electric cash

白皮书 v2.0.2

electriccash.global

2021 年

目录

法律免责声明

本文件不是最终技术规范。

本文件所述项目处于初始概念阶段，可以修改、更改甚至放弃（例如，出于经济、技术或监管原因），本文件中的任何内容均不得视为对项目、服务或其任何部分或组成部分，或者关于它的执行的最终和有约束力的描述或观点。

本文件不构成财务建议。

本文件（白皮书）中的信息不被视为投资建议。加密货币市场是剧烈波动的。结合自身的情况和财力，您应该仔细考虑加密货币是否适合您。通过关注文件（白皮书）的其余部分，您承认您没有向作者或与作者有正式关系的任何各方寻求投资建议，因为上述作者和各方可能不提供此类建议。我们并不期望或邀请您根据本白皮书所载的任何资料，以任何形式投资、购买或进行任何相关金融活动，并且您承认任何此类活动完全由您个人负责。

Electric Cash
白皮书

Eyal Avramovich
白皮书 v2.0.2

摘要.2009年，第一种加密货币比特币（Bitcoin，1）问世。11 年后的今天，尽管比特币打破了价格纪录，但无论是比特币还是任何其他加密货币都尚未得到大规模采用。大多数加密货币虽然安全，但其功能与现金不同。交易处理效率不高，往往成本高昂，并且许多项目仍不重视用户体验。然而，新的技术解决方案使我们能够设计出一种更好的加密货币，它与大多数区块链一样安全，同时实现快速、免费交易。在本文中，我们介绍了一种新的去中心化快速支付协议 Electric Cash（ELCASH）。这是一种基于 SHA-256 算法的币，像现金一样，可供日常使用。快速、免费的交易功能使 Electric Cash 成为交易、日常支付的理想之选。此外，Electric Cash 协议的管治机制使其持有者可以参与构建生态系统发展的未来。我们相信，这种方式填补了市场现有的空白，能够满足广大用户的期望。

1. 引言

1.1. 问题陈述和解决方法

区块链交易费用

第一种加密货币比特币实现了一种简单但相当可靠的交易费用机制，以保护网络免受垃圾邮件的侵害。交易费用可能会有所不同，并取决于几个因素，包括网络拥塞、交易确认时间和交易规模。当网络负载较低时，所有交易都会以最低的费用快速处理。费用很低，个人申请交易几乎不需要付出成本。随着负载的增加和接近预先规定的限额，对交易确认的需求增加，因此矿工可以增加手续费（2）。最近的许多项目延续了这种设计，但没有解决随着网络的增长而导致交易费用增加的问题。

如今，由于其中许多公司越来越受欢迎，它们背负起了高昂的交易费用。在某些情况下，每笔交易的成本可能高达几十美元。这样的成本使得它们在日常使用场景下无利可图，阻碍了新的和现有的网络参与者使用它们。

对于工作量证明加密货币，交易费用用于保护网络免受恶意溢出，并对添加到区块链的交易进行优先级排序。ELCASH 协议的机制也是如此。不过，ELCASH 解决方案会奖励那些积极参与网络的用户，从而为质押人提供免费交易。质押 ELCASH 的用户每天都有资格进行几笔免费交易，这取决于他们的质押参数。

区块链性能

尽管区块链已经在金融界大受欢迎，但它作为一种分布式可信技术的实际用途却因其缺乏可扩展性而受到阻碍（3）。大多数工作量证明区块链的交易处理能力有限。随着网络的普及和使用的增加（越来越多的交易通过区块链进行），网络及时处理这些交易的能力减弱。因此，大多数被认为最安全的、使用共识机制的 PoW 加密货币很少作日常使用，而是作为黄金的替代品。其他加密货币，如以太坊（Ethereum）（4），意识到了这个问题，并正在从工作量证明转向权益证明机制。

迄今已提出了许多解决办法。在这个项目中，我们采用了最理想的解决方案：所谓的“快速层级”体系，以提高区块链吞吐量。我们结合了最优的两种方案，即在工作量证明协议下进行挖矿的区块，确保区块链安全，同时交易可以在区块链的第二层级（L2）进行，实现几乎即时的交易（5）。

社区影响

加密环境中的项目通常由区块链团队或核心开发人员管治，因此它们是集中管治的。关于任何进一步开发和网络变化的决定都是由相对较少的人控制和作出的。由于缺乏技术知识或财务杠杆，许多主流用户在决策方面要么没有发言权，要么没有足够的影响力。

Electric Cash 通过建立 Development Fund Treasury 改变了这一状况。该“金库”使用一小部分工作量证明挖矿奖励创建，并存储起来。此外，Electric Cash 的社区成员获得了管治权力。这使得该网络可以去中心化，由项目社区推动有关未来项目开发和 Development Fund Treasury 资金使用的决定。网络民主的实现得益于区块链内置的投票机制（6）。

2. Electric Cash 生态系统

Electric Cash 是一种基于 SHA-256 的币，它是一种类似现金的加密货币，用于日常使用，并带有额外的质押功能。Electric Cash 协议由其持有者管治——他们有资格管理生态系统的未来发展。所有这些方面都整合在一个生态系统中，使得 Electric Cash 能够覆盖各种各样的市场和用户需求。

质押

管治

第二层级

为了将激励措施不仅用于矿工，也用于其他网络用户，Electric Cash 区块奖励分为三份。第一份奖励，也是最大的奖励，分配给工作量证明矿工。矿工对确保网络正常运行和安全至关重要。但矿工并不是唯一的利益相关者。每天使用网络和扩展 ELCASH 生态系统的人对项目的增长至关重要。

ELCASH 币是生态系统不可分割的一部分

ELCASH 币的关键之处在于它能长期提供给每一个处理活跃状态的用户。因此，我们设计了一个全面的生态系统，在这个生态系统中，权益质押可以获得奖励和探索其他的可能性。得益于管治体系，内部资源可以用于网络完善。

为了实现这样一个体系，在协议中实施了一个独特的分发模型（图1），允许所有网络用户因其贡献获得奖励，即：

- 在最初的预挖矿（根据币分配计划累计分配的币）结束后，最大的部分，即币总供应量的 80%，被分配给矿工。
- 总供应量的 10% 用于质押奖励。
- 总供应量的 10% 被分配到 Development Treasury Fund。用于未来的开发（协议完善）。网络社区成员（质押并获得 GP 的用户）是唯一有权管理它（即通过投票）的人。

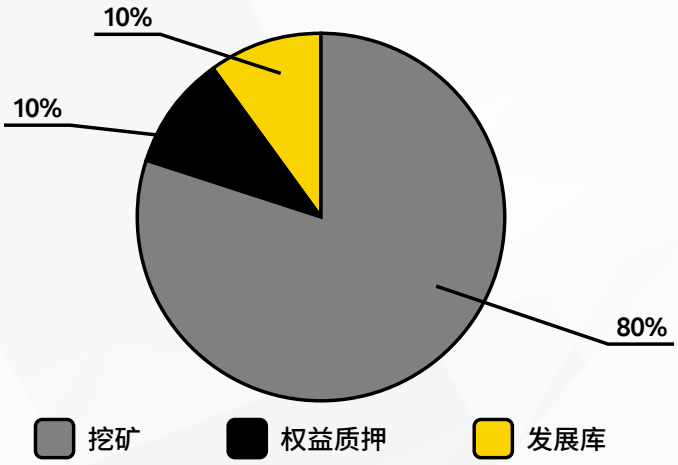


图 1。 区块奖励分配

我们相信，这一方案一推出就可以吸引矿工。因此，在导引阶段结束后，应该就会有足够的币流通，并有大量的散列能力来保护网络，以便可以使用其他网络功能，并促进日常使用中的大规模采用。

2.1. 质押

Electric Cash 的一个核心功能是质押。它为我们的用户创建一个健全的管治体系，并激励网络参与者的积极行为。质押是储存资金的一种形式。通过质押，从长远来看，每个用户都能为网络增长做出积极贡献，并有助于防止可能影响未来几年整体通胀问题的供过于求问题。这反过来又增加了网络的稳定性。

2.1.1. 质押过程

Electric Cash 网络的参与者可以通过投资 ELCASH 来管治网络，并从中获得回报。ELCASH 也向用户提供额外奖励（图 2），比如免费交易和管治权力（GP）。

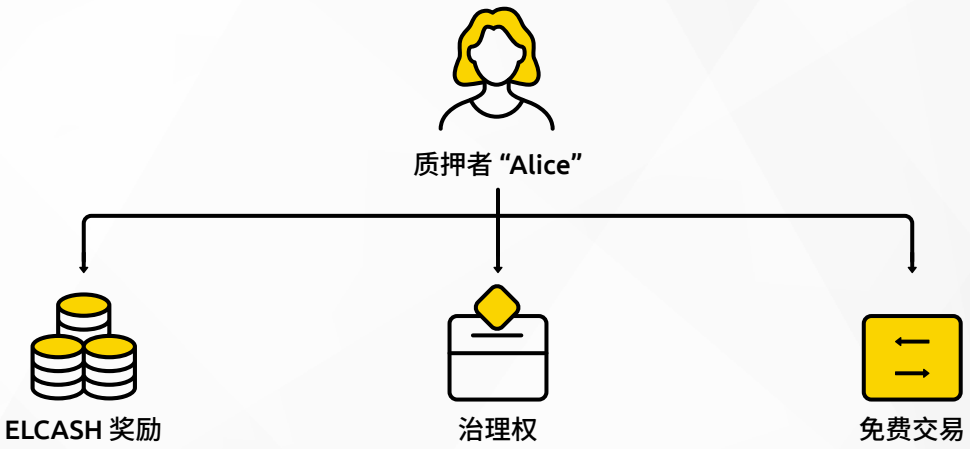


图 2。Electric Cash 质押权益

每一个 ELCASH 的用户都可以从他们的 Electric Cash 钱包管治整个质押过程。用户完全控制资金，并直接与协议签订质押协议。

2.1.2. 质押参数

质押过程的规则对于每个参与者和每个质押值都是相同的。每个用户都可以选择一个固定的质押合同，它对应于特定的利率和期限。

表 1。 根据合同期限支付 ELCASH 质押利息（每年）。

~天	区块	~奖励[% 每年][1]
30	4,320	5
90	12,960	6
180	25,920	7.25
360	51,840	10

因为区块链是以区块的数量来运作的，所以质押的持续时间是以区块而不是以时间为单位来计算的。上表中所示的天数是根据平均新区块时间估算的，对于 Electric Cash 区块链而言，新区块时间约为 10 分钟。

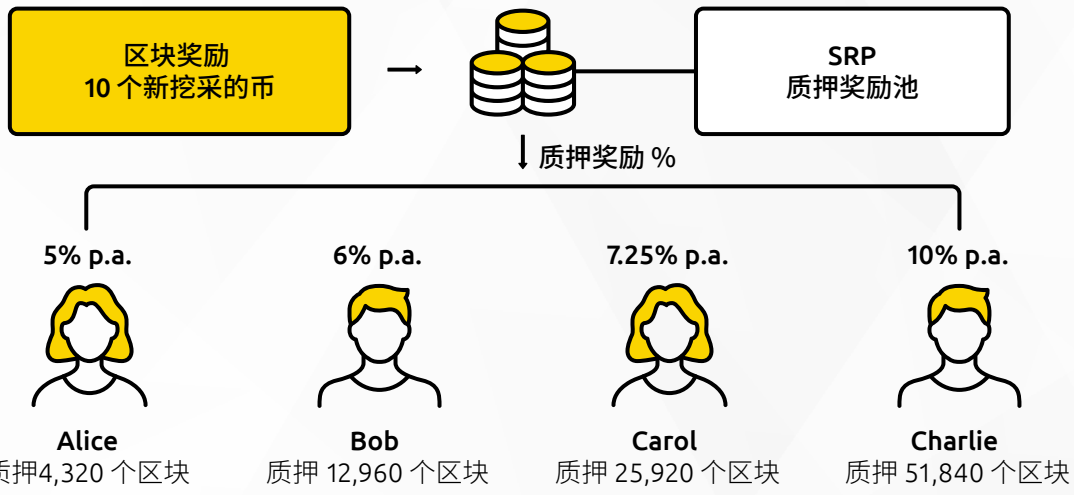


图 3。根据质押期限的奖励率

质押奖励根据合同期限的不同而不同——质押期限越长，质押奖励就越高。奖励按区块计算，分配给用户的值显示在他们的钱包中。质押奖励为年近似值；最终的奖励可能略有不同。

为避免严重的舍入错误，可质押的最小值为 5 ELCASH。没有固定的最大值。

2.1.3. 质押奖励池（SRP）

在 Electric Cash 协议中，质押奖励直接来自工作量证明挖矿奖励。从每一个新挖矿区块奖励中提取 10% 并分配到质押奖励池（SRP）。

1 注：给定值仅为估计值，由于网络变量，在合同期间可能略有不同。

奖励只能在锁定（质押）期结束后才可以转移给质押人。提前终止合同将导致迄今为止获得的奖励被扣除并且承担赔偿责任。未累积的奖励留在池中，随后分配给所有活跃的质押人，赔偿从用户转移到 SRP。

