NERVE

白皮书

目录

摘要

NerveNetwork 是一个去中心化的数字资产服务网络。它是基于 NULS 微服务框架，使用 NULS ChainBox 开发搭建的区块链跨链交互协议。旨在打破区块链价值孤岛，建立跨链互通的资产交互网络，为 DeFi 应用生态提供底层支持。让数字资产持有者享受真正安全、自由、透明的 DeFi 应用服务。

一、背景

加密市场当前已经发展到万亿市值，超过了很多国家的主权货币市值。在区块链发展历史的必然进程中，各个公链也相继兴起。公链越来越多，每一条区块链都是一个独立的闭环，包括链上应用也只能在本链资产中使用。各个链上资产成为价值孤岛，一些突破性 DeFi 使用场景也因为链上资产的限制不能最大的发挥其价值，区块链这个新兴行业也无法聚力继续向前强突破。

人们追求自由的过程从未停止过，DeFi 应用让人类第一次可以完全自由的享受每个人都应该拥有的资产服务。NerveNetwork 旨在实现这一愿景，打造一个多资产交互的价值世界，与各个社区一起探讨价值互通的通用跨链协议，为大型 DeFi 应用的催生提供更好的支撑，聚集行业力量，使得 DeFi 能不断向前发展。

二、NerveNetwork 的愿景

制定一个通用的区块链跨链交互协议。通过 NerveNetwork 这套标准的协议转换层，可以匹配通用的接口标准进行开发，接入更多主流的数字资产，形成一套通用的跨链交互协议。只需要遵循通用的接口标准开发一个模块，通过虚拟银行和共识节点的验证升级，即可载入 NerveNetwork 的跨链交互协议。

为 BTC/ETH 等主流数字资产提供一个新的智能闪电网络。比特币/ETH 等资产链上确认时间长，转账费用高，通过 NerveNetwork 可以使用低廉的手续费发起快速交易，在 NerveNetwork 上可以实现秒级确认。BTC 等大部分主流的数字资产是没有智能合约的，例如去中心化的抵押借贷、去中心化交易所等 DeFi 应用，是不能直接在自身的链上去实现。那么通过跨链可以轻松地实现更多的应用场景或者生态。

打开主流数字资产的区块链闭环，可以快速转移到 NULS 生态体系的各条区块链中。任何一条区块链就像是一个局域网，链上资产只能在闭环中流通，NULS 是一个搭建区块链的基础设施，通过 NULS 的模块搭建的区块链都是可以实现资产流通的，只需要配置跨链的模块即可。NerveNetwork 的目标是将其他网络结构类型的局域网接通，例如 BTC/ETH 等。

多资产、公开透明的价值交互平台，为 DeFi 应用生态提供底层支持。我们把 BTC 等数字资产存入中心化的平台，例如交易所，中心化的理财钱包等，他们可以随意挪用你的资产，这些平台就是一个黑箱，无法确保自己的资产是否安全。在 NerveNetwork 上面，可以搭建资产交易的平台，所有的数据都是公开透明的，你的资产通过跨链虚拟银行节点进行管理，保证资产的安全。

三、NerveNetwork 是什么?

NerveNetwork 是一个去中心化的数字资产服务网络。它基于 NULS 微服务框架，使用 NULS ChainBox 开发搭建的区块链跨链交互协议。旨在打破区块链价值孤岛，建立跨链互通的资产交互网络，为 DeFi 应用生态提供底层支持。让数字资产持有者享受真正安全、自由、透明的 DeFi 应用服务。

通过 NerveNetwork 跨链交互协议，只需要通过标准的接口进行少量的开发，即可将不同结构的区块链转化成为一套 NULS 生态中跨链模块能够识别的通用资产类型。从而打通 NULS 生态体系内外的资产交互，同时也为主流的数字资产例如 BTC/ETH 等提供丰富的 DeFi 使用场景。

四、NerveNetwork 的技术设计

（一） 区块链底层

NerveNetwork 使用 NULS ChainBox 区块链开发框架进行搭建，ChainBox 是一个快速搭建区块链的工具，封装了账本、账户、交易、区块、共识和网络六个底层模块，屏蔽了分布式数据存储、点对点传输、共识机制、加密算法等复杂区块链技术，开发者可使用它实现分钟级搭建一条基础链，或根据标准通信协议开发业务模块，然后通过 ChainBox 驱动组成一条全新的应用链。

