



白皮書

Umbru旨在为用户和开发人员提供一流的体验，同时使用下一代工具和软件。

版本1.0

目录

介绍

1. 摘要	4
2. 网络	5
2.1. 分散治理	5
2.2. 主节点	5
3. 技术	6
4. 项目概况	7
4.1. 为什么选择 Umbru?	7
4.2. 问题	7
4.3. 解决	8
5. 分布模型	9
5.1. 采矿	9
5.2. 主节点	9
6. 概述	10

UMBRU 项目

7. 愿景	12
7.1. 基本权利	12
8. Umbru 实验室	13
9. 协议体系结构	14
10. 路线图	16
11. 团队	18
12. 工具书类	19
13. 合法的	20

第一章

介绍

Umbru网络的技术和协议允许一个分散的、自融资的治理平台。它还允许开发工具和软件来扩展和增强网络上的功能。

1. 摘要

随着比特币代码库和协议的升级，破折号代表着加密货币进一步分权的飞跃。然而，DASH于2014年推出，需要进一步发展，以促进更快、更安全和匿名的私人加密货币。Umbru的目标是进行Dash开发的核心升级，并在分散、私有、安全和匿名加密货币的理念上进行扩展。

Umbru建立在仪表盘代码库的基础上，结合了几个核心功能。包括确定性分散主节点系统、区块链治理和网络预算和融资系统。

比特币是隐性财富的根源和基础，是数字存储价值的“金本位”。比特币及其继承者未能实现的一件事是，将其扩展为一个分散、私有和匿名的支付系统。由于交易和公共分类账的性质，交易细节永远不会是完全匿名的。可以分析和跟踪事务数据，从而破坏所需的任何在线隐私。这将创建所有过去和现在的交易的永久公共跟踪。比特币及其大部分后续交易都是化名交易，而非私人和/或匿名交易。

创建于2019年，翁布鲁设想一个完全分散、私有、匿名和安全的区块链。用户和商家可以在没有风险或担心交易和/或信息公开的情况下进行交易。在这个时代，隐私是一种卑鄙的行为，不值得讨价还价。

该网络不含ICO、预售、开发基金或费用，通过工作证明和锁链确保公平分配。它通过使用Sinovate创建的X25x哈希算法的工作证明（挖掘）得到保护，该算法是一种ASIC、FPGA、Quantum-Resistant算法，可确保进一步分散的网络。

2. 网络

2.1. 分散治理

翁布鲁关于如何解决加密货币中两个重要问题的选择：治理和融资。分散式项目中的治理是困难的，因为根据定义，没有中央机构来为项目做决策。在翁布鲁，这样的决定是由网络作出的，也就是说，由 masternode 的所有者作出的。治理体系允许每个 masternode 对每个提案进行一次投票（是/否/弃权）。如果提案通过，那么 Umbru 的开发人员可以实施（或不实施）。

2.2. 主节点

除了挖掘 umbru 的传统工作证明（POW）奖励之外，用户还可以运行和维护称为 masternodes 的特殊服务器。由于这一创新的双层网络，Umbru 可以以一种不信任和分散的方式提供创新功能。masternodes 目前用于管理和财政系统。用户因运行 MasterNode 而获得奖励；从块奖励的 20% 开始，每月增加 5%，直到分配 50% 用于支付 MasterNode 网络。

MasterNodes 启用以下服务：

ChainLocks，通过在块被挖掘时签名来保护翁布鲁区块链免受 51% 的挖掘攻击。

治理和财政部，允许 MasterNode 持有者确定项目的方向，并将 10% 的区块奖励投入到项目和生态系统的开发中。

MasterNode 所有者必须拥有 5000 个 Umbru，他们通过签署一个写入区块链的特殊交易中包含的消息来证明这一点。Umbru 可以随时移动或使用，但这样做会导致 masternode 退出队列并停止赚取奖励。MasterNode 用户还享有对提案的投票权。每个 masternode 都有一个投票，此投票可用于预算提案或影响翁布鲁的重要决策。

MasterNode 需要花费资金和精力来进行托管，因此它们将获得块奖励的百分比作为奖励。因为每个块中只支付一个 masternode，所以支付的频率可能会有所不同，而且支付的 umbru 值也会有所不同。未来，MasterNode 也有可能从费用中赚钱。

10%

每个区块的奖励由网络持有，
用于每月预算。

每月从可用的总池中创建/投票提案。如果预算没有用完，
就不会结转到下个月。

3. 技术



主节点

除了挖掘umbru的传统工作证明(POW)奖励之外，用户还可以运行和维护称为masternodes的特殊服务器。由于这一创新的双层网络，Umbru可以以一种不信任和分散的方式提供创新功能。masternodes目前用于管理和财政系统。



