微米链

WIENCHAIN

分布式自治组织孵化型公链

1.1 版本

微米链
WIENCHAIN

摘要——价值转移的变革已经从基础的价值转移进化到智能合约。Wienchain 是由去中心化自治组织（DAO）管理，专注于孵化和搭建进入数字时代新纪元的商业桥梁，主要应用基础区块链技术和去中心化程序实现(i) 直接发送，即时交易；(ii) Wien（微米）管理，去中心化自治组织根据可塑造和决定 Wienchain 未来发展提案来分配区块奖励;(iii) Wien（微米）应用，可以在 WIEN（微米）网络上构建和处理应用程序，确保该应用程序永久存在于 IPFS 网络上；(iv) Wien（微米）资产，资产发行平台，根据业务逻辑需求提供元数据;(v) Wien（微米）孵化，通过使用资产股份制，股东可以轻松地在区块链中被追踪并自动获得利润分配

工作量证明机制（PoW）和服务证明机制（PoSe）是区块链技术中常用的两种验证方法。Wienchain 利用这两种验证方法的优点，结合成一种混合方式来提高区块链的安全性和可持续性。通过 Wien（微米）主节点网络（WMN），区块奖励将会发放至工作量证明矿工和服务证明所有者。

I. 引言

2008 年以前，物联网商业严重依赖金融机构，因为尚未存在可以提供信用需求的方法。反过来，信用机构作为中介收取服务交易费。这些费用加上交易总是可逆的事实，造成一些小额临时交易不能成交。2008 年，中本聪提出了点对点电子现金系统，即比特币，促使价值转移交易成为可能[1]。加密货币的引入降低了金融机构在网络交易中作为中介角色的重要性。伴随着初期的比特币区块链技术发展，互联网交易方式发生革命化的变革。比特币公开提供发送者和接收者的人对人匿名交易账目。这可提供网络上所有进行交易的永久记录[2]。在学术圈，比特币被广泛认为具有较低的隐私性，尽管有此局限，许多人仍旧将自己的财务历史委托给区块链。

比特币中的工作量证明机制概念允许分散化共识的存在，在大规模互联网中，无中心化主权也可以实现点对点的全部交易。然而，由于分散化的性质，区块链本质上不够快速。这对用户的使用有明显的影响，因为需要所有节点确认的区块链上的所有的交易都可被追踪。所以，Duffield, E., & Hagan,K. [3]在 2014 年提出了即时发送协议，该协议提供使用常规节点和可选主节点以分散的方式来锁定交易的扩展功能。2015 年，暗黑币被重新命名，现广泛被称作达世币（Dash），数字现金（Digital Cash）的合并简写。

通过完全信任他人网络进行转移价值日益被更多人接受并得到关注。Gawin Wood 博士[4]开始着手记录他基于交易状态机的新概念，这种新概念被称作以太坊。引入执行代码的功能可以在区块链中更改状态，使用特定成本单位计算费用，而不是仅仅依靠比特币使用的输入和未交易输出规模来计算。以太坊以创始状态开始逐步执行交易，将其转为最终的交易状态。我们正是把这种以太坊世界的典型“版本”接受为最终状态。这种状态可以包括诸如账户余额，声誉，信托安排，关于物理世界信息数据等情报，简而言之，目前任何可用电脑表示的东西都是可容许的。通过以太坊协议，读者可以在以太坊网络上实现一个节点并在分散的安全社交操作系统中加入其它节点。为了实现在算法上指定并自主执行交互规则，可以编写智能合约。

本文提出一系列针对比特币，达世币和以太网的改进措施，利用防篡改直接发送的交易和执行根据对应主节点分配负载的智能合约带来的分散高效，

灵活，可量化，高匿名性的加密货币。所以负载在矿工和主节点间是平均分配的。

II. 混合验证方法

A. 最佳工作量证明与服务证明机制

Wienchain 是一个包含工作量证明和服务证明两种机制的混合系统，用以解决关于安全和分散化可持续并且可量化的固有问题。初始阶段，Wienchain 是一个以工作量证明机制为中心的货币，通过传统的挖矿和矿工获得区块奖励来增加网络流通。在初期，散列难度等级低且工作回报率高的指数增长已被证实。

Wienchain 的价值在于，网络流通和散列难度增加，玩家通过工作量证明算法获得金币奖励。因此，正如传统挖矿随着时间推移回报减少一样，服务证明的进程会增加可持续性，因为网络需要的能量显著减少了。

