Whitecoin 技术白皮书

A Decentralized Blockchain For Multi-chain Ecosystem

目 录

一、内容摘要 4

1.1 名词解释 4

1.2 文档声明 5

1.3 免责声明 5

二、项目背景 7

2.1 区块链行业的发展趋势 7

2.2 Whitecoin 的历史 7

三、Whitecoin 的特性 10

3.1 跨链互通互联 10

3.2 百分百准备金 10

3.3 高效 10

3.4 智能合约 11

3.5 手续费灵活性 13

四、随机多资产权益存储共识机制（RPOS） 14

4.1 参与者 14

4.2 Whitecoin 挖矿和存储机制 15

4.3 Whitecoin 随机多资产权益存储共识 RPOS 竞争算法 16

4.4 激励机制 18

4.5 RPOS 共识机制的安全性 20

五、社区治理 22
5.1 Wallfacer/面壁者的选出 22
5.2 Wallfacer/面壁者的权利和义务 22
5.3 Wallfacer/面壁者的链上更替流程 23
5.4 Wallfacer/面壁者的惩罚机制 24
5.5 社区治理方式的优势 24
六、跨链 25
6.1 跨链的实现 25
6.1.1 Multi Tunnel Blockchain Communication Protocol（MTBCP） 25
6.1.2 Whitecoin Axis 25
6.1.3 Whitecoin Wallet 25
6.1.4 智能合约 26
6.1.5 闪电网络 29
6.2 跨链的操作流程 29
6.2.1 初始化流程 29
6.2.2 账户的创建 30
6.2.3 跨链充值流程 31
6.2.4 跨链提现流程 33
6.3 侧链资产的安全性 34
6.3.1 资金动态平衡策略 34
6.3.2 资金动态平衡期限 35
七、技术要点及创新 36

7.1 合约和虚拟机 36

7.2 可共识的随机数发生器 38

7.3 事件及回调 39

7.4 本地查询接口 40

7.5 资产区块链接入模型 40

八、项目的开发规划 41

8.1 面壁计划（Wallfacer Project） 41

8.2 威慑计划（Threatening Project） 41

8.3 阶梯计划（Staircase Project） 41

8.4 黑域计划（Black domain Project） 41

九、结论（Conclusion） 42

十、References 43

一、内容摘要

Whitecoin 是一条通过创新的 Multi Tunnel Blockchain Communication Protocal (MTBCP)协议实现区块链间价值互通互联的公有链。Whitecoin 生态系统通过使用 Random Proof of Stake（RPOS）共识、Whitecoin Axis、Whitecoin Wallet、去中心化矿池、智能合约平台构建成一个跨链的区块链生态综合体。

Whitecoin 具有很多高性能的特性:

- **区块链资产管理**

实现了现有区块链（BTC、LTC、BCH、ETH、EOS、ERC20、OMNI 等）之间的跨链流通，以及本链的多资产管理。

- **图灵完备的智能合约**

支持通过图灵完备的智能合约实现各种复杂的数字资产业务，例如：链上 OTC、资产通证化等，通过机制设计，实现复杂的金融衍生品合约，比如借贷合约，期货合约等。

- **底层虚拟机**

Whitecoin 提供的区块链底层虚拟机、支持多种开发语言的 SDK 和 RPC 接口，为构造多资产分布式商业应用生态打造基础。

Whitecoin 的主链资产称为 XWC，XWC 的持有者可以通过共建生态，来享受生态服务、分享生态收益，其他公有链比如 BTC、LTC、BCH、ETH、EOS、ERC20、OMNI 等也可以通过 Multi Tunnel Blockchain Communication Protocal（MTBCP）协议进入 Whitecoin 生态，打通区块链间的壁垒，创造互通互联的全新区块链世界。

1.1 名词解释

Whitecoin：Whitecoin 中文名白币（简称 XWC）是一个拥有四年历史的去中心化全球区块链。

XWC：XWC 指 Whitecoin 链上的资产代币。

MTBCP（Multi Tunnel Blockchain Communication Protocal）协议：是 Whitecoin 创新的用于支持跨链信息传输的点对点的通信协议。

WAMP(Whitecoin Anchored Multi-properties) ：指 Whitecoin 上对应锚定的其他资产链数字资产。例如：WBTC 指 Whitecoin 上对应锚定的比特币资产。

Miner ：指 Whitecoin 参与记账权争夺的群体。

1.2 文档声明

本文为了阐述方便，使用比特币 BTC、莱特币 LTC 进行举例，并不代表本项目只实现 BTC、LTC 这两个链的跨链。本项目支持市面上以及未来绝大多数数字资产的跨链流通。

1.3 免责声明

本 Whitecoin 技术白皮书仅供参考。我们不保证本白皮书的准确性或结论，本白皮书按事实提供。我们不作出明确的声明和保证，明示，暗示，法定或其他方式，包括但不限于：

- 适销性，特定目的的适用性，适用性，使用;
- 本白皮书的内容没有错误;
- 此类内容不会侵犯第三方权利。

我们及其关联公司对使用，提及或依赖本白皮书或本文包含的任何内容不构成任何形式的损害赔偿责任，即使被告知有可能发生这种损害。在任何情况下，将不会阻止任何人或其附属机构对任何直接或间接的任何损害，损失，责任，成本或费用负责，后果性，补偿性，偶然性，实际性，示范性，惩罚性或特殊性使用，参考或依赖本白皮书或本文包含的任何内容，包括但不限于任何业务损失，收入，利润，数据，使用，商誉或其他无形资产损失。

二、项目背景

2.1 区块链行业的发展趋势

2008 年，中本聪发布了比特币的创世白皮书《比特币：一种点对点的电子现金系统》，将区块链带入了公众的视野。自那之后，越来越多的开发者，加入到了开发和推广区块链的行列，不断创新区块链技术，支持更加广泛的应用场景。在比特币诞生的这 10 年时间里，行业从业者不断的探索区块链的更多技术方案，更多的应用场景。区块链也经历了从 1.0 阶段的点对点支付到 2.0 阶段的智能合约，并且向 3.0 阶段演进。

区块链 2.0 时代，以太坊的发展带来了区块链生态的极大丰富，产生了很多应用方向各异，价值突出的公链项目。然而公链生态的丰富，也带来了新的问题。目前主流的区块链之间信息和价值无法自由流通，客观上形成了一个个的区块链孤岛，极大地限制了区块链的应用价值。相比互联网价值的产生的网络效应，区块链公链的隔离性，极大的制约了区块链的网络价值。因此，区块链的互联互操性将是区块链价值提升的重要解决方向，而跨链技术就是实现区块链价值互联的关键。

大量的区块链的先行者在探索这条路，某些区块链试图通过公证人机制、侧链（中继）、哈希锁定、分布式私钥控制等不同的路径来解决跨链问题。Whitecoin 将打造一条公有链，能以去信任的方式打通不同链之间的价值互通互联，整合现有的区块链资源，打造全新的区块链世界。

2.2 Whitecoin 的历史

Whitecoin 产生于 2014 年 4 月份，是一个超过 5 年历史的区块链数字资产。Whitecoin 至今已经经历了两个历史阶段，即将进入第三阶段。

2.2.1 第一阶段：2014 年 4 月-2017 年 4 月 POW 阶段

2014 年 Whitecoin 创世区块诞生，在这一阶段采用 POW 机制运行。在这一阶段项目建立了分布式开发和运营机制，开发团队主要来自欧洲。项目代币 XWC 也成功登陆了 Bittrex、Poloniex、Cryptopia 等全球知名的交易所，成功的获取了全球数字货币投资者对项目的关注。

