

Neutrino Protocol 白皮书

Neutrino: 由原生平台生产的令牌所支持的“验算价格稳定”加密货币协议

不同差异组合：*USD-Neutrino, EUR-Neutrino, BTC-Neutrino* 等等。

Sasha Ivanov – sasha@wavesplatform.com

Aleksei Pupyshev – aaapupyshev@icloud.com

版本 0.0.7

发行日: 2020 年 3 月 23 日

免责声明

本文文件中提供的信息不构成或不打算列为法律或财务建议；相反，本文文件中包含的所有信息、内容和材料仅供一般参考。本文文件中的信息可能不包含最新信息。对于本文中任何特殊的法律和财务事项，本文文件的读者应与他们的律师和财务顾问联系以获取相关建议。在没有征求任何有关司法管辖和财务顾问的法律和财务建议首肯的情况下，本文档的任何读者均不得基于本文文件中的信息采取行动或避免采取任何行动。只有您个人律师和财务顾问可以提供保证，其中包含的信息 – 以及您对信息的解释 – 适用于或适合您的特定情况。

使用本文文件及其中包含的信息不会在读者与作者之间建立法律或其他关系。本文档中表达的观点仅代表每位作者的个人观点。

在此明确声明，不承担基于本档内容所采取或不采取任何行动的所有责任。本文档的内容按“原样”提供。并没有代表该内容为无错误的陈述。

总览

流行的数字资产，例如比特币（BTC），以太坊（ETH）或 WAVES，非常易变，无法用作通用货币或低风险储蓄的金融工具。这些特征阻碍了加密货币的大规模采用，并阻止了去中心化应用程序开发人员，产品制造商，金融机构，贸易商和零售商人将此技术集成到他们的工作流程中。

为了解决波动性问题，创建了几种基于法币的稳定币，例如 USDT，TUSD，GUSD 或 USDC。这些加密货币的主要问题在于，他们的用户必须依靠集中实体，并相信他们拥有足够的资金储备来支持市场上发布的稳定币代币，但情况并非总是如此。

在本文中，分析了上述的困难，并描述了作为算法稳定币协议的 Neutrino Protocol 中可能的解决方案。

Neutrino Protocol 回避了可能为不可信任的法定储备金策略，转而采用一种演算方法，该算法使用公共区块链平台的原生令牌（例如 ETH，WAVES 或 ATOM）作为锁定在智能合约上的储备货币。基于 Neutrino 的稳定币可能有不同的变化形式，具体取决于将其固定在何种外部资产上：USD-Neutrino（USDN），EUR-Neutrino，BTC-Neutrino，S&P 500-Neutrino 等。稳定币对储备代币的汇率由一组外部预报器来做确定。

在某些情况下，由于加密市场的动荡或在看跌趋势中基础资产的价值下降，可能无法完全赎回稳定币。为了解决这个问题，可以添加新的令牌工具，以确保在基础资产储备减少的情况下，有机会通过购买所谓的 Neutrino 系统基础令牌（NSBT）来补充这些储备。

交换 Neutrino 代币皆通过智慧合约来进行管理。此外，可以实施 Neutrino 基本代币的其他流动性应用。

Neutrino Protocol 可以为面向 DeFi 的区块链平台（如以太坊，EOS，Cosmos 或 Waves）提供通缩机制。在本文档中，描述了在 Waves 平台的区块链上实施协议，它是具有抵押功能的 DeFi 平台的著名范例。

Neutrino Protocol 令牌的特征和功能

Neutrino Protocol 包括了三种类型的令牌，并通过智慧合约将三种令牌用算法链接在一起。

Waves

WAVES 是 Waves 公共区块链的原生令牌，基于称为 IPoS（租赁权益证明）的共识机制。它用于支付公共网络中的交易费用，并为区块产生的节点生成余额。该代币的市场价格由加密货币交易所的供求动态决定。

USDN

USDN (US dollar neutrino) 是 Waves 平台上的稳定币代币。它的价格与美元绑定。

USDN 的最大资本和供应受 WAVES 代币的最大可能资本限制。通过智能合约系统可以生成 USDN，并由 Neutrino 用户手动进行。此令牌没有预分配或预挖。USDN 供应量的减少也由用户自己控制。Waves 平台上的任何帐户都可以成为 Neutrino 用户。该令牌在加密货币交易所的平均价格为 1 美元。与 \$1 的任何偏差均由下一章中描述的仲裁机制来进行补偿。USDN 代币 ID:

DG2xFkPdDwKUoBkzGAhQtLpSGzfXLiCYPEzeKH2Ad24p

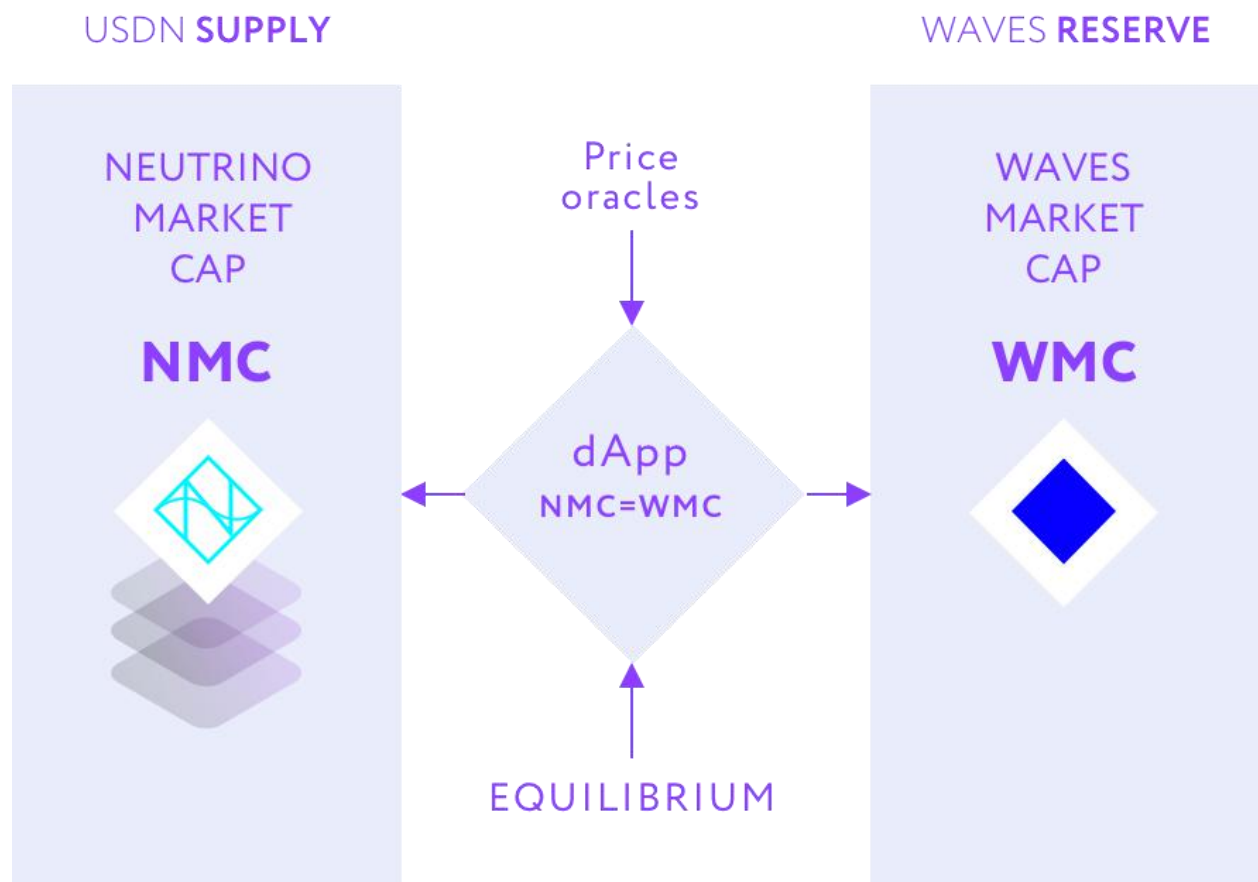
NSBT

NSBT (Neutrino 系统基本令牌) 是 Neutrino Protocol 的实用程序令牌，旨在稳定储备并支持 USDN 供应。NSBT 代币只能通过智能合约生成并只能使用特殊的拍卖算法，其参数取决于 USDN 的储备赤字值。相似的，在 WAVES 资本化和准备金余额大幅增长期间，可以使用 Neutrino 智能合约清算 NSBT 代币。NSBT 代币用于 Neutrino 系统内的付款（即建立储备金，生成新型 Neutrino 代币），并在 Neutrino 持续批准投票系统内为其持有人提供投票权。此令牌没有预分配或预挖。NSBT 的市场价格取决于加密货币交易的供需动态以及 Neutrino 智能合约，在某些条件下（即在剩余状态下）可以至少 1 USDN 的价格购买代币。令牌 ID:

6nSpVyNH7yM69eg446wrQR94ipbbcmZMU1ENPwanC97g

加密支持的 USD Neutrino

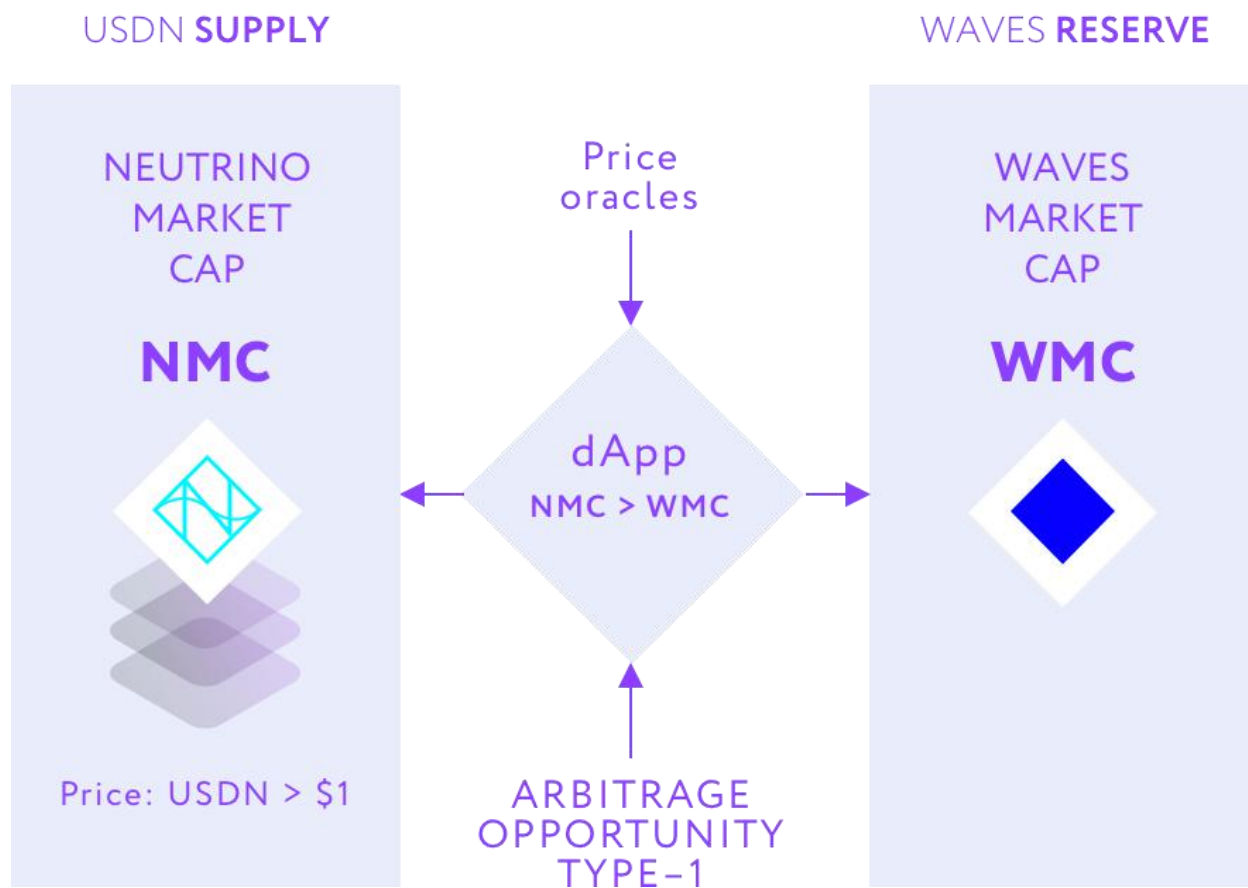
基于 WAVES 代币相对于参考资产（例如美元）的市场价格始终高于零的假设，某些 WAVES 代币可以锁定 X 金额的智慧合约账户，可以“铸造”与美元价格绑定的 USD-Neutrino 稳定代币（USDN）的 X 代币。当 USDN 的市值与锁定资产相等时，在市值之间达到平衡，其中 Neutrino 市值（NMC）等于 $\text{价格} \times \text{数量} - \text{USDN 市值}$ ，而 WAVES 市值（WMC）为所有绑定的 WAVES 市值。



通过外部去中心化的预报器系统提供最新汇率，该系统从流动性最高的交易所和场外交易（场外交易）中获取数据。

套利机会 (类型一)

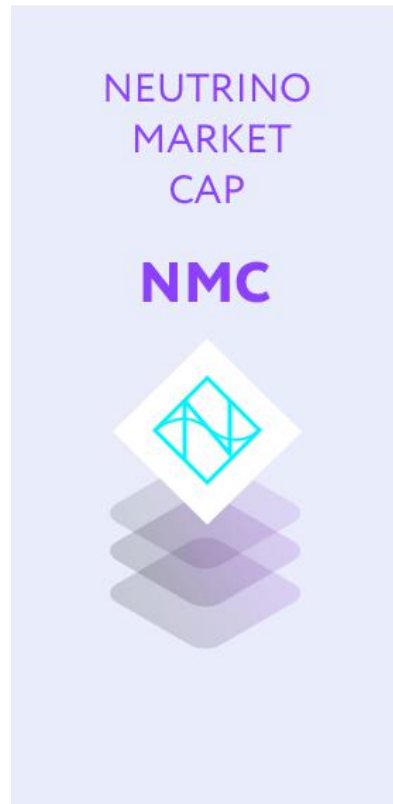
让我们假设交易所对 USDN 的需求已显著增长，并推动了 USDN 的价格上涨，高于 1 美元。在那种情况下，类型 1 套利机会的情况将出现。交易者可以通过 Neutrino Protocol 智能合约或 dApp 将 WAVES 代币交换为 USDN，然后再以更高的价格出售 USDN，从而将这一情况转变为有利可图的机会。此活动将增加市场上的 USDN 供应并导致价格稳定，从而为利用此套利机会的交易者带来一些利润。



套利机会 (类型二)

在相反的情况下，USDN 的交易所供应量可能会显著增长，这将导致 USDN 的价格低于 1 美元。这是套利机会情况的第 2 种类型。在这种情况下，要赚钱，交易者可以在市场上购买 USDN 并通过 Neutrino Protocol 智慧合约或 dApp 将其交换为 WAVES。