此外，这还提升了针对围绕比特币和工作量证明为基础的加密货币漏洞的安全性，他控制了网络超过 51%的挖矿能力，这种控制也被称作 51%算法攻击[5]。当同时获得 Wien（微米）主节点网络（WMN）的 51%和 51%的挖矿能力明显变得更为困难的时候，与 51%的挖矿能力和指数难度截然相反，WIEN（微米）的价值和流通得到提升。

B. X16Rv2 工作量证明

工作证明是一个概念，其中的一个系统需要一个可行的工作量，以阻止恶意使用计算能力，如发起拒绝服务(DoS)攻击或发送垃圾邮件[6]。尽管它在比特币出现之前就已经存在了，但比特币成为了第一个将概念变为现实，实现在大规模商业场景中应用的货币。

Wienchain 采用了数字分布式账本技术，即"区块链"作为基础。区块链包含所有 Wienchain 交易记录，资产交易和在连续的"块"中安排的其它元数据，防止任何用户二次消费持有物。为了规避篡改或改建，账本公开且共享给所有用户，所以修改版本很容易被检测到并被其他用户拒绝。

账本篡改是通过散列，即服务工作量证明机制的长数字串来检测的。通过散列（哈希）函数(X16Rv2)得到的一组给定数据，它只会生成一个散列。然而由于瀑布效应，即使是很微小，任何一部分的原始数据的变化，都将导致完全无法识别的散列。同时，无论原始数据集的大小如何，根据选定函数生成的散列长度总是相同的。散列是一个单向函数，它无法逆向工作去获取原始数据。它只能通过检查来确定生成散列的数据是否与原始数据相匹配。

工作量证明机制也解决了大多数决策中确定公平代表的争议。如果大多数都采用一个 IP 地址一个投票，那么这可以被任何分配到大量 IP 的人破坏。工作量证明机制是一个 CPU 一个投票。主要决策用最长的链表示，因为它对此贡献出最多的工作量。如果大多数 CPU 力量被诚实的节点控制，诚实链将会以最快速度增长并超过其他竞争对手。为了修改一个过去的区块，攻击者将不得不重做该区块的工作量证明以及它之后的所有区块，然后追上并超越诚实节点的工作。随着后续新添加的区块不断增加，较慢的攻击者迎头赶上的可能性会呈指数级降低。为冲抵随着时间推移，运行节点中硬件速度的提高和变化的影响，工作量证明的难度由每小时移动平均线瞄准区块平均数量决定。如果它们生成得太快，难度就会增加。

每一个以防止 ASIC（专门设计来完成特定计算任务的集成电路）存在为目的工作证明算法都可能失败，即使没有确凿的方法可以避免，但通过创造使用不同算法提升难度这些方法可以减缓它的存在。

X11 是一种常用的散列算法，一种利用非常规的方法，也被称作算法规则变化。X11 包含所有 11 个 SHA3 候选算法，链中每个散列的计算被提交至下一个算法。通过适应多种算法，货币的 ASIC 被创建的

可能性很小。

尽管散列算法的链很复杂，来自 Bitmain 的 D3 ASIC 矿工使用 GPU（图形处理器）和 CPU（中央处理器）进行了 X11 挖掘，尚未盈利。因此，在 Wienchain 中我们将使用另一种类型的散列算法。为确保业余爱好者能利用CPU和GPU在Wien（微米）中挖矿，一旦存在 X16Rv2 的 ASIC，Wienchain 将会尽快持续修改散列算法。

C. Wien（微米）主节点网络服务证明

服务证明是一个解决工作量证明机制问题和缺点的实施概念。这些问题之一是挖矿所消耗的能源。执行加密所需的计算能力只会随着难度的增加而增加，因此消耗了更多的电力。长期来看，这样会对机密货币的健康起反作用，因为矿工不得不大量出售他们的部分货币兑换成法定货币来支付电费，这会让加密货币贬值。

服务证明通过授予与矿工拥有的主节点数量成比例的挖矿能力奖励来解决这个问题。因此一个 PoSe 矿工受限于与主节点数量相关的挖矿交易比重，不像 PoW 矿工利用原始能源（电能）。例如，一个拥有 1/1000 主节点的矿工挖矿最大值为所有可采区块的 0.1%。这也大大减少了网络的能量需求。

