Celo：用于去中心化社会支付的多资产加密协议

C-Labs团队

草案版本0.24

摘要

大规模采用加密货币作为支付手段的两大障碍是易用性和购买力波动性。我们在此向您介绍Celo，这是一种协议,通过基于地址的加密方案和价值稳定的代币来解决这些问题。我们将展示如何将这些属性结合起来，以促进包括全球参考货币，本地和区域价值稳定货币以及社会红利在内的货币生态。我们的第一个应用是以移动电话为中心的社会支付系统。

内容

1 介绍

相对于以法定货币进行支付的方式，加密货币有一些优势。只要您拥有智能手机，它们就可以以可公开审计和安全的方式使用全球可访问的技术，以较低的成本（特别是对于国际支付而言），以比银行电汇快得多的方式进行价值转移。此外，加密货币可以被编程；允许签订金融合同，进行托管和投保，所有这些都不需要中介。

但是，目前，主流采用加密货币作为支付手段仍然存在一些障碍。首先，由于确定性的供应规则和不可预测的金币需求，成功的金币[1] 经历通货紧缩的价格不稳定。因此，用户理性地倾向于将它们用作存储价值而不是交换媒介。 其次，即使人们确实希望使用价格波动的加密货币作为支付手段，他们也需要生成私钥/公钥对以接收付款，并输入某人的公钥以便发送付款。虽然这些障碍可能看起来很小，但经验表明，用户体验的微小差异将导致使用结果的巨大差异。

要使加密社会付款系统繁荣发展，发送付款应该像发送短信一样简单，并且货币的波动性应该降至最低。 我们将Celo描述成一个解决这些问题的协议。为了便于发送付款，Celo引入了一种加密方案，我们将其称为基于地址的加密，参与者可通过该方案验证一系列手机号码到公钥的映射，从而允许用户将自己朋友的手机号码用作公钥。

为了解决价值稳定性，Celo引入了一个代币，其价值通过具有弹性供应规则的货币政策稳定，并由可变价值储备支持。此外，它引入了一种管理结构，允许协议创建一系列本地、区域和工具性价值稳定的货币，其中向家庭引入新的成功的价值稳定的金币来增强现有金币的稳定性特征。

最后，Celo引入了移动区块奖励机制，其中参与交易的所有用户均能够参与验证，创建广泛的参与者基础并使日常用户更容易获得区块奖励。

这些共同构成了引人注目的社会支付协议。

2 通过轻量级身份使用的易用性

主流采用加密货币作为支付手段的一个重要障碍是缺乏直观，去中心化的公钥基础设施。因此，为了在今天的去中心化系统中发送支付，用户必须知道预期接收者的公钥（除非他们通过集中式网关进行操作）。并且为了接收付款，用户必须首先建立私钥/公钥对并进行广播。如果可以将付款直接发送到电子邮件地址或电话号码，并且无需先设置钱包就可以收到付款，这将变得容易得多。

基于身份的加密 [18]为此目的作出承诺。在此方案中，当Alice想要通过bob@company.com向Bob发送加密消息时，她只需使用公钥字符串bob@company.com，而无需获取Bob的公钥证书。虽然基于身份加密的加密货币系统可以带来更加无缝的用户体验，但原始提案和后续实施 [4],[6]都受到需要受信任的第三方（称为私钥生成器）来生成私钥这一事实的阻碍。因此，这些方案在开放、无许可的系统中不太有用。

[1] 学术机构、监管机构、企业家和其他人士可互换使用“钱币”和“代币”来描述资产，这些资产充当分布式分类账固有的数字化价值表示形式。在本文中，我们是指具有一般互换性的“数字资产”、“钱币”、“加密货币”和“代币”。

