

# Edgeware: 一种自适应智能合约区块链

联邦实验室 (founders@commonwealth.im)

2019年2月25日, 草案版本 V 1.02

## 摘要

Edgeware是一种相当成熟、管理积极的智能合约平台。它整合了一些高级功能, 如股权证明验证、网络装配智能合约以及用于链上身份辨别和治理的接口。

通过将余额分配给其他对其代币进行时间锁定的加密货币持有者, Edgeware确保了早期利益相关者社区的安全, 这些利益相关者被激励参与网络的治理。

使用由社区管理的区块奖励和链上管理过程, 利益相关者对升级提议进行投票。此治理过程用于资助、管理和部署网络改进, 创建一个自我改进的系统, 以协调和支持其自身的开发。

## 内容

### 1 引言 1

### 2 技术规范 1

2.1 模块 .....	2
2.2 合约 .....	3
2.3 共识 .....	4
2.4 获得股份 .....	4
2.5 余额和账户 .....	4
2.6 Edgeware 代币 - EDG .....	5
2.7 互操作性 .....	5

3 网络启动.....	5
3.1 锁定合约规范 .....	6
3.2 锁定参与.....	7
3.3 初始区块 .....	8
4 治理	8
4.1 治理模块 .....	9
4.1.1 信令 .....	9
4.1.2 身份 .....	10
4.1.3 民主 .....	12
4.1.4 理事会 .....	13
4.1.5 司库 .....	13
4.2 治理接口 .....	14
4.3 治理程序 .....	14
4.4 实验平台 .....	15

5 结论	15
------	----

## 1 引言

公共区块链已经使得创建“不可阻挡的应用程序”成为可能，这些应用程序在共享计算环境中运行，在开放数据上操作，并且不能被任何一个中央中止。

许多令人兴奋的应用程序已被提议建立在这种基础设施之上，包括数字现金的形式、用于借贷和证券化的金融工具、以及最大限度减少寻租和最大化互操作性的市场。虽然区块链应用的潜力令人兴奋，但它们受到许多挑战的限制。特别是，将区块链扩展到相当大的吞吐量水平需要大量的技术进步，包括构建高效的运行时、节点间区块的快速路由、通过侧链和状态通道将计算从链中移出以及横跨多链的切分。

Edgware旨在通过采用一种根本不同的架构来解决可扩展性问题。Edgware代币

持有者可以使用链上投票来投票升级网络，之后节点自动下载新的运行时版本。关键决策是在链上做出的，创建一个协调开销较低的系统，以及一个决定改进的透明过程。

## 2 技术规范

Edgeware是一个智能合约区块链，可编译为客户端运行时，一组可以在本地构建和运行或在Wasm虚拟机中执行的网络装配（WASM）代码块。无论哪种方式，当编译Edgeware本机二进制文件时，它都包含一个Wasm虚拟机，该虚拟机可用于执行从网络下载的客户端运行时的更高版本。

客户端运行时与网络代码和由奇偶校验基板提供的其他组件进行接口。基板包括libp2p网络、PBFT共识和股权证明区块验证和最终性证明[4]。最终，客户端仅负责从网络下载、执行和验证区块。

区块定义如下：

- Header := Parent + ExtrinsicsRoot + StorageRoot + Digest
- Block := Header + Extrinsics + Justifications

乍一看，区块和标题格式类似于传统的区块链；但是，帐户和合约的概念被扩展并抽象为一个外部性的。标题内的根存储在16进制修改过的Merkle树（“Trie”）数据结构中。

外部性定义运行一个链所需的功能和数据。除了范围更广外，它们与交易类似，因此，对链状态的任何修改都是外在的。这个额外的抽象层，允许将单个交易、批量交易或其他类型的状态更改都编码为外部性。