PoW 系统的另一个潜在问题是，长远来看，挖矿是垄断的。伴随着挖矿难度增加，区块奖励减少，矿工的数量无疑会减少，这使网络容易受到51%攻击。51%攻击是当单一矿工或者矿池控制了 51%的网络计算能力，然后制造交易的欺诈区块并亲自验证它们[5]。这使他/她从网络中吸走大量的货币为己用成为可能。

然而，具备了 PoSe 系统，想要获得网络垄断的攻击者必须拥有51%的加密货币，由于货币升值，这只会变得更加困难且昂贵。此外,对这种攻击最大的威慑是一个拥有51%货币股份的矿工是无法攻击这个他自身拥有大量股份的网络的，这不符合他/她的最大利益。这样的攻击，将会立即导致货币贬值，因此，他/她会更有动力去维持网络安全。

1) Wien（微米） Masternode 操作: 只有两种类型的消息被用来激活网络中的主节点-主节点信息和主节点网络信息。除了这两个，还有一些其它的消息用来运行直接发送，第二层共识和 Wien（微米）管理。

主结点由存款 25,000 个 WIEN（微米）的钱包形成，钱包会激活节点，因此，会允许它在整个网络中增值。然后生成一个辅助备份秘钥以便对所有后续消息进行签名验证。这个秘钥将在独立工作条件下为钱包上锁。

通过使用辅助备份秘钥可以在两台不同设备上实现冷模式。主要的"热"客户通过辅助备份秘钥提交25,000个WIEN（微米）到该消息。当"冷"检测到一个消息和辅助备份秘钥，主节点被激活。随后，这将使主节点中的"热"客户和2,5000个WIEN（微米）无效，从而实现激活后被攻击的几率为零。开始时，主节点通过网络"主节点信息"消息，声明:

- 附属担保 25,000 个 WIEN（微米）
- 公共 IP 地址
- 主节点签名(辅助公钥)

每隔15分钟发送一条网络消息来证明该节点保持激活状态。一旦活动时间过期，网络将消除系统中不活动的节点，并阻止客户端使用节点。网络也可以被节点发现，但是如果端口关闭，它将被标记为未激活并且不会得到补偿。

2) Wien（微米）主节点网络奖励程序: 这些主节点通过向矿主提供奖励，增强了比特币网络中常用的现有完整节点体系结构；从而确保一致的效益成本比率。这很重要，因为随着网络的扩大和矿主们付诸行动，导致服务质量降低和交易速度放缓，传统全节点的维护呈指数级增长。

该节点必须至少存储 25,000 个 WIEN（微米）才能启动主节点。一旦激活，网络客户将从节点接

收服务并获得激励奖金。通过评估所有区块奖励的50%后，分配至 WIEN（微米）主节点奖励程序，然后从与管理者，PoW 和主节点之间共享的同一区块奖励中获得支付款。主节点奖励根据当前激活的总主节点的不同而产生差异，因为奖励程序有固定的百分比数值，尽管主节点网络是波动的。

III. 去中心化自治组织

区块链技术的一大亮点就是它们是分散的。这意味着它们不受单一机构，如政府或中央银行的控制，但换言之，它们被切割分散到大量计算机，网络和节点之间。在许多情况下，区块链项目利用这种分散的状态是为了获得一定程度的隐私和标准法定货币及交易中无法获得的安全性。

去中心化自治组织也被称为 DAO，DAO 是一个被设计成自动化且分散的组织。DAO 不隶属于任何特定的国家，公司或个人集团。DAO 是一个拥有操作资金决策权来消除错误的自动化系统和群众外包系统。

在 Wienchain 中，DAO 由 WIEN（微米）提供燃料和主节点矿工群，DAO 的设计方式让社区里的任何人都可以用一定数量的 WIEN（微米）创建一个提案，并且允许社区就该提案进行投票。每个主节点在投票期投赞同或反对间。如果提案通过大多数人投赞同票通过，WIEN（微米）会分配给提出这个提案的人。这个提案可以是运营一个营销活动，经营一个矿池，搭建一个包含信息的网站，甚至是在现有核心的顶端进行创新。DAO 的设计允许主节点为公链的开发方向投票。

IV. 区块奖励和补给

不像许多其他公共区块链协议那样，持续给予矿工和主节点运营者奖励，导致区块奖励逐渐走向衰败，Wienchain 将引入 6%的区块奖励削减膨胀，每 525,600 个区块预估为 1 年。区块奖励在前100,000 个区块后，从 280 个 WIEN（微米）/每区块起。