质押奖励池详细信息：
在包含每个区块后的质押奖励池（SRP）值的变量中，将执行以下操作：
- SRP 的值按 10% 的区块奖励上增。
- SRP 的值按提前提款罚款和为终止质押的质押人锁定和预留的资金上增。
- SRP 的值按为所有达成了质押协议的质押人预留的质押奖励而下减。

所有关于质押值的数据都保存在质押数据库（sDB）中，该数据库是 Electric Cash 区块链的一种表示方法，并且会自动更新，因此所有数据都是安全的。在每个区块之后，通过以下操作更新数据库：
- 如果找到新权益质押的交易，则会将其添加到数据库中。
- 如果给定条目的质押期已结束，或者发现提前支付（取消质押），则会将其从数据库中删除。
- 根据质押金额计算所有的质押奖励（百分比）并添加到每个条目（活跃质押）。

注：数据库只是作为区块链的一个更方便的表示，但是可以使用区块链从数据库中恢复所有数据。

2.1.4. 质押钱包

Electric Cash 生态系统的核心元素是用户友好和直观的钱包（图 4）。钱包应用程序包括一个支出钱包和一个质押钱包。通过质押钱包，用户可以轻松地质押他们的币来获得管治权力、免费交易和质押奖励。

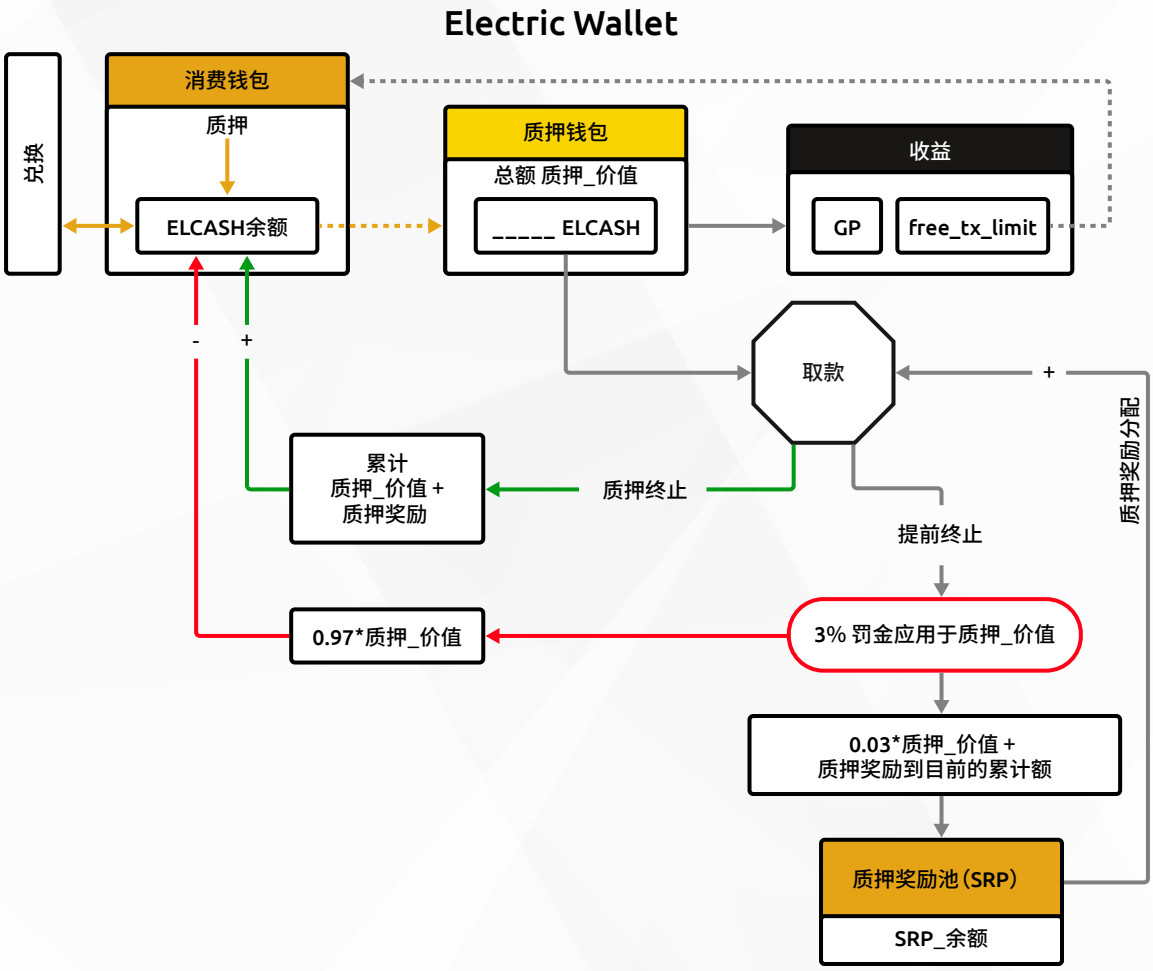


图 4。Electric Cash 质押过程

质押钱包没有一个单独的地址，它和支出钱包共用一个地址。交易安全、数据恢复，一举两得。质押钱包是一个使用支出钱包地址的 UTXO 实例。它是一种单独的区块链钱包，但存储在同一地址。

当创建一个新的质押（图 5）时，启动一个交易：从用户的支出钱包中获取输入，并用所有的质押参数创建输出，然后用质押资金创建一个新的质押 UTXO。如果支出钱包中的资金高于质押金额，那么变化也会分配到新的支出 UTXO 中。

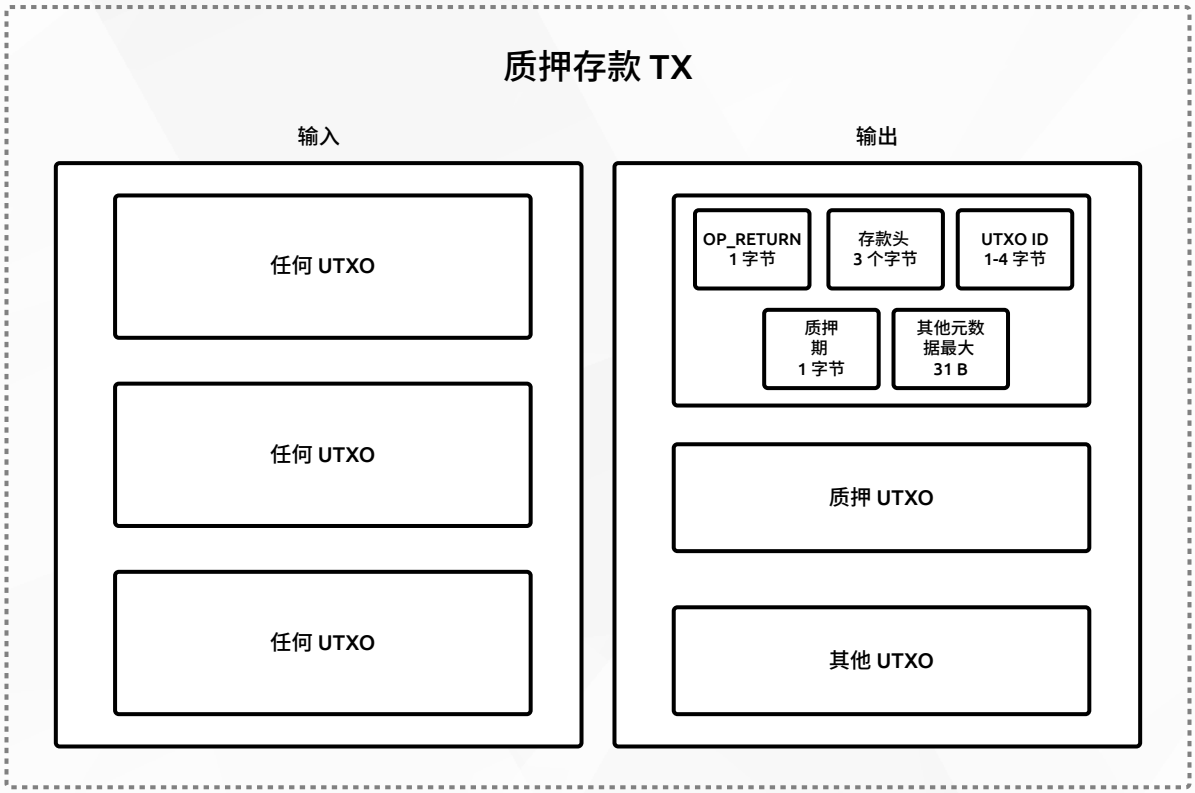


图 5。启动质押的交易

验证规则：

1. OP_RETURN + 质押报头是 tx 的第一个输出
2. UTXO ID > 0
3. 质押期 ⩽ 4（查找表索引）
4. 质押 UTXO 金额必须 ⩾ 5e8 sat
5. 所有正常的交易规则

当质押结束时，协议查验质押是否已经到期或被用户终止。如果过早终止，将受到处罚，并且质押奖励不会转移给用户。如果质押已经到期，来自质押 UTXO 的资金和奖励 UTXO 将转移到支出 UTXO，如下图所示（图 6）。

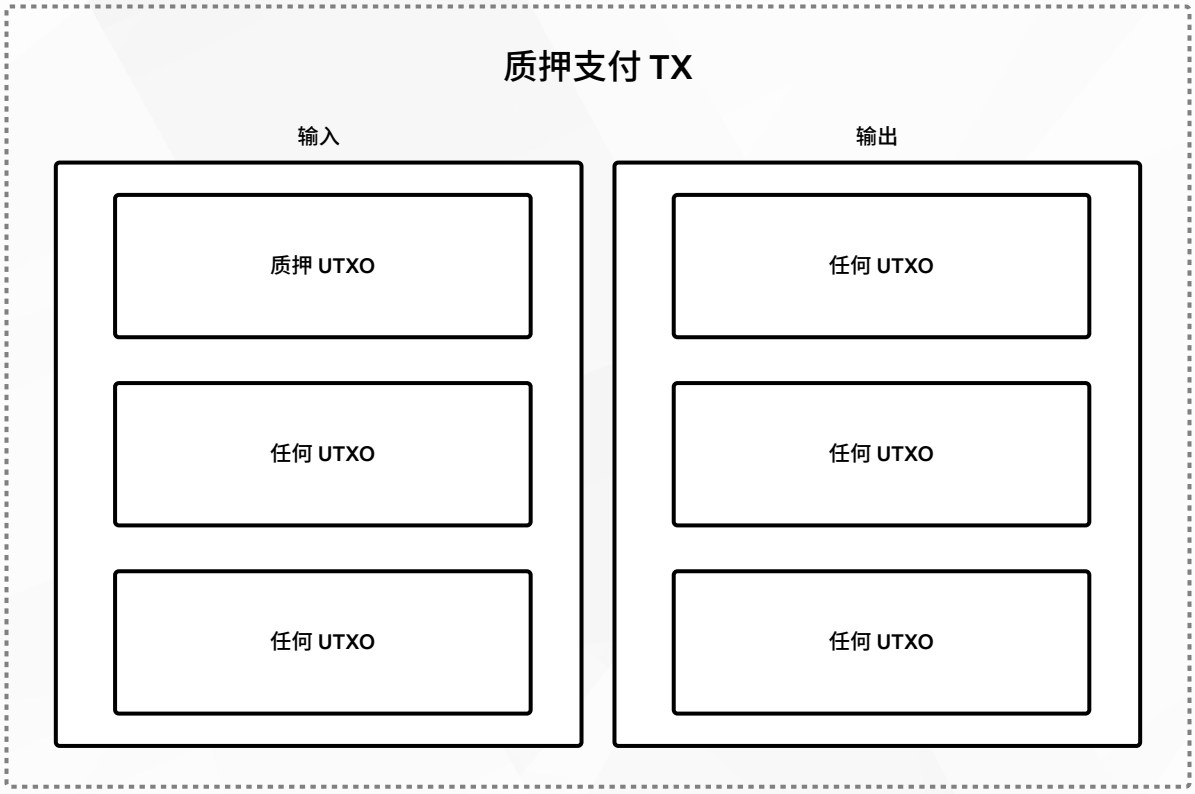


图 6。质押付款的交易

验证规则：

1. 查验质押 UTXO：查验输入 TX 是否为质押押金 TX（检查第一个输出）
2. 检查是否满足质押期（当前区块高度 ≥ {输入 UTXO 的区块高度 + 质押期}）
   a. 如果是：检查输出值是否小于{输入 + 质押奖励}（计算质押奖励）
   b. 如果否：检查输出值是否小于{输入 – 质押惩罚}（计算质押惩罚）
3. 所有其他正常的交易规则