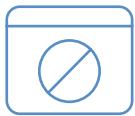
暗重力波

DGW或暗重力波是一种开源的难以调整的比特币加密货币算法，最初用于破折号，后来出现在其他数字货币中。DGW是由Dash的开发者和创建者EvanDuffield撰写的，这是对Kimoto重力井中发现的时间扭曲漏洞的回应。



链锁

锁链是Umbru网络提供的一项功能，它在接受付款时提供了确定性。这种技术创造了一种环境，在这种环境下，付款可以立即被接受，而不存在“区块链重组事件”的风险。



X25X 算法

Umbru使用Sinovate项目创建和使用的X25x工作证明算法，这是一种ASIC、FPGA、Quantam抵抗算法，确保进一步分散网络。

4. 项目概况

4.1. 为什么 Umbru?

创建于2019年，翁布鲁设想一个完全分散、私有、匿名和安全的区块链。用户和商家可以在没有风险或担心交易和/或信息公开的情况下进行交易。在这个时代，隐私是一种卑鄙的行为，不值得讨价还价。

该网络不含ICO、预售、开发基金或费用，通过工作证明和锁链确保公平分配。它通过使用Sinovate创建的X25x哈希算法的工作证明（挖掘）得到保护，该算法是一种ASIC、FPGA、Quantum-Resistant算法，可确保进一步分散的网络。

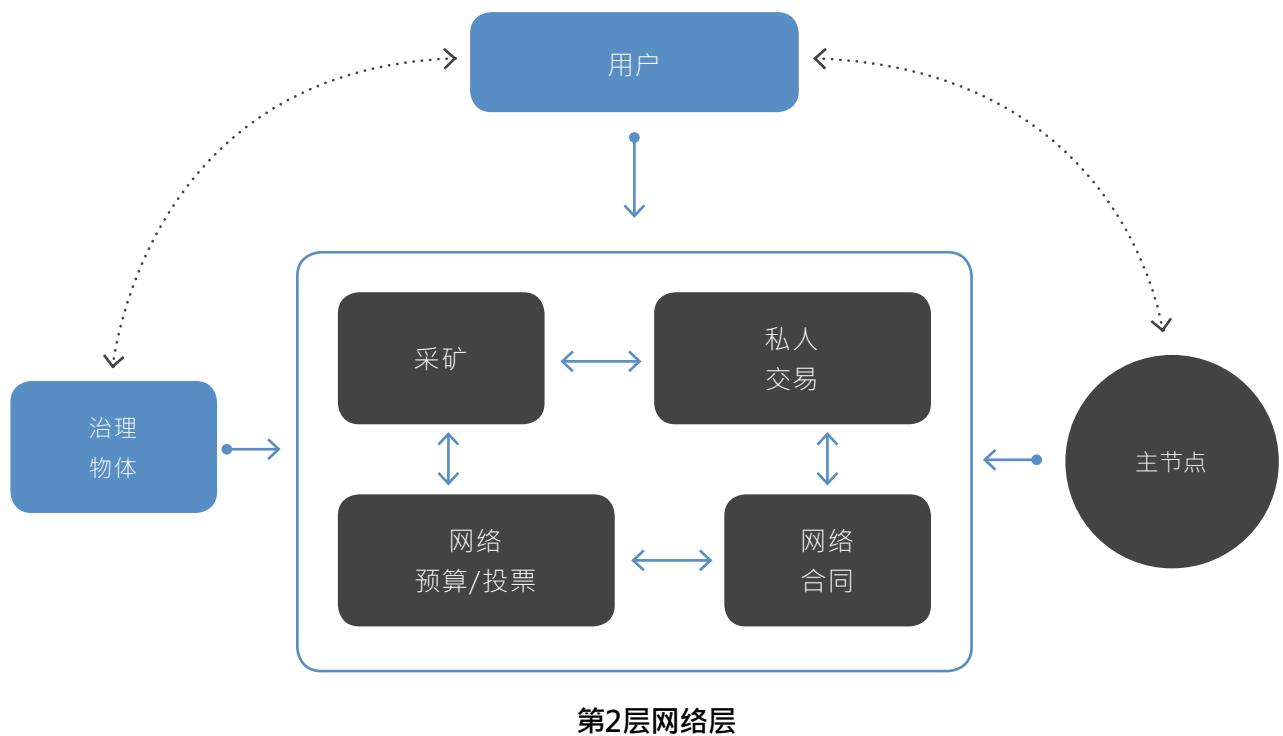
4.2. 问题

比特币的后继者面临的主要问题是缺乏隐私、可扩展性或激励性，以帮助分散网络。大多数项目似乎专注于这些问题中的一个，但缺乏包含另一个问题的方向或动机。Umbru的目标是关注项目中出现的所有负面方面，并为所有人提供快速、安全和稳定的解决方案。