2.2.2 第二阶段：2017 年 4 月-2019 年 8 月 POS3.0 阶段

随着区块链技术的不断革新，Whitecoin 开发团队于 2016 年筹备对项目进行全面的升级。2017 年 4 月，Whitecoin 完成了由 POW 机制到 POS3.0 的全新升级。升级后的 Whitecoin 团队依托去中心化的社区治理机制，成功推出了 Whitenode 矿机、Whitecoin 硬件钱包、Whitecoin 区块链手机、XWCDice、XWCPoker、XWCMall 等生态应用。项目代币成功上线了 ZB.COM、XT.COM 等 20 多家行业头部交易所。同时 XWC 也成为 Weiss Ratings 评级的首批 78 个币种之一。

2.2.3 第三阶段：2019 年 8 月-未来 RPOS 阶段

面对区块链行业日新月异的发展速度，Whitecoin 原有的技术架构和社区开发人员组织形式已经无法跟上区块链的发展新形势。2018 年下半年，社区开始酝酿 Whitecoin 的再次升级。

经过近一年的准备，Whitecoin 选择了从区块链基础层面解决行业痛点问题，跨链成为项目的最终方向。同时，为更好的创造 Whitecoin 公链的价值，社区核心开发人员也将从原来的兼职模式转变为全职开发模式。

全新的 Whitecoin 项目将整合社区原有的开发优势、生态优势、社区优势、伙伴优势开启项目的新纪元。

三、Whitecoin 的特性

3.1 跨链互通互联

创新的 Multi Tunnel Blockchain Communication Protocal(MTBCP)协议率先实现了区块链间价值互通互联。跨链功能的实现，对当前的区块链领域有着重大的意义：

- 实现了区块链间的价值互通互联。
- 打通了独立区块链间的壁垒，为构建区块链世界互通生态提供基础。
- 让现有区块链实现更好的扩展和价值共享。
- 帮助现有互联网业务的基础设施对接区块链。

3.2 百分百准备金

为了确保生态系统的稳定和安全，Whitecoin 的准备金比率为百分百，每个 WAMP 都有一个真实的原链资产（如 BTC、ETH）存储在原链上由 RPOS 共识管理的冷热多重签名地址里。这确保 Whitecoin 的所有资产都不会凭空增加或销毁，每一个资产的增加或减少都一一对应着用户在原链上资产的充值或提现。

3.3 高效

依照 RPOS 共识，Whitecoin 主链每 6 秒产出一个块，相对于 BTC 每 10 分钟一个块和 LTC 每 2.5 分钟一个块，交易确认速度有了显著的提升。在 Whitecoin 主链上进行 BTC 或 LTC 资产转移或者交易时的性能分别约为 BTC 主链的 100 倍，LTC 的 25 倍。

Whitecoin 的理论 TPS(每秒处理交易数)值达到 1 万,足以承载多条链上的高负荷交易。

具体对比如下图所示：

区块链	产块间隔	区块大小	理论 TPS
XWC	6 秒	20M	10000

BTC	10 分钟	4M	28
ETH	17 秒	无上限（800 万 gas）	22
EOS	1.5 秒	无上限	百万
NEO	20 秒	无上限	1000

Whitecoin 在产块速度、区块大小和理论 TPS 上，其性能较 BTC、LTC、ETH、NEO 等链都有明显的提升，Whitecoin 的产块间隔为 6 秒，理论 TPS 为 1 万，足以应付高频率、高容量的业务需求。

EOS 的超级节点要求服务器之间具有非常稳定的网络连接，并且其对服务器的性能要求很高。EOS 的产块机制是 21 个超级节点按顺序产块，规律明显，存在被攻击的风险，诸如 DNS 欺诈、DDOS 等。

相比之下，Whitecoin 链对服务器和网络的性能要求则没有那么高，适应性更强，更容易接入其他链上的资源。相对于 EOS 网络容易被攻击，Whitecoin 的产块是从所有的 Miner 中随机选出的。这样的网络特性意味着 Whitecoin 的产块节点具备很大的不确定性，很难在网络中被发现。Whitecoin 在机制上最大程度地规避网络攻击的风险，并且部分节点被攻击完全不会影响全网的稳定。

3.4 智能合约

Whitecoin 用户通过使用图灵完备的智能合约，可以灵活扩展定制复杂的业务逻辑，以及复杂金融合约等。

在不对原链代码修改的基础上，Whitecoin 可以实现 Token 合约，交易合约，锁仓合约，各种 DAPP 合约等有限制可控地动态扩展功能。

- **有限制可控**

遵循智能合约的标准,调用预定义的函数库进行程序开发。

- **动态扩展**

动态扩展指的是不需要对原链底层代码做修改，也不用进行硬分叉。

当业务环境发生改变的时候，可以非常方便的通过对智能合约灵活的修改，对业务需求进行匹配。

例如，未来挂单交易逻辑发生改变，或者要使用其他挂单合约逻辑时，将交易逻辑修改为每笔成交最小单位为 100 个代币，或者设置限时交易等情况，只需要在新的交易中修改智能合约即可。

- Native API

Whitecoin 链上每次智能合约调用执行时，都会先初始化一个独立的轻量级执行环境，在链上查找到合约字节码，然后执行合约字节码，执行中可以通过 Native API 来访问链上数据。Whitecoin 提供常用操作的 Native API 使得智能合约在绝大部分场景下可以有较好的性能。

- **独立状态存储区 Storage**

每个智能合约有各自的独立状态存储区，称作 Storage。合约交易的执行导致某个智能合约的状态存储区发生数据变化时（Storage 改变），不会保留所有历史的 Storage 的全量备份，而是只保存 Storage 的当前状态和 Storage 每次变化的变化量。比如：某个包含有 1、2、3 三个数字的数组的 Storage，当它变化为 1、2、3、4 四个数字的数组，然后又变化为 1、2 两个数字的数组时，只会记录当前值 1、2 数组以及两次的变化量（增加 4，移除后两个位置的数字 3、4）。

通过这样的设置，用户想要得到智能合约的执行结果时，可以很轻易地获取 Storage 的当前值，而无需读取所有的数据，这样大大降低用户的工作量，也减少了节点的数据存储要

求，节省了系统资源，提升了系统的处理效率，还方便按 Storage 的实际变化按需计算 Gas。同时，用户也可以通过历史变化量还原或者回滚得到 Storage 的每次历史的值。

3.5 手续费灵活性

Whitecoin 链上的手续费可以是 XWC,也支持多种 WAMP 支付，让用户拥有 XWC 或者 WAMP 任意一种时都可以直接进行交易，而不需要关心手续费的问题。

Whitecoin 上手续费兑换比率并不是固定比例，而是由市场动态决定。随着 Whitecoin 资产价格的波动，交易所需的 WAMP 也会上下波动。

四、随机多资产权益存储共识机制（RPOS）

Whitecoin 使用随机多资产权益存储共识 RPOS(Random Proof of Stake)作为去中心化共识算法。

随机多资产权益存储共识 RPOS 是 Whitecoin 资产跨链交易所的共识算法，为 Whitecoin 进行跨链交易定义了参与者，激励制度以及社区运营模式。

4.1 参与者

4.1.1 社区成员类型

去中心化共识算法定义了 Whitecoin 社区成员包括以下四类：

- Citizen:普通用户
- Miner:矿工
- Wallfacer:面壁者
- Swordholder:执剑人

4.1.2 各角色之间的关系:

按照参与 Whitecoin 社区的层次，Whitecoin 的参与者之间关系：

Citizen/普通用户可通过购买或挖矿获取一定数量的 XWC，通过自己提供或者其他用户支持提供链上资产存储成 Miner/矿工。

Miner/矿工通过提供责任保证金和节点投票来升级成为 Wallfacer/面壁者。

Wallfacer/面壁者中会选出一部分的关键角色成为 Swordholder/执剑人。

4.1.3 各角色之间的责任和权力

Citizen/普通用户：Whitecoin 链上的所有用户以及与 Whitecoin 互通的其他链上的所有用户。普通用户可以通过花费一笔 XWC 代币注册，也可选择不注册。