质押销毁交易用于将资金从普通 UTXO 转移到质押奖励池。采用这种方法的主要原因是用之前的适当挖矿奖励百分比来填充质押硬分叉后的质押奖励池。

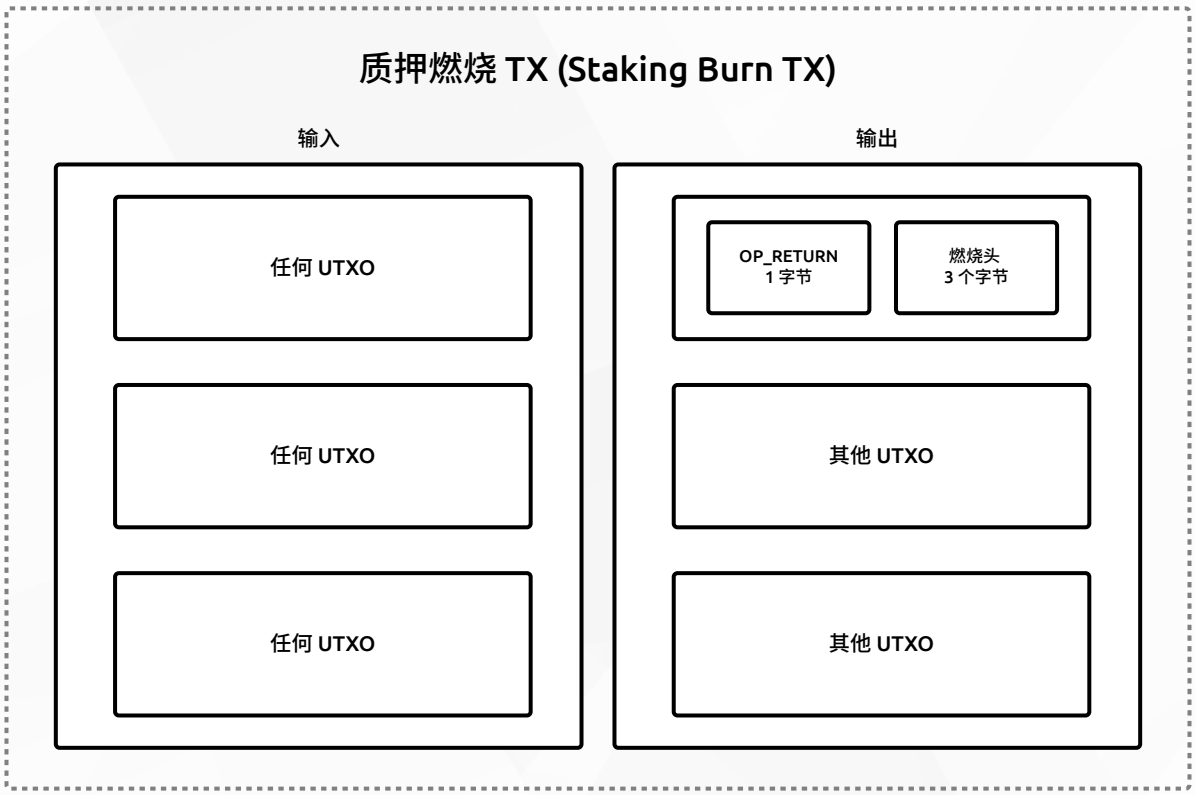


图 7。质押销毁交易

验证规则：

1. OP_RETURN + 销毁报头是 tx 的第一个输出
2. SUM（输入）≥ SUM（输出）+ burn_amount:
   以区块数或包含区块数的预定义表的索引表示的质押期

注：用户不断控制资金和私钥相关的质押和支出钱包；因此，安全性与用户的个人标准一样强。

2.1.5. 提款

质押到期后，质押人将可以使用质押支付交易申请奖励。所有参与者必须等到质押期结束后才能提取资金[质押金额+质押奖励]，否则将被处以 **3% 的固定罚款。处罚的目的是保护网络上的免费交易不被滥用，阻止在网络之外投票，防止 ELCASH 经济受到干扰。**

提前提取资金将导致迄今为止获得的奖励被扣除并且承担赔偿责任。在规定的质押期结束之前，不会累积任何奖励。未累积的奖励和从用户处获得的罚款将被转移回**质押奖励池（SRP）**，并随后分配给持有其头寸的其他质押人。

2.1.6. 奖惩计算

针对每个新的区块对质押奖励池和个人质押奖励进行更新。协议计算用户应获得的所有奖励，并在此基础上查验 SRP 的状态。同时，协议查验质押是否到期，如果到期，奖励将转移给用户。如果质押仍在进行中，协议会将信息发送到质押数据库，并更新用户获得的奖励（图8）。

表 2。协议更新 - 输入参数

康斯坦斯（Constans）	质押数据库条目
MINING BLOCKS PER DAY= 144	STAKE {
MINING BLOCKS PER YEAR= 365*MINING BLOCKS PER DAY= 144*365	STAKED,
STAKING_PERCENTAGES = [0.05, 0.06, 0.0725, 0.1]	PERIOD,
STAKING_PERCENTAGE_VS_PERIOD: {	COMPLETE_BLOCK,
“lmo”: 0.05,	COMPLETE,
“3mo”: 0.06.	REWARD,
“6mo”: 0.0725,	SCRIPT,
“12mo”: 0.1}	TXID,
STAKING POOL EXPIRY BLOCKS = 180	NUM OUTPUT
STAKING MAX-YEARLY PROFIT PERCENTAGE = 0.1	}
PENALTY RATE = 0.03	
全球的	
STAKING POOL	
TOTAL_STAKED = { “lmo”: XXX ELCASH, “3mo”: XXX ELCASH, “6mo”: XXX ELCASH, “ly”: XXX ELCASH}	

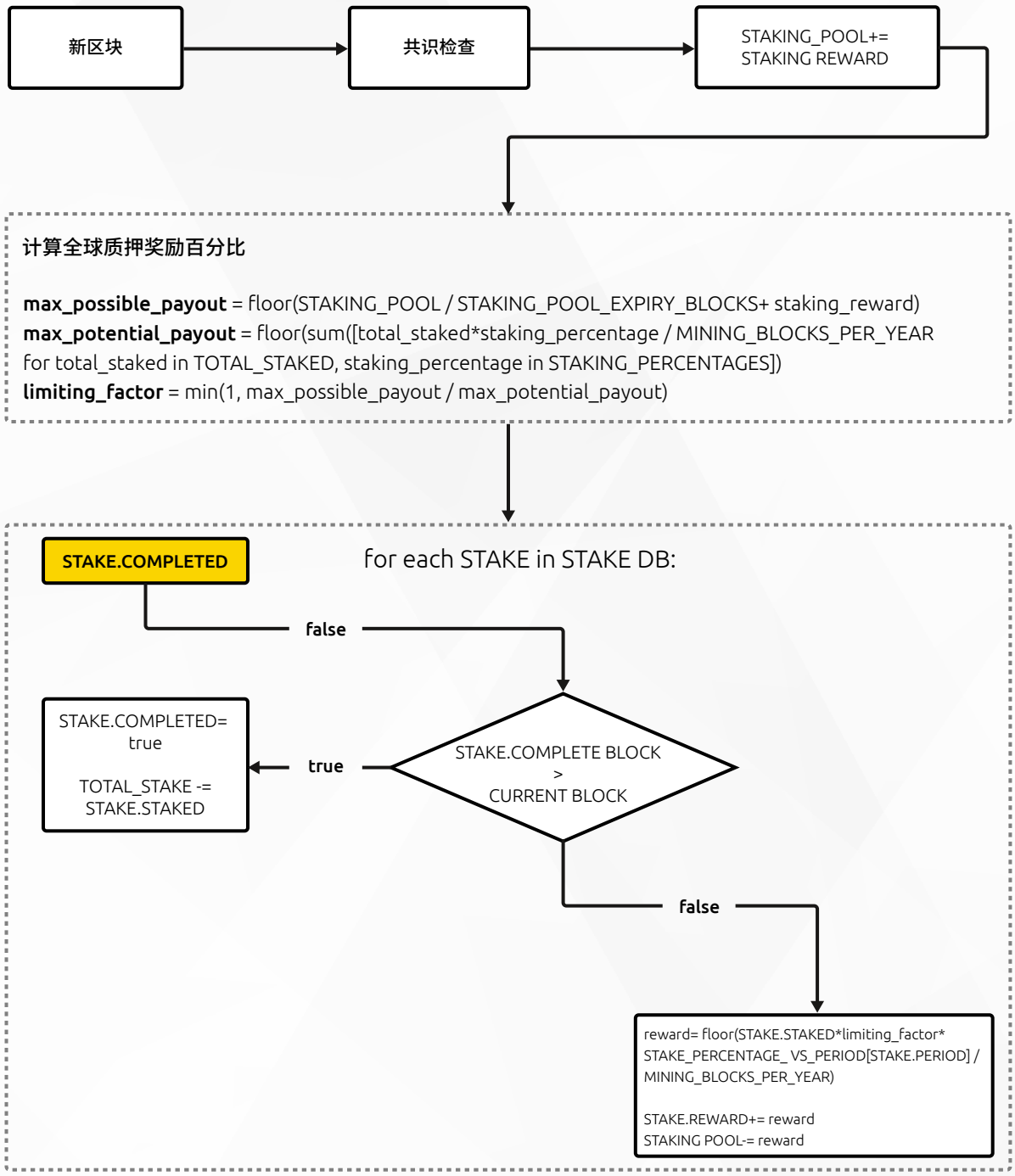


图 8。质押计算算法

协议一直在寻找结束用户质押的交易。如果发现了这样的交易，协议将查验质押是否提前终止，或者质押合同是否已经到期。如果质押在到期日之前终止，则将处以罚款，用户支付的金额不得超过计算出的存入币百分比。如果质押已到期，则转移已质押的资金和累积的报酬。已到期的质押将从数据库中删除。