分配给基础、孵化实验室和区块链生态系统建设的货币将在首批 10 万个区块中开采。

基础	8%	1.93 亿 WIEN（微米）
孵化实验室	4%	0.97 亿 WIEN（微米）
区块链生态系统建设	3.5%	0.85 亿 WIEN（微米）
未来 30 年待开采	84.5%	20.25 亿 WIEN（微米）

表 1

区块奖励分配

在区块高度达到 129,600 之前，100%的区块奖励将会给到工作量证明机制的矿工，主节点奖励，服务证明机制将在 129,600 上启用。因此，129,600 和 259,200 之间的区块将会根据 70%的工作量证明机制和 30%的服务证明机制进行分配。区块高度达到 259,201 开始，区块奖励将根据 30%的 Wien（微米）管理，剩余 70%按照 70%的服务证明机制主节点网络和 30%的工作量证明机制比率划分，即 30%的 Wien（微米）管理，49%的服务证明机制，21%的工作量证明机制来进行分配。

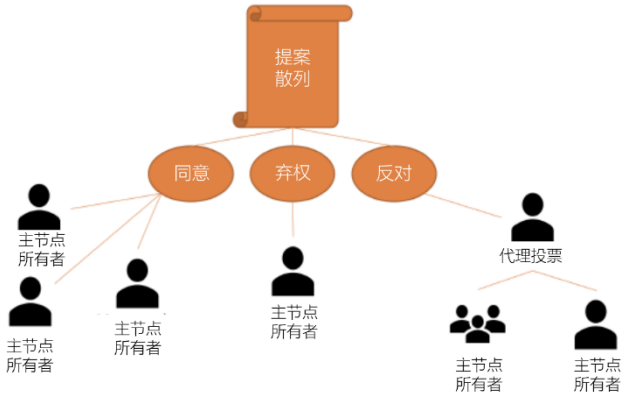
V. 使用案例

A. 直接发送（DS）

Wienchain 还引入了一个名为直接发送（DirectSend：锁定交易和主节点一致）的新概念。这项技术将允许加密货币，比如 Wienchain 不依靠中心授权，与近似即时交易，如销售点情境下的信用卡支付竞争。通过利用主节点之间的一致性，交易信号被锁定，并且只能在特定的交易中使用。可被广大供应商接受的 Wienchain 和 DS 可以进化加密货币，通过将交易确认时间的延迟由长至 1 小时（使用比特币）压缩到短短数秒。

B. Wien（微米）管理

在 Wienchain，它可以自己运行一个系统，只需设置或预编程规则即可。DAO 持有会员基金，并将基金使用在明确的目的中。为了在 DAO 中创建一个提议，需要明确指定 4 个参数——收件人、金额、提案详情、资金周期。收件人将创建一个提议并拟定提案的交易金额，创建者必须根据区块链中包含获胜者奖励的超级区块来计算天数，明确投票持续



时间。较长的持续时间更为有利，因此，创建提议者应该尽早创建提案，以便主节点所有者有时间阅读并为提案投票。创建者需花费 500 个 WIEN（微米）创建提案，这样可以防止滥发提案，并允许主节点过滤高质量提案。如果参数中有任何虚假信息，交易将失败。

图 1. 代理人投票

Wien（微米）DAO 治理规则——1.提案所有者需花费 500 个 WIEN（微米）来创建提案。2.主节点所有者能够找到已创建提案，并投票赞成、反对或者弃权。3.Wienchain 的主节点创建过程允许主节点所有者定义投票地址，且不需要暴露抵押品和奖励的私钥，从而使得代理投票成为可能。4. 对于每一个有效的提案，应该有 10%的所有活动主节点投赞成票。5. 在每隔 43,800 个区块间发生的超级区块中，有效的提案将获得他们要求的资助金。

C. Wien（微米）资产（孵化）

Wien（微米）资产是一个新的创业孵化功能，初创企业可以在区块链上发行新的数字代币资产。资产的元数据是在一个散列文件或文档之后创建，发布在IPFS上，并且该散列存储于Wienchain区块链。散列是什么?我们为什么要做散列？散列是函数，他的设计是任意输入都得到一个固定长度的输出。散列将返还散列值和散列代码。Wien（微米）资产是原始数据的组合和散列代码。散列对于数据安全和数字代币是很重要的。如果有人想解密数据的话，使用散列代码的数据都不会被成功解密，但是他们可以验证文档的身份。