Miner/矿工：是 Whitecoin 链上的生产者和社区治理者，负责记账和产块。同时 Miner/矿工是链上的去中心化矿池。

Wallfacer/面壁者：是 Whitecoin 生态中的资产管理者和社区治理者。Wallfacer/面壁者负责共识管理存储在 Whitecoin 链上的资产，并通过 Wallfacer/面壁者共识最终完成各主链之间的资产流通。

Swordholder/执剑人：是 Whitecoin 社区中的核心角色，Swordholder/执剑人拥有 Wallfacer/面壁者的所有职能。同时，他们还是系统喂价的执行者。

4.2 Whitecoin 挖矿和存储机制

Whitecoin 社区提供不同的模式为社区参与者分享 Whitecoin 挖矿奖励。无论是作为 Miner/矿工还是 Citizen 普通用户，只要通过存储资产到 Whitecoin 网络，都可以获得独立出块的机会或者挖矿奖励。

随机多资产权益存储共识 RPOS(Random Proof of Stake)为 Whitecoin 社区参与者获得挖矿收益提供具有天然优势性的保障和维护。

Miner/矿工通过存储资产得到独立出块的机会并获得奖励。

Miner/矿工或 Citizen 普通用户也可以通过存储资产来分享挖矿奖励。

Wallfacer/面壁者和 Swordholder/执剑人可以通过出块来得到 Whitecoin 奖励，同时按照其他参与者(Miner /Citizen)预置的存储金权重来对获得收益进行分配。随机多资产权益存储共识 RPOS(Random Proof of Stake)为这个权益分配过程提供实现机制。

Whitecoin 存储机制的优势：

- 存储挖矿和权益奖励是由全网节点共同验证，自动实时的对节点收益进行分配。接受存储资产的 Miner/矿工在获得出块奖励之后自动奖励，不会像中心化的矿池一

样，存在很多不确定因素。

- POS 矿池需要用户把存储资产实际转账给挖矿节点，而 Whitecoin 链上只是存储资产，私钥仍然由自己保管，无需转账给 Whitecoin 的 Miner/矿工，不会有安全问题，用户随时可以撤回存储资产。

4.3 Whitecoin 随机多资产权益存储共识 RPOS 竞争算法

随机多资产权益存储共识 RPOS 定义了 Whitecoin 节点出块和权益分配的详细算法和机制。

节点记账权基本条件:

Miner/矿工通过竞争来争夺记账权的基本条件是存储资产，包含 XWC 和所有 WAMP。存储金数量越多，在争夺记账权算法中占有的权重越大。

节点出块机制:

随机多资产权益存储共识 RPOS 依靠链上随机数在每一轮共识开始时依据资金权重随机合作出块。

Miner/矿工产块规则如下:

每当区块数是 25 的整数倍时，进入启动一次流程:喂价，选举，产生区块，确认。

- **喂价**

喂价是指由 Swordholder/执剑人根据现行交易所的实时价计算出所有 WAMP：XWC 的汇兑比例，然后分别进行喂价。喂价的作用是通过所有 Swordholder/执剑人的参与提供 Miner/矿工竞争出块的权重。

喂价的最终结果值为所有 Swordholder/执剑人喂价去掉最高值和最低值，剩下的取平均数。喂价结果的输出会影响 Miner/矿工竞争出块时的权重。

- **产生区块**

RPOS 共识算法使得 Whitecoin 准确地每 6 秒生成一个区块，并且在任何时间点只有一个被授权的生产者来生成区块。如果一个区块在规定时间之内未被生产出来则这个区块的生产者将会被跳过，由排序的下一个 Miner/矿工账户进行替补出块。当一个或多个 Miner/矿工没有出块时，区块链上将有 10 秒或以上的延迟。

- **确认**

通常 Whitecoin 链会有 100%的 Miner/矿工账户参与，一个 Whitecoin 原生交易从广播开始后平均 3 秒就可以 99.9%被认为是确认的了。

为了避免特殊情况，例如：软件出现 bug、网络拥塞，或一个恶意的 Miner/矿工账户制造了两个或更多的分叉，为了确保一个交易绝对是不可逆的，一个节点需要等待 17 个块的确认。基于 Whitecoin 的软件配置，在一般情况下这需要平均 85 秒的时间。

默认情况下，所有的节点将认为当一轮出块的 25 个生产者中有 17 个生产者给出确认后这一区块就是不可逆的了，并且不管长度如何都不会切换到没有这一区块的分叉。通常情况下在 100%参与率的状态下推荐用户延迟 6 个区块。

RPOS 竞争机制的优势在于：

- **大大节省了系统资源，减少了能源的浪费**

与 POW 算法相比，Whitecoin 链上由被随机选中的 Miner/矿工按顺序合作出块，因此 Whitecoin 链上的 Miner/矿工只需要记账，无需耗费精力去找哈希值。

- **避免分叉**

Whitecoin 链上的 Miner/矿工是由合作而非竞争的方式进行出块。

- **节点选择的随机性增加了 Whitecoin 生态系统的安全**

Whitecoin 链上的 Miner/矿工的选出具有随机性，且处于不断地更替变化之中，不仅如

此，即使两轮的 Miner/矿工一样，出块顺序也会不一样。使得 XWC 链上出块的 Miner/矿工节点很难被攻击者找到，极大地保障了 Whitecoin 生态系统的安全性。

- 增加了 Whitecoin 参与用户的资产安全性。

与 POS 和 DPOS 机制相比，Whitecoin 采取的是存储机制，私钥仍然掌握在用户自己手上，可随时收回，极大地保障了资产的安全性和挖矿的灵活性。用户可将资产存储给 Miner/矿工参与挖矿奖励，亦可以随时收回。

4.4 激励机制

Citizen/普通用户

作为 Whitecoin 的 Citizen/普通用户，可以获得合约提现手续费（侧链资产）奖励。通常情况下，每 10W 块链上进行一次奖励。奖励依据持有的 XWC 数量进行分配。

Citizen/普通用户花费一定的手续费可以注册成为 Miner/矿工，经过 1 天的竞价公示期，即可成为一个合格的 Miner。

Miner/矿工

用户还可以通过成为 Miner/矿工或者通过存储资产获得出块奖励。

在 RPOS 共识机制中用户通过成为 Miner/矿工或者通过存储资产获得出块奖励。

用户花费一定数量的 XWC 注册成为 Miner/矿工，投入资产进行存储，并在社区内吸引其他用户参与存储，最终依靠 RPOS 共识竞争记账权，成为 Miner/矿工，参与出块，获得区块奖励。

Miner/矿工（含支持用户）享有出块奖励和合约提现交易手续费中的相应比例奖励。

具体公式如下：

Miner/矿工支持者享有的存储收益按存储资产的权重平分。

为保证 Miner/矿工能长期在线打包，不仅需要激励也需要引入惩罚措施，当一个 Miner/矿工连续 Miss 超过 5 块时，链上共识降低此 Miner/矿工的参与率,从而降低该节点被选举为出块节点的概率。

Wallfacer/面壁人& Swordholders/持剑人

Wallfacer/面壁人和 Swordholders/持剑人平分 20%区块奖励以及获得合约提现交易手续费中的 20%奖励。

基金会

基金会获取 30%区块奖励。

Whitecoin 的三种激励：

- 区块奖励
- 区块交易手续费（包括普通交易手续费和合约交易手续费），种类为 XWC
- 区块中合约提现手续费，种类为多种资产 WAMP（WBTC、WLTC、XWC 等），手续费万分之一（由 Wallfacer/面壁人共识决定和修改）。Wallfacer/面壁人获得合约提现手续费总额的 20%，剩余部分由所有用户根据 XWC 持币量进行平分。

