摘要

WAVES 是一个去中心化的区块链平台，专注于自定义区块链代币操作。通过合规的网关运营商在 WAVES 区块链上维护本国货币转移。分布式代币交易促进了区块链上的筹资，众筹和金融工具交易。轻量级客户端为最终用户提供了简单的安装过程和平坦的学习曲线。

介绍

“假设：将尝试使用每种可能的区块链技术应用程序，但 p2p 数字现金将仍然是最常用的应用程序”。

Ryan X Charles

“区块链技术的杀手级应用是区块链本身。”

共同的智慧

自成立以来，区块链技术对其最自然的应用（使用网络代币进行价值转移）一直充满争议。去中心化货币是一项突破性的发展，但区块链技术不能仅局限于此。区块链实质上是一个分布式数据库，他允许各种类型的分布式分类帐条目，其性质取决于区块链用户对它们的解释。

引入区块链作为数字货币的基础吸引了对该技术的极大关注，使全球的监管机构和政府在此过程中保持高度警惕。毫无疑问，比特币将建立自己的有效货币体系。但是很明显，目前不应该有太多的区块链代币被用作货币，因为这造成的低流动性和高波动性阻止了新兴区块链被用作价值的安全存储。

我们建议将重点放在区块链代币的其他用途上—那些经常被忽视而偏向于区块链技术可能提供的低级机会，例如智能合约。经典有色硬币方法有未被开发的诸多潜力，并且 WAVES 平台旨在最大程度地实现这一目标。

智能合约是比特币脚本的自然发展，他的发展是必然的，并将成为区块链技术的基石之一。另一方面，使用其他方法更容易实现某些功能。为区块链交易的自定义代币操作非常灵活，可以用于各种应用程序中，从通过区块链进行本国货币转移到去中心化交易。专注于此类操作可能会很好地补充以太坊引入的方法。

在以下各节中，我们将描述 WAVES 平台功能的技术动机，并通过用例进行说明。我们打算确定当前区块链技术中最“可用于生产的”方面，并将其应用于实际问题。

自定义区块链代币及其用法。

技术动机。

大约在 2013 年左右出现了区块链资产和有色硬币方法，当时实施了几种利用比特币区块链的协议。除此之外，还尝试了一些从头开始构建自定义区块链代币平台的尝试，其中最引人注目的是 Nxt。

我们开发 Nxt 实施的方法，通过添加到区块链交易的附件实现自定义代币的创建和转移。这种方法具有明显的优点，例如能够轻松实现新的事务类型，但是从实际的角度来看，它充满了强制性的硬分叉问题 - 添加新的事务类型时，必须更新网络客户端软件，因为老客户端无法支持新的交易类型。

WAVES 通过提供可扩展的解决方案来解决此问题，在该解决方案中，新的事务类型通过插件引入，这些插件未包含在核心软件模块中，而是作为扩展安装在其顶部。未安装相关插件的客户端仍可以继续这些自定义事务。这种方法允许第三方开发人

员引入新的交易类型，并创建一个类似于 App store 的生态系统。
核心级别仅支持最基本的事务类型，包括：
–自定义代币的创建，删除和转移
–分散式代币交换，实现为分布式订单匹配引擎，其中，出价和要价网络交易相互匹配
–匿名功能–匿名订单簿是行业级交易平台必不可少的
值得注意的是，WAVES 通过提供一个自定义代币与另一个自定义代币的交易（资产到资产交易），在去中心化区块链交易方面迈出了关键的一步。这带来了全新的机会，包括与本国货币挂钩的代币进行交易，从而复制了传统的交易基础设施。

