每秒最多 240 个链上交易。通过闪电网络，大多数交易将在这里进行，Stakenet 区块链可以通过即时和几乎免费的交易进行非常规模的扩展。它的用例是为加密货币

币提供交叉链架构，个人只需使用 **Stakenet** 的本机硬币 **XSN** 即可轻松操作任何区块链，因为区块链通过闪电网络和其他交叉链技术相互连接。与绝大多数加密货币不同，**Stakenet** 并未强加一个全新的标准，而是坚持现有的 **BTC / LN** 协议和现有的智能合约解决方案，这些都是区块链经济的现在和未来。加密货币，**Stakenet** 并没有强加一个全新的标准，而是坚持现有的 **BTC / LN** 协议和现有的智能合约解决方案，这些都是区块链经济的现在和未来。

Stakenet 提供任何股份证明区块链中最高级别的安全性之一。它通过使用其发明去信任的证明来轻松安全地放置其货币 **XSN**，有效地实现分散的冷铆。**TPoS** 允许经销商通 **Stakenet** 区块链上的特殊协议冷藏硬币，这意味着验证人员甚至可以从硬件钱包中放置他们的 **XSN**，从而消除任何不必要的安全风险。此外，**Stakenet Masternodes** 创建了一个巨大的分散式计算机网络，可以产生令人难以置信的计算能力。它们提供高端网络服务并运行基于区块链的 **dApp**。例如，**XSN Masternode** 网络通过在不同硬币，主机闪电通道之间执行闪电互换和标记化的互换为 **XSN Dex** 提供动力，并通过 **Masternodes** 的附属品为闪电网络提供流动性。

Stakenet 是第一个使用 **Masternodes** 成功执行闪电网络兼容性的股份区块链证明，除了比特币和莱特币之外，它还是首先通过闪电网络（闪电互换）执行原子交换。因此，**Stakenet** 区块链可以与任何与闪电网络兼容的商家，应用程序，钱包或即将推出的加密设备进行交互。由于 **Stakenet** 的交叉链功能，用户可以向任何接受比特币或任何其他闪电网络兼容硬币的人支付与 **XSN** 无缝连接，从而大规模提高采用率，因为成千上万的商家已经通过闪电网络接受比特币支付。

Stakenet 通过将闪电网络，不同的智能合约解决方案和冷藏与去信任的股权，交换和支付相结合，为区块链经济建立最安全，最快速，最便宜的链间架构。