外部性是在模块中定义的，任何客户端都可以提议在下一个区块中包含一个有效的外部性。

## 2.1 模块

模块用Rust编写，编译为Wasm，并作为客户端运行时的一部分进行链接。它们定义Edgeware逻辑的核心，并且可以访问未计量的图灵完全计算，因此仔细审核和测试模块代码至关重要。特别是，任何客户端都不能通过提出一个需要比区块时间更长时间来执行的外部性来破坏链。否则，验证人将无法及时调用作者区块来生成有效的区块。

Edgeware包含这些模块，此列表并非详尽无遗。其他模块使用的工具模块以及计划中的升级（如费用模块）不包括在内：

## 外在性和它们的描述

余额:

维持账户余额。

共识:

允许编写区块的一组权威。

Aura:

允许编写区块的一组权威。

Grandpa:

面临行为不当的验证人确保区块的最终性。

获得股份:

处理成为验证人所需的股份。

会话:

在会话之间轮换验证人。

合约:

允许创建和执行燃气计量智能合约。

司库:

由治理管理的链上司库。

信令:

允许代币持有者使用离链信令来就提案达成非正式共识。

民主:

允许代币持有者通过直接民主通过提案。

理事会:

允许通过批准投票选出的理事会通过提案。

身分:

用于链上身份的简单原语。

## 2.2 合约

Edgware智能合约可以使用任何与Wasm兼容的更高级语言编写。已经有经过充分测试的工具链用于把C、C++和Rust编译到Wasm，并且独立的工作正在进行，通过AssemblyScript项目将JavaScript的一个子集编译到Wasm。随着其他区块链和网络基础设施项目进一步开发Wasm工具链，Edgware还将受益于安全性、可移植性和表现力方面的改进。

否则，合约的功能与在以太坊或其他EVM兼容区块链上的功能大致相同。任何拥有EDG余额的用户都可以部署合约，合约也可以调用其他合约。以EDG计价的燃气必须预先购买并限制计算。消息呼叫使用达到交易限额的燃气，任何多余的将退款。如果所有燃气告罄，则计算终止，并且效果被恢复。

合约还将能够通过一组有限的白名单接口与其他Edgware模块进行交互，特别是在身份和理事会模块中查询帐户。智能合约系统的其他改进，如平行交易和状态租金，预计将在链推出后跟进。

3

## 2.3 共识

Edgware的推出具具有一个指定的股权证明Sybil抵抗机制。分配轮换的验证人组以便执行和密封区块。验证人最初是使用集体性的硬币投掷算法进行选择的。

为了避免不占有股份问题，Edgware使用GRANDPA最终性小工具来实现区块最终性[2]。链上治理使Edgware能够优雅地实施改进的共识机制。

五秒钟的区块时间允许足够的网络延迟，同时仍然保持高吞吐量。

## 2.4 获得股份

个别验证人必须将其股份担保三个月。Edgware维持X个验证人的一组验证人，在一段时间内保持领导地位。

Edgware帐户可以将其余额委托给一个指定的股权证明（NPOS）系统中的其他验证人，以接受区块奖励的一部分。在NPOS中，区块奖励首先在所有活跃验证人之间平均分配，然后在支持该验证者的余额中按比例分配。因此，Edgware帐户受到激励，在避免过度集中的同时寻找值得信赖的验证人。

## 2.5 余额和账户

余额保持在基于帐户的系统中，由ed25519椭圆曲线派生的密钥保护。账户和余额转让必须满足这些约束，这些约束作为整个链的全局变量得以维护：

- TotalIssuance: 系统上的股份总额。
- ExistentialDeposit: 允许保持帐户开立的最低金额。
- TransferFee: 转让所需的费用。
- CreationFee: 创建帐户所需的费用。至少和ReclaimRebate一样多。
- FreeBalance: 给定帐户的“免费”余额，用于确定合约执行环境中的余额。当此余额低于“ExistentialDeposits”的值时，“当前帐户”将被删除。
- ReservedBalance: 外部保留的给定帐户的余额金额，可以被削减，但是，是最后被削减。