在 ChainBox 的基础上 NerveNetwork 做了以下优化、扩展：

1. 增加跨链模块；

2. 使用 POCBFT 共识模块替换 ChainBox 中的 POC 共识模块；

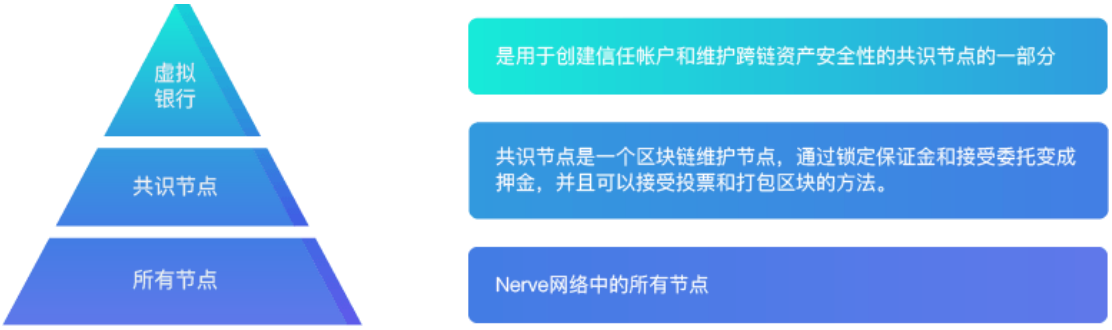
3. 增加协议转换模块，用于与其他区块链的通信。

NULS 基于微服务实现的模块化架构可以降低区块链的研发门槛，降低搭建区块链的开发和时间成本。通过 NULS 跨链协议，可以对接所有 NULS 生态资产，同时 NerveNetwork 支持与其他异构区块链的通信。由此实现对 NULS 生态的扩展和自身价值。

4. 增加了 AMM 和订单簿模块，实现底层对去中心化的 AMM 协议和撮合交易的支持，对 NerveNetwork 接入的网络资产、跨链资产提供二层网络的资产管理和功能应用。

（二） 共识算法

NerveNetwork 的共识算法基于 NULS 的 POC（Proof Of Credit）共识算法扩展实现，POC 是一种安全、合理和公平的共识机制，它具有 DPOS 和 POS 两者的优点，并在去中心化和效率上做到了很好的平衡，NerveNetwork 是一个去中心化的数字资产服务网络，在未来需要为海量应用和服务提供底层支撑，对性能和稳定性都有非常高的要求，为此 NerveNetwork 基于 POC 共识算法，设计了高效、稳定的共识算法 POCBFT，POCBFT 在 POC 的基础上增加了 PBFT 机制，实现区块的最终确认性，减小区块出块时间间隔为秒级，更快的确认时间增强用户体验。区块确认即为交易确认，交易确认后不会回滚。



NerveNetwork 的网络由三层网络组成：

1. 虚拟银行：由虚拟银行负责跨链资产的维护，包括创建和管理平行链的多签账户或智能合约，创建并广播资产转出交易等。虚拟银行从共识节点中选出，默认的选择方式是所有节点中，保证金金额最多的 15 个共识节点。虚拟银行的收益权重是普通共识节点的 2 倍。
2. 共识节点：由共识节点负责区块链的维护，抵押保证金可以创建共识节点，保证金不可以低于 200,000 NVT，上不封顶。共识节点数量固定为 35 个，选择所有节点中保证金最高的 35 个节点维护整个 NerveNetwork 网络。