用户权益对比表

	Citizen/普通用户	*Miner /矿工*	Wallfacer /面壁者	Swordholder /执剑人	备注
Wallfacer 注册费	无	无	无	无	链上直接销毁
普通交易手续费	无	有	有	无	手续费种类 XWC
区块奖励	无	有	有	有	固定 XWC 奖励
合约交易手续费	无	有	有	无	手续费种类 XWC
合约提现交易手续费(侧链资产)	有	有	有	有	手续费种类为 XWC 和 WAMP (XWC/WLTC/WBTC 等)

4.5 RPOS 共识机制的安全性

RPOS 拥有极高的系统安全性，足以防范各种恶意攻击和突发情况，确保网络和资产安全：

- **Miner/矿工只要有一个能正常工作就不会影响 XWC 网络出块**

Miner/矿工是维护系统稳定的重要角色，随机出现的不工作 Miner/矿工中，只要有一个 Miner/矿工上线，它就能连续出 25 个块。在这种极端异常情况下，依靠链上的激励还是可以过渡到下一轮调整。

在正常情况下如果一个 Miner/矿工每连续 5 次不出块，那么 RPOS 共识算法将会降低该 Miner/矿工的参与率，参与率会以系数方式降低 Miner/矿工的存储资产数量，其计算公式为 Miner/矿工最终存储 XWC 金额 = 用户存储 XWC 金额 *参与率（0-100%）。

因此，随着 XWC 网络的运行，最终所有的 Miner/矿工都会是优质的节点。

- **恶意 Miner/矿工在同一时间产出 2 个不同的区块**

当本轮产块结束，为避免双花攻击， Whitecoin 将会根据恶意 Miner/矿工产生的两条链的长度进行自动切换，以长的为准。在这样情况下面，只要保证 17 个块的确认数，就可以避免双花攻击。

- **矿池不超过 51%资产的双花攻击**

假设有矿池占据了链上很多资产，也不能保证每轮都占有超过 50%的产块节点。因此在超过 17 个块的确认数基础上，也很难造成双花攻击。

- **矿池 51%资产的双花攻击**

假设矿池联合占据超过 51%的资产。在这种极端场景下，矿池是有可能造成链上数据回滚问题。但因为矿池的资产不只是链上 XWC 还有很多 WAMP，而 WAMP 的跨链控制权掌

握在 Wallfacer/面壁人手中。矿池联合作恶，那么很有可能面临社区投票被制裁的风险，利益和风险相比完全不占优势。

五、社区治理

为了主链的长远发展和生态建设，区块链必须有一套治理机制。比特币依靠比特币开发者群体及矿工群体来协调更新，但是这个过程很缓慢，且由于二者之间在扩容问题上的矛盾直接导致了比特币的分叉。以太坊在采用硬分叉解决 The DAO 黑客事件后，却分裂成了 ETH 和 ETC。

鉴于历史上主流数字货币的社区经验，设计更优的社区治理方式一直是区块链世界非常关心的问题。Whitecoin 拥有一套设计完善的社区治理机制，Whitecoin 社区的治理者为 Miner/矿工、Wallfacer/面壁者、Swordholders/持剑人。三者通过共识协作管理跨链资产及参与社区规则的制定和修改。

5.1 Wallfacer/面壁者的选出

成为 Wallfacer/面壁者必须存入由基金会设定的最低限度的责任保证金，初始 Wallfacer/面壁者的最低资产存入门槛为 1000 万 XWC。

Wallfacer/面壁者数量为 15 个。

初始的 Wallfacer/面壁者由基金会从持币量最多且拥有达到足够安全标准的环境的用户中甄选出 15 个。

5.2 Wallfacer/面壁者的权利和义务

- Wallfacer/面壁者日常要参与链的管理，包括 Whitecoin 基本参数的共识修改，Whitecoin 上手续费的共识修改。引入新的资产链需追加的保证金数额的共识等。
- Wallfacer/面壁者负责跨链资产的管理。Wallfacer/面壁者通过在资产链上建立冷热多重签名钱包来对跨链资产进行管理，跨链资产的提现也必须在至少获得 2/3 的 Wallfacer/面壁者共识的情况下才能达成。
- Wallfacer/面壁者享有合约提现交易手续费中的相应比例收益和 5%挖矿奖励。

- 在发生意外情况，造成资产丢失后，比如热钱包出现损失时，Wallfacer/面壁者将进行赔付。

5.3 Wallfacer/面壁者的链上更替流程

- **新增 Wallfacer/面壁者提案**：

Wallfacer/面壁者新增由任意一个现有 Wallfacer/面壁者发起新增 Wallfacer/面壁者的候选提案，此候选提案收到不低于 2/3 的现有 Wallfacer/面壁者的签名同意后，转换为新增 Wallfacer/面壁者的正式提案。

新增 Wallfacer/面壁者的正式提案由 Wallfacer/面壁者进行投票，Miner/矿工的投票权重由 Miner/矿工的存储金比例决定，当正式提案收到不低于 2/3 的 Miner/矿工的共识投票后，提案通过。

- **卸任 Wallfacer/面壁者提案**：

卸任 Wallfacer/面壁者由任意一个现有 Wallfacer/面壁者发起卸任 Wallfacer/面壁者的提案。此提案收到不低于 2/3 的现有 Wallfacer/面壁者的签名同意后，提案通过。

- **Wallfacer/面壁者变更要求如下**：

每一次 Wallfacer/面壁者变更请求需要最小间隔 25000 块才能发起。每次 Wallfacer/面壁者变更请求会无条件重置 Wallfacer/面壁者变更请求间隔。

每次变更 Wallfacer/面壁者的数量不能超过当前 Wallfacer/面壁者人数的 1/5。

任意 Wallfacer/面壁者的变更必须在 10000 块后生效。

变更 Wallfacer/面壁者产生的相关变动必须在 10000 块内完成。

新增或废弃 Wallfacer/面壁者提案生效后需要重新创建对应的多重签名钱包，并在 Whitecoin 上广播共识。原有钱包内的资产需要原 Wallfacer/面壁者共识转移到新的多重签

名钱包中。旧的充值地址将在 20000 块后废弃，在废弃前旧地址的充值同样会进行入账，并且旧冷热多重签名钱包的资产在发生变化后会触发往新冷热多重签名钱包的入账。

5.4 Wallfacer/面壁者的惩罚机制

在极端情况下，当系统出现资产损失时，Wallfacer/面壁者缴纳的责任保证金将用于赔付。

5.5 社区治理方式的优势

Wallfacer/面壁者通过共识对资产和社区进行管理，Miner 通过共识来对 Wallfacer/面壁者的更替进行投票，二者利益一致又互相牵制，最大程度上保证了 Whitecoin 的全网络的安全和稳定。

整个 Whitecoin 网络由不超过 15 位 Wallfacer/面壁者优质节点通过共识进行治理，极大程度上保证了决策的效率。

Wallfacer/面壁者的利益和社区的利益是息息相关，Wallfacer/面壁者可以从 Whitecoin 生态中获得持续稳定的收益。同时，在 Whitecoin 链上成为 Wallfacer/面壁者有较高的门槛，必须存入相当多数量资产，在发生资产损失的情况下，Wallfacer/面壁者缴纳的责任保证金将会用于赔付。

六、跨链

6.1 跨链的实现

Whitecoin 率先通过创新的 Multi Tunnel Blockchain Communication Protocal(MTBCP)协议、Whitecoin Axis、Wallet、智能合约等区块链技术成果和创新，实现了区块链间的价值互通互联，为实现打通链间复杂的分布式商业应用打下了基础。

6.1.1 Multi Tunnel Blockchain Communication Protocol（MTBCP）

Multi Tunnel Blockchain Communication Protocol（MTBCP）是 Whitecoin 独创的用于区块链间点对点信息传输的通讯协议。