4

- TransactionBaseFee: 为进行交易所支付的费用；基础部分。
- TransactionByteFee: 为进行交易所支付的费用；每字节部分。

## 2.6 Edgeware 代币 - EDG

最初铸造5,000,000,000（50亿）EDG代币，最多可分割到18位小数。最初，通胀率设定为每个区块158 EDG。这意味着第一年约有997,220,160个EDG，或者通胀率略低于20%。

铸造的EDG总量将年复一年地保持不变，导致百分比通胀率反通胀，第二年的年通胀率降至约16.6%。此外，全系统投票可能进一步增加或减少通胀。

Edgeware的首批提案之一是将通胀与特定的参与率或安全率挂钩，使通胀上下浮动以达到预期的总份额。具体的提案将通过修改通胀率的运行时升级来进行投票和执行。

在Edgeware上，EDG具有多种功能。EDG赋予持有人获得股份的权利和投票权，以及将此权利委托给另一个账户的能力。EDG还被用于支付Wasm智能合约模块中的状态变化。

## 2.7 互操作性

Edgeware通过Polkadot实现了跨链互操作性的具体路线图，Polkadot是Parity与Substrate同步开发的交叉链桥接网络[6]。Polkadot将连接包括Edgeware和以太坊在内的区块链，允许资产被锁定在一个网络上并在另一个网络上进行管理。

从长远来看，用户将能够同时运行以太坊和Edgeware dapps - 可能使用以太坊作为高风险金融应用程序的稳定网络，而Edgeware作为需要高吞吐量和一流身份的应用程序的渐进式网络。

## 3 网络启动

Edgeware网络将通过向以太持有人发行Edgeware代币的“锁定”启动。锁定是一个空投，其中网络代币持有者在智能合约中将他们的代币锁定一段固定或可变的时间段，即“锁定阶段”。这种新颖的代币分发方法的目的是为了更公平、更安全和更广泛地协调积极参与者之间的激励选择，并激励网络的已承诺初始参与者，以及利用现有的代币分发来创建相对更多样化和广泛的分发。

对于Edgeware而言，以太持有人将能够通过两种交互类型参与：“锁定”，他们发送并使其以太坊代币无法访问，可选期限3个月、6个月或12个月，或者“信令”他们参与Edgeware网络的意图。“信令”类似于空投没有锁定持续期间且参与者的代币仍然可以访问 - 但是，与锁定交互相比，信令参与者获得的分发减少。对于那些选择锁定其代币的人，锁定时间更长的人相应地按比例收到更多的Edgeware代币，这些代币在网络启动时分发。