2.1 基于地址的加密

我们提出了一种基于身份的加密变体，称为基于地址的加密。我们让用户以传统方式生成自己的私钥/公钥对，而不是直接使用电子邮件地址或电话号码作为公钥，然后依靠可信私钥生成器生成相应的私钥。然后，用户将其公钥注册到一个公共的仅附加（append-only）数据库，该数据库存储[地址 ->公钥]元组。该数据库在功能上是分散的，因此没有中央所有者负责存储、管理或维护数据库，但逻辑上是统一的，这样每个人都可以随时查看数据库中的所有条目。至关重要的是，[地址 ->公钥]元组由对等网络验证。为了执行验证，在网络中随机选择的验证器将向注册者发送签名和安全消息，然后注册者使用她的私钥对消息进行签名并将其返回给验证智能合约。验证合同将检查验证器是否确实发送了消息，以及签名是否与接收者的公钥匹配。

此协议不仅适用于电子邮件地址，还适用于可以发送安全消息的任何通道，例如手机号码、IP地址，甚至是银行路由和帐号。此外，可以将任意字符串附加到数据库密钥中的地址，允许为每个地址存储多个公钥，每个公钥用于不同的应用程序。因此，加密方案支持大量加密应用程序，从双因素身份验证到去中心化社交网络，而不依赖于受信任的第三方。

对于社会支付用例，它允许两个重要功能。首先，用户可以使用她的电话号码作为公钥将Celo货币发送给朋友，从而可以轻松地向联系人付款。其次，即使朋友尚未下载Celo钱包，用户也可以将Celo货币发送给朋友。

2.1.1 基于单节点地址的加密

出于解释的目的，我们首先描述基于地址的加密方案的简化版本，其中称为验证器节点的单个节点维持系统的状态。

验证器节点的关键作用是维护[地址 -> 公钥]映射的公共、仅附加数据库。在单节点情况下，验证器节点类似于传统的密钥服务器，它不仅存储[地址 -> 公钥]映射，还验证它们，如下所示：

当用户希望向该方案注册公钥时，它们生成私钥/公钥对，然后将它们的[地址 ->公钥] 映射提交给验证器节点。（在我们的用例中，地址是用户的手机号码，但在一般情况下，它可以是可以发送秘密消息的任何地址。）验证器节点向条目中的地址发送签名秘密消息。用户接着将该消息发送到验证智能合约，后者将验证两个签名，方法是使用用户和验证器的公钥将其解密。如果解密的消息与秘密消息匹配，则智能合约将以下条目写入数据库 [地址、用户公钥、秘密消息，用户签名的秘密消息、验证器签名]。

2.1.2 缺点

这个简化版有以下缺点：

*地址搜集。*具有未加密电话号码的可公开查看的数据库允许垃圾邮件发送者收集所有用户的手机号码。作为解决方案，我们可以存储地址的单向散列而不是地址本身。为了增加底层字符串的熵（使反向散列变得更加困难），我们可以在要散列的字符串后面添加胡椒粉[2]。

*每个地址单密钥。*实际上，人们可能希望存储与其地址相关联的多个公钥。简化的协议没有提供这样做的机制。作为解决方案，我们可以允许密钥是与可选的任意字符串连接的地址的哈希值。例如，这允许Bob以hash（“415 555 1212 || application _ name”）存储应用程序密钥，或者以 hash（“415 555 1212 || application _ name || 2017 11 17”）存储短暂的应用程序密匙。

*节点故障。*任何依赖单个节点维护状态的模型都容易受到该节点故障的影响。我们可以通过让多个节点参与维护状态来解决这个问题。（在这样做时，我们还必须确保只有少数节点向发出验证请求的用户发送秘密消息，以避免用户过载。）在这个模型中，秘密消息也必须由其他验证器验证，即使它们没有构造该密匙。这是通过使用发送它的验证器的私钥对消息进行签名来实现的。为避免重复攻击，来自同一验证器的每条消息必须是唯一的。

*恶意验证器。*恶意验证器节点可以选择绕过消息/响应步骤，而是在分类帐中写入一个条目，在该分类帐中，它们选择其他人的地址，为该地址生成自己的密钥对，然后使用他们生成的私钥对秘密消息进行签名。这样做允许验证器欺骗地址，声称为其他人付款。我们可以通过要求多个没有机制串通的验证器达成共识来解决这个问题。

交易透明度。 如果我们使用哈希电话号码作为公钥，那么传统的比特币式区块链将允许用户在其地址簿中查看联系人的交易。我们可以通过实现zk-snarks的计算效率版本来解决这个问题，如[12]中所述。

*DDoS。*最后，恶意用户可能会向验证器提交数千个虚假请求，这两者都会绑定验证器并有效地将验证器用作垃圾邮件代理。我们可以通过引入验证成本来缓解这种情况。

2.1.3 分布式方案

我们在这里介绍一种分布式方案，它引入了上面提出的每个特性。在该方案中，不是由我们在第 2.1.1节中描述的单个验证器节点，而是由多个验证器节点的对等网络维护数据库。网络是开放的，没有许可；任何人都可以作为验证者加入，验证者可以随意离开

[2] 即使附加了胡椒粉，也可能出现以下情况：垃圾邮件发送者单向散列每个可能的10位数字以及每个可能的胡椒粉，然后检查查看数据库中的散列值。然而，即使在今天，通过获取每个可能的10位数字，向每个数字发送短信，并查看它是否通过，也可以以高成本进行搜集。因此，我们的目标是使解密的有效成本比发送批量短信的成本更高。

并重新加入网络。每个验证器都维护一份验证待处理队列和验证用户数据库的完整副本。对于每个验证请求，都会随机选择验证器来处理验证。

验证工作流程将如下所示。首先，用户通过将请求发送到验证智能合约以及支付验证费用，来发出验证请求。然后，验证合同从验证器集中随机选择一个验证器，并为验证器生成一条消息；接着，验证器对该消息进行签名，将其发送给注册者，注册者也将对该消息进行签名，然后将其发送回验证合同。接着，验证合同会验证注册者和验证器的签名；如果它们匹配，则记录该验证。大多数应用程序都需要多次验证，在这种情况下，如果链上记录的验证不足，则它们只会请求更多验证。

具有多个验证器可解决节点故障问题。需要多次验证可解决恶意验证器问题。验证费用解决了DDoS问题。并且验证请求作为（地址|胡椒粉|应用程序字符串）的散列发出，以便避免地址获取，并允许每个地址拥有多个密钥。

2.1.4 行动摘要

构建协议的另一种方法是描述系统中每个节点允许的角色和操作。

任何用户可以：

- 通过将她的[散列(地址|可选附加字符串) -> 公钥]元组广播到验证待处理队列，请求验证与其地址相关联的公钥

经验证的用户可以：

- 通过创建[散列(地址|可选附加字符串) -> 公钥]映射添加新公钥
- 撤销与其地址相关联的任何公钥
- 更改与其地址相关联的任何公钥

验证器可以：

- 与其他验证器竞争编写区块的权利并向验证待处理队列中的地址发送秘密消息，并验证先前区块验证的签名响应。

任何人都可以：

- 在已验证的用户数据库中查找给定地址散列（或地址散列||字符串连接）的公钥。

2.2 通过加密的EigenTrust聚合信誉信号

存在电话号码到公钥的分散映射后，它可用于引导信誉系统，帮助用户确定他们可能与之交易的任何新用户的可信度。

一个人的手机联系人列表是一个粗略的一阶代理，用于列出她对其具有一定信任度的人员列表。可以想象通过显式信号（例如，用户可以以特定于应用的方式对她的联系人列表中的人进行评级，或者证明他们的地址簿中的联系人是否是某人），以及隐含信号（例如，如果用户向其联系人列表中的某人付款）以及隐含信号。这些信号可以在用户的手机上进行本地维护，而无需与其他任何人共享。

这种基于地址簿的信任信号定义了信任网络，该信任网络在逻辑上是分散的而且在功能上也是分散的。没有单一实体存储或可见整个信任网络；每个用户只知道他们信任的人以及他们信任的人的信任级别。我们在下面描述如何在给定此去中心化信任网络的情况下计算抗sybil，保护隐私的聚合信誉分数。

2.2.1 EigenTrust

EigenTrust [14]是一种用于计算全局信誉得分的去中心化算法，给出成对的本地信任得分。EigenTrust背后的关键直觉是，一个人的信誉得分可以定义为信任该人的人数，并通过他们的信誉得分加权。这种递归计算将所有节点收敛到信任矩阵T的主特征向量$\vec{t}$，其中T_{ij}是0和1之间的数，并且其大小与节点 i信任节点 j[3]。

在EigenTrust中，T的主特征向量是使用幂方法[20]的分布式变量计算的。在社会支付网络的背景下，它将按如下方式进行：信任网络T_{ij}将是支付网络的一些变体，其中如果节点 i已经支付节点 j，则T_{ij}将是非零的，并且节点 j在节点 i的地址簿中。每个节点存储它们自己的当前t_i，并且可以访问行 i和列 j中的T_{ij}的值（节点与之交互的人）。然后，如下以迭代方式计算原理特征向量$\vec{t}$。在每次迭代中，每个节点将$t_i \cdot T_{ij}$分数发送到他们过去支付的每个节点 j。节点 j等待从过去向它们支付的节点接收所有分数，然后计算它们自己的 t_j，然后将它们$t_j \cdot T_{jk}$传递给它们已支付的节点 k 。

2.2.2 通过零知识证明保护隐私 - EigenTrust

我们提出的算法与原始的EigenTrust算法有两点不同。

首先，上面的简化描述允许节点伪装自己 t_i。最初的EigenTrust算法通过依靠分数管理器来管理每个节点的t_i计算。在原始方案中，每个节点具有三个得分管理器，通过分布式哈希表随机分配，其存储每个节点的T_{ij}值并为每个节点计算和存储t_i。虽然这解决了不诚实的节点攻击，但它在社交支付方案中并不理想，因为它需要与网络中的其他对等方共享交易信息。我们通过让每个对等方按照简化版本自己执行计算来解决这个问题，但是也很有可能向所有相邻节点证明它们已经正确地执行了计算。人们可以通过使用各种加密手段构建零知识证明来做到这一点，包括 [10], [3], [5]。

2.2.3 个性化的预信任的对等方

其次，为了打破恶意群组，并确保幂方法的收敛和主要特征向量的唯一性，EigenTrust引入了预信任对等方的概念，即一组活跃且被假定为普遍受信任的对等方。这确保了图形是非循环且强烈连接的（并且矩阵是不可约的，而问题是条件良好的）。但是，它要求系统定义一组普遍信任的对等方，并集中权力为那些预信任的对等方赋予声誉。

我们可以通过个性化解决这个问题。系统可以为每个对等方计算个性化的全局信誉向量，而不是计算单个全局信誉向量，从单个对等方 i的角度给出网络中每个对等方j的信誉得分。为了计算对等方 i的个性化EigenTrust，可以简单地执行传统的EigenTrust计算，而非使用对等 i的联系人列表作为预信任对等方的集合。

[3] 的相对水平成正比。构建问题的另一种方法是计算信任网络描述的遍历马尔可夫链的平稳分布。

这比单个EigenTrust计算的计算成本高得多；但是，我们应用了许多计算节省技术，使个性化的PageRank [13]能够进行个性化的EigenTrust计算。

2.2.4 实际意义

在社交支付案例中，人们向朋友汇款时，基于地址的加密方案足以作为轻量级身份代理，允许人们直接向他人的手机号码汇款，这些人还没有注册钱包。

由于人们有兴趣使用该协议向其直接联系人之外的人付费，因此用户能够聚合其网络中的人的信任信号以进行购买、支付和信用决策，并减少不良行为者。

此外，如我们所描述的信誉方案实现了更稳健的身份识别方案。大多数身份识别方案都是基于其他人的证明，并且如果能够通过证明者的信誉分数对这些证明进行加权，这将是很有用的。

3 稳定价值

使用加密货币作为支付手段的最大障碍可能是它们的波动性。消费者不太可能想购买价值易变的加密货币，因为他们的账户购买力会因市场对该货币的需求而波动很大。接受加密货币的商家可能会在付款后转换为法定货币，因为他们的商业模式不涉及对加密货币的推测。而今天最成功的加密货币不仅仅会发生价值波动而且还会通货紧缩 - 它们的成功导致价格上涨；结果，以货币计价的价格下跌。理性行为是将这些货币用作价值储存而不是交换媒介，而实际情况就是这样。

价值稳定的加密货币将为加密货币生态系统带来许多好处。首先，稳定的价格消除了使用加密货币作为交换媒介的相当大的障碍；工资、货物价格、固定义务，都可以用稳定的加密货币设定，而不要求任何一方推测货币的未来价值。此外，金融合约更容易用稳定的价值钱币建立，因为发行人可以将合约的功能与其计价的货币的价格风险分开。

虽然单一的价值稳定的货币会有所帮助，但是一个价值稳定的货币家族最能提供繁荣的加密经济，就像我们今天拥有的可变价值加密资产家族一样。当然，与美元挂钩的加密货币有多种用途，包括美国的社会支付到高通胀市场中用户启动的美元化，以及高频加密资产交易的有效结算。与此同时，与欧元挂钩的加密货币也有许多用途，比如在希腊，加密货币与一篮商品的价格挂钩，或者在旧金山，加密货币与一桶石油的价格挂钩。价值稳定的本地、区域和工具性货币允许人们通过以与他们经常使用的商品价格相比稳定的货币计算其个人经济的一部分来对冲其生活中的价格风险。

3.1 弹性钱币供应和转移波动风险

已经提出了几种用于价值稳定的分散加密货币的协议（例如 [17], [2], [1], [19]）。虽然对这些提案的全面审查超出了本文的范围，但它们通常有两个共同的属性。首先，它们不是确定性的钱币供应规则（其中钱币供应和增长率是预先确定的，与外生信息无关），它们各自引入弹性钱币供应规则，通过调整钱币的供应来满足需求，从而稳定钱币的价值。其次，它们各自引入了多资产生态学，其中一个钱币趋向于稳定，而一个或多个互补的加密资产承担稳定钱币需求减少的风险（并且在稳定钱币需求增加的情况下获得奖励）。

从本质上讲，它们都会将钱币持有者的波动风险转移到互补的资产持有者身上。

Celo协议使用相同的两个关键直觉，具有五个新颖的特征：(a)它引入了支持多种本地和区域价值稳定的货币的多资产分层储备，(b)它设定了调整到分层储备金定义的储备比率的扩展和收缩参数，(c)它引入了一个去中心化的交易所，其中不同的地方和区域货币和储备货币可以在没有中央方的情况下相互交易，并且该协议可用于进行扩张和收缩，(d)它以储备货币释放区块奖励和其他激励措施，并且(e)它有一个管理机制，其中储备货币的长期利益相关者负责管理储备资产和引入的新当地货币。

3.2 协议总结

在高级别，协议进行如下：

1. 该协议建立了一个固定的储备代币供应，称为Celo金币，其中一部分随着时间的推移而分配。从初始代币分配，一部分被置于储备并进行多样化。

2. 该协议还建立了一种支付方式货币，称为Celo美元，旨在与美元挂钩，遵守以下弹性钱币供应规则：
   当钱币供应需要扩大时（当Celo Dollar的价格高于挂钩价格时），协议会创建新的钱币，如 [17], [1], [2]所示。但是，协议不会将它们分配给利益相关者，而是利用它们购买一篮子加密货币[4]。这些购买被添加到储备中。这类似于中央银行通过在公开市场上购买金融资产并将其存入储备来扩大货币供应量。
   钱币供应仍然需要紧缩时，则该协议使用储备资产在公开市场上购买Celo美元。这类似于中央银行通过在公开市场上购买金融资产来收缩货币供应。

3. 协议对Celo金币收取可变利率转让费，以鼓励长期持有储备货币。该费用的收益用于支持准备金，而且该利率基于准备金率——准备金率越低，转让费用越高。

4. 协议使用保证金证明模型进行管治。治理决策中节点的权重取决于它们拥有的Celo金币的数额以及Celo金币绑定剩余时长[5]。这进一步鼓励了长期持有储备货币，并促使治理决策者的利益与Celo美元的长期稳定性保持一致。

5. 每次分配区块奖励时，都会释放等值部分的Celo金币。如果准备金率大大高于目标准备金率，那么释放的金额主要用于激励（例如，给开发者和用户）。如果储备比率大大低于目标储备比率，则释放的金额主要用于支持储备。

此协议的稳定性特性分析在[7]中提供。

[4] 最初，Celo金币通过交叉链分散交易，通过智能合约以市场价格，通过一篮子加密资产在可用时长期购买

[5] 更具体地说，治理决策中的节点权重取决于其拥有的数量以及必须提供以便提款的通知期限长短。请参阅 4.1部分了解更多详情

3.3 共享准备金

虽然单一稳定货币可用于多种用途（例如，用于加密交易和互联网商务），但一个本地、区域和效用型的具有稳定价值的货币体系可以构成更强大的生态系统。这种货币生态系统的好处已经得到广泛论述，例如在 [9], [16], [15] 中，但在这里我们只关注一点：稳定的货币只有在与使用该货币购买的商品和服务的价格相比稳定时才有意义。采用全球货币来开展地区性交易会在某些地区造成价格波动，特别是当地消费者价格动态与全球消费者价格动态变化存在不一致时[6]。

从协议的角度来看，我们在此对两种机制感兴趣：(a) 在治理方案中确定协议如何决定引入新的地区稳定性货币，以及 (b) 在结构中成功引入新的稳定货币后，能提高体系中的货币稳定性。

作为起点，我们可以想象有这样的一个协议，其中每种新的稳定货币都是相互独立——每种个新引入的货币都有相应的区块链和准备金。在这个方案中，管治问题很简单——团队将独立地在协议之外选择引入具有稳定价值的新货币，投资者可以独立选择购买货币及互补性加密资产。这个问题的管治是由市场决定的。

然而，这种简单操作是有代价的：新的稳定钱币的成功引入对现有的稳定钱币没有稳定作用，并有小量边际性破坏作用 [7]。

为了解决这个问题，我们引入共享准备金的构想。当协议引入一个具有稳定价值的新的货币——例如，与欧元挂钩的稳定货币，该货币与 Celo 欧元使用同一准备金。当 Celo 欧元的供应需要扩大时，它使用与 Celo 美元相同的机制扩展——该协议发行新的 Celo 欧元，并使用它们来为其准备金购买一篮子加密资产。Celo欧元供应需要紧缩时，该协议使用与前面相同的机制：出售储备资产以兑换为Celo欧元并淘汰Celo欧元。

该协议可以通过以下方式提高此流程的效率：在售出准备金之前，首先要看 Celo 美元的供应是否需要扩大。如果需要，它会发行 Celo 美元，以现行汇率直接兑换 Celo 欧元，并退出 Celo 欧元。这在功能上等同于卖出准备金以换取 Celo 欧元，退出 Celo 欧元，然后购买准备金以换取 Celo 美元；它只是免除了准备金的中间媒介作用。如果 Celo 欧元的收缩需求大于协议支持的所有其他稳定货币的扩展需求，它只会直接使用准备金。

共享准备金体系必须采用周全的方法来针对引入何种新的稳定货币以及何时引入的问题做决策。如果引入一种对生态系统具有负面效用的新的稳定货币，对该货币的需求足够高并且波动性足够强（例如，早期的名人效应稳定币），或者如果货币减少了对协议支持的其他货币的总需求（例如，在同一区域引入了几个没有差异化的重复性区域货币，从而造成混淆），便有可能对其他货币的稳定性产生边际负面影响。出于这个原因，有必要在管治模型中做出规定，仅在人们普遍预期新的稳定币的引入会增加对货币体系的长期性总体需求时，才有必要加以引入。我们将在 4.4.2一节讨论管治模式。

值得注意的是，共享准备金体系不要求所有新货币都使用共享准备金。事实上，对于本地或功能型货币，有几个原因可以解释为什么不参与共享准备金模型是有用的；我们会在 4.4.4一节加以讨论。为了支持这些货币，我们还允许用自己的准备金发行新的

[6] 例如，欧元进入希腊，或者在在乌拉圭使用美元

[7] 如果新的稳定钱币的需求足够高，它可能会导致对现有稳定钱币的需求紧缩，减少与现有钱币的补充资产相关的价值，并增加现有钱币长期需求的不确定性。

代币；我们称之为分割准备金。简而言之，该机制以与单一稳定值货币具有相同的运作方式。不同点在于，第三方可以发行代币并启动其准备金。对于分割准备金，准备金的每个份额最初为 25% Celo 黄金，25% 当地准备金货币，其余从额与共享准备金等同。

3.4 价格发现和准备金资产购买机制

Celo 协议作为以太坊的分支实施。Celo网络中的计算成本以Celo金币支付，就像以太坊用来在以太坊网络中支付天然气一样。Celo 稳定代币作为 ERC20 代币的等效物而实施。Celo 和以太坊之间的一个区别是，虽然 Ether 本身不符合 ERC20 代币标准，但 Celo 黄金却符合。这允许通过智能合约在 Celo 稳定价值代币和 Celo 黄金之间进行分散交易，就像 0x [21] 那样。这允许自动购买储备和分配钱币，而无需交叉链的分散交易。

为了确定Celo稳定货币的价格，我们在利益相关者中使用谢林点(Schelling-point)计划，利益相关者投票的权重取决于拥有的Celo金币数量和持有剩余时间。可以想象，通过治理方案确定的交易所提供的价格源会进一步扩展谢林点方案。

4 治理和激励

Celo的一个主要激励机制是区块奖励的分配，这些奖励分配给系统中的各个贡献者，包括那些维护协议的人员（通过选择验证器、验证交易、验证用户和参与谢林点价格发现机制），那些有助于储备稳定性的人员，那些在存在紧缩的情况下承担风险的人员，那些使用协议作为付款方式的人员，那些邀请其他人使用协议的人员，以及那些改善协议的人员（通过参与治理以及对协议做出技术贡献）。我们在下面加以描述。

4.1 维护系统

系统使用保证金证明机制来选择验证器集并参与治理决策。验证器选举和治理决策均通过抵押保证金加权投票方案做出。任何Celo金币持有者都可以设置抵押保证金，这涉及将Celo金币发送到智能合约，并指定一个通知期限，以在要求[8]。投票（针对验证器和治理）均按抵押Celo金币数量和通知期限时间加权。这进一步激励了长期持有储备货币，并促使治理决策与长期观点保持一致。在参与验证器选择和治理决策的人员中分配区块奖励。

用户不为验证器直接投票。相反，验证器需要将自己组织成组，并且帐户持有者将为这些验证器组投票。就像民主国家中的任何人都可以创建自己的政党或试图被选举代表某个政党参加选举一样，任何Celo用户都可以创建一个验证器组并将自己添加到其中，或者要求现有验证器组将其包括在内。验证器选择每个时期举行一次，大约相当于每天一次。

验证器一经当选，将投入一笔可观的抵押保证金，参加共识计划，发送验证消息，参加价格发现的谢林点计划，并获得区块奖励，以支付其费用并激励他们的系统维持工作。

[8] 提款后等待的时间最少为抵押期限60天

4.2 在必要时提升储量并收缩稳定价值货币的供应

Celo 黄金持有人通过