白皮书

作者： sasha ivanov

1.摘要

WAVES 是一个致力于实现可定制代币发行、去中心化交易、区块链法币的公有区块链平台。区块链法币是通过合规的网关来实现的。去中心化的代币交易可以用来融资、众筹以及交易区块链上的金融资产。

轻钱包的安装非常简单，终端用户使用也非常简单。

1. 简介

假设：

“如果将所有区块链应用都进行测试的话，点对点的数字货币将会是使用最广泛的应用。
- Ryan X Charles.

“区块链技术的杀手锏应用就是区块链本身。”
- 群体智慧.

区块链技术从一开始就因为其最本质的应用 – 区块链代币价值转移 – 而备受争议。去中心化的货币是一个突破性的成果，但是区块链技术不仅限于此。区块链本质上是一个分布式数据库，允许各种类型的分布式账本输入，其特性取决于用户对它的理解。

作为数字货币基础的区块链吸引了很多人对区块链技术的关注，使得全球很多监管者和政府都对此提出了警告。毫无疑问，比特币是一种有效的货币系统。很明显，目前也不应该有很多区块链代币用作货币，因为很低的流动性和很高的波动性妨碍了将区块链用于安全的价值储存。

我们提议应该关注在区块链代币的其它使用领域 – 这些使用案例因为其使用机会很低而被忽视了，例如智能合约。在经典的彩色币方法中还有很多尚未被充分挖掘的潜力，WAVES 平台想要充分开发和利用这方面的潜力。

智能合约的发展也是必然的，而且将会是区块链的基础技术。另外一方面，一些特定的功能可以通过使用其它的方法来更容易地实施。可定制代币作为区块链交易的附属物是非常灵活的，可以应用在很多领域，从基于区块链的法币转账到去中心化交易等。以太坊可能已经很好地介绍了这方面的方法。 *[1]*

在接下来的内容中，我们将介绍 WAVES 平台功能的技术方面，并用使用案例进行详细阐述。我们想要确定目前区块链技术最可行的方面，并将它们应用到真实世界的问题中。

2. 可定制代币及其用途

2.1 技术层面 Technical motivation.

区块链资产和彩色币方法大概是在 2013 年出现的，当时有很多协议都使用比特币区块链来进行实施。 *[4] [5] [6]*
此外，也有很多完全重新创建的可定制区块链代币平台，其中最著名的就是 Nxt。*[7]*

我们使用了 Nxt 所实施的方法，通过添加到区块链交易中的附件来实现可定制代币的创建和转账。
该方法的优点很明显，例如，能够很容易地实施新的交易，但是从实际角度来看存在的问题就是强制硬分叉 – 当添加了新的交易类型时，网络客户端软件需要更新，因为之前的客户端不支持新的交易类型。

WAVES 通过可扩展的解决方案来解决这个问题，其中新的交易类型是通过插件来引入的，但是并没有包括在核心软件模块中，相反只是作为扩展部件。没有安装相关插件的客户端仍然能够广播这些交易。这种方法允许第三方开发者引入新的交易类型，形成了一个类似苹果商店的生态系统。

在核心软件中，只支持最基本的交易类型，包括：

- 可定制代币的创建、转账和删除
- 去中心化的代币交易，以去中心化的订单匹配引擎、买单和卖单交易互相匹配来实现
- 匿名功能 – 对于工业级交易平台来说，匿名的订单是必须的

值得一提的是，WAVES 提供了资产与资产之间的直接交易，这在去中心化的区块链交易中迈出了重要的一步。
这开启了全新的机遇，包括与法币代币的直接交易，因此重现了传统的交易基础设施。

2.2 使用案例

2.2.1 区块链法币

使用主网络代币用于价值转移是很自然的，但是也必然会引起其它问题。商家使用流动性很低、波动很大的代币很明显存在问题，而且也带来了监管压力。

但是，完全去中心化的货币是可行的，比特币已经逐渐成为了一种货币。

然而，为了能够实现充足的流动性以及避免波动性，用于货币目的的代币数目应该是有限的（至少在区块链技术发展的初始阶段）。因此，我们强烈建议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多重签名网关方法。 *[2]*

以比特币为例，有一方（或多方）负责维护比特币的进出交易过程，并将其兑换为相应的网络代币。因为我们就可以使用 WAVES 区块链来转移比特币。

由于比特币内在的限制，很明显该方法是中心化的。与市场锚定方法不同，它们通过特定的做市过程来实现动态的锚定。乍一看，似乎市场锚定方法是一种在去中心化平台上映射金融资产的不错的方式，但是在中心化的表面下需要进一步的考虑。

通过引入中心化的区块链法币和 BTC，我们能够为现有的金融机构开启新的视野。他们的角色仅仅是为这些法币资产提供流动性和 KYC/AML（知晓你的客户/反洗钱）过程。维护支付基础设施完全外包给了去中心化的区块链。