基于以下原因，，锁定进程是桩网证明网络中更公平、更安全的分发代币的方式：

**非零机会成本：**为了参与锁定，个人在锁定期间放弃以太坊的机会成本 - 例如能够以复合发生借贷。对于长期的以太坊持有者来说，这个机会成本无关紧要。因此，长期以太坊持有者与EDG锁

定最为一致。EDG代币的创建将允许代币持有者参与分发给Edgeware参与者的所有权利 - 成为网络提案的验证者或投票人。

**下行保护**：在锁定结束时，参与者将分别拥有对两种生产性实用代币以太坊和EDG的访问权。由于Edgeware是一种新的实验链，在Edgeware网络上如发生恶意攻击或剥削，锁定参与者仍然会保留他们的以太坊，消除参与的长期风险。

**简单、开放和可访问的流程**：向Edgeware主锁合约发送以太坊的单个交易允许人们接收EDG代币。任何帐户都可以从硬件或软件钱包（例如，Trezor、Metamask等）执行此操作。此外，任何以太坊持有人都可以参加。

**经济上的安全性**：在新的PoS链上引导安全性。以太坊正在从最初的众筹销售和PoW大众奖励中引导Serenity版本。同样地，Edgeware可以利用以太坊持有者已经广泛的分布来引导Edgeware链的经济上的安全性。

**合同的安全性**：从主锁合约上调用锁时，创建一个单独的锁定用户合同，该合约实际上持有参与者的时间锁定的以太坊。这显著改善了资金安全，因为价值不是存储在一个单一合同中，而是存储在一组特定于用户的合同中。

## 3.1 锁定合约规范

锁定合约是一种简单的双功能智能合约。当通过主合约锁定使用下面指定的接口调用功能锁定时，创建了一个新的锁定用户合约，其中包含时间锁定的以太坊。注意，当isValidator为yes时，分配的EDG总额可能会被分割。值得注意的是，主锁定合约（MLC）本身并不持有锁定的以太坊，

相反，当调用锁时，会创建一个单独的锁定用户合约（LUC）来保存参与者的时间锁定以太坊。这种两步安排降低了恶意攻击的潜在价值和可行性。此外，主锁定和锁定用户合约非常简单。特别是，LUC合约是四十五条指令，没有跳转直到完成。这些已经过第三方审核。

Quantstamp.

名称	数据类型	描述
term	术语	一个指定以太坊可能被锁定的时间长度的枚举。
edgwareKey	字节	在创始时将分配到EDG代币的指定Edgware地址。
isValidator	布尔	允许个人指定这个Edgware地址是否要在启动时成为验证者。

### 3.2 锁定参与

主锁定合约将在九十天的贡献期间内接受“锁”和“信令”。在Edgware上，锁定交互可能持续三个月、六个月或12个月，奖金分别为0%、30%和120%。为了减少Edgware上的权力集中并增加

利益相关者声音的多样性，没有任何一个贡献以太坊地址或接收EDG地址将能够获得大于或等于通过锁定铸造的EDG总量的20%。

锁定长度	方法	重量	收到的EDG
0个月	信令	0.20x	启动时为25%，启动后365天为75%。
3个月	锁	1.00x	在网络启动时
6个月	锁	1.30x	在网络启动时
12个月	锁	2.20x	在网络启动时

鉴于贡献期间的持续时间较长，也将鼓励早期专门参与锁定交互，以平衡用户在估计锁定结果时的利益与参与的可获得性之间的平衡。因此，贡献期间从2019年6月1日开始分为六个15天的奖励期。当下一个15天期间开始时，早期参与奖金减少。该时间表概述如下。

日期范围 (2019)	奖金	以太坊上限
6月1日至6月15日	50%	无上限
6月16日至6月30日	35%	无上限
7月1日至7月15日	23%	无上限

7月16日至7月30日	14%	无上限
7月31日至8月14日	8%	无上限
8月15日至8月29日	5%	无上限
8月30日-8月31日	0%	无上限 - 锁定结束

锁定交互将与信令交互并行接受，使参与者能够通过创建多个LUC来进行这两者。在这些信令交互中，个人将能够通过使用类似于碳投票的功能调用，在任何期间内不锁定以太坊的情况下接收EDG。信令对冷钱包和硬件钱包都开放。请注意，如果个人通过信令参与，他们将在网络启动时收到他们25%的EDG，并且在网络启动之后365天（12个月）内收到剩余75%的EDG。此外，对于从单个钱包发出信令的以太坊，当时收到的EDG数量将扣除80%。

信令的接受支持这样一个目标：让以太坊生态系统的长期贡献者参与Edgeware的启动。这些贡献者的很大一部分代币仍然存在于冷钱包和硬件钱包中，并且激励他们参与的尝试必须包括来自热钱包和冷钱包的非锁定交互。为了防止Sybil攻击或双重信令交互尝试 - 个人可能将他们的资金从一个地址移动到另一个地址，以尝试并两次发出代币信令，在2019年9月1日00:00 UTC投送结束时拍摄主以太坊链的快照。