3. 普通节点：其他节点负责交易的收集、区块和交易验证、为应用提供服务等功能。

（三） 喂价机制

每个共识节点必须提供准确的多个交易所、预言机或报价机构的均价的喂价程序，类似于指数，通过分布式共识节点提供的喂价程序提供给系统判断权重的数据称为喂价指数。

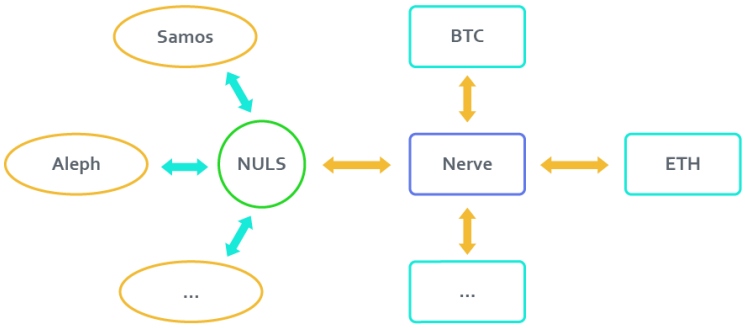
喂价指数每日变更，变更结果写入区块。

1. 淘汰 2 个最低值，淘汰 2 个最高值的喂价；

2. 基于所有共识节点的平均价格提交给系统作为权重依据；

根据支持接入的币种进行质押抵押挖矿，根据其市值来进行权重分配。

（四） 跨链交互

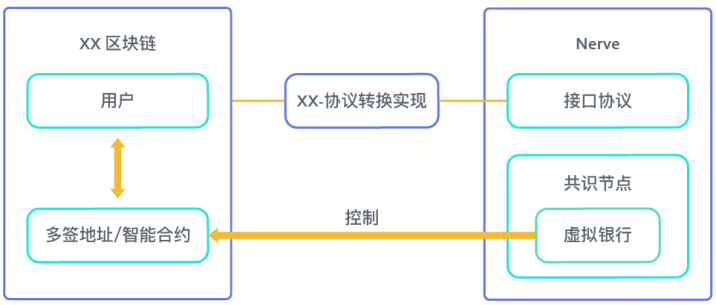


NerveNetwork 的跨链交互分为两个部分

- NULS 跨链生态对接：以通用的 NULS 跨链协议为基础，实现 NULS 大生态中所有平行链的交互。
- 对比特币、以太坊、币安链等独立的公链，NerveNetwork 定义一套接口协议，可以方便的实现各种不同区块链的交互。跨链接口交互协议包括如下几个方面；
  - 地址映射
  - 创建多签地址/创建智能合约
  - 交易验证
  - 交易组装
  - 交易广播
  - 签名验证
  - 追加签名

跨链交互协议架构设计如下：

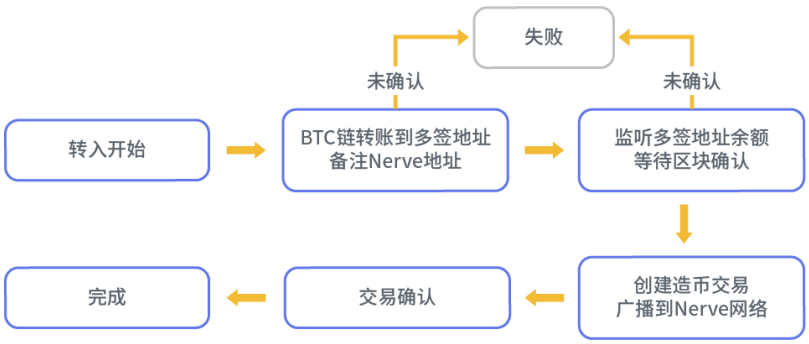
每对接一条区块链，就需要实现一套接口协议组件，用于两条链之间的数据交互。共识节点中选出一定数量的虚拟银行，用于创建和管理多签地址（智能合约），虚拟银行负责资产的转入验证和转出执行操作。



以 BTC 为例，跨链交互流程如下：

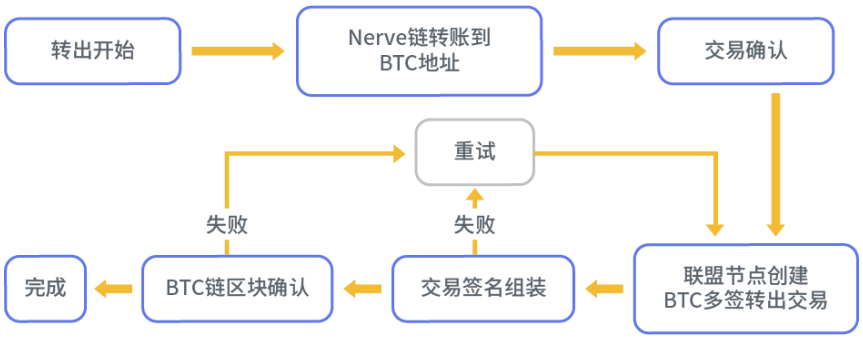
跨链转入流程（充值）：

用户将 BTC 转入由虚拟银行管理的 Bitcoin 链的多签账户，并在转账备注中填写用户在 NerveNetwork 的地址 Nerve-ADDR，NerveNetwork 的虚拟银行监听到 Bitcoin 网络的交易，验证确认数，防止分叉回滚攻击，组装一笔造币交易给用户在 NerveNetwork 的映射地址 Nerve-ADDR，并签名。广播该交易，收集够 66%虚拟银行签名，交易打包进区块，更新账本，此时用户就在 NerveNetwork 生态内拥有了 BTC 资产，在 Bitcoin 上的实际 BTC 资产，由虚拟银行保证其不被动用。