在区块链上提供法币的方法已经在 Nxt 区块链上尝试了 CoinoUSD 代币。这也与 Ripple 的网关方法类似。

我们认为这样的策略能够与新出现的授权区块链方法进行竞争，并吸引金融机构参与到公有区块链中。

2.2.2 众筹、去中心化金融工具等等

我们认为区块链是管理社区项目的一种有效方式，从财务到组织方面。区块链由于其本身的延迟性，无法支持高频交易。绝大多数中心化的解决方案则通常都可以用于高频交易，而且执行时间都是毫秒级别。但是对于无需实时交易的应用，区块链则提供了一个非常自然的环境 – 例如，发行众筹代币和管理社区的财务资金流。在这个领域使用去中心化的方案是很有好处的，而中心化的方案则基本上没有太多用处。

如果我们考虑 Kickstarter 模式，将一定量的资金抵押用于换取将来发布的某个产品，我们就能看到很明显的局限性。 项目的支持者无法通过出售而退出自己的投资。另外一方面，这样的使用案例很自然地会使用区块链系统，其中可定制代币可以交易和转账。

在绝大多数司法管辖区，发行证券都是受到严格监管的。代币可以与证券相关，特别是如果项目代币的发行方承诺支付分红的话。但是，区块链的监管还不明确。如果法人实体希望利用区块链来发行证券的行为符合当地的法律和监管的话，那么在区块链上发行证券与在股票交易所发行证券是一样的。

初创企业融资、私募发行和风投阶段的投资似乎是区块链金融工具最合适的应用领域。另外，也可以用于大型企业的特定金融操作等，例如结算和清算，只要它们对速度没有过高的要求即可。

在绝大多数的司法管辖区（尤其不包括美国），没有超过规定界限的区块链融资是完全合法的。美国的股权融资法律允许通过美国证监会的简单注册程序来进行融资。

美国严格的证券法是为了预防欺诈，因为需要一个强有力的中心化监管机构，例如美国证券交易委员会。但是去中心化技术的发展会带来某些形式的商品，而且去中心化的发行者审核也会最终取代中心化的监管机构。

WAVES 将众筹作为其核心使用案例之一，这意味着必须要在系统中整合某些形式的KYC/AML（知晓你的客户/反洗钱）。到那个时候，我们会实现一个去中心化的信用系统，将会消除 WAVES 区块链上的欺诈者。

3. 轻量级客户端，双层技术架构，权益证明和可用性

3.1 技术

3.1.1 双层架构和轻量级客户端

经典的比特币方法本质上是通过共识交易记录来同步一个分布式系统的一种方式。它要求每一个网络节点都存储完整的交易历史记录备份。很明显，扩展性不好，因为最终并不是所有节点都能够存储完整的交易记录。有一些不同的方式来实现这一目的 - 简单支付验证程序允许节点只存储必要的数据；链下交易；双向支付通道；减少区块链膨胀；直接与系统状态作用。*[8]* 通过最简单的方法，其中所有节点在创世块都是相同的，可能会出现中心化的区块，因为低能力的节点需要依赖那些能够存储所有区块链数据的高能力的节点。

一种有效的双层架构出现了。

这会让系统中心化吗？
不会，因为如果一个新的节点有充足资源的话，它可以随时进入网络并成为一个全节点。而且也会成为不良全节点的受害者。但是，有方法可以解决这些问题，例如对节点进行投票，维护可信节点列表，等等。

WAVES 平台采用的方法对于传统的密码学货币支持者来说可能有点极端。轻钱包节点根本无需下载区块链，相反所有的支付验证和网络互动都依赖全节点。该方法是基于 SuperNET 轻量级客户端[3]的，而它已经在 Nxt 平台上成功运行了 1 年多时间。

WAVES 是基于 Scorex 平台[8]而建立的，该平台使用目前的网络状态作为完整交易历史记录的一种替代方法。轻量级节点将会实现简单支付验证程序，增加了额外的安全保护层。轻量级节点可以下载系统状态，而简单支付验证程序也是基于该状态的。

3.1.2 权益证明共识和权益租赁

我们选择权益证明（Proof of Stake,PoS）协议作为 WAVES 的共识机理。这种选择是基于它已经成功在 NXT 中运行，以及一些理论考虑。同时我们改善了 PoS 协议，可以减少交易时间并增加交易吞吐量 – 租赁 PoS（Leased PoS ，LPoS）。