此外，还存在称为通用锁的第三类交互，其中信令通过初创规范被授予3个月的锁定。如果调用“信令”的地址在整个12个月的锁定持续时间内无法签署msg.value大于0的交易，则该信号符合通用锁处理的条件。这类交互旨在进一步使那些可能无法正常参与但对整个Edgeware网络提供重要价值的承诺参加者参与。

在以太坊代币被锁定的期间，在网络启动时接收EDG的个人，也将能够通过分割和参与其他网络活动来获得代币。最后，当任何用户的锁定期间结束时，他们只需向他们的LUC发送一个任何类型的交易，以触发返回他们的以太坊。

我们假设，所提议的代币分发机制，应该以比以前的预设、初始硬币发行或类似的分发方案更公平的方式，激励更积极的参与和扩大分发。

### 3.3 初创区块

启动之后，个人将能够通过查找锁定和信令事件并计算Edgeware上相应的计算余额，来单独验证锁定或发出信令的以太坊总额。我们希望在锁定中分发90%的初始Edgeware代币。需要公平和广泛的代币分发来引导治理，并表明共识算法在不利条件下行得通。Edgeware是一个最初由联邦实验室开发和管理的項目。其他代币将分发给联邦实验室（4.5%），协助该项目的其他合作伙伴，如Parity Technologies（3.0%），以及为初始开源贡献者保留额外的部分代币，社区参与者和测试网用户（2.5%），最初将由联邦实验室或通过网络的司库模块进行管理。

EDG持有人或可确定但未来的EDG持有人，也可投票将一些额外的发行分配给其他社区，如DOT持有人。

## 4 治理

工具代币和智能合约区块链的绝大多数（估计80%）表明他们打算转向链上和分散治理。但是，在撰写本文时，很少有成功实施链上治理。

迄今为止推出的少数几个系统主要是链上司库、委托股权证明（DPoS）系统和直接代币加权投票模型。直接代币加权的链上流程通常很容易被链中的大型经济持有者捕获，例如区块生产商、矿工和交易所[1]。此外，目前很少有治理系统具有任何级别的积极使用。通信、对话和投票都受到同样不直观的接口的限制，这些接口妨碍了加密货币整体的发展。

Edgware旨在成为开发有效的链上治理的先驱网络。通过迭代产品接口、投票系统以及其他管理原语，Edgware可以加速核心技术的实施和部署，如切分、股权证明、高效的SNARK实施和运行时更改，以比其他区块链更快的速度实现技术进步。通过使用明确定义的链上管理流程，Edgware网络升级将更容易协调并更快地部署。

### 4.1 治理模块

治理的核心功能在几个可扩展模块中实现：

- 信令：非约束性民意调查对现有区块链是治理流程的重要组成部分。用户还应该能够创建和分发民意调查，以表明对不同提案、策略和方向的兴趣。
- 身份：Edgware需要一种一流的身份原语，以便人们可以在治理流程中相互识别。
- 民主：民主模块最初限制对二元投票提案的投票。该模块允许委派投票-提高分配给投票的总份额。未来的升级应该允许用户在对提案进行投票的许多不同方法之间进行选择（例如，二元或排名选择）。

- 理事会：Edgeware允许投票人提名一组拥有网络某些权利的账户。理事会成员可以偏袒提议。
- 司库：该模块允许个人对新铸造EDG的一部分分配进行投票。

在随后的Edgeware迭代中，将包括对另外治理功能的支持。另外功能的开发将由链上司库提供资金，包括：

- 安全投票：用户应该能够匿名投票，以防止投票购买攻击，要求在协议层实施加密原语。
- DAOs：随着Edgeware生态系统的发展，群体在网络的初始治理结构之外进行协调的需要将会出现。从长远来看，我们预计这将通过用户构建和管理DAOs来实现，这允许在不改变核心治理的情况下探索替代决策结构。例如，DAOs可以遵循决策过程，包括简单的一人一票、委托投票、二次投票和更复杂的模型。