USDN **SUPPLY**



WAVES **RESERVE**



Price
oracles



dApp
 $NMC < WMC$

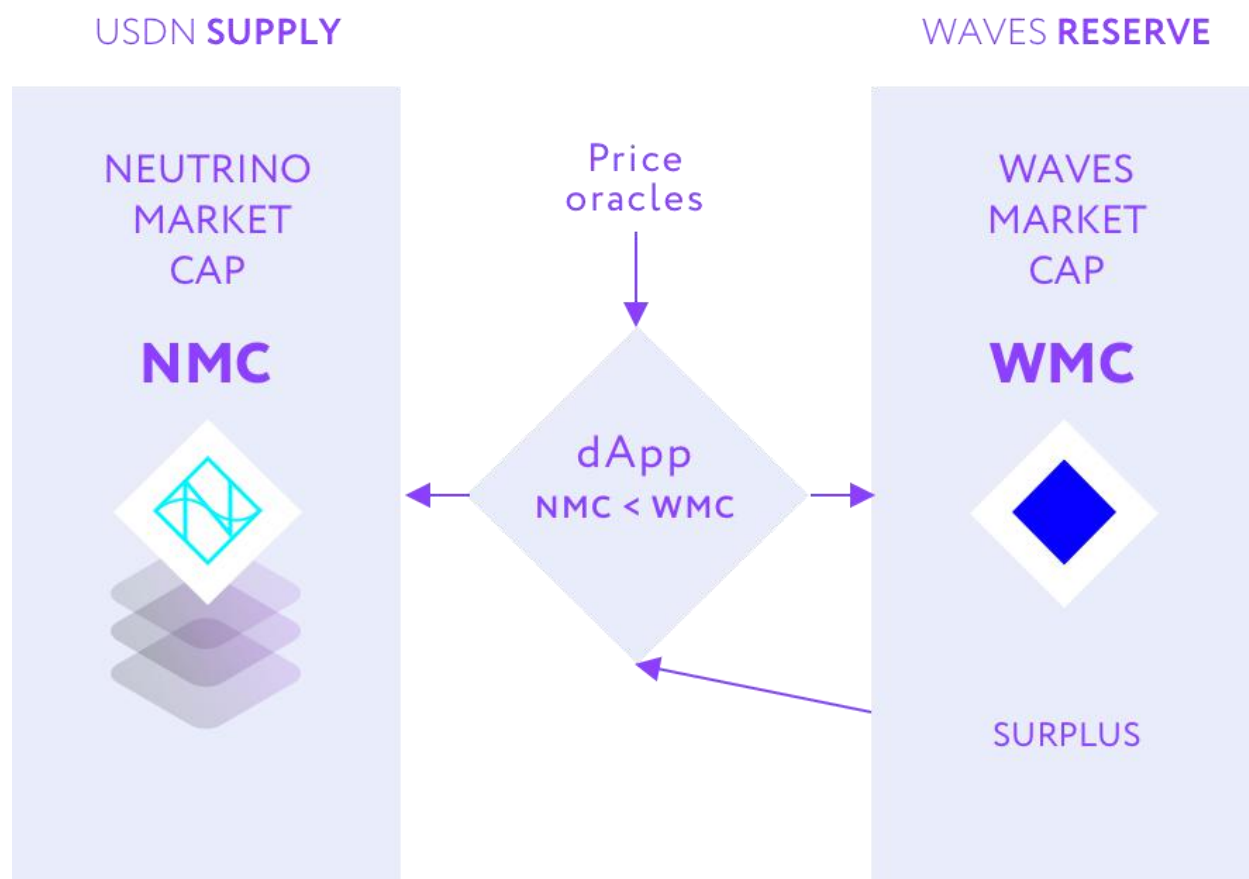


ARBITRAGE
OPPORTUNITY
TYPE-2



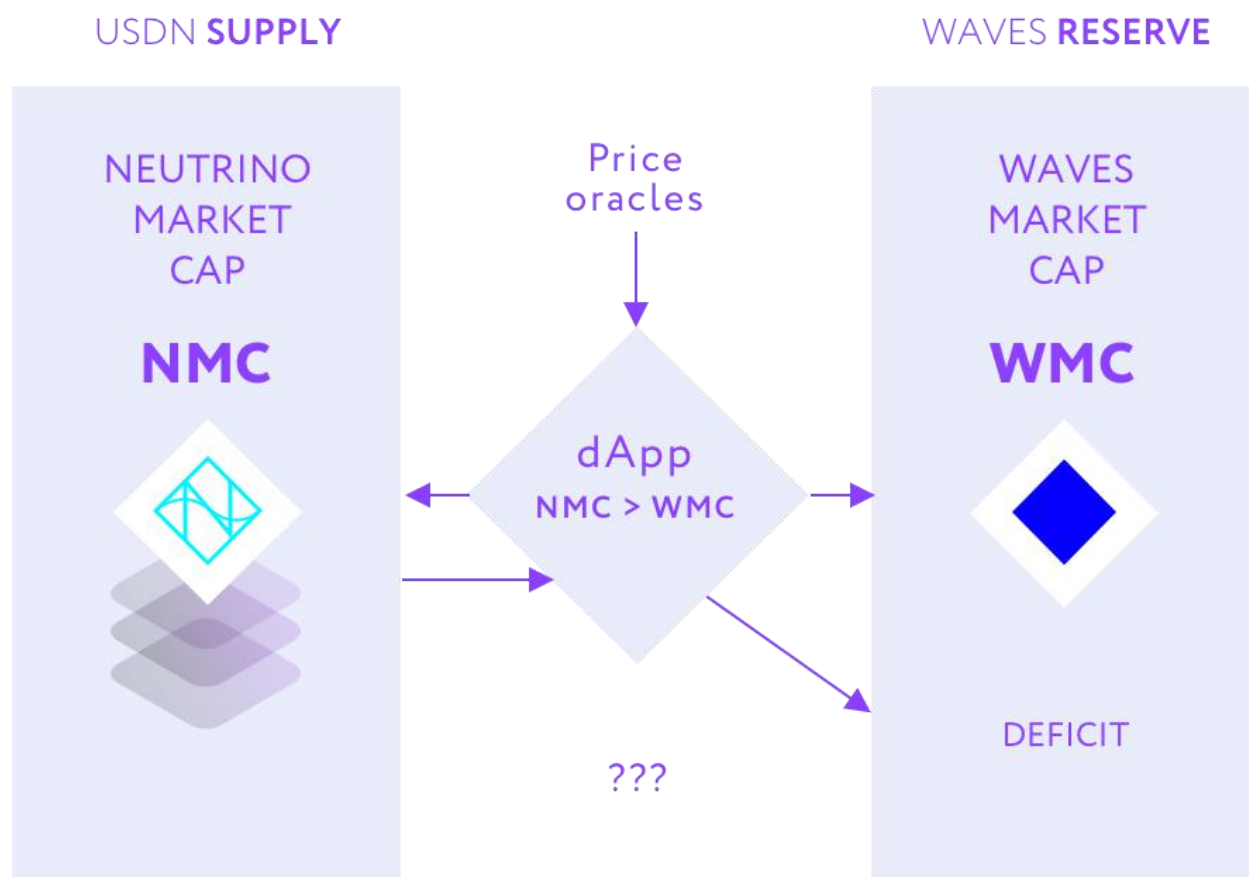
USDN 价格稳定机制