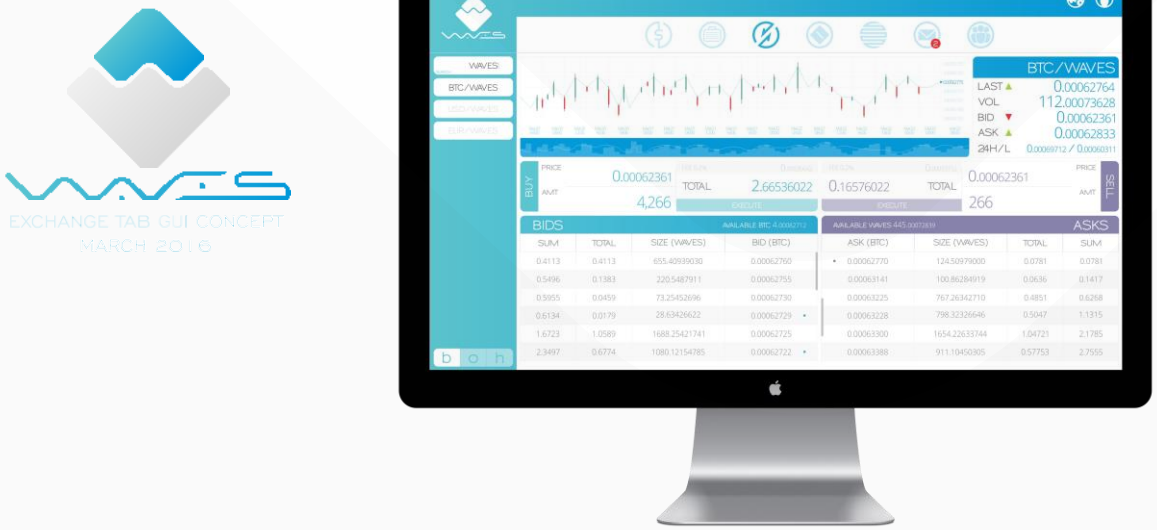
在一个权益证明系统中，每一个持有主网络代币的节点都有机会（与所持有的的代币余额成比例）生成区块。在双层架构中，将支付处理过程转移到全节点在逻辑上是合理的。同时，所有余额非零的节点仍然可以获得权益奖励。

因更少的节点权益而导致的理论上的安全性降低问题可以通过将轻量级节点的余额租赁给全节点来解决。通过将它们的余额租赁给可信的全节点，轻量级节点实际上也增加了它们获得交易费的几率，因为它无需一直在线，而且全节点也增加了生成区块链的几率，因为其余额增加了。

账户租赁不是余额转账；轻量级节点仍然可以将其余额转账给其它节点以及执行其它操作。通过租赁它们的余额，轻量级节点可以有效地选择哪个全节点来执行网络中大部分的支付处理。节点数量的减少可以实现更快的区块确认时间、更少的延迟以及更高的系统吞吐量。

4. 轻量级节点的实现与浏览器插件

轻量级节点是用 JavaScript 编写的浏览器插件。它与基于 Scorex 的全节点进行互动。该插件可以从浏览器应用商店中安装。因为无需下载区块链，只需要进行简单的安装用户就可以立即获得完整的区块链钱包。



钱包界面与传统在线银行/经纪商的界面类似。原生代币转账时可以以整合的法币计价。法币进出区块链是通过可信的网关供应商来实现的。一旦用户完成法币代币的购买，他就可以将其转账给其它用户或在去中心化的交易所中进行交易。

资产与资产的直接交易提供了一个股票市场类似的交易界面，允许与美元、欧元和人民币等进行交易。总之，平台的界面与传统的金融界面非常类似。我们发现提供一个用户已经熟悉的界面是非常重要的，同时还使用了区块链技术。用户可以实现传统金融平台无法实现的事情，但是无需专门的学习与培训，这也是获得主流市场应用的一个关键因素。

5. WAVES 的其它核心功能

WAVES 将首先以社区开发和项目为目标。之后会实施去中心化的投票和信息功能。允许类似 DAO 模式的社区项目管理，但是从技术角度来讲也是比较容易的。

WAVES 将允许以可定制代币（资产）来支付网络交易费。除了正在处理中的交易，资产交易为主网络代币的订单也将发送至去中心化交易所中，而且只有在订单执行后，交易才会写入到下一个区块中。

6. 结论

WAVES 平台是以大规模应用为出发点。在此基础上，我们试图使用技术解决方案来为终端用户提供前所未有的机遇，为区块链技术的快速应用奠定基础。

参考文献

[1] https://github.com/ethereum/wiki/wiki/White-Paper
[2] http://multigateway.org/
[3] https://github.com/Tosch110/SuperNet-Lite
[4] https://github.com/CounterpartyXCP
[5] https://github.com/OpenAssets/open-assets-protocol
[6] https://github.com/OmniLayer/spec
[7] http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
[8] http://arxiv.org/abs/1603.07926