请注意，可以在合约或模块级别实施进一步的治理改进。

#### 4.1.1 信令

信令模块允许用户投票以创建非约束性民意调查。非约束性民意调查对现有区块链来说是治理过程的重要组成部分，而非约束性民意调查先前都是以临时方式进行管理。用户本身应能够创建和分发民意调查，以表明对不同提案、策略和方向的兴趣。

### 9

个人可以在对提议的多种不同的投票方法（如二元或等级选择）中进行选择，而且还允许委派投票-提高分配给投票的总份额。一旦选择了一个方向，理事会或民主模块就可以创建一个具有约束力的链上公投。

#### 4.1.2 身份

在互联网上，电子邮件地址已经成为用户身份和身份认证的事实标准。它们具有普遍的互操作性，并在服务之间得到认可。区块链上尚未出现如此广泛被采用的身份识别系统。最近才在现实世界中部署的区块链应用程序的几个领域大大受益于某种形式的持久用户身份，其中包括贷款、协议治理或策展网络。对于贷款协议，身份是必要的，因为除非贷款人或承销商知道其对手方的身份，否则抵押贷款是不可行和具有风险的。对于协议治理，身份是建立社会共识所必需的。

虽然有些人可能选择保持完全匿名，但Edgeware网络上的参与者可能会发现将身份或声明链接到匿名地址很有用。通过在Edgeware中构建一个可选身份解决方案

作为一流的本本原，Edgeware成为分散金融、治理和其他dApps的理想平台。

理想情况下，身份标准将用于前面提到的用例，同时易于使用和具有电子邮件登录的通用可寻址性。Edgeware身份系统实现了这一点，详见IdentityRecord:

10

名称	数据类型	描述
account	AccountId	与身份相关联的特定Edgeware帐户。
identity	Vec <u>u8</u> >	对应于身份的字节数组。可以加密或不加密。
stage	IdentityStage	显示提案生命周期的枚举-已注册、已证明或已验证。
expiration	BlockNumber	身份在其中变为无效的区块。该字段是可选的。
proof	Attestation	用于身份的已发布证明。
verifications	<Vec(AccountId,bool)>>	一个具有相应的元组帐户和布尔的数组。显示第三方个人是否可以验证身份和帐户是否确实已链接。
metadata	MetadataRecord	一个允许人们在Edgeware上添加头像、标语或显示名称的可选字段。这允许在系统上有一个人类可读的标识符。

身份模块中的公共功能允许帐户进行注册、证明或验证该身份。帐户首先注册一个身份。此后，个人通过链接到外部证据来证明这一点。第三方现在可以验证该链接的身份是否有效，投票决定该证明是否有效。验证必须来自专门选定的验证人，而不一定只是任何第三方个人。初始的验证人集合是Edgeware网络上的证明人。可以将验证身份的工作委托给守护程序来管理此过程。

注册和证明的发送者必须相同，这有助于减少虚假证明。因此，区块链可作为身份注册证明的唯一真实来源。验证者只应查询存储在链中的证据，以决定身份注册是否有效，而不应查询任何其他形式或证明的呈现。不同情形的证明示例：

- Github: 身份是Github用户名。用户名注册后, 注册处应在用户名的帐户下发布Github Gist证明, 并附有到Edgeware上的注册链接。

- 以太坊: 身份是以太坊公钥或地址。用户名注册后, 注册处应向刻录地址发送一个0值交易, 以象征化其相应Edgeware帐户公钥, 并提交交易哈希作为证明。一经检查, 验证人应有足够的证据证明以太坊账户也不拥有接收者Edgeware账户(在以太坊上作为目标地址表示), 因此他们不会签发此一交易。