当用户在 Whitecoin 中创建账户时，Whitecoin 会根据 MTBCP 生成对应的隧道账户，并与 Whitecoin 账户绑定。当发生跨链交易时，通过 MTBCP 将相应数据进行封装打包安全传递。

MTBCP 产生的隧道账户可以帮助 Whitecoin 确认转入资产的唯一对应性。MTBCP 只承认通过隧道账户进行跨链交易的资产，并根据共识发行或销毁对应的 WAMP 资产代币。

6.1.2 Whitecoin Axis

Whitecoin Axis 是 Whitecoin 中实现跨链的重要组成部分。作为一个多资产的去中心化账本，它负责记录、验证、广播跨链数据以及生成和销毁对应的 WAMP 代币，并完成跨链资产的转移。在 Whitecoin Axis 中，通过 Wallfacer/面壁人的共识来保证网络安全性，Whitecoin 账户和对应的隧道账户的绑定关系由 Wallfacer/面壁人在链上进行共识验证，且每一笔资产的跨链交易也要由 Wallfacer/面壁人进行共识验证，保证每一条资产链和 Whitecoin Axis 的状态保持一致。

6.1.3 Whitecoin Wallet

Whitecoin Wallet 是 Whitecoin 的用户端，Whitecoin Wallet 负责生成 Whitecoin 生态

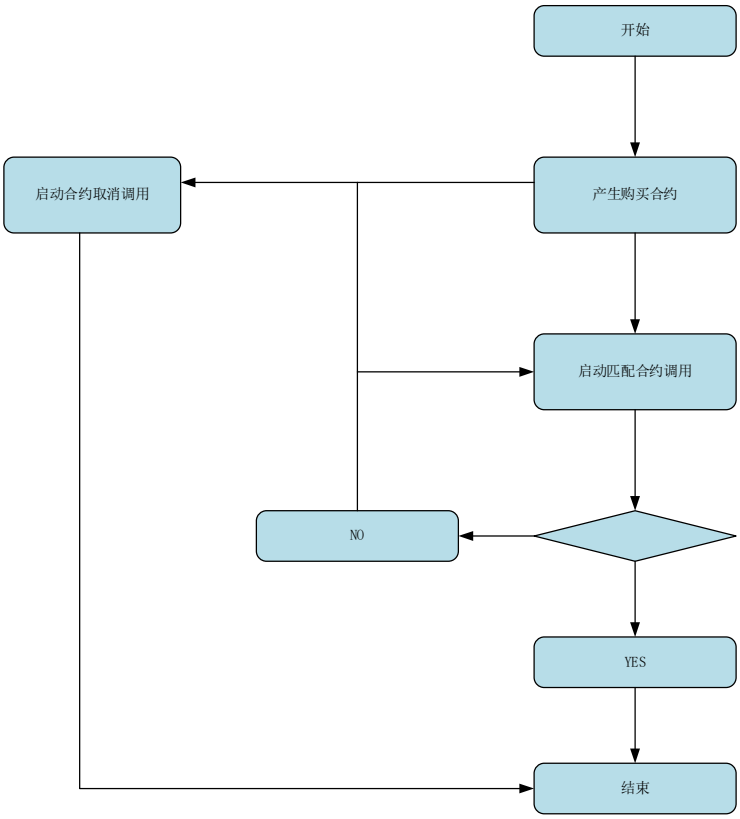
内的相应数据，用户通过 Whitecoin Wallet 实现 Whitecoin 账户注册、成为生态角色、参与生态建设，例如挖矿、跨链交易等，获得相应的生态收益。

6.1.4 智能合约

智能合约可以帮助 Whitecoin 用户实现复杂的跨链交易、资产通证化等，为构建 Whitecoin 生态中跨链分布式商业应用打下基础。

Whitecoin 上的多资产挂单求购等交易行为是通过智能合约来实现的。包括以下几个要点：

- **挂单求购规则**
  - 挂单求购使用智能合约实现，一个挂单求购就是一个新智能合约
  - 挂单求购允许部分匹配，部分成交
  - 挂单求购允许撤单
  - 挂单求购的匹配成交和撤单都是一个智能合约调用的合约交易
  - 求购挂单交易，匹配挂单交易，撤销求购交易都需要手续费。



➢ **智能合约模版**

- 挂单采用智能合约进行，用户可以灵活制定挂单逻辑。一次挂单就是一个新智能合约。
- 使用智能合约做挂单和匹配而不是底层直接实现挂单和匹配，具有可扩展性，可以扩展出更复杂的挂单逻辑，比如一次性成交有折扣，限定每笔部分成交的最小单位数量等。
- 考虑大部分情况大部分挂单逻辑基本一致，为了避免每次都传新智能合约字节码，可以在链上预先将合约字节码注册为合约模板，每个合约模板有一个唯一的链上地址，创建合约的时候可以使用合约模板地址，创建人地址等信息创建新合约，而不用每次传合约字节码，方便用户使用也节省链的存储空间节约花费。
- 充分抽象化模板，大幅度降低合约使用门槛。

- 链上多资产交易不在链上撮合，用户在链上挂买单或者卖单，其他用户主动匹配相应订单进行链上交易。

➢ **手续费规则**

- Whitecoin 上资产转账，创建合约，调用合约，创建合约模板，发起挂单求购交易，撤单挂单求购交易，匹配求购交易等都需要缴纳手续费.
- 用户可以发起手续费承兑挂单，用 XWC 购买 WAMP，用来按价格排列匹配挂单时的手续费兑换。
- 用户发起交易时可以使用 XWC 支付手续费，也可以使用其他资产支付手续费，系统自动匹配相应手续费承兑挂单。

手续费承兑挂单不能随时撤单，需要先发起申请撤单交易，一轮出块后，如果此挂单没有被用户匹配使用，才可以再发起撤单，如果发起申请撤单后一轮出块周期内，此挂单有被用户匹配使用，撤单申请失效，无法被撤单，需要用户重新选择发起申请撤单交易。

➢ **手续费种类**

所有手续费最小收费 0.00001 个系统代币（0.00001 可以由共识修改） 。

	金额	归属
转账手续费	交易基本手续费（XWC）	系统手续费地址
合约创建手续费	交易基本手续费（XWC）	系统手续费地址
合约模板创建手续费	交易基本手续费（XWC）	系统手续费地址
合约调用基本手续费	交易基本手续费（XWC）	系统手续费地址
合约资产充值手续费	合约调用手续费（XWC）	系统手续费地址
合约资产提现手续费	提现的资产的一定比例（多资产）（合约创建人不收取） + 合约调用手续费（XWC）	合约提现的一定比例进入资产奖励池，合约调用手续费进入系统手续费地址
其他	交易基本手续费（XWC）	系统手续费地址

6.1.5 闪电网络

闪电网络是一个用来支持即时，大量的小额支付，可以移除将资金托管权转让给信任的风险第三方的去中心化系统。

Whitecoin 闪电网络极大的拓展了网络的可扩展性，通过创新的 MTBCP 协议、Whitecoin Axis、Wallet、智能合约等区块链技术成果和创新，打通了各种不同区块链之间的壁垒，实现了区块链间的价值互通互联，为实现打通链间复杂的分布式商业应用打下了基础。

Whitecoin 闪电网络的资金被放置在一个双方，多重签名的被称作"通道"的地址当中。为了从通道花费资金，双方必须在余额上达成共识。当前的余额存储为双方签署的从通道地址指出的最新交易。在需要付款的时候，双方从通道地址签署一个新的退出交易。所有旧的退出交易都通过这样做。

闪电网络退出通道时不需要另外一方的许可，任何一方都可以选择单方面关闭通道结束他们的关系。由于各方都有多个多重签名通道在 XWC 网络上。所以各方可以通过该网络向任何其他方发送付款操作。