应用案例
区块链上的本国货币。
尽管使用主网络代币进行价值转移是很自然的事情，但它仍然引发了一些问题。使用低流动性和高波动性代币进行价值转移，对商人来说有明显的缺点，并与监管机构产生了紧张关系。尽管如此，完全去中心化的货币仍然可行，这可以通过缓慢而稳定地采用比特币作为货币来证明。
但是，为了提供足够的流动性并减轻波动性，防止分散使用货币作为价值存储，用作货币的代币总数应受到限制（至少在技术开发的初始阶段）。因此，我们强烈建议仅使用比特币作为货币。
我们处理外部价值转移代币和货币的方法源于“ Multigateway”方法。在比特币的情况下，有一个（或多个签名）政党维护着一个进出比特币的交换程序，将其交换为其相应的网络代币。因此，我们使用 WAVES 区块链促进了比特币的转移。
由于比特币本身固有的限制，这种方法显然是集中的。它与“市场挂钩”方法相对，后者依赖于通过某些做市程序提供动态挂钩。从表面看，市场挂钩法似乎是在去中心化平台上镜像金融资产的一种适当方法，但要进一步考虑，隐藏的集中化始终无所不在。
通过将集中化明确引入支持区块链国家货币和 BTC 的方式，我们能够为现有金融机构开辟新的视野。他们的作用可以简化为法定资产和 KYC ／ AML 程序提供流动性。维护支付基础设施已完全外包给去中心化的区块链。
在 Nxt 的区块链上使用 CoinoUSD 代币率先采用了在区块链上提供本国货币的方法。

这也类似于 Ripple 的网关方法。我们认为，这种策略可以与新兴的许可区块链方法竞争，并吸引愿意在开放式区块链上工作的金融机构。

众筹，分散的金融工具及其他。

我们认为，区块链是管理基于社区的项目（从财务到组织元素）的大多数方面的有效手段。区块链技术由于其固有的延迟而无法支持高频交易。对于毫秒级执行时间的大批量交易，最有可能采用集中式解决方案。但是对于不需要即时交易的应用程序而言，区块链提供了一个非常自然的环境，例如，用于发行众筹代币和管理社区内的资金流。在这个领域中，使用分散式解决方案是有好处的，而集中化几乎没有什么用。

如果我们考虑一种类似 Kickstarter 的模式，即以一定数量的资金来交换将来要发布的产品，那么我们可以看到其明显的局限性。项目支持者无法通过出售另一个用户来退出其对项目的“投资”。另一方面，在基于区块链的系统中，这种应用案例是很自然的，自定义代币可以通过设计交换和转移。

在大多数辖区，发行证券受到严格监管。代币可以与证券相关联，特别是在对未来代币价格做出某些预测或代币发行人承诺支付一定股息的情况下。但是，区块链是与法规无关的工具。如果希望利用区块链进行证券发行的法人实体符合当地法律法规，则在区块链上发行证券与进行证券交易所上市一样合法。

创业集资，私人投资和风险投资似乎是区块链金融工具最合适的领域。另一方面，较大的企业也可以将其用于特定的财务操作，例如清算和结算，只要这些操作不会导致对速度要求过于苛刻。

在大多数辖区（特别是美国除外），可以合法地完美地进行不超过给定限制的基于区块链的筹款。美国的股权众筹法允许通过简化的 SEC 注册程序进行筹款。

严格的美国证券法旨在防止欺诈，为此，需要强大的集中监管机构，例如美国证券交易委员会。但是去中心化技术的进步会引入某种形式的社区和去中心化发行人审查，最终可能会取代集中式监管机构。

将众筹作为 WAVES 平台的主要用例之一意味着必须将某种形式的分散式 KYC ／ AML 集成到系统核心中。为此，我们正在实现分散的信誉系统，该系统应消除 WAVES 区块链上不道德的行为者。