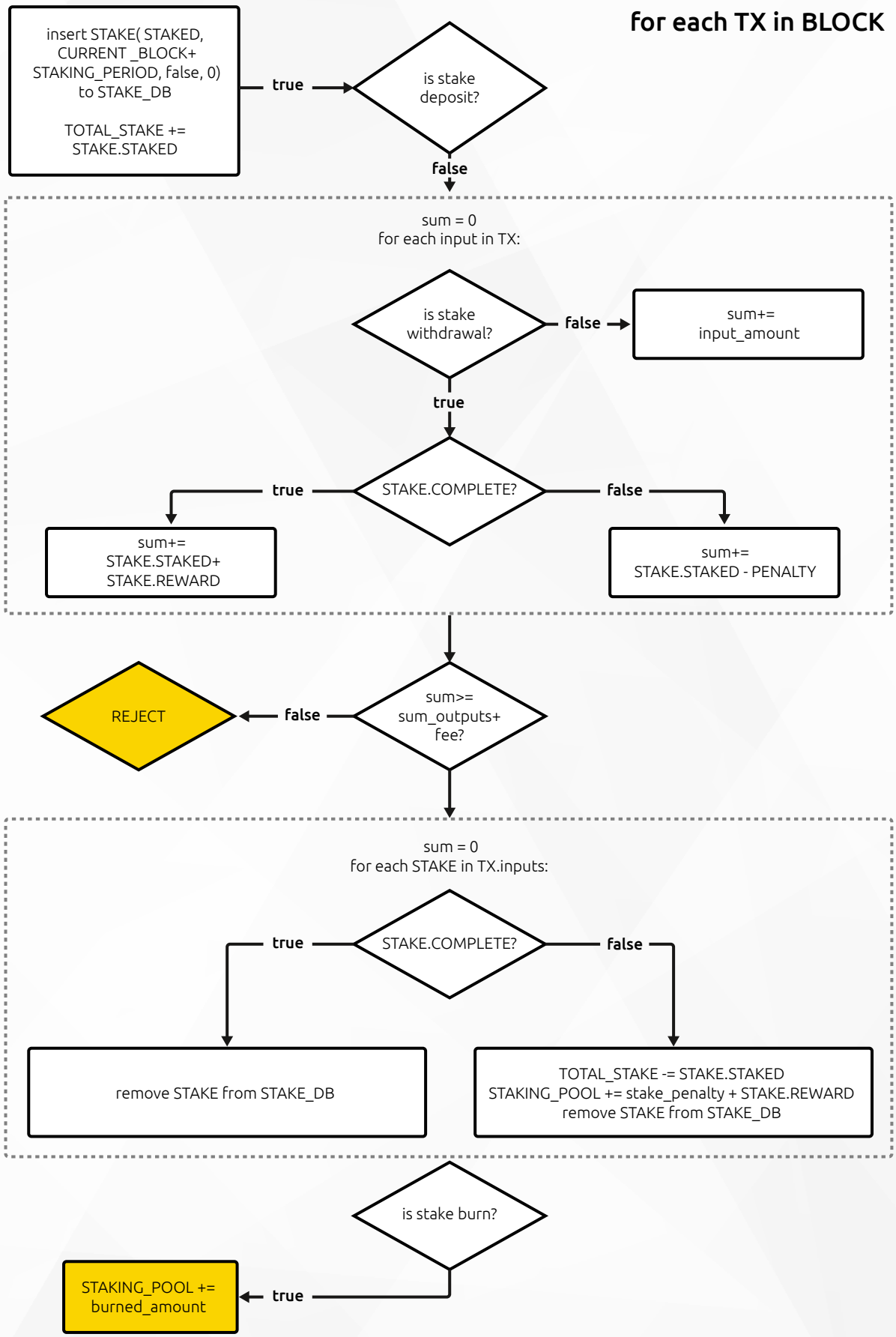


图 9。质押奖励池和用户的奖励更新逻辑

质押奖励 (SR) - 提前提款

在质押到期前提取质押的 ELCASH 的用户必须支付提前提款罚款 (EWP)，即质押值的 3%。

质押奖励 - 成功到期提款

对于每个区块，协议计算预期的质押奖励 (PSR) 和最大可能的质押奖励 (MPSR)

MPSR 等于当前日期可使用的质押池部分 (例如，总质押池储备的 1/180)。通过将 MPSR 除以 180，将保证用户获得更长时间的质押奖励 (180 是任意选择的天数，其目的是确保质押奖励的变化尽可能小)。PSR 是体系应根据所有活跃的质押协议支付的奖励的总和。

从池储备中扣除已使用的质押池储备金额。如果潜在质押奖励 (PSR) <最大可能的质押奖励 (MPSR)，每个用户将获得合同奖励金额 (即每年 5/6/7.25/10%)。如果潜在质押奖励 (PSR) > 最大可能的质押奖励 (MPSR)，则必须计算限制因子 (LF)。LF 确定了当天可提供的最高每日支出。这个过程对所有用户的影响与他们的质押金额成比例，并可能导致略有不同的奖励。这确保来看在质押奖励池中始终有足够的资金来奖励所有质押人。

2.1.7. 管治权力与免费交易

参与 ELCASH 质押让用户可以获得额外好处，如管治权力和免费交易。管治权力 (governancepower, GP) 是基于用户的质押值和质押期限生成的不可转移的值。它允许用户参与 ELCASH 管治投票并制定新的管治提案。免费交易的数量也取决于质押值和质押期限。限额按日计算，未使用的免费交易不累计。主要的假设是奖励最低质押 (4320 个区块 5 ELCASH)，每天一次免费交易。

将在相应章节中详细介绍管治权力和免费交易计算的所有具体细节。

2.1.8. Staking Explorer（质押资源管理器）

质押数据和网络性能之后，可以将 Staking Explorer（质押资源管理器）与管治仪表板结合在一起。实现交易数据和质押数据实时更新。用户可以很容易地获得一般的统计见解，如总网络质押，SRP 实时状态和一般网络分析检查。

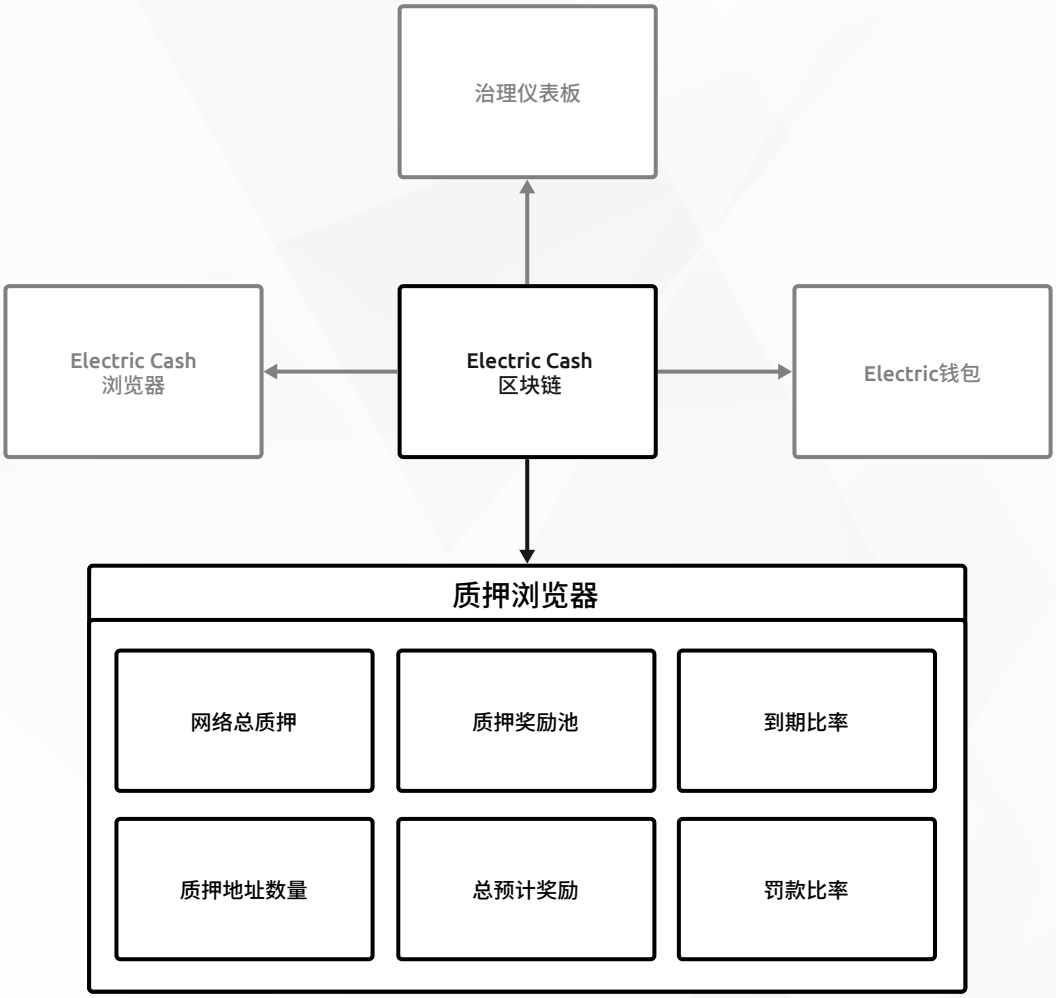


图 10。Staking Explorer（质押资源管理器）概述

2.1.9. 安全

Electric Cash 质押是一个安全的过程，因为所有质押参数都嵌入到区块链协议中，整个质押过程是自动的——Electric Cash 开发人员在任何时候都没有对资金的托管权。开发人员无法干预钱包中的资金（包括支出钱包和质押钱包），团队也不会以任何方式使用质押资金从中获利。

用户是唯一一个有权同时使用质押钱包和支出钱包中的资金的人。

开发人员无权访问质押奖励池。SRP 是一个由协议自动更新的值，并显示在质押资源管理器中。

2.2. 管治体系

为了实现直接民主，Electric Cash 实行管治体系。在管治过程中，可以提出、设计、商定和实施最新的变更。变更不仅限于区块链源代码技术细节，还可以涵盖其他重要的网络和社区问题。使用区块链的内置投票机制，用户可以对社区成员和/或 Electric Cash 核心管治团队提出的提案进行投票。

管治的重要性

区块链管治不仅仅是对社区的象征性管理。它也是区块链生态系统的一个重要元素。它使项目更加透明和易于管治。在 Electric Cash 中引入管治体系使项目更具竞争力，因为决策可以更快、更好地满足市场和用户需求。

加密市场的成功离不开利益相关者的参与。加密货币通常是建立在开放源代码的基础上的，这种代码很容易复制，而且它们唯一的不同就是项目支持人相异。社区必须被视为每个区块链生态系统中最重要和最独特的部分。

2.2.1. 管治权力 (GP)

在 Electric Cash 协议的质押过程中，网络参与者（质押人）获得管治权力（GP）。管治权力直接受质押参数的制约：

质押的值越高，质押期限越长，质押人对生态系统的投票权（管治权）就越多。

管治权力是不可交易和不可转移的，它创造了一个由“风险共担”的可信用户组成的生态系统，这些用户的质押更多，质押期限更长。该体系旨在确保更多的 GP 只提供给 ELCASH 社区最活跃、贡献最大的成员。 因此，如果用户在网络中不再活跃，他们获得的管治权力将随着时间的推移而改变。

Electric Cash 管治体系的目标是创建一个项目，即：

- **去中心化：**每个网络用户都可以参与管治。每个质押人都可以提出提案并投票；
- **透明：**所有投票结果及其实施阶段都可以在 Governance Explorer 站点上查看；
- **安全和隐私：**所有用户都可以匿名投票。区块链网络仅显示参与管治过程的用户的钱包地址。

2.2.2. 计算管治权力 (GP)

管治权力是用来奖励最重要和最活跃的网络参与者的。每一个质押 Electric Cash 的用户都将获得管治权力 (GP) 。管治权力因子取决于以下参数:

1. **质押金额——**质押的 ELCASH 越多，用户在质押期间获得的管治权力就越大。
2. **质押时间——**由于长期质押对网络更为有利，因此质押时间越长的用户获得的收益就越多，即用户一次质押时间越长，连续时间越长，获得的 GP 就比那些反复质押的用户多，即使累计质押时间相同。
3. **协议对生成 GP 的最低要求:** 5 ELCASH 质押 1 个月获得 1 个 GP

GP 不是一种独立的币。它是一种与用户的 Electric Cash 地址相连的非货币权利，不可交易且不可转移 (从钱包到钱包) 。

2.2.3. GP 销毁和铸币方法

为了维持一个健康的网络，每次投票和提案都要求用户使用自己的 GP 作为“支付”方式，这样可以保护 Electric Cash 区块链不被阻塞。在投票过程 (图 11) 和提案创建 (图 12) 中，每个用户都需要使用所选的 GP 量 (满足给定的最低要求) 。在这个过程中使用的 GP 将被销毁，而不是被转移。在区块链中销毁意味着从网络中移除给定价值的资产。在这种情况下，用于“支付”提案的 GP 不会被转移到另一个地址，而是被协议“销毁”，因此没有人可以再访问它。