6.2 跨链的操作流程

6.2.1 初始化流程

- 初始化 Whitecoin，进行初始资产分配，基本参数配置。
- Whitecoin 上 Wallfacer/面壁人通过共识在 BTC、LTC 等资产链上分别创建多重签名账户，并把多重签名账户的地址由所有 Wallfacer/面壁人签名后广播到 Whitecoin 上。
- 每个 Wallfacer/面壁人充值基金会规定的责任保证金，用于维护链的稳定。

6.2.2 账户的创建

为了完成跨链转账，Citizen/普通用户需要在Wallet上创建Whitecoin账户，Wallet会提供隧道账户创立选项，并与Whitecoin账户进行绑定。

这样当资产链（比如 BTC）往多重签名账户充值的时候，Whitecoin 在确认后会将等量的 WAMP，发放到绑定的 Whitecoin 账户上。

在整个 Whitecoin 初始化或者是有新的 Wallfacer/面壁人加入 Whitecoin 网络的时候，需要在资产链(BTC,LTC 等)创建或更新多重签名账户。

账户类型包括：

- **Whitecoin 账户**

用户首先需要创建一个 Whitecoin 账户，用于存储、交易 Whitecoin 上的多种资产，包括 WAMP、XWC 等。

- **隧道账户**

当用户在Whitecoin中创建账户时，Whitecoin会根据隧道协议生成对应的隧道账户，并与Whitecoin账户绑定。隧道账户绑定Whitecoin账户每日免费限额1万笔（1万笔可共识修改），超出限额需Wallfacer/面壁者审核。

- **冷热多重签名账户**

跨链资产将会保存在由 Wallfacer/面壁人共识创建和管理的各个资产链上的冷热多重签名账户里。

6.2.3 跨链充值流程

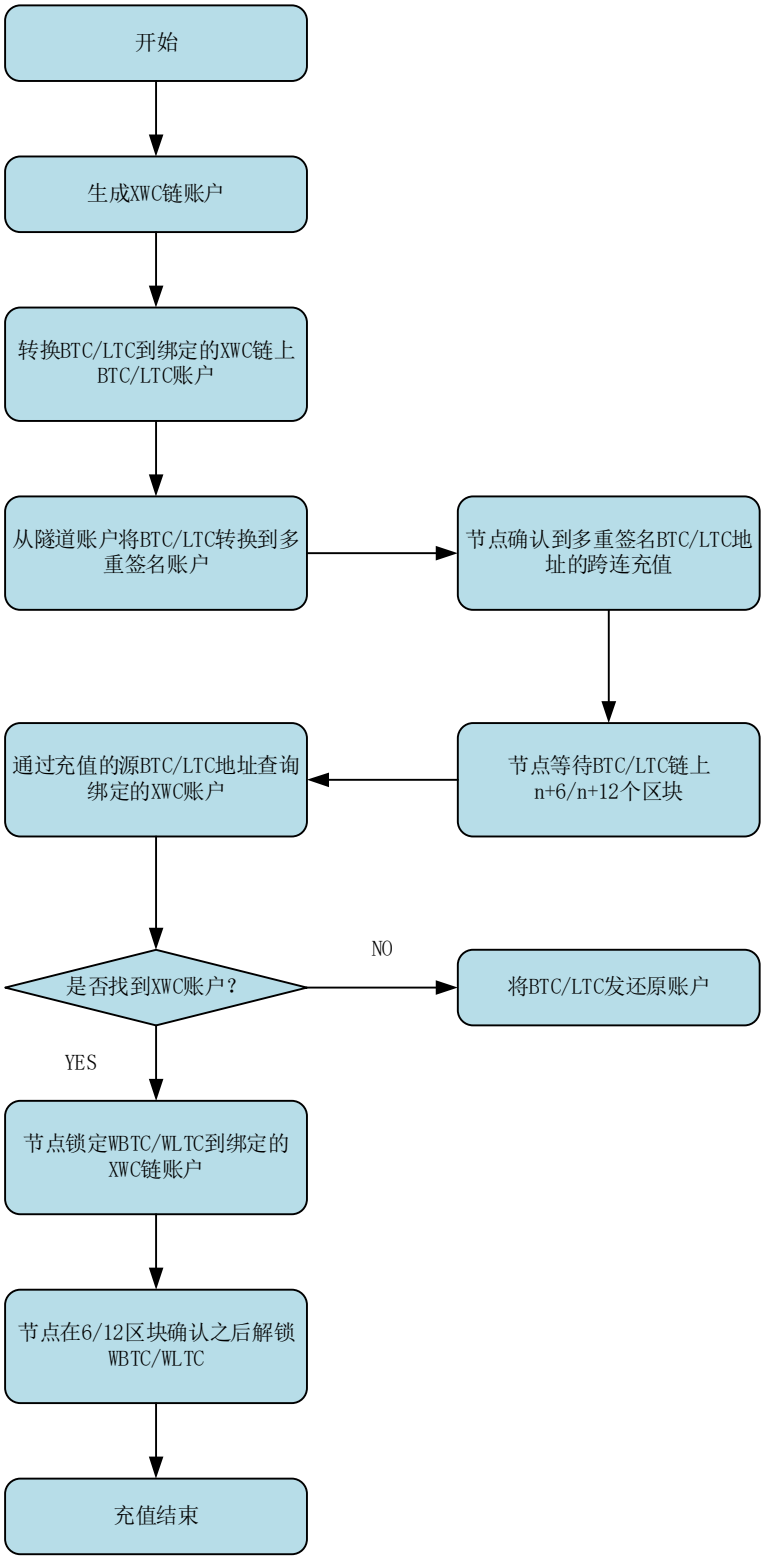
用户在 Whitecoin 中除了有 Whitecoin 账户外，还拥有若干个绑定的隧道账户，通过 Whitecoin 包含的其他资产链的轻钱包组件，用户可以从其他资产链地址或从中心化交易所中充值到 Whitecoin 账户绑定的隧道账户地址里。

Whitecoin上的Miner检测到关联的多重签名的充值地址收到转账后，等待块数到达一定确认高度后， 根据充值的来源地址，找到关联的Whitecoin账户，并在Whitecoin上共识给这个账户地址相应的WAMP（例如WBTC/WLTC等）。Whitecoin上WAMP（例如WBTC/WLTC等）默认为冻结资产(m块)，等待Whitecoin块数到一定高度（比如m+6）后新共识生成的WAMP（WBTC/WLTC等）资产从冻结状态转为可用状态。

在 Whitecoin 上充值分为以下环节：

- 用户充值到 Whitecoin 账户绑定的隧道账户里，这个交易确认依赖于原资产链上确认时间，如 BTC 延迟 6 块确认，LTC 延迟 12 块确认。
- 从隧道账户转账到由Wallfacer/面壁人共识管理的多重签名地址里。这个交易确认同样依赖于原资产链上确认时间，如BTC延迟6块确认，LTC延迟12块确认。
- Whitecoin 上 Miner 通过共识在 Whitecoin 上给用户生成对应的 WAMP，并等待 Whitecoin 上区块延迟 17 个区块后确认。

跨链充值的底层操作流程图如下：



在实际操作中，XWC Wallet 会在人机交互上包装简化大部分流程，用户只需要比较简单的步骤即可完成跨链充值。

6.2.4 跨链提现流程

- 用户发起提现交易，交易中包含其他资产链的提现地址。
- Wallfacer/面壁人收到提现交易后，进行签名，并在网络中广播，同时收集别的 Wallfacer/面壁人对该交易的签名。
- 当轮到某个 Miner 要出块时，判断当前是否收集到不少于 2/3 的 Wallfacer 的签名，如符合条件则将该交易及所有收集到的签名打包进块，否则该交易将不会打包进块，由后面的 Miner 负责处理。
- 交易被打包进块后，用户所拥有的对应 WAMP（比如 WBTC、WLTC 等）即销毁。
- Wallfacer/面壁人验证后判断多重签名热钱包的余额是否充足，然后进行提现转账处理。
    - 如果充足则在此资产链上发出从 Wallfacer/面壁人管理的冷热多重签名钱包到提现地址转账的签名，满足多重签名条件后则提现完成。
    - 如果余额不足，即从多重签名冷钱包中提取资产到多重签名热钱包，等热钱包里的资产充足后 Miner 再发起转账流程。