## 11

最初, 验证人集合是至少有0.1%的EDG代币的帐户集。身份验证的投票是硬币加权的。Edgeware这样做是为了有机地为系统的其他区域建立一人一票政府。

### 4.1.3 民主

民主模块在投票过程中创建和移动不同的具有约束力的公投。公投允许以根用户身份在链上执行任意外部调用。这允许执行相当重要的操作(例如, 设置余额、修改时间戳等)而无需执行运行时升级。该模块目前仅支持二进制绝大多数通过投票, 除非由理事会成员提交(理事会成员提交也支持绝大多数不通过和简单多数)。个人在二进制选票上进行投票, 这些选票由带有锁定时间调整的硬币加权计算。

开始时, 所有投票将限制在两周的固定期限内。未来, 民主模块将扩展到许多投票类型, 它们是:

- 二进制: 传统的是或否投票。
- 多个选项: 个人可以选择多个选择
- Commit-Reveal: 通过发布投票的哈希来承诺特定投票的方案

在投票决议中, TallyType更改投票加权的方法。它们列举如下:

- 硬币加权: 个人账户投出的选票按每枚硬币加权-一枚硬币相当于一票
- 当一个帐户以特定的锁定持续时间进行投票时, 较长的时间对应于更多的投票权力。例如, 一个投票可能被锁定一个或两个星期, 后一时间对应于两倍的投票权力增加。
- 一人一票: 一个帐户或身份可以投一票。在Edgeware上, 一人一票可能涉及一组特定的已被验证身份, 如已被验证的Github帐户。

最初，所有在Edgeware上的公投都将采用硬币加权和锁定时间加权。重要的一点是，对于硬币加权投票，用户不能进行“部分资金投票”-用户只能在锁定期间内投票并锁定给定账户的所有资金，或者根本不投票。锁定时间加权允许具有较小代币余额的单个帐户在治理过程中行使更多权力。在投票决议之后，在实施任何变更之前会有一段延迟-最初设定为两周。

此外，民主模块允许委派投票，委派投票是直接民主和代表民主之间的中间点。在投票结束之前的任何时候，帐户可以以不同于与该帐户可能已经委托的帐户的不同方式进行投票。自愿委托有可能增加政治参与、减少选举过程中的战略激励、并改善政治性的客户-代理问题。委托可以是递归的。Edgeware缓解恶意的个人可能将委托树的深度操纵到极端深度的攻击。Edgeware不会强制所有节点统计投票以遍历委托人的深层树，而是将委托限制为五层。另外还防止循环委托。

通过增加对不同投票类型的支持，如启用排名选择和匿名投票（其中帐户直接链接到他们的投票选票上），或者通过添加不同的计票类型，如二次投票[5]，民主将得到扩展。

#### 4.1.4 理事会

分散式系统为在线和积极的参与造成一个有问题的情形，往往导致低投票率。因此，理事会成员可以偏袒法定人数，法定人数是所需票数以及赞成票和非赞成票之间的相对差异。Edgeware理事会模块最终将扩展到允许24个人帐户对网络持有一些独家权利，其中理事会成员的固定任期为12个月。在网络启动时，理事会成员人数将为6人。

理事会在对等基础上进行投票，也就是说，没有硬币加权投票。法定人数偏袒允许理事会改变有效的绝对多数，以便在没有明显支持或反对提案的投票权多数的情况下，使提案更容易或更难通过。如果所有理事会成员都投票赞成一项提案，那么所需的非理事会成员投票数量就会减少。反之亦然。当理事会投票并且不止一个成员持异议时，法定人数就会负面地偏袒。

#### 4.1.5 司库

虽然验证人通常在其他区块链中是本地激励的唯一利益相关者，但Edgware建议使用区块奖励来激励所有利益相关者。区块通胀将被分配给一个链上司库，这将由具体的财务提案进行分配。

最初，链上司库将由区块奖励的50%资助。Edgware代币持有者可以将资金分配给：

- 核心技术：实现扩展技术，如运行时改进、切分和链下扩展。
- 治理：治理系统，包括链上身份以及组织和协调核心开发人员工作的工具。
- 开发人员经验：用于开发、调试和测试智能合约的成熟工具链。
- 用户体验：钱包和用户体验原语（例如，JavaScript库），使分散式应用程序简单易用。
- 生态系统支持：通过现场活动吸引开发商、最终用户和其他利益相关者。