跨链转出流程（提现）：

用户组装转出交易，目标地址是 Bitcoin 链的 BTC-ADDR 地址，签名并广播交易，共识节点收到该交易，验证交易签名，通过后交易打包进区块，区块确认后各个节点组装多签交易，并广播到 NerveNetwork 中，当签名数量足够后，把交易广播到 Bitcoin 主网，从 Bitcoin 多签账户转账给 BTC-ADDR，完成交易。



五、应用协议模块

NerveNetwork 采用 NULS 微服务框架进行搭建，我们可以灵活的使用微服务模块来拓展其应用性。与智能合约不同的是 NerveNetwork 将应用模块直接与区块链底层交互，它的安全性与整个区块链网络共享安全。

（一）AMM 协议

NerveNetwork 分别支持 AMM Swap 和 Stable Swap 两种协议。AMM 采用 k=x*y 算法进行交易。Stable Swap 使得不同区块链之间的资产进行等比例兑换并且不会有滑点，这通常用于资产的跨链兑换中。

（二）订单簿模块

NerveNetwork 支持了订单簿撮合交易模块，开发者可以通过 NerveNetwork 创建撮合交易的 DEX 以及相关的应用。

（三）Stake 模块

Stake 模块可以让开发者轻松的创建一个 Stake 或者 LP Farm，只需要配置一些参数就可以实现。

（四）StableSwap 协议模块

StableSwap 模块允许在 NerveSwap 中创建不同区块链的相同资产的兑换池，该兑换池没有滑点和交易费用，完全按照固定比例兑换。

六、NerveNetwork 的经济模型

NVT 是 NerveNetwork 中内置一种原生资产，NVT 发行的最大总量为 21 亿枚 NVT，初始发行量为 11 亿枚，10 亿枚通过节点共识产出。

（一）初始发行分配（11 亿枚）

前期发展：2 亿枚（空投：1000 万枚 0.48%）9.5%

用于前期的社区建设和推广，以及虚拟银行招募。其中 1000 万枚按照 NULS 持币比例空投到对应地址。

基石投资：3 亿枚 14.3%

用于机构和合作伙伴参与，为 NerveNetwork 和 NULS 生态带来更多资源和机构伙伴，推动 NerveNetwork 项目的发展。

NerveNetwork 基金会：6 亿枚 28.6%

用于 NerveNetwork 的团队发展和第一阶段和第二阶段的研发。以及项目长期发展的基金支持，保证 NerveNetwork 项目的可持续发展。

其中 2 亿枚永久进入虚拟银行节点质押，保证网络和链上资产安全运行。

其中 4 亿枚在主网上线 1 年后逐月线性渐解锁，20 个月解锁完毕。

（二）节点共识产出（10 亿枚）

- **Stake：**

NerveNetwork 链上支持多种资产直接参与 Stake 并获得共识奖励。

- **创建节点：**

创建共识节点需要锁定保证金，保证金也和其他资产的 Stake 拥有同样的效力。Stake 的方式是把资产锁定在一个 Stake 池中，用户只有资产的所有权，没有操作权，直到退出 Stake 后，才可以恢复操作权。

- **权重系数：**

NerveNetwork 的激励机制中设计了一套不同资产、不同 Stake 方式拥有不同权重的机制。

- **共识奖励：**
  - 初始每天总奖励：86400
  - 区块奖励递减时间：100 天
  - 区块递减系数：0.822%
  - 截止：到达总量 21 亿不再产出新币，预计需要 100 年左右。

每个账户的每一笔 Stake，都可以计算一个权重(Weight)，根据权重可以计算该笔 Stake 的奖励数量。权重是根据 Stake 金额和权重系数(weightCoefficient)计算得到的一个结果。