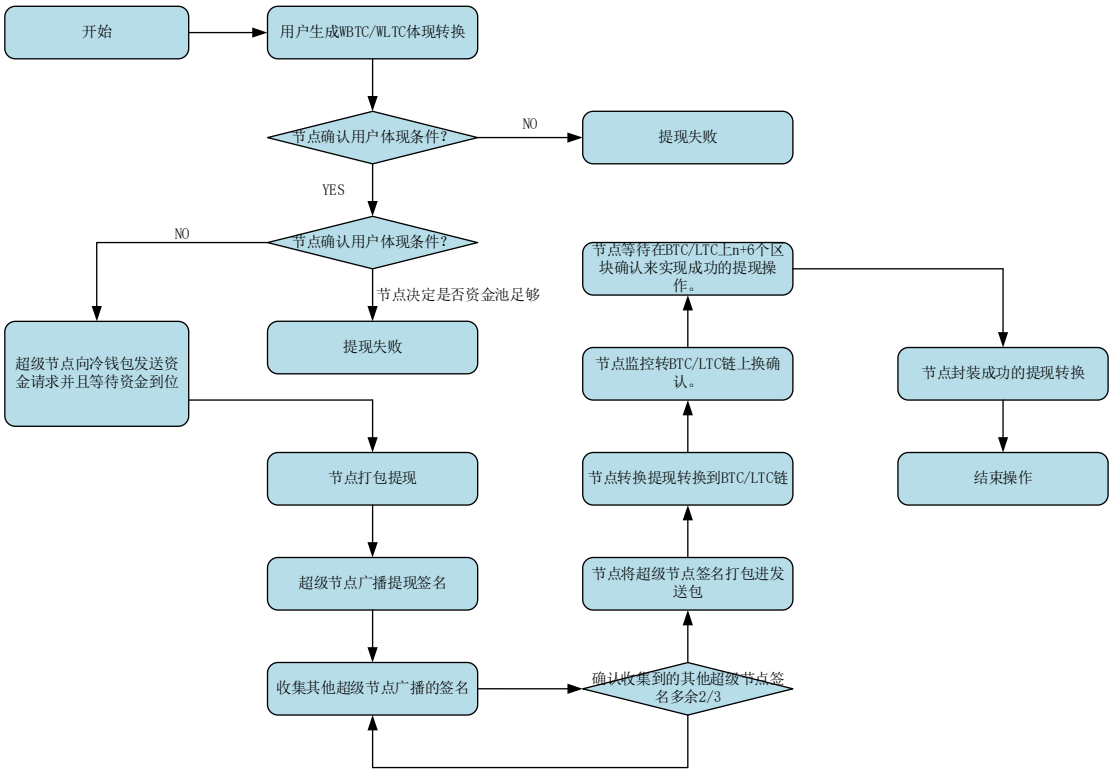
跨链提现分为两步：

用户在 Whitecoin 上发起提现申请，等待 Miner 账户打包后（平均 3 秒），等待收集不低于 2/3 的 Wallfacer/面壁人账户对该提现请求的签名。

- 若有超过 1/3 的 Wallfacer/面壁人账户不认可该请求，则该交易作废。
- 若收到不低于 2/3 的 Wallfacer/面壁人的签名后，Wallfacer/面壁人将会生成一笔对应资产链出账交易，交由对应资产链确认后（需等待相应的块数），Whitecoin 上 Miner 打包提现完成交易，当该交易被 Whitecoin 上认可时，即算完成提现交易。

具体技术实现过程为：用户发起提现申请后，Miner 发起对应的从多重签名地址转账到用户目标地址的原始交易，将原始交易包装到 src_trx 中广播到 Whitecoin 上。Wallfacer/面壁人同步到 src_trx 然后验证后，将对 src_trx 的签名包装到 sig_trx 广播并记账到 Whitecoin 上。当全网收集到足够的 Wallfacer/面壁人签名后，Miner 把收集的签名打包后生成完整的提现交易，然后在 Whitecoin Wallet 内置的对应的资产链轻钱包组件中调用相应资产链的交易广播接口，广播到相应资产链的网络中去。

跨链提现的底层操作流程图如下：



6.3 侧链资产的安全性

6.3.1 资金动态平衡策略

Whitecoin 支持多重签名冷热钱包资金动态平衡，如果热钱包多重签名账户资产超过 3 倍限额则发起资金动态平衡流程，将多重签名热钱包地址内的资产转到多重签名冷钱包地址。

实现方案:

- 由一个 Wallfacer/面壁人发起资金动态平衡流程，链上打包后通知其他 Wallfacer/面壁人。
- 其他 Wallfacer/面壁人会进行验证，验证成功后会将签名交易广播，然后由 Miner 打包到 Whitecoin 上。
- 当 Miner 收集到不少于 2/3 的 Wallfacer/面壁人的签名后将交易打包，确认 WAMP 对应的原链的交易。
- 最后广播到原链上完成资金动态平衡流程。

6.3.2 资金动态平衡期限

- 每 10000 个区块执行一次资金动态平衡流程，根据多重签名热钱包的资产多寡，将多重签名热钱包的资产总额调整至设定范围内。
- 上述资金动态平衡交易由该块的出块 Miner 创建基础交易广播后由不低于 2/3 的 Wallfacer/面壁人追加签名。

七、技术要点及创新

7.1 合约和虚拟机

使用一种图灵完备并为区块链智能合约定制设计的字节码规范作为智能合约虚拟机的实现规范。提供静态类型的高级编程语言比如 C#，Java, TypeScript 等的编译器实现从高级语言生成智能合约字节码。

- **智能合约虚拟机**

智能合约虚拟机实现为一种图灵完备的字节码虚拟机，做到运行时具有确定性，执行逻辑可控性，状态变化可监控。

- **智能合约语言**

使用现有编程语言比如 C#，Java, TypeScript 等流行的编程语言的主要特性的子集作为智能合约的高级编程语言，编译到符合智能合约字节码规范的字节码，作为智能合约使用。

- 智能合约的内置库：

智能合约提供一些常用数值操作，字符串操作等的基本库，以及一些链上查询，交易等的内置函数库，在智能合约中可以调用内置库。

- 智能合约的互相调用：

智能合约部署到链上后，除了可以被用户直接调用或者存取资产，还可以调用其他智能合约/内置原生合约，或被其他智能合约调用。

部分功能逻辑可以以智能合约实现并部署在链上，作为第三方库被链上其他智能合约使用，起到扩展区块链的功能的作用。

- 智能合约的功能范围和限制：

智能合约可以用图灵完备的编程语言编写业务逻辑，可以查询链上数据，可以确定性存取本合约的状态 Storage，可以调用其他智能合约/原生合约，可以输出返回信息给调用者。

限制：不能读取链外数据；不能非确定性产生各节点不一致的逻辑；执行指令数和使用内存空间量受区块链控制；区块链可以随时立刻终止智能合约的执行，比如在合约执行费用超预算时。

- 智能合约的状态存储：

每个智能合约有一个独立的状态存储空间，称作 Storage。Storage 的存储格式是非结构化的数据结构。链上存储智能合约的 Storage 的变化，而不是每次完整存储最新 Storage 到链上。比如在一次合约调用中，将合约 Storage 从 {"name": "chain" } 修改为 { "name": "chain", "count": 123 }，链上只记录变化的部分 { "count": 123 }，并且就算合约调用手续费时，存储部分收费也只计算变化的部分的大小而不是完整 Storage 的大小。从而即使一个智能合约的状态存储空间较大，只要每次调用合约产生的变化量不大，链上数据增量和手续费也不高。