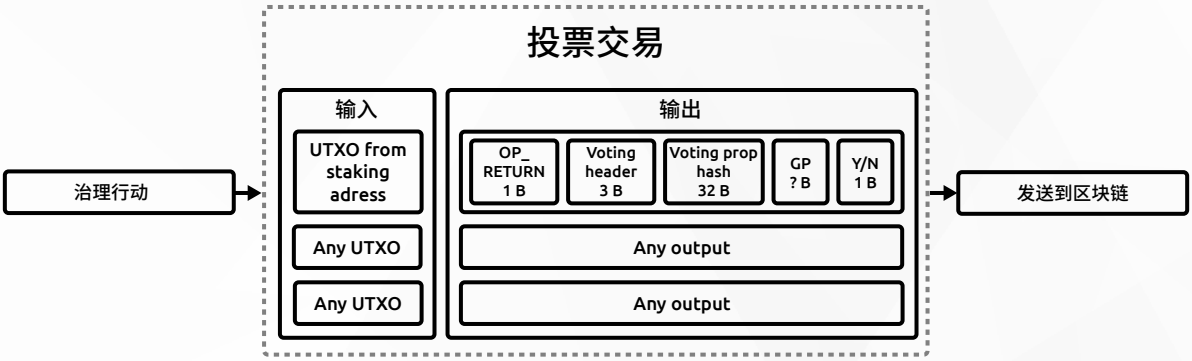


图 11。投票过程

当用户投票时，将创建投票交易。区块链保存用户的地址、使用的 GP 数量和选择的选项。投票结果是根据用户进行的所有投票交易计算的。

MintGP 方法允许用户获得额外的 GP 奖励。铸币创建了一定数量的额外 GP，因此 GP 不是从任何地址发送的，而是由协议创建的。

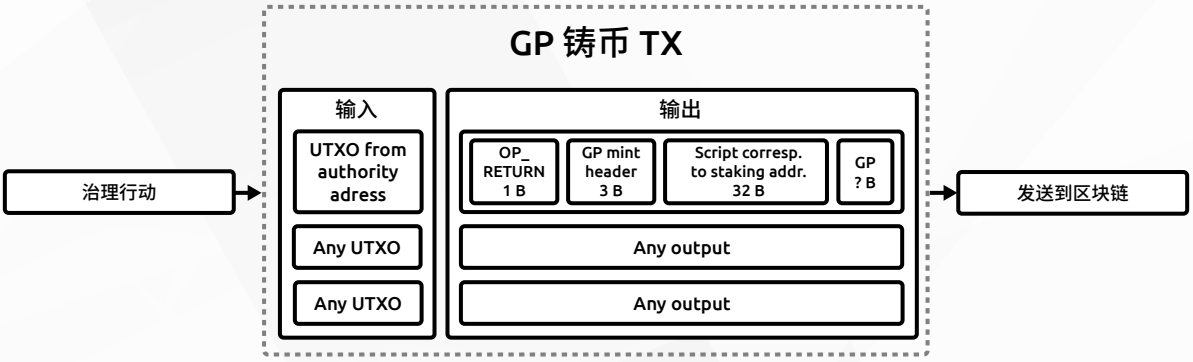


图 12。管治权力铸币过程

当用户执行符合 GP 回报条件的操作（投票或创建成功的提案）时，区块链执行 GP 铸币交易。输入来自授权地址，一个特殊的硬编码地址，它通知协议需要输入一定数量的 GP。

2.2.4. 创建提案

Electric Cash 社区决定了币的经济性和生态系统。每个用户都可以创建一个新的提案，然后进行网络投票。成员们不仅可以对附加功能进行投票，还可以对 Electric Cash 挖矿参数进行投票，比如币的最大供应量，这将有助于 ELCASH 在未来开发出具有竞争力和最新的项目。

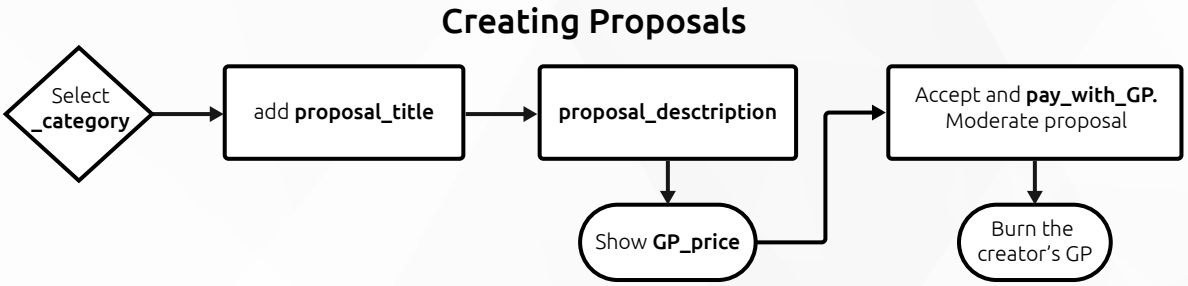


图 13。Electric Cash 管治提案创建机制。

可以使用电子钱包创建提案。但是，为了防止网络过载并强制执行提案的更改，创建新的提案需要用户使用其管治权力。提案的初始价格为 304 GP。这一数值可以在将来根据网络的需要进行更改。

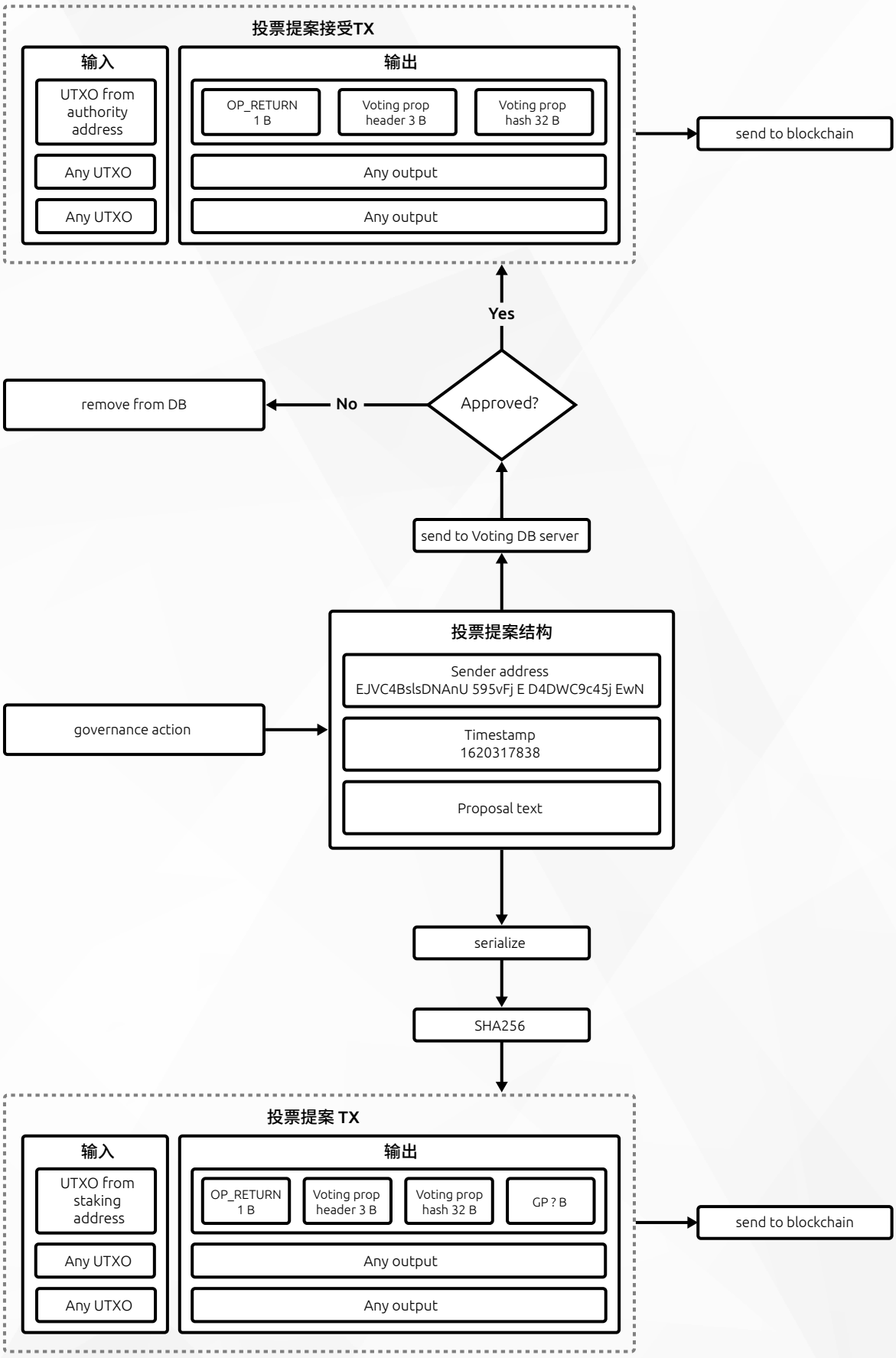


图 14。投票提案创建过程

当用户创建提案时，所有数据（发送者地址、时间戳和提案文本）都会被散列，并通过一个特殊的投票提案交易发送到区块链。同时，提案数据也被发送到外部投票数据库。这个过程是透明和安全的，因为每个用户都可以将来自数据库的提案哈希与发送到区块链的哈希进行比较，以确保没有人对提案数据进行更改。提案经过审核后，投票就开始了。

2.2.5. 提案生命周期

社区和 ELCASH 开发人员都可以提交提案。新提案只能在开放的投票窗口添加，使整个投票过程更易于管治和遵守。提交后，社区提案由 ELCASH 团队进行审核，以排除任何恶意或非法提案。已批准的提案将被添加到 active_proposals_list 中，并且可以进行投票。如果投票人投票赞成提案，它就通过了，然后，ELCASH 团队决定是否将其添加到团队的待办事项中。

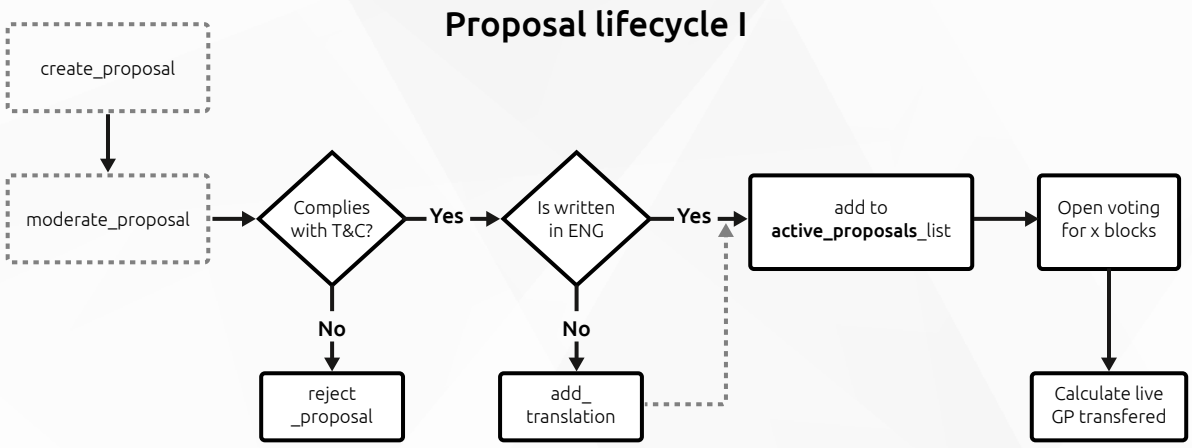
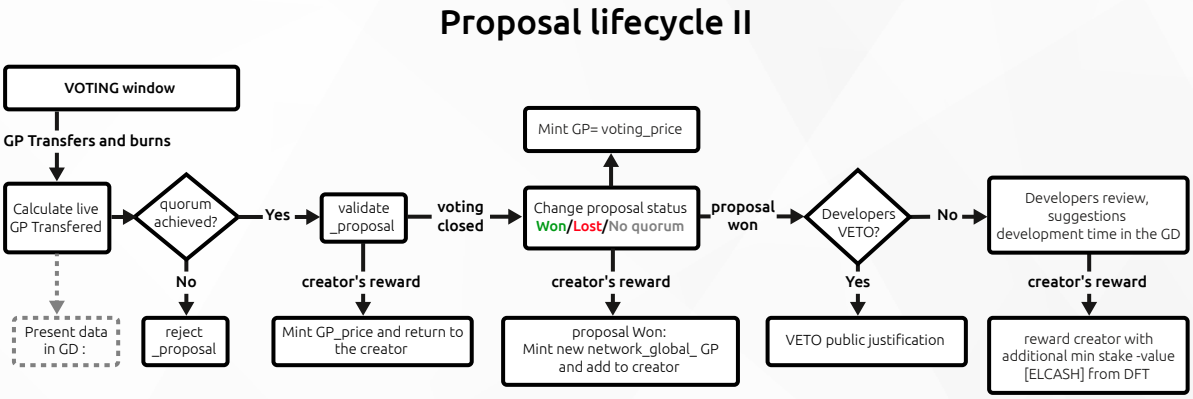


图 15。Electric Cash 管治提案生命周期 1/2

一旦提交了创建和积极审核，每个提案都会立即显示在桌面管治仪表板（GD）上，并可以在电子钱包中进行投票。每个提案都有相同的投票窗口，所有转移的管治权利都在此时实时计算。