输入	散列代码
欢迎	548aed7438aadb5934ffdb7d79cb47c 2cadb5934ffdb7d79cb63acef80125da0

表2. 散列代码图

散列代码有一些质量约束——

- 散列代码的每个输入应该不同。
- 应该是不可被解密的。
- 输入相同的散列代码应该是相同的。
- 文档进行任意修改后，散列应该是完全不同的。

图2.Wien（微米）资产发行

作为稳定市值战略的一部分，发行资产将要求发行者花费5,000个WIEN（微米），同时支付5,000个 WIEN（微米）作为交易手续费。长远来看，这将使 Wienchain 市值减少，并且成为发现 Wien（微米）资产发行交易矿工的头奖。

D. Wien（微米）应用

区块链技术在很多领域都有应用，而且它不局限于金融领域。例如，零售和电子商务服务、医疗服务、金融服务和房地产行业。Wien（微米）应用是针对所有领域进入区块链市场的解决方案和机会，

可以使他们在 Wienchain 平台的基础上定制应用系统。利用简单的编程语言，新商家只需向 Wienchain 支付低额的费用就可以集成他们的应用。

Wien（微米）应用可能会消除多方沟通中存在的问题。以医疗行业为例——行业内的一个通用应用程序可以在病历上签字。医疗可适应多种签名（仅在授权方指定的一定数量被批准或签署时，交易才可以发生）来授权其他机构读取完整或部分病例。另外，应用也可以验证主要或次要的程序已经发生。区块链的使用确保信息是加密的，且对于授权打开的人是可访问的。

如今，移动应用正在被顶端集中组织收购，这意味着应用程序开发者需要支付注册费用才能在这些平台上发行，另外还需要支付高达 30%的销售佣金。

E. Wienchain钱包

Wienchain 钱包是一个加密货币钱包，允许您存储多种加密货币，包括 WIEN（微米），代币以及在利用 Wien（微米）资产仅在唯一一个钱包中标记过的资产。Wienchain 钱包被设计为，你可以不用将你拥有的加密货币转化，随时可用加密货币支付的钱包。不需创建另一个钱包和下载其他的钱包，就可以让你发送一种加密货币，并且接收者可以以他偏好的任一货币类型来接收。

商家可以选择他们偏好的加密货币类型，并且系统会做转换，给予付款人广泛的，市场中可用的加密货币选择范围。

VI. 结论

通过运用 Wienchain 技术，包括 Wien（微米）管理、Wien（微米）资产、Wien（微米）应用、Wien（微米）孵化器，Wienchain 的目标是成为一个分散的平台，核心是用区块链技术改善现有商业业务和并使其成为初创企业坚实的后盾。此外，同时使用工作量化证明与服务证明算法，并与 Wien（微米）主节点网络相结合，Wienchain 的目标是形成集中于可长期持续实现自给自足，规模发展的生态系统。双列网络可以作为一个高度可配置平台来提供服务，平台可以轻松地为其它功能提供空间，也可以在后期进行改进，从而在本质上保证了 Wienchain 项目始终是一个不断进化的存在。

除了商业，公众用户也从这些功能中受益，如私人发送和直接发送的服务增强了用户的可触及性、私密性并为广大的个人和商业活动提供安全、直观的交易系统。

此外，Wienchain 的另一个目标是成为一个可以轻松集成到现有电子商务解决方案中的平台，就像金融机构和社交媒体一样。可以实现通过使用一个无缝的抽象层，允许现有的商业、金融和社交媒体平台利用这些功能，如不需要重新搭建基础结构便可直接发送。因此，我们坚信在未来，具有开放式设计的 Wienchain 作为一个强大的基础层，必能高度适应并服务大量的金融和商业协议。

参考文献

[1] Nakamoto, S.(2008) 比特币:一个点对点的电子现金系统

[2] Meiklejohn, S.,Pomarole, M., Jordan, G., Levchenko, K.,McCoy, D.,Voelker, G. M., & Savage, S.(2013年10月) 一些比特币:描绘那些无名人士的付款方式.2013年互联网测量大会(第127-140页)ACM

[3] Duffield, E.,& Hagan, K.(2014).达世币：匿名区块链交易的点对点加密货币和工作量证明系统的改进.比特论文.信息

[4] Wood, G.(2014) 以太网:一个安全去中心化的交易帐本.以太网项目黄页，151,1-32

[5] Bradbury, D.(2013) 比特币的问题，电脑欺诈&安全, 2013 (11),5-8

[6] Back,A. (2002) 现金算法——柜台服务的拒绝