最初的功能已经被精心挑选，以创建一个稳定、快速和安全的基础，为乌姆鲁建立。Dash的Master-Node和治理系统是我们分散、自筹资金和安全的区块链最理想的基础，提供了防止网络和区块链攻击的功能。在此基础上，我们可以着手实现缺少的特性——隐私和可伸缩性。

Blockchain Reorganization Events – 区块链重组的风险通常通过在交易被安全接受为付款之前要求多次“确认”来解决。这种间接安全性是有效的，但代价是时间和用户体验。链锁是这个问题的解决方案。

Project Funding – 分散化治理，是翁布鲁如何解决加密货币中两个重要问题的选择：治理和融资。分散式项目中的治理是困难的，因为根据定义，没有中央机构来为项目做决策。在翁布鲁，这样的决定是由网络作出的，也就是说，由masternode的所有者作出的。



4.3. 解决

区块链本身是第一层，第二层建立在它之上。有了这个第二层，Umbru可以以一种不信任和分散的方式提供创新功能。MasterNode目前用于为治理和财政系统供电，在不久的将来，它们将用于为本白皮书中概述的功能供电，等等。为将来的特性提供真正的分散层，masternode也可以通过块奖励来补偿它们在帮助分散网络方面的贡献。

这也允许翁布鲁在不久的将来创建私人、匿名和不信任的交易，为用户和企业提供应得和需要的隐私和安全。网络合同也可以通过这一第2层来实现，这提供了比特币许多继承者都没有看到的另一种权力下放来源。

分散化治理，是翁布鲁如何解决加密货币中两个重要问题的选择：治理和融资。分散式项目中的治理是困难的，因为根据定义，没有中央机构来为项目做决策。在翁布鲁，这样的决定是由网络作出的，也就是说，由masternode的所有者作出的。

5. 分布模型

5.1. 工作证明(采矿)

在Umbru等加密货币背景下的挖掘是指寻找密码难题解决方案的过程·作为在区块链上保护区块的一种方法。采矿过程创建新的货币代币作为对矿工的奖励。可以在一系列硬件上进行挖掘。Umbru实现了一种称为X25X的算法·矿工必须解决该算法才能获得奖励。可用于挖掘的最简单和最通用的硬件是每台计算机中的通用CPU·一个CPU被设计成多功能的·但是提供的效率比一个GPU要低·后者被设计成快速并行计算数百万个向量。虽然与加密技术相关的特定CPU指令增强(如AES或AVX)可以提供相当大的提升·但由于GPU的多个管道能够处理与加密货币挖掘相关的可预测重复计算·因此其性能显著提高。

5.2. 主节点

不过·翁布鲁的运作方式与比特币略有不同·因为它有两层网络。第二层由masternodes(支持网络功能)和分散的治理和预算系统提供支持。由于第二层非常重要·当矿工发现新块时·masternode也会得到奖励。明细见下表。masternode系统被称为服务证明·因为masternode向网络提供关键的服务。

阻止奖励分解

月份	矿工	主节点	预算
1	70%	20%	10%
2	65%	25%	10%
3	60%	30%	10%
4	57.5%	32.5%	10%
5	55%	35%	10%
6	52.5%	37.5%	10%
7	50%	40%	10%
8	47.5%	42.5%	10%
9	45%	45%	10%