16。Electric Cash 管治提案生命周期 2/2

在 voting_period，每个提案都有相同的生命周期。提案经过审核后，首要任务是实现网络法定人数。如果所有 network_global_GP 的 15% 被转移到提案中（赞成票和反对票），则达到法定人数。达到法定人数意味着在网络上有很多的兴趣，因此，创建者获得提交提案所支出的 GP 的 80%（0.8*proposal_GP_price）。这一“回报”是使用“铸币”方法计算的。如果提案在整个投票期间未达到法定人数，则该提案将被拒绝，用户将失去在提交提案过程销毁中的

GP。这种方法鼓励用户只提交最相关的提案，并通过其他专用沟通渠道与其他网络参与者就提案进行沟通。

在投票期间，网络将在管治仪表板和电子钱包上显示链上提案数据，详细信息如下:

投票期结束后:

- 每个提案都会将其状态更改为以下状态之一:
  - **WON** (GP transferred for majority vote – yes)
  - **LOST** (GP transferred for majority vote – no)
  - **NO_QUORUM** (GP_transferred for vote –_yes & vote -_no < 15% of network_global_GP)
- 如果提案状态 = WON，提案创建者将收到额外的铸币 Gp，其值为 0.01*network_global_GP。这一规则清楚地表明，网络中 GP 的全球价值增加不仅仅是因为新的质押币。
- 开发人员可以使用否决权的方法。在必要的情况下，由于币代币经济规则及其开发，开发人员可以使用否决权，不接受社区选择的方案。使用否决权的原因必须始终由开发人员团队使用管治仪表板上的专用面板进行适当的分析和证明。但是，如果提案达到了 WON 的状态，即使提案被否决，用户也会得到奖励。

2.2.6. 管治审核

所有新提案都由 Electric Cash 团队负责审核，以确保所有提案都是为了网络利益而制定的，而不是出于恶意甚至非法目的。如果一个提案被认为是恶意的，它将被删除，并且不进行投票。

如果 Electric Cash 团队批准了一个提案，就可以进行投票，并且可以在管治仪表板上查看。

当提案以非英语语言提交并由 Electric Cash 团队翻译时，也应进行审核。这意味着这些提案可以稍有延迟地进行投票。有鉴于此，整个社区将始终看到提案说明的原始版本，以及管治仪表板上的同等英语版本和电子钱包中的简化 GD。

2.2.7. 投票

在质押过程中获得管治权力的每个用户都可以对管治仪表板上显示的建议进行投票。投票开放时间为一个区块的投票时间，相当于从提案公布之日起约 4 周。投票结束后，每个用户都可以在管治仪表板上查看结果。

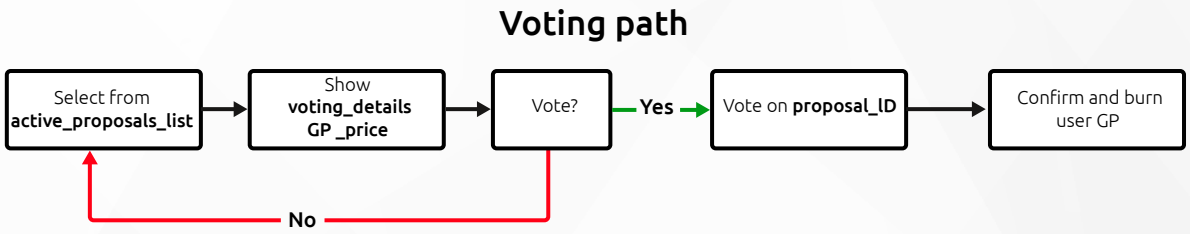


图 17。Electric Cash 管治投票机制

投票也需要支付 GP。然而，每增加一次投票，价格就会改变。给定用户的第一次投票被设置为 1 GP 的成本。

任何进一步的投票都需要一个二次方值:
GP_price = x²,
其中 x – 投票数
(即第二票 - 4 GP, 第三票 -9 GP, 依此类推)。

这样的解决方案确保了最大的质押人不会控制网络, 因此每个用户对社区都有同样的重要性, 使 ELCASH 真正民主。

2.2.8. 管治仪表板

为了提高 Electric Cash 项目的透明度, 让每个人都可以跟踪管治过程(即使没有专用的钱包), 管治仪表板已经创建。它是一个专门的网站, 提供有关管治的最重要信息, 包括所有现行和过去的提案、投票结果、投票人活动、网络管治权力和其他参数

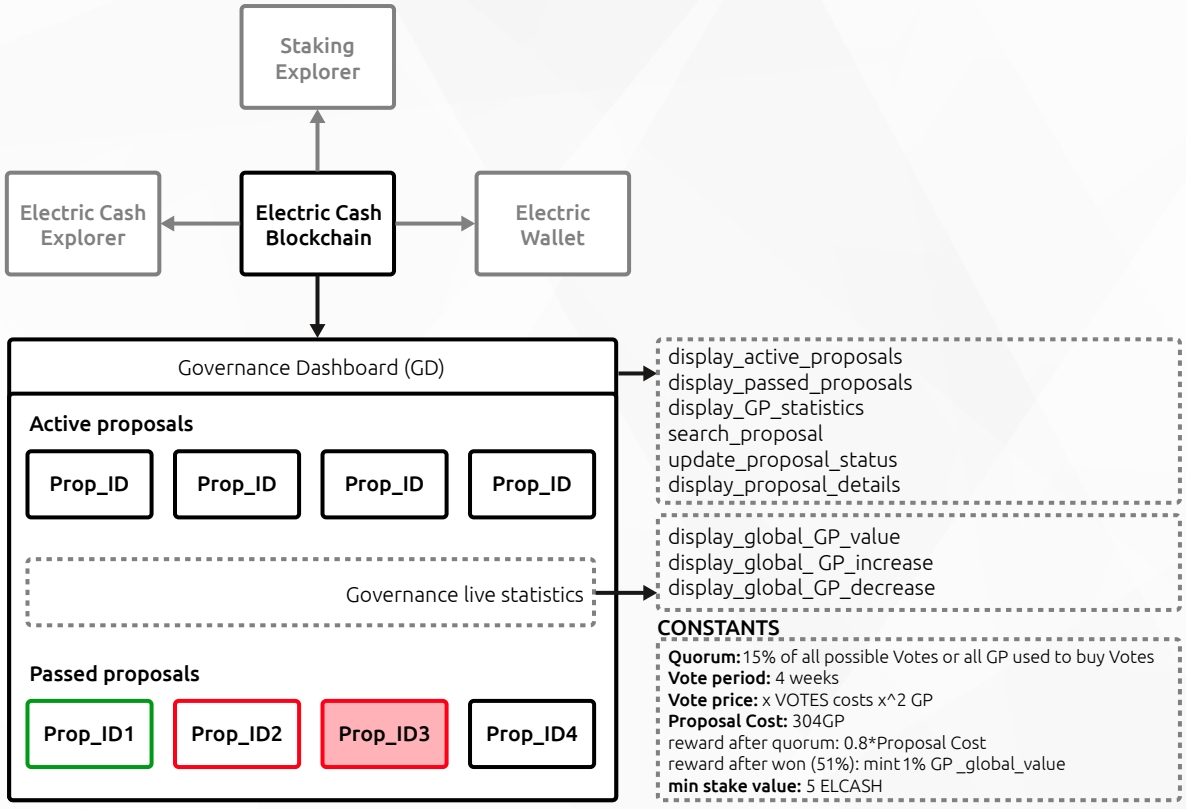


图 18。 Electric Cash 管治仪表盘概述

通过的提案 (voting_period 后) 分为四种状态:

表 3。可能的提案状态

Prop_ID1	Prop_ID2	Prop_ID3	Prop_ID4
WON	LOST	VETO	NO QUORUM

管治仪表板也是一个很好的媒介, 可以交流想法和联系开发人员, 他们可以对每个 WON 提案发表意见, 或者证明他们的决定是正确的。

2.2.9. 提案执行

为了确保网络安全，特别是在早期，管治提案不会自动执行。ELCASH 团队负责验证所有提案，并选择对网络影响最大的提案。

2.3. 合并挖矿

在开发的早期阶段，ELCASH 将采用合并挖矿方法。在这种情况下，ELCASH 可以利用更大的基于 SHA-256（类似于比特币）链的散列能力的链，确保新网络的整体安全。

合并挖矿是通过比特币实现的，因为两种加密货币使用相同的 SHA-256 散列函数。在这种情况下，BTC 是父链，ELCASH 是辅链。因此，比特币的（父）工作量证明解决方案可以用来验证 ELCASH（辅链）是否采用了辅助工作量证明（AuxPoW）共识机制(7)。

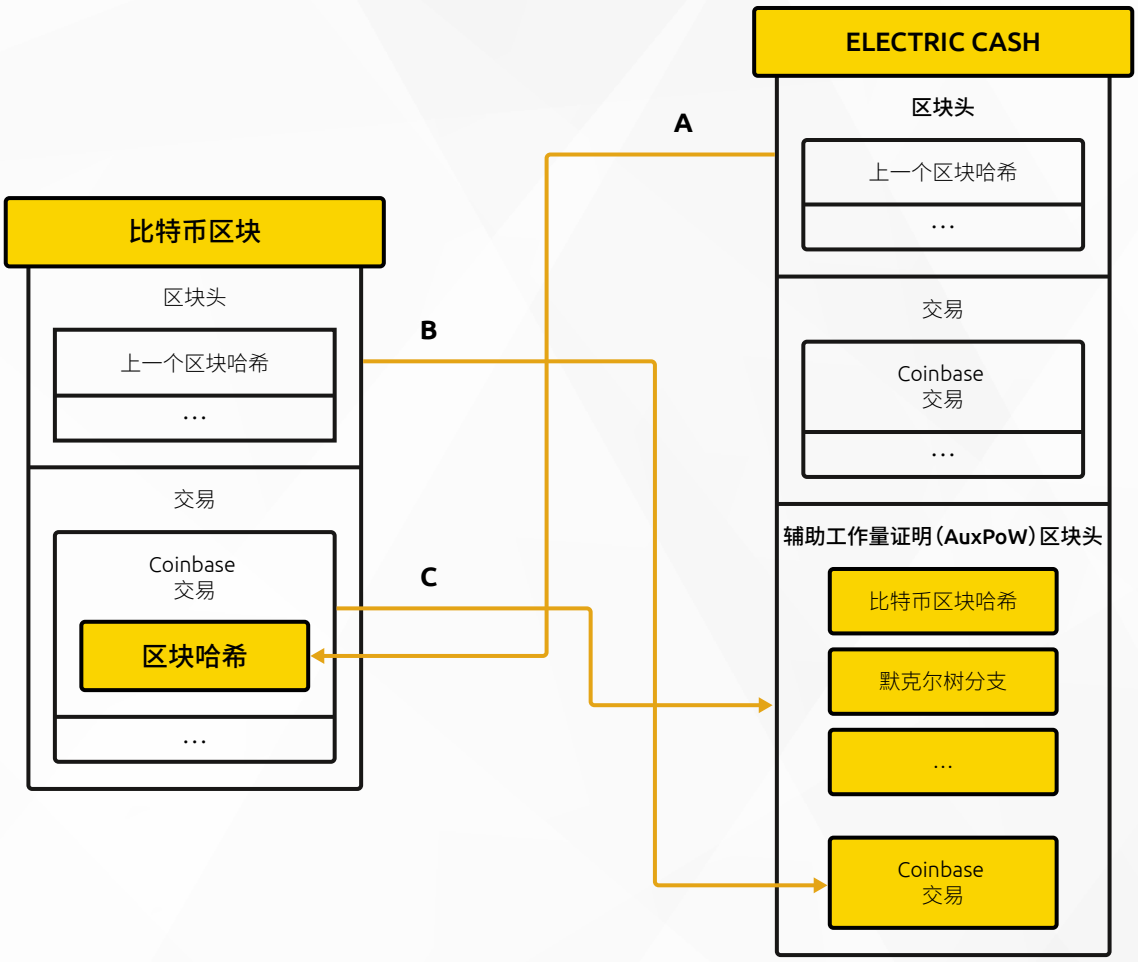


图 19。在 Electric Cash 中合并挖矿区块的结构。

合并挖矿对于新区块链（如 ELCASH）来说是一种很好的方法，可以提高安全性并减少 51% 的攻击。在生态系统中实施集成挖矿架构让我们相信 ELCASH 符合当前的行业安全标准。