- 智能合约的状态查询：

智能合约可以直接查询本合约的 Storage 的部分值，也可以通过类 SQL 的编程语言取出嵌套数据结构中的部分数据。在智能合约的 Storage 较大的时候，可以通过这种方式减少数据加载量提高查询速度，避免全表扫描，提高智能合约的数据存取部分的性能上限。

比如：某智能合约的 Storage 结构类似

```
{
 "name": "blockchain",
 "userBalances": [
   { "userAddress": "a", "amount": 10000, "freeze": false },
   { "userAddress": "b", "amount": 20000, "freeze": true },
   { "userAddress": "c", "amount": 30000, "freeze": false },
```

..... 更多数据，比如几十万条记录

]

}

可以使用类似 var freezedUsers = storage.query("select userBalance.userAddress from userBalances as userBalance where freeze=true") 这样的类 SQL 语法查询出本智能合约中所有冻结了账户的用户地址，数据读写量大大减少，并且避免了全表扫描，可以满足在智能合约中存储较多数据但是每次读取量不大的业务场景，比如在智能合约中实现简单 push 交易所，实现智能合约资产，实现合约保险等。

- 智能合约的生命周期：

1. 通过高级编程语言或者手动构造字节码产生智能合约字节码文件
2. 部署智能合约字节码到区块链上，可以创建为智能合约，也可以创建为智能合约模板供下次创建合约时使用
3. 调用智能合约 API，或向智能合约地址转账
4. 区块链每次调用智能合约，先初始化独立的轻量级智能合约沙盒执行环境，在其中加载智能合约并执行
5. 执行完智能合约后，根据执行退出状态异常与否，将执行结果和合约 Storage 变化保存。

7.2 可共识的随机数发生器

智能合约具有获取可共识的随机数的需求，为了生成可共识的随机数，输入必须是链相关数据数据。这里提供了两种随机数获取方法:

简单随机数:合约中直接调用一个接口获取一个随机数,提供基于当前随机种子的随机数。

复杂随机数:用户在合约中指定一组连续的块，系统以该组块的 prev_secret 作为输入，产生随机数。用户可以指定未产生的一组块记录在设定在合约中，在该组块被产生后，随机数被确定。

用户能够在合约中直接调用接口获取简单随机数。

此种方式，对于一次合约调用，在执行结果利益相关方恰好是当前产块人时，存在产块人根据随机数结果以及自身利益选择不打包该调用的可能性。在希望避免这种可能的情况时，可以采用复杂随机数。复杂随机数以连续块的 prev_secret 作为输入，产块者若想产生对自身有利的随机数，需要在根据组内其他块的 prev_secret,调整当前块的 prev_secret,但是 prev_secret 是在前一轮产块时就已经确定无法修改，即产块者无法控制随机数的产生。

7.3 事件及回调

事件是指在合约代码内抛出的特定数据，会记录在区块链上。一旦事件发生，所有的区块链节点都能观察到这个数据。

回调则是为合约中的事件绑定处理方法，在接收到指定类型的事件时，则执行绑定的方法。

官方钱包提供默认的 Script 脚本回调，也可以由用户根据自己的情况自定制。Miner 节点执行合约，触发某个事件事件，会将其一起打入区块中，并进行广播。

事件机制的优点:

由于一个智能合约在不同的时间点或者不同的外部条件调用下，可能会走入合约代码的不同分支，执行不同的代码逻辑。对于调用者来说，并不能很好得了解合约执行的状况，有了事件机制，用户就拥有了了解合约执行中的状况，以及获取合约执行结果的能力。

拥有了这样的能力，用户可以根据接收到相应的事件，做出相关的反馈动作，比如说再次发 起一笔交易，或者发起一个合约的调用，或者一些本地的动作，比如说记录日志，或

者记录 数据库，或者进行一个 HTTP 请求 这些。甚至用户还可以制作一个具有决策能力的程序来对接到我们的区块链中，进行一些实务的决策，并根据决策结果来实施不同的反馈操作。

7.4 本地查询接口

智能合约 Storage 区的数据可以通过合约接口来查询，但是这样会消耗手续费，并且需要等区块打包才能获得结果。对于一些不涉及到共识的简单查询功能，合约支持本地查询接口（offline）。通过查询本地区块链数据，获得合约的当前数据状况，不但速度快，而且无需消耗手续费。

7.5 资产区块链接入模型

每个新的资产区块链接入，都是以插件模式实现的。普通节点可选择是否挂载跨链插件，Miner和Wallfacer/面壁人强制要求挂载所有跨链插件。

新增跨链插件流程如下：

- Miner 和 Wallfacer/面壁人约定停机时间;
- Miner 和 Wallfacer/面壁人在约定时间内分批次完成重启和加载插件;
- 所有 Wallfacer/面壁人完成补充保证金的操作;
- 等约定时间到达后，发起新币种的初始化操作（创建多重签名地址，广播新币种相关参数，进行新币种喂价）；
- 完成区块链升级；
- 选择挂载跨链插件的普通节点选择新插件，然后进行挂载。（普通节点可自选挂载哪种链的跨链插件，因此不影响共识）。

八、项目的开发规划

Whitecoin 将分为四个阶段发展分别是面壁计划（Wallfacer Project）、威慑计划（Threatening Project）、阶梯计划（Staircase Project）、黑域计划（Blackdomain Project）。

8.1 面壁计划（Wallfacer Project）

本阶段将从 Whitecoin 从 POS3.0 升级至跨链方案筹备到老 XWC 与新 XWC 互换结束，时间持续一年时间。本阶段是 Whitecoin 技术路径选择与筹备的重点阶段。当老 XWC 在预定时间完成切换之后，本阶段也将顺利完成。

8.2 威慑计划（Threatening Project）

本阶段将从 Whitecoin 区块链创世块诞生起到 5256000 个区块结束，本阶段为期一年时间。本阶段 Whitecoin 区块链将开启跨链运行，通过提供较高的挖矿收益吸引了更多的人关注并参与到开发中来。通过建立和完善 Whitecoin 生态体系，实现 Whitecoin 的生态价值。

本阶段将着重建立 Whitecoin 生态项目培育、Whitecoin 工具、Whitecoin 钱包体系、Whitecoin 相关基础设施等内容。

8.3 阶梯计划（Staircase Project）

阶梯阶段将从区块 5256001 开始至 26280000 结束，为期四年时间左右。本阶段区块奖励将呈阶梯状下降。而区块链网络也将步入稳定运行阶段。同时，跨链的资产品种也将覆盖所有的主流数字资产，区块链的应用也将覆盖更多的应用场景。Whitecoin 区块链将呈现阶梯状升级状态。

8.4 黑域计划（Black domain Project）

进入区块 26280001 后，Whitecoin 正式进入了黑域计划。黑域计划的开启也标志着 Whitecoin 进入了茫茫的区块链未来世界。进入本阶段后，Whitecoin 将真正成为区块链的

基础设施。

九、结论（Conclusion）

Whitecoin 区块链系统将是打破区块链孤岛，实现区块链价值传递、价值再造的基础工具。随着 Whitecoin 四个发展阶段的推进，最终实现区块链互联互通的网状结构发展，实现区块链的网络效应。

十、References

1 Bitcoin: https://bitcoin.org/bitcoin.pdf

2 Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

3 TheDAO: https://download.slock.it/public/DAO/WhitePaper.pdf

4 BitShares: http://docs.bitshares.org/bitshares/history.html, 2013

5 https://en.wikipedia.org/wiki/The_Three-Body_Problem

6 https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md