储备代币价格上涨



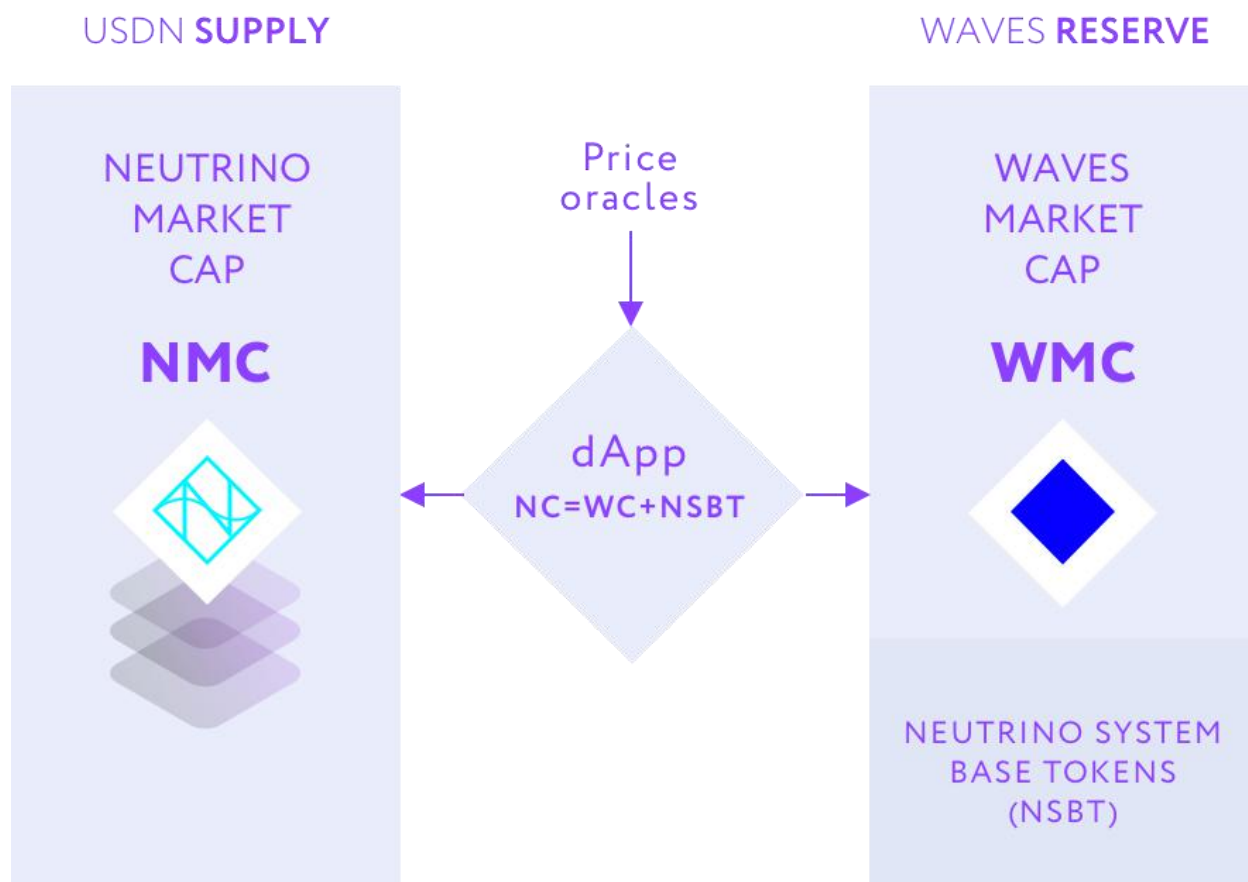
当基础资产（WAVES）的价格上涨时，Waves 的总市值开始超过 USDN 稳定代币的总市值。在这种情况下，智慧合约会检测到超额准备金并生成相应数量的 USDN，以回购 NSBT 清算订单。如果没有代币的清算排程，那么 Wave 上限大于 Neutrino 供给的情况仍然存在。