3. Electric Cash 基础架构

Electric Cash 是一种支付协议，旨在实现可访问性和轻量级，重点是降低交易费用，并且可以几乎无缝集成到日常使用中去。 在安全和中心化的网络中进行快速和免费的交易，这使得 ELCASH 成为日常支付的理想之选。

3.1. 快速交易层级

为了实现快速交易，区块链需要足够的区块容量来包含所有等待确认的交易，并尽快将交易通知网络。快速交易是实现全球采用的关键，但在传统的工作量证明区块链中，由于安全原因，很难实现即时交易。交易的接收者需要等待协议在下一个区块中添加交易，这受到挖矿难度的限制。平均来说，一个新的 ELCASH 区块挖矿大约需要 10 分钟。采用这种方案，可以方便快捷地向朋友转移币，但对于零售支付来说就不是很理想了。这就是 ELCASH 采用快速交易层级的原因，它将转移币所需的时间缩短到 10 秒左右，使 ELCASH 成为区块链行业的领导者。具体时间可能因网络拥塞而有所不同。

在网络的顶部创建了主节点的快速交易层级（第 2 层级），以提高交易速度。主节点查验新创建的交易是否有效，并确保该交易是不可逆的，甚至在通过质押输入并与所有节点共享有关它的信息而添加到新块之前也是如此。得益于此，网络将适用于新挖矿区块的交易。

图 20。Electric Cash 区块链生态系统的架构 (8) 。

这种快速层级解决方案可以实现快速交易，并确保高级别的网络安全。使用第 2 层级将交易传播到主区块链，交易在 PoW 矿工批准之前得到确认。Electric Cash 网络上的所有交易都由快速交易层级处理，这意味着所有 Electric Cash 交易都是快速的，不需要额外的交易费用，也不需要用户执行任何特殊操作。

每笔交易的过程类似于标准交易验证，但它包含几个附加步骤，其中主节点锁定交易 (图 21) 。

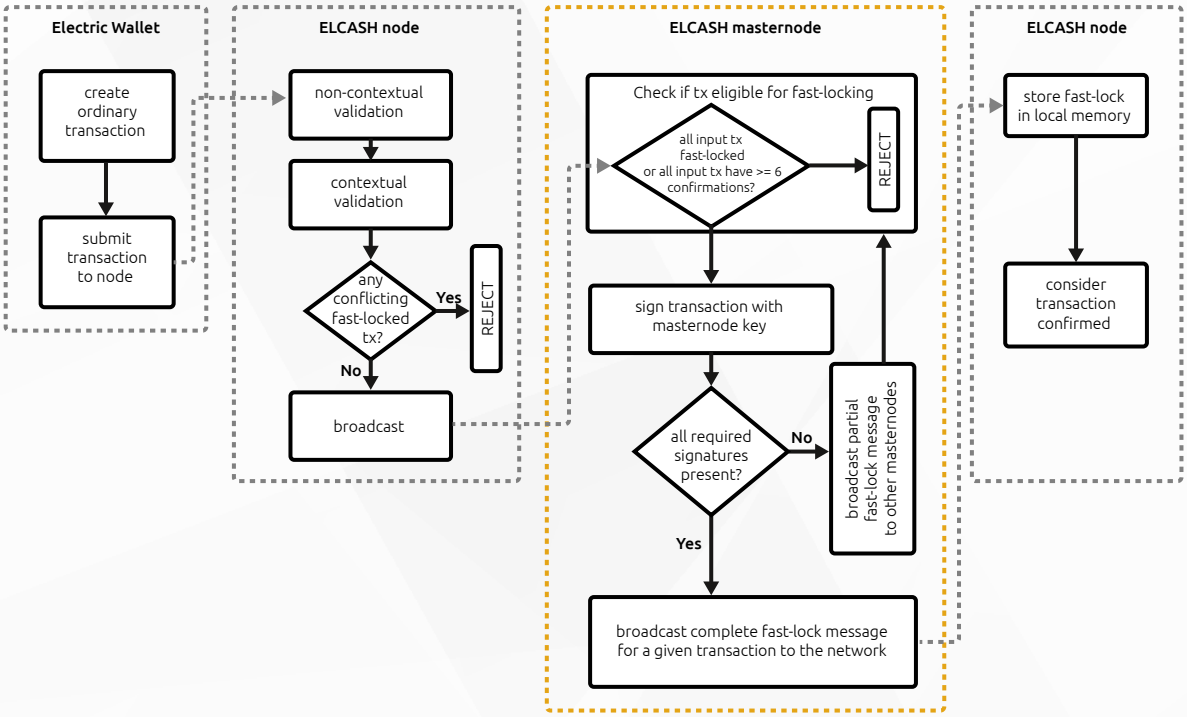


图 21。快速交易确认流程

用户在钱包中创建新交易后，该交易将被提交到 ELCASH 节点。该交易将被验证，如果没有冲突的交易，则该交易将由 ELCASH 节点发送到 ELCASH 主节点，否则该节点将拒绝该交易。主节点查验交易是否符合快速锁定的条件。如果交易被批准，则由主节点使用主节点密钥对其进行签名。这就防止了资金的重复支出。交易的输入被锁定，因此它们只能在特定的交易中使用，一旦交易被锁定，就不可能两次发送相同的资金或以任何方式更改交易。通知所有节点交易已锁定，它将与下一区块一起添加到区块链中。

如果主节点层级在锁定上达成共识，则所有冲突交易或冲突区块都将被拒绝，除非它们与相关锁定的交易 ID 匹配。

得益于该解决方案，在日常生活中使用 ELCASH 会方便得多，无论是在商店里买东西还是只是把 ELCASH 转给朋友。此外，Electric Cash 区块链仍以安全的工作量证明共识机制为基础。

3.2. 免费交易

加密货币，无论多么安全，使用起来往往很昂贵，特别是当项目越来越受欢迎，网络使用增加。这就造成了这样一种情况：项目越受欢迎，使用成本就越高。更少的新用户愿意参与，因此阻碍了项目的发展。为了实现全球采用，项目需要达到一个临界量，即一定数量的用户，吸引新用户加入。像加密货币或社交媒体平台这样的项目对于每一个新用户来说都变得更加有用，因为人与人之间的联系更加紧密。实际上，如果项目的网络用户越多越多，但是交易费用却不断上涨，就很难实现，甚至不可能实现，全球采用 (9)。

在这方面，通过 Electric Cash 进行交易可大力推动加密货币的大量采用。Electric Cash 实施的快速、免费解决方案不仅与其他区块链项目展开了竞争，还与传统金融机构进行竞争。

3.2.1. 免费交易验证机制

得益于区块链架构实现了免费交易：在质押过程中，质押人生成了“免费交易限额”来进行支出。费用被应用到交易中，这将使恶意网络攻击更加难以实施。然而，质押用户将有资格进行几笔免费交易，具体数量取决于质押资金和质押期限。

免费交易与正常交易略有不同。免费交易包含关于发送者的质押 UTXO 的附加信息，以确认用户有资格进行免费交易（图 22）。

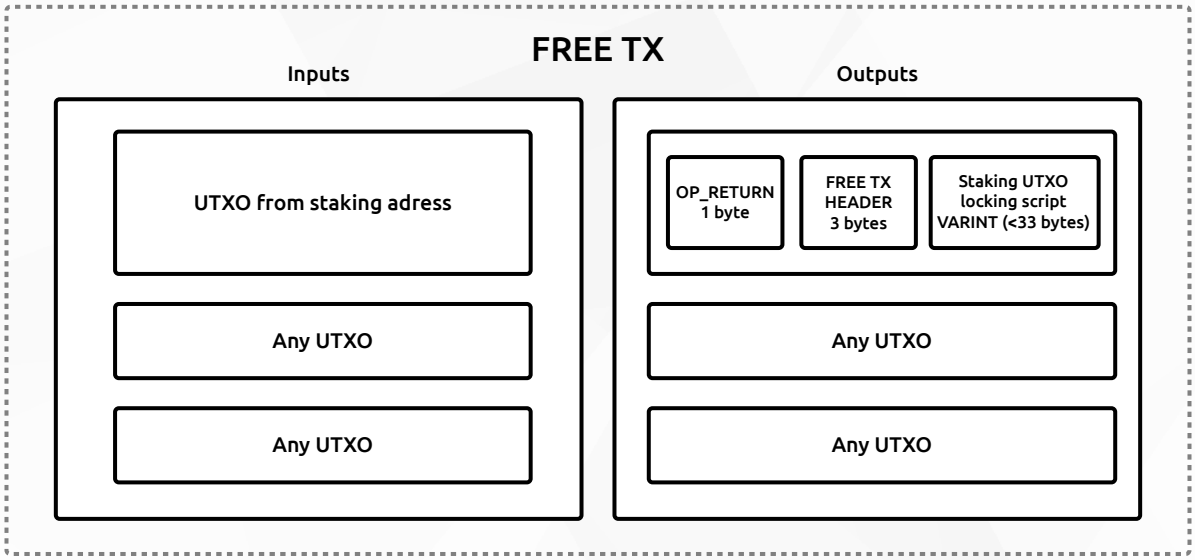


图 22。免费交易结构

非上下文验证规则：

1. OP_RETURN + 免费 TX 报头是 tx 的第一个输出
2. 所有正常的交易规则

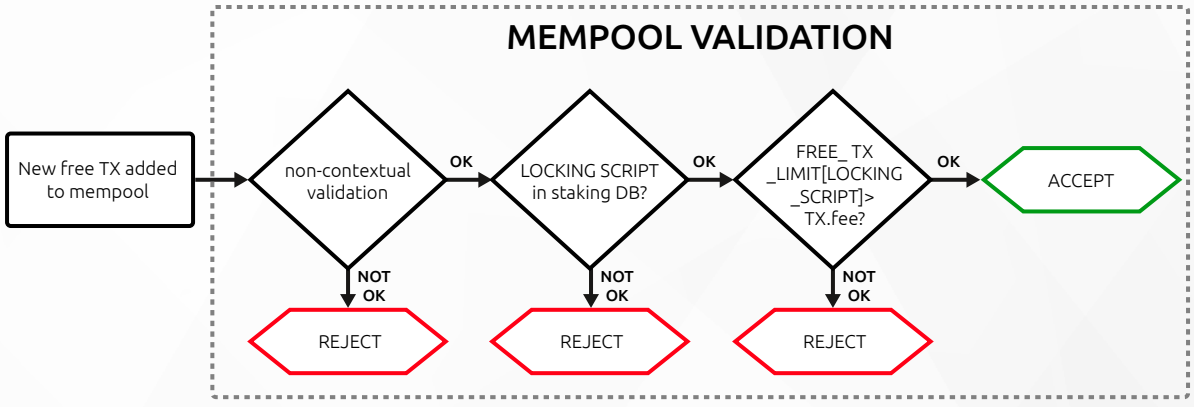


图 23。免费交易内存池验证

与所有其他交易一样，免费交易在内存池中等待添加到新区块。但是，除了标准验证之外，还会查验发送者是否有资格进行免费交易。如果交易无误，并且发送者是具有足够免费交易限额的质押人，则接受该交易并将其添加到新的区块中。