轻量级客户端，两层体系结构，权益证明和可用性。

技术动机。

两层体系结构和轻量级客户端。
经典的比特币方法本质上是一种通过通用事务日志同步分布式系统的方法。它要求每个网络节点都存储事务历史记录的完整副本。显然，这不能很好地扩展，因为最终并非每个节点都能够存储完整的历史记录。有多种方法可以缓解这种情况—简化的付款验证程序，该程序仅存储给定节点必不可少的数据；链下交易；双向支付隧道；减少区块链膨胀直接在系统状态下工作。使用最简单的方法，即在 Genesis 块中所有节点都相等的情况下，集中化可能会出现，因为低容量节点必须依赖能够承受存储完整区块链的完整，高容量节点。实际上，出现了两层体系结构。
这会使系统固有地集合吗？不可以，因为如果有足够的资源，新节点始终可以进入网络并成为完整节点。
当然，新兴的集中化带来了信任问题，因为轻量级节点必须信任完整节点，并且可能成为流氓完整节点的受害者。但是，有一些方法可以减轻这种情况，例如轮询几个节点，维护受信任的节点列表等等。
WAVES 平台执行的方法乍一看对于经典的加密货币倡导者来说似乎是极端的。轻量级节点根本不下载区块链，而是依靠完整的节点进行支付验证和网络交互。该方法基于已在 Nxt 平台上成功运行了一年以上的 SuperNET lite 客户端。
WAVES 建立在 Scorex 平台上，该平台基于使用当前网络状态作为完整交易历史的替代方法，开发了一种方法。将为轻量级节点实现简化的付款验证过程，从而增加另一个安全层。轻型节点可以下载系统状态，并基于此状态简化付款验证过程。

权益证明共识，股权租赁。
我们选择了股权证明协议作为 WAVES 的共识算法。该选择基于其在 Nxt 中的成功使用以及某些理论上的考虑。同时，我们提出了对 PoS 协议的增强，该协议应缩短交易时间并提高交易吞吐量—租用 PoS（LPoS）。
在 PoS 系统中，在主网络代币中拥有余额的每个节点都有机会（与其余额成正比）产生一个区块。在两层体系结构中，将付款处理移到整个节点上是合乎逻辑的。同

时，所有余额非零的节点仍必须有资格获得奖励。
可以通过从轻量级节点到完整节点的显式平衡租赁来解决由较少的节点放样导致的安全性降低的理论问题。通过将它们的余额出租给受信任的完整节点，轻量级节点实际上增加了收取交易费用的机会，因为它不必保持在线状态，并且由于其余额增加，完整节点产生区块的机会也增加了。
帐户租赁不等于余额转移；轻量级节点仍可以将其余额转移到另一个节点并执行其他操作。通过释放它们的余额，轻量级节点有效地选择了哪些完整节点将执行网络的大部分付款处理。减少可能产生块的节点数量可以缩短确认时间，降低等待时间并提高系统吞吐量。

轻量级节点实现和浏览器插件。
轻量级节点被实现为用 JavaScript 编写的浏览器插件。它与基于 Scorex 的完整节点进行交互。该插件是从浏览器应用商店中安装的。由于不需要下载区块链，因此用户只需执行简单的安装过程即可立即获得功能齐全的区块链钱包。
钱包界面类似于传统的在线银行/经纪人界面。综合本国货币允许以法定货币计价的本地价值转移。本国货币进出区块链的交易由受信任的提供商进行。用户完成本国货币代币的购买后，便可以将其转移给另一用户，或在去中心化交易所中进行交易。
通过允许对美元，欧元，人民币等进行交易，资产到资产交易可以提供类似于股票市场的交易界面。总而言之，平台接口比常规的加密货币客户端更接近传统的金融接口。我们发现，重要的是提供一个界面，大多数用户已经习惯了该界面，同时使用区块链技术对其进行授权。用户可以完成传统金融平台无法完成的工作，但是学习曲线却保持平稳，这是采用大众市场的关键。

WAVES 的其他主要功能。
首先，WAVES 的目标是基于社区的开发和项目。 为此，实施了分散投票和消息传递。 它将在管理社区项目中提供类似 DAO 的经验，同时从技术角度来看仍然很简单。
WAVES 将允许以自定义代币（资产）支付网络交易费。 与所讨论的交易一起，将资产交换到主网络代币的订单被发送到去中心化交易所，并且只有在执行该订单之

后，交易才能包含在下一个区块中。

结论。

从一开始就考虑到大规模采用 WAVES 平台的情况。 在此概述中，我们尝试展示了可用于为最终用户提供以前看不见的机会的技术解决方案，并为快速采用区块链技术铺平了道路。