储备代币价格下降



当目标资产 WAVES 的价格下跌时，资本额不足以覆盖 USDN 稳定代币的资本额。在这种情况下，智慧合约会检测到储备不足，可通过拍卖消除该储备不足的状态，在拍卖中会生成一个名为 NSBT 的特殊代币并出售给 WAVES。

当储备资本化再次增加时，可以清算一项 NSBT 以获得一定数量的 USDN。交易者可以通过公开拍卖中的“拍卖”面板购买 NSBT，他们可以下订单以不同的折扣率（NSBT / WAVES 价格）购买一定数量的 NSBT。Neutrino 基本令牌订单是根据市场订单记录的订单（按 NSBT / USDN 价格）来执行。



范例：USDN 的市值等于 10 万美元，储备的代币价格下跌了 10%。在这种情况下，Neutrino Protocol 只有足够覆盖 9 万美元的 USDN 资本的储备金。为了解决\$ 10,000 的上限差异，智慧联系人会发出 NSBT。NSBT 的发行量取决于订单记录册上的订单以及交易者的折扣。为简单起见，让我们假设只有一个交易者下了 15% 的建议折扣订单。这意味着将支付 10,000 USDN 来购买 11,765 NSBT。当备用代币价格再次上涨时，交易者将能够通过拍卖面板中创建清算订单来清算 11,765 USDN 或更高的 NSBT（通过将 NSBT / USDN 价格设置为高于 1）。交易者的利润将达到 11,765 USDN 或更多。

稳定币对储备代币价格的影响

本章节以在 Waves 区块链上实施 Neutrino Protocol 的实用为例，介绍了对 Neutrino 系统内令牌资本化产生重大影响的各种效应。

有了 USDN 稳定币代币的足够资本和流动性，Neutrino 系统开始影响用作储备的代币（例如 Waves）。这种影响可以描述为两个因素共同作用的结合。

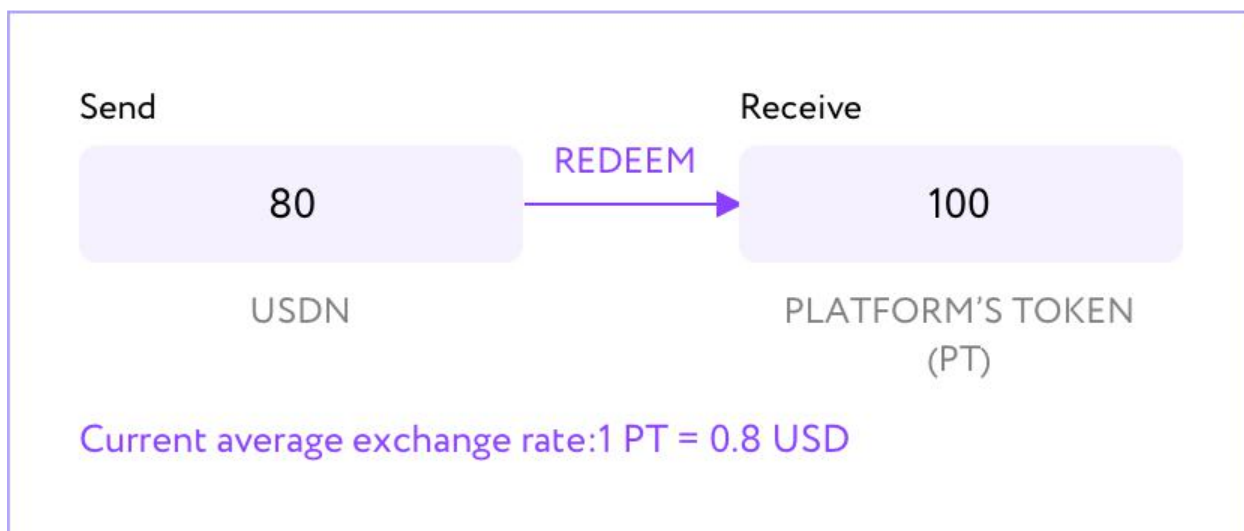
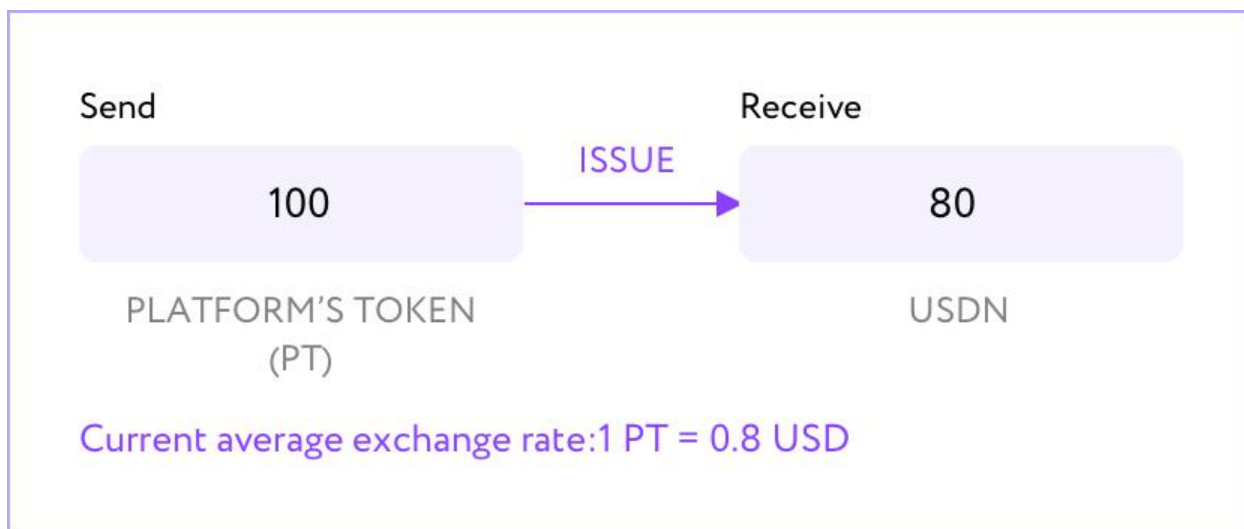
第一个因素是拥有通缩机制的储备构造。 由于 USDN 代币的生成取决于智慧合约中储备的大小，因此 Neutrinis 的供应随着自由流通的代币数量增长而增长。Wave 代币离开公开市场，成为 Neutrino 智慧联系人的储备。随着流通量跟着 USDN 资本的增加而下降，此系统使原生 WAVES 令牌本身通缩。