6. 概述

简要概述Umbru区块链和二级网络的当前、计划和未来功能。



分散的



透明度

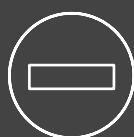


安全

翁布鲁区块链上没有管理机构。社区成员投票决定的项目方向及其反馈/输入。不信任的系统抵抗集中化的尝试。

通过Umbru钱包和治理UI随时可以查看所有投票和提案·进行投票、创建提案并轻松反馈。

我们的第2层通过链锁提供区块链安全·以创建一个抵抗“区块链重新定义攻击”(51%攻击)的环境。



不可逆性

所有匿名、私有、屏蔽或正常的交易都记录在区块链中·并由LLMQ成员(MasterNode持有者)保护·允许在未来进行即时确认。



可扩展

通过umbrascript·可以在umbru网络中集成的私有网络数量是无限的。每次添加都可以运行特定的应用程序或多个功能。



数据

除了使用Umbru的私有网络/应用程序的安全性之外·企业和机构将能够访问企业级的应用程序和/或功能解决方案。



第二章

UMBRU 项目

7. 愿景

7.1. 我们的愿景帮助用户维护基本权利

DDPS(动态、分散、私有和安全)是翁布鲁的愿景。基本权利只是一种基本人权·而不是可选的·而不是私人的基本人权。我们承诺为您提供一个不需要经常担心您的隐私的网络。或者一个更高的管理机构正在控制你或者网络。翁布鲁的目标是在一个安全和安全的环境中提供这一点·这一环境很容易适应和动态地应对出现的问题。如果你相信我们的愿景·那么加入我们的社区委员会·让你对翁布鲁应该领导什么/在哪里/如何领导发表意见！

动态

分散的

私人

保护

隐私

交易隐私不仅对于用户·而且对于希望建立在翁布鲁网络上的企业和机构来说也是必要的。

使用zk starks和我们的第二层(特别是masternodes)·我们的目标是提供一个完全不信任的分散支付和交易系统。

如果您的财务交易和付款历史被捆绑并出售给第三方·那么您必须担心的日子已经一去不复返了。

长期而言·我们的目标是将这些私人或匿名交易包括在即时零确认交易中。消除了在网络上等待几分钟再确认的可能。

企业、机构、投资者、矿工和最终用户都从中受益。

分散的

翁布鲁网络没有管理机构。矿工通过他们的工作证明来保护网络·主节点执行分散的共识。

我们的masternode和治理对象的第2层网络层进一步强化了这一思想。该网络层还允许完全分散的自筹资金网络预算。

该预算可供所有人查阅·任何希望为改进和调整Umbru提供的服务获得资金的人都可以提出建议。

这些提案随后由masternode持有者投票表决·以确保达成公平、无篡改的共识。

8. Umbru 实验室

发展基金提案



Umbru实验室是一个网络资助计划·为核心开发人员提供预算·以维持和改善Umbru的幼年期。其主要目的是为研究和开发提供资金·支付开发成本·并通过社交媒体和营销提高知名度。

完全透明



网络提供的资金是完全透明的·任何人都可以在其希望的任何阶段进行审计。Umbru核心团队还将发布月度财务报表·以确保每个人都了解支出和进度。

开源



我们相信开源是未来。利用翁布鲁实验室提供的资金开发的所有工具、软件和程序都将是开放源代码和可审计的。这也符合我们完全透明的理念·并且允许其他用户/开发人员捕获任何代码中的任何潜在风险/错误。