## 4.2 治理接口

联邦实验室已经开发了一个用于管理分散式网络的接口。该界面将支持对提案的讨论和投票，创建和管理与Web 2.0社交媒体帐户链接的身份，并在不同的沟通渠道中跟踪有关Edgware提案的讨论。

联邦实验室还可能为Edgware生态系统中的参与者提供Slack、Riot或Discord聊天，以便彼此进行交流。

由于Edgware遵循标准Parity Substrate API，因此用户可以替代地使用标准Substrate库来手动访问链，读取治理提案的状态，并在本地签署交易以向网络提交投票。

## 4.3 治理程序

通过对特定项目和提案进行非正式投票，Edgware利益相关者将能够通过链上信令，在网络路线图上进行协作。这一规划阶段是链上治理过程的自然前提，并举行正式投票以供资金支持，在此基础上实现商定的特征。

建立健全的链上升级程序将是确保网络安全的重要步骤。所有网络升级都应由多个独立方进行审核和测试，并另外获得EDG持有人大量法定人数的批准。

## 4.4 实验平台

从长远来看，Edgeware的发展和成功将需要一大批做出承诺的利益相关者，包括验证人、投票硬币持有者、应用程序开发人员和核心技术人员。我们预计，协调这些类别中的每一类利益相关者的治理结构将会随着时间的推移有机地出现。

然而，为了加快这一过程，Edgeware将为利益相关者群体提供一套工具，以试验新的治理形式，如不同的投票模式或决策过程。原生治理工具允许DAOs有机地出现，以测试不同治理系统的有效性。

例如，虽然个人和链下公司将作为司库基金的第一批接收者，但DAOs可能会出现来协调伪匿名在线参与者之间的工作，他们可以在Edgeware网络上建立身份和跟踪记录。或者，随着部署匿名投票系统，应该有可能使用可链接的环签名对受信任的开发人员、投资者或专家群体进行民意调查，以建立围绕关键网络升级和治理决策的情绪。

通过这个实验过程发现的成功模式可以在进一步的迭代中被重复使用和改进。它们可以在第2层协议、公共物品资助DAOs以及在Edgeware链本身上孵化的其他项目中被重复使用。

## 5 结论

目前，分散式计算处在其开发的早期阶段，应该以快速的迭代周期和雄心勃勃的路线图来开发。创建一个新的、积极管理的、具有渐进式升级政策的链，可以有效地实现这一目标，并有适当的激励措施。

作为一种递归地自我改进系统，Edgeware可以资助、开发和部署支持网络性能和可用性的网络升级。这使得Edgeware成为现有区块链的新颖替代方案。它使激励措施保持一致，以便快速发展和开放的治理过程形成良性循环，治理的早期成功体现在网络、社区和生态系统的价值中。

## 参考

[1] Vitalik Buterin. Governance, Part2: Plutocracy Is Still Bad. URI: [vitalik.ca/general/2018/03/28/plutocracy.html](https://vitalik.ca/general/2018/03/28/plutocracy.html).

[2] Byzantine Finality Gadgets. 2018. URI: <https://github.com/w3f/consensus/blob/master/pdf/grandpa.pdf>.

[3] Dillon Chen. What's in a Lockdrop. 2018. URI: <https://medium.com/commonwealth-labs/whats-in-a-lockdrop-194218a180ca>.

[4] Parity Substrate. URI: <https://github.com/paritytech/substrate>.

[5] Drew Stone. Anonymous Voting: A Design Survey. 2018. URI: <https://medium.com/commonwealth-labs/anonymous-voting-a-design-survey-12de869dc97f>.

[6] Dr. Gavin Wood. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. URI: <https://polkadot.network/PolkaDotPaper.pdf>.