- **权重计算**

权重系数默认为 weightCoefficient =1，以下情况可以获得权重系数的增加：

1. NVT 资产在计算时，权重系数乘以 2；
2. 虚拟银行的保证金，在计算的时候权重系数乘以 4；
3. 非虚拟银行共识节点，在计算的时候权重系数乘以 3；
4. 锁定 Stake，根据不同的锁定时间，设置了不同的权重系数，如下表：

期限	权重系数
三个月	1.2
半年	1.5
一年	2

两年	2.5
三年	3
五年	4
十年	5

5. 当以上三种情况中任意两种情况同时满足时可以叠加；

6. 计算公式：

$$\mathrm{Weight} = \mathrm{nerveAmount} \times \sqrt[2]{\mathrm{weightCoefficient}}$$

7. 权重计算示例：

   a) 当一个账户创建了一个共识节点，并交纳了 200000 NVT 的保证金后，此账户的权重为$200000 \times \sqrt{1 \times 2 \times 1.5}$，等于 346000；

   b) 当 a 账户成为虚拟银行后，此账户的权重为$200000 \times \sqrt{1 \times 2 \times 2}$，等于 400000；

   c) 假设某一个账户转入 5 个 BTC，按当日喂价系统换算比例，1 个 BTC 等于 3500 个 NVT，该账户将 5 个 BTC 进行了定期 Staking 的操作，锁定日期为 5 年，则此账户的权重为$5 \times 3500 \times \sqrt{1 \times 4}$，等于 350000；

   d) 假设某一个账户转入 1000 个 NULS，按当日喂价系统换算比例，1 个 NULS 等于 12 个 NVT，该账户将 1000 个 NULS 进行了定期 Staking 操作，锁定期限为半年，则该账户的权重为$1000 \times 12 \times \sqrt{1 \times 2 \times 1.5}$，等于 20760；

- **奖励计算**

奖励计算公式中用到的参数说明：

Field	Type	Remark
Weight	Long	某一笔 Staking 的权重值
TotalWeight	Long	所有账户的权重值之和
Height	Long	当前高度
Credit	Double	本节点信用值

奖励计算公式中用到的常量说明：

关键数字	说明
86400	每日区块数量
8640000	一个奖励衰减周期（100 天）的区块数量
0.00822	递减比例

- Stake 奖励计算公式（每日奖励）

$$Reward = \frac{\text{Weight} \times 86400 \times (1 - 0.00822)^{(height \div 8640000)}}{TotalWeight}$$

- 节点奖励计算公式（出块奖励）

$$Reward = \frac{\max(0, \text{credit}) \times \text{Weight} \times (1 - 0.00822)^{(height \div 8640000)}}{TotalWeight}$$

- **虚拟银行：**

保证金最多的前 15 名将会成为虚拟银行，虚拟银行具有 2 倍的出块收益权利，同时这 15 个虚拟银行将会通过多重签名保护跨链资产安全，虚拟银行也是整个 NerveNetwork 项目和整个价值交互平台的核心。

- **NVT 资产的用例：**

1、跨链手续费的结算费用；

2、NerveNetwork 项目的投票权，链上治理工具投票权益；

3、链上交易手续费；

4、作为节点创建的抵押押金；

5、参与委托共识获得收益；

6、应用模块协议的部分交易手续费烧毁；

7、订单簿模块创建交易对费用烧毁；

8、其他 NerveNetwork 生态的应用场景。

七、团队

发起人

Berzeck，NTC 理事成员，玻利维亚拉巴斯军事工程学院，系统工程学士学位，近 20 年系统开发和团队管理经验，曾担任跨国公司 IT 总监，国家运输总局项目外部顾问。在使用模块化方法和微服务方面有丰富经验，主导并完成了 NULS 2.0 底层核心的模块化重构和微服务架构的设计、开发。

核心团队

NTC（NULS Technical Community）是 NULS 核心技术社区。 NTC 成员对

NULS 架构和产品有着深入的了解。 NTC 的成员享有自治和社区全力支持所带来的灵活性和创造性。NerveNetwork 项目由 NULS 核心技术社区成员发起，并获得了社区全力支持。NerveNetwork 项目由 NTC 参与开发，NULS 核心团队提供孵化支持，为 NULS 和 NerveNetwork 生态构建多链互通的区块链网络。

八、NerveNetwork 开源社区

NerveNetwork 是一个由社区驱动的、全球性开源软件项目，社区生态是开源项目的生命力所在。NerveNetwork 开源社区将会持续地开发和建设，促进开源生态的安全、和谐、发展。