第二个因素是，在智慧合约上将 WAVES 换成 USDN， 与购买 USDN 来换取 WAVES 代币的交易所或 DEX 交易有很大不同。两者的区别在于，此过程不会影响 WAVES 代币的市场价格，因此举在智能合约上没有流动性，订单或其他类型的有限流动，不会导致 WAVES 价格下降。因此，与从 WAVES 到 USD 或从 WAVES 到另一种稳定币或加密货币等类似的互换过程相反，从 WAVES 到 USDN 的流动性和资本的转移不会对 WAVES 的资本化造成任何损失。

*范例:*在最新的白皮书版本（2020 年 3 月 20 日）发布之时，有 10200 万 - 5600 万 = 4600 万个自由流通的代币，其中有 5600 万个被锁定并抵押以生成挖掘节点的余额。Neutrino 智能合约上锁定了 650 万枚代币。也就是说，锁定在智能合约上的流通供应中约有 15% 是 USDN 代币的储备。

dApp 用户接口草图

Neutrino 仪表板



交易者可以通过智能合约连接到浏览器扩展程序的特殊仪表板上交换 USDN 来签署交易。无需注册或 KYC。所有生成的 USDN 均可在“钱包”面板中进行交易或转移。只需点击“箭头”按钮，就可以将 USDN 反向交换成平台令牌。用于签署交易的浏览器扩展程序还可用于从用户侧对所有交易进行签署。

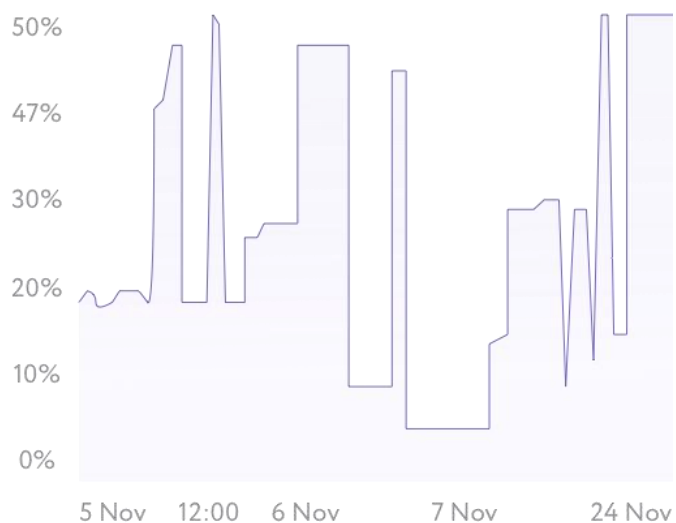
Auction 拍卖仪表板

AUCTION

| USDN | Discount (%) | NSBT |
|------|--------------|------|
| 95 | 5 | 100 |
| 90 | 10 | 100 |
| 70 | 30 | 100 |
| 50 | 50 | 100 |

| NSBT Discount (%) | | |
|-------------------|---|-------------------|
| 50 | 5 | Buy for 47.5 USDN |

DISCOUNT (%)



交易者可以购买 Neutrino 基本代币或在类似于订单的接口中清算它们。即使尚未发行基本令牌，也可以下订单。NSBT 购买订单按折扣价执行。任何订单都可以在执行前随时取消。清算单按时间顺序执行。