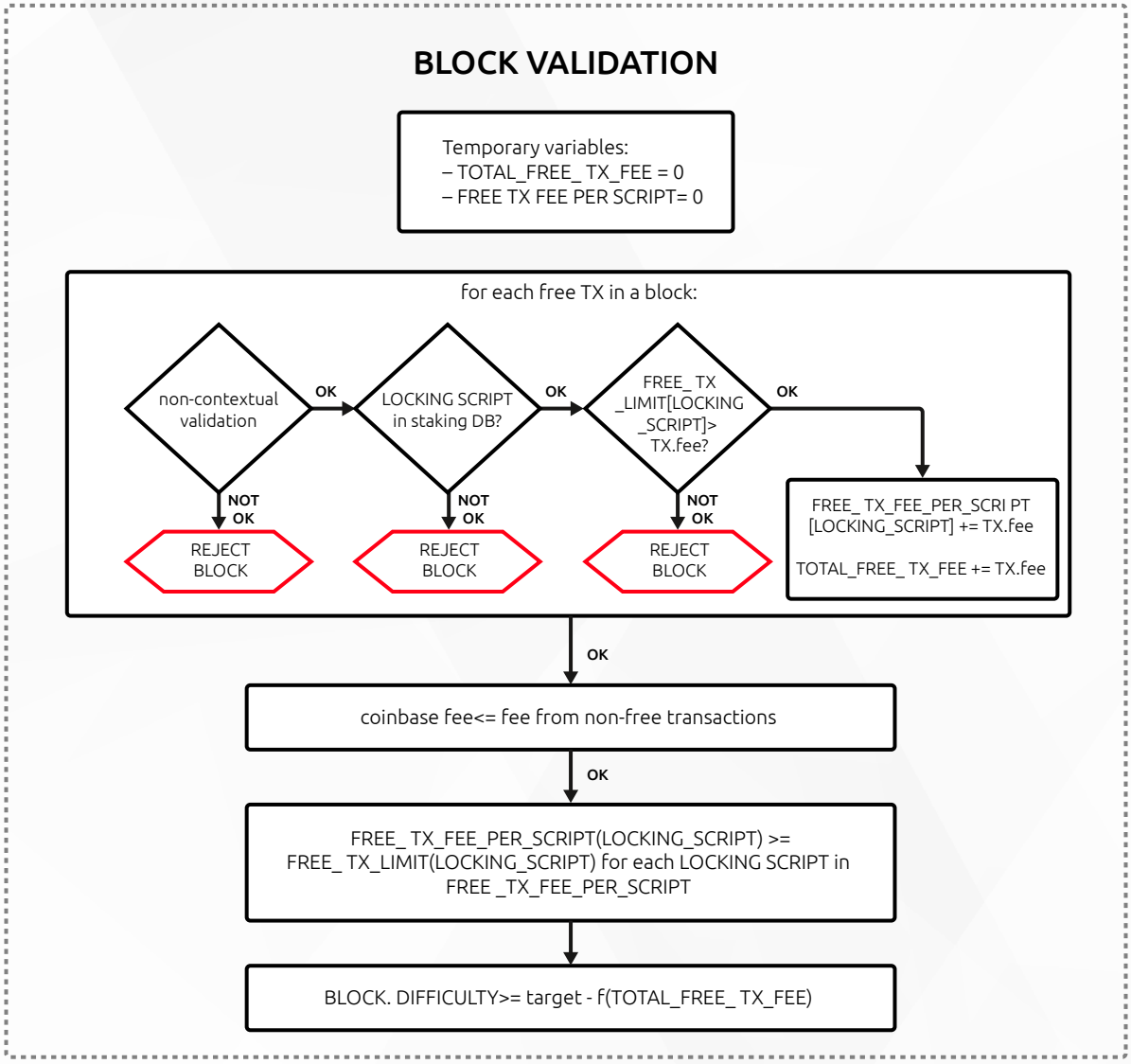


图 24。区块难度计算

对于新区块中的每笔免费交易，协议计算如果交易不免费将收取多少费用，并将所有预估费用相加（图 24）。对于接受免费交易进入区块的矿工将给予报酬，区块难度根据免费交易的预估费用总和降低。

ELCASH 免费交易限额

ELCASH 区块链要收取交易费用，但每个质押 ELCASH 的用户每天都有资格进行几笔免费交易。免费交易限额取决于用户的质押参数。

这有助于保持网络安全，防止恶意溢出，使攻击代价高昂，从而确保真正的用户能够进行免费交易。

如果不向矿工提供报酬，矿工就不需要承担额外的工作。如果要进行免费交易，挖矿难度将自动与区块中包含的免费交易值成比例降低。**因此，矿工的全部和最终区块奖励在任何意义上都不会受到免费交易的影响，矿工的额外工作将得到相应的奖励。**

限额计算

每一笔质押都有每日免费交易的限额。该限额取决于质押值和质押期限。
[tx_limit] ∈ N → STAKE_WEIGHT⩾1.

协议假设必须：质押权重 = 1（最低质押每日一次免费交易），并且一个月质押 5 ELCASH 也是最低限额所需的最低质押；

stake_weight = (stake_period[blocks])/4320×(stake_value[ELCASH])/(5 ELCASH)

例如：

12 个月质押 5 ELCASH：

stake_weight=510840/4320×5/5 ≅ 12 free tx/day

免费交易限额不叠加。当天未使用的限额不能在当天结束后使用。质押开始后用户可免费进行 20 个区块的交易。**质押结束或用户终止时，将无法继续进行免费交易。**

3.2.2. 免费交易，技术细节

免费交易语法

1. 其中一个输出是指向质押地址的元数据。
2. 其中一个输入来自点 1 所指的地址。
3. 这些交易不包含包括费用。不需要回报。

免费交易执行

1. 为了能够执行免费交易，需要进行一次性钱包设置（可以在押金质押时执行的内部交易）。
2. 用户必须指定一个质押地址，进而获得免费交易限额（可以通过钱包自动完成）
3. 用户必须至少有一个活动质押。

矿工薪酬

1. 矿工不会从免费交易中收取费用。
2. 包含免费交易的区块的难度要求将降低。特定区块的修正挖矿难度表示为：

MODIFIED_DIFFICULTY= (1-FTX×TXS_total)×PoW

FTX – 免费交易系数
TXS_total - 总区块免费交易数量
PoW – PoW 难度

3.3. 区块减少和奖励策略

Electric Cash 挖矿是从一个新的创世区块启动的。表 1 所示的策略旨在满足币的预期市场需求，同时防止早期供应过剩。

计划继续进行预挖矿，直到挖出 10% 的供应量，并将其分配给包括但不限于项目开发、营销、促销等的各种活动。

在开发早期，鉴于币及其生态系统尚未成熟，我们会尽最大努力避免出现任何意外活动。确保上述 10% 的 ELCASH 总供应量的计划还可以防止大量 ELCASH 潜在持有人操纵市场。

表 4。区块减少和奖励策略。

周期	日期	区块	区块奖励	币
1	2020 年 12 月	4,200	500	2,100,000
2	2021 年 1 月	52,500	75	3,937,500
3	2022 年 1 月	52,500	70	3,675,000
4	2023 年 1 月	52,500	65	3,412,500
5	2024 年 1 月	52,500	55	2,887,500
6	2025 年 1 月	52,500	40	2,100,000
7	2026 年 1 月	52,500	25	1,312,500
8	2027 年 1 月	52,500	15	787,500
9	2028 年 1 月	52,500	7.5	393,750
10	2029 年 1 月	52,500	3.75	196,875
…	…	…	…	…

这些预先挖出的币将用于各种活动，这些活动有一个主要目标：将潜在用户的注意力吸引到 ELCASH 生态系统上来。对于项目来说，将指定数量的币分配给营销和开发活动是一种常见且被广泛接受的解决方案。我们相信这个解决方案将为项目的开发提供一个健康的融资方式，并为区块链生态系统创造一个更加光明的未来。

预挖的的 Electric Cash 总供应量 10% 的用例示例：

- 宣传空投
- 业务拓展
- 质押人的额外奖励
- 营销工作
- 社交媒体广告
- 软件预算

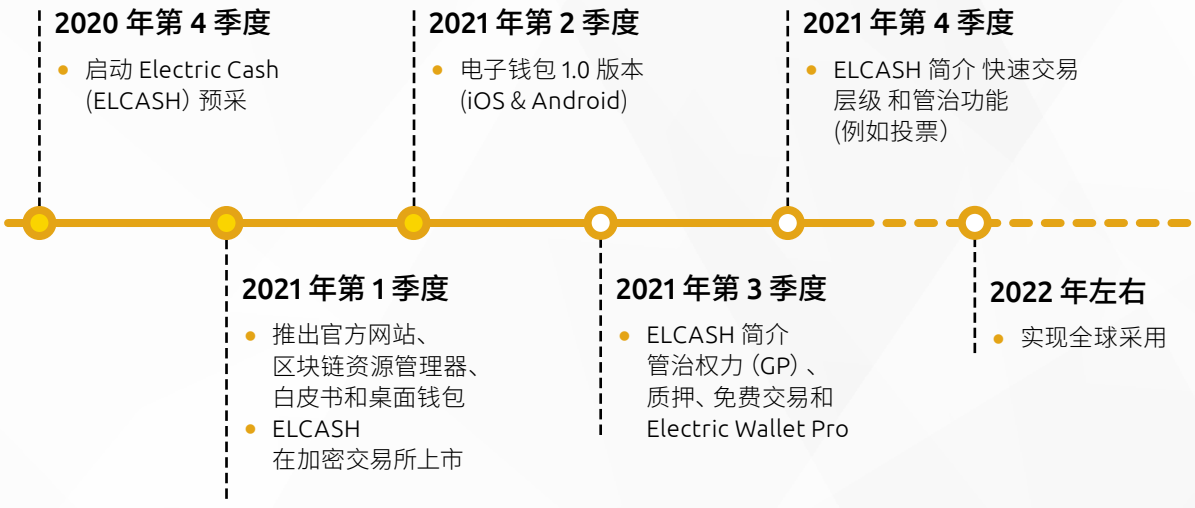
在第一年，区块奖励将达到 75 个币。以后会逐渐减少。七年后，网络将转向一种称为“减半”的奖励策略，从那时起，区块奖励每年减少 50%。

目前，Electric Cash 的总供应量上限为 2100 万枚币，与比特币的总供应量持平。固定供应量有助于最大限度地减少潜在的通胀和稀释。然而，如果项目在未来获得普及，并且对币的需求量增加，最活跃的网络用户将能够通过民主投票（得以管治体系工具）增加供应量——这可能会降低通胀率。

3.4. Development Treasury

ELCASH 项目开发了一个专用的 Development Treasury Fund，该“金库”占由 Electric Cash 管治体系管治的特殊钱包中收到的挖矿奖励的 10%。这些资金被安全保管，直到社区投票决定使用它们。它们可以用来支付协议完善和变更的成本，例如在 Electric Cash 生态系统中开发新功能。为了保持整个过程的透明性，所收到的资金的余额可以在 Governance Explorer 站点上查看。

Electric Cash 路线图



摘要

本白皮书介绍了 Electric Cash。项目的目标是提供一个全面的生态系统，并解决加密货币行业的几个主要问题。ELCASH 有助于促进日常支付。通过对区块链实施额外的第 2 层级，可以在确保网络安全的同时执行快速交易。得益于这种解决方案，可以在约 10 秒（视网络拥塞情况而定）的时间内完成 ELCASH 交易，这使得 Electric Cash 网络成为区块链行业的领导者之一。用户不需要采取任何额外的操作来发送快速交易，默认情况下所有交易都是快速的。

ELCASH 协议旨在实现可访问性和轻量级，重点还在于降低交易费用。所有质押参与者都会获得享受免费交易的奖励，具体笔数视总质押金额和质押时间而定。快速和免费的交易使得 ELCASH 非常适合于小额的日常支付，这为加密货币的全球应用创造了许多机会。

生态系统不仅带来了快速和免费的支付，还带来了额外的好处，比如管治权力。通过积极参与网络，每个币持有者都获得了管治权力（GP），并可以对协议的更改产生直接影响。GP 的分配取决于用户的质押参数和网络活动。它赋予参与管治进程和对现有提案进行投票的权利。得益于社区管治，项目能够快速响应市场需求并更快地引入变革。我们相信，这种去中心化和以社区为中心的生态系统将能够健康增长和实现未来的全球采用。

资源

欲了解更多有关该项目的信息，请访问：

官网: electriccash.global
Twitter: twitter.com/elcash_official
Telegram: t.me/elcash_official
Facebook: facebook.com/electriccash.official
GitHub: github.com/electric-cash
YouTube: youtube.com/c/ElectricCash

参考资料

1. Nakamoto, S. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf: 无名氏, Oct 2008年.
2. N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas. Stochastic models and wide-area network measurements for blockchain design andanalysis. IEEE Conference on Computer Communications: IEEE INFOCOM, 2018.
3. A Next-Generation Smart Contract and Decentralized Application Platform. [联机] 2020年December月. https://ethereum.org/en/whitepaper/.
4. N Papadis, L Tassiulas. Blockchain-based Payment Channel Networks: Challenges and Recent Advances. New Haven, CT 06511 USA: Department of Electrical Engineering, and Yale Institute for Network Science, Yale University, 2020.
5. N Kshetri, J Voas. Blockchain-Enabled E-Voting. University of North Carolina at Greensbor: IEEE SOFTWARE, 2018.
6. L Gudgeon, P Moreno-Sanchez, S Roos, P McCorry. SoK: Layer-Two Blockchain Protocols. London: Imperial College London, 2019.
7. Zamyatin, A. Merged Mining: Analysis of Effects and Implications – DIPLOMA THESIS. 无出版地: TU Wien, 2017年.
8. Shapiro, C. Information rules: a strategic guide to the network economy, 1999.
9. Shapiro, C. Information rules: a strategic guide to the network economy, 1999.