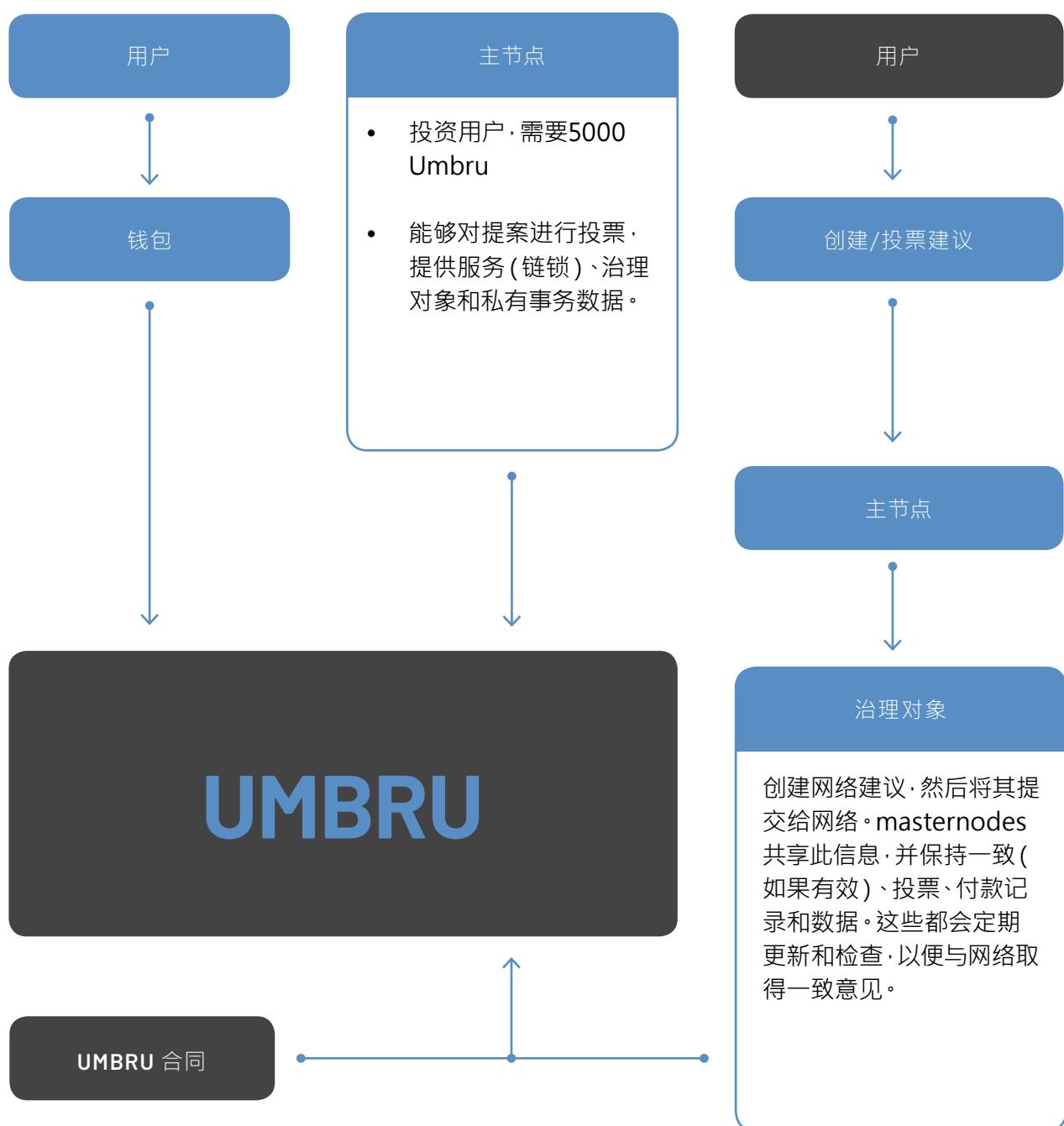
反馈/支持



我们将始终欢迎反馈和支持。我们认识到·事情从来没有错误的处理方式·因此我们感谢并请求您的反馈和支持。翁布鲁和核心开发者一样是你的·所以请大声说出来·发表你的意见！

9. 协议体系结构

下面详细介绍用户和网络交互。Umbru是一个1层，下面添加了以下2层协议。随着开发的继续，协议和层不断更新、增加或减少。



10. 路线图



2020年第一季度

- tumbru zk stark在testnet上实现了不信任的事务。

2020年第一季度

- 多资产/货币Umbru钱包，带有更新的用户界面/用户体验。
- 支付网关与新钱包、随发布的开发者工具包集成。

2020年第二季度

- 提案/治理Web UI和钱包界面，供用户/开发人员交互和创建。

2020年第二季度

- UmbruScript 多/跨链分散合同。

2020年第3季度

进一步的开发(添加/删除)将基于对生成的提案的反馈和投票。

社区领导的发展/倡议也可以通过这种方式进行支付/投票。



第三章

团队和参考资料

11. 管理团队

创始人



Ryan Lorz, 创始人和开发者

最初是对挖掘比特币的好奇心·从好奇心转变为爱好·现在变成了乌姆布。Ryan的技术和创业背景有助于开发、维护和营销Umbru项目伞。当你把他从键盘和要完成的大量任务列表中撬出来时·Ryan喜欢大笑和社交。

社区成员



Bryan Evans, 社交媒体/支持

12. 工具书类

- [1] <https://sinovate.io/whitepaperv2light.pdf> - X25X Algorithm
- [2] https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof - zk-STARKS
- [3] <https://en.bitcoin.it/wiki/Mining> - Bitcoin Mining
- [4] <https://docs.dash.org> - Dash background
- [5] <https://docs.umbru.io> - Umbru documentation
- [6] <https://umbru.io/> - Umbru website
- [7] <https://pool.umbru.io/> - Official mining pool

13. 法律说明

本白皮书及其详细信息仅供一般信息参考。

任何人·包括但不限于任何与

UMBRU保证此信息的准确性、完整性或有用性。本白皮书不是任何类型的合同·包括投资合同。

UMBRU将从第一区完全发挥作用·您选择使用UMBRU网络不会与任何人产生法律关系。

翁布鲁是一个分散的加密货币网络·而不是一个公司。因此·您不应期望与任何其他用户的努力有关的任何利润、股息、收益或任何形式的价格增值·或

翁布鲁的贡献者。

了解虚拟货币(如UMBRU)需要高级的技术知识。虚拟货币背后的技术是新颖的·而且还没有经过测试。虚拟货币通常用非常专业的技术语言来描述·这需要对应用密码学和计算机科学有一个全面的了解·以便认识到固有的风险。

请自担风险使用翁布鲁。

20