Neutrino Protocol 的风险管理

Neutrino Protocol 的成功开发，部署和操作面临许多潜在风险。Waves 小区（交易者，节点所有者，团队，开发人员）必须采取所有必要步骤来减轻这些风险，这一点至关重要。下表列出了已识别的一些风险以及相应的风险缓解计划：

风险 1: 针对智慧合约基础架构的恶意黑客攻击

在系统的早期阶段，对系统来说最大的风险是已部署智慧合约中的漏洞，在漏洞被修复之前，该漏洞有遭外部闯入系统或从中窃取的可能。最坏的情况是，在 Neutrino dApp 智慧合约中保留为备用的所有权杖都可能被盗而没有任何修复的机会。为解决此问题，Neutrino Protocol 提出了一种紧急关机的机制，该机制允许 USDN 和 NSBT 用户找回他们拥有的余额价值。例如，使用 RIDE（一种用于去中心化应用程序的语言）可在智能合约逻辑中插入异常检测的工具。

RIDE 还可在无需进行状态更改或重新平衡 dApp 智慧账户资产的情况下迁移智能合约逻辑。

在 beta 测试期间，原件更新验证逻辑的复杂性将逐渐增加并可能到达一个无法接受未来更新的阶段。

风险 2: 储备代币价格中的黑天鹅事件

如上述所说，Neutrino 智能合约将发行 Neutrino 系统基本代币来弥补储备金的不足。

在 WAVES 价格大幅下跌的情况下，紧急情况预警系统（Emergency Oracles）可单方面触发智能合约操作的紧急关闭功能。

风险 3: 定价错误，DDoS 攻击，不合理和不可预测的事件

有许多不可预测的事件可能会发生，例如来自 Oracle 预演系统的不正确价格信息，或者不合理的市场走向可能导致 Neutrino 价格在长期下有所浮动。如果对系统失去信心，利率调整甚至 Neutrino 稀释都可能达到极限，且仍无法为市场带来足够的流动性和稳定性。为了减轻此类风险，需要使用智能合约来确认各种操作的不同参数，限制和门坎级别。问

题在于：如何找到合适的参数来保持系统稳定？未来如何透过 Neutrino 最大利益持有者/代币持有者们发起的特殊管理方式来改变这些配置？

要回答这些问题，可能有必要对 Neutrino 的状态及过渡期间进行建模，并将其与历史市值的度量值做关联，包括对这些模型使用具有不同参数集的蒙特卡洛模拟，以估出最佳的极限，参数和门坎值。

主要的外部行动系统

除了智能合约基础结构之外，Neutrino Protocol 还依赖某些外部行动系统来维持运营。

Price oracles 价值设定预演系统

当前汇率是通过外部去中心化的预报器系统来做确定，该系统提供了来自流动性最高的交易所和 OTC（临柜交易）的数据。应由最大的 NSBT 持有者们发起选举程序来组织一份可信任的预报列表。过滤储备代币价格的消息提示应通过去除在某些区块间隔内所计算出的“左”和“右”尾数（离群值）和中间价格值来完成。这将使价格更为稳固，从而减少波动噪音。

Emergency oracles 紧急情况预演系统

紧急情况预演是类似于价值设定预演的外部行动系统，在发生攻击时，它们是 Neutrino Protocol 的最后一道防线。由多数 Neutrino 持有者推选出的紧急情况预演系统应有权单方面发动紧急关机。除此权限外，这些行动系统在本体系统中不具有任何其他特殊通行或控制权。这些情况预演 oracles 也是由 NSBT 持有者推选出。

Pacemaker oracles 频率调节预演系统

根据各个不同使用协议的平台需求，有些平台可能需要额外安装一种名为频率调节预演系统，它会触发交易并处理复杂的验算。与价值默认或紧急情况预演系统相比，频率调节预演系统的内容可由大众公开设置和运行。例如，Waves 智能合约语言 RIDE 并不是图灵完备的，意味着它不允许循环，递归或会自动触发的交易，这就是为什么频率调节预演可以使整个系统正常运行。

协议实作

Ventuary Lab 与 Tradisys и KozhinDev 共同开发了 Neutrino protocol 第一个开放源码的实作。

用户接口 dApp : <https://beta.neutrino.at/>

技术文档 : <https://docs.neutrino.at/>

协定扩展 : <https://medium.com/@neutrinoteam/neutrino-protocol-2020-vision-challenges-1fec59e1577b>

使用条款 :

<https://docs.google.com/document/u/1/d/1gQPtVj5LZ9tbZlyBUYISYvqAjPpKmEH3ksfilYlp5CM/edit#heading=h.lvi5m440j6n3>

GitHub: <https://github.com/ventuary-lab/neutrino-contract>

CoinMarketCap: <https://coinmarketcap.com/currencies/neutrino-dollar/>

参考文献

1. <https://medium.com/mastering-web3-with-waves/mastering-web3-with-waves-module-2-aa98f7dfcdde>
2. <https://makerdao.com/en/whitepaper#malicious-hacking-attack-against-the-smart-contract-infrastructure>
3. <https://wavesplatform.com/products-ride>
4. <https://medium.com/@neutrino-team/neutrino-protocol-2020-vision-challenges-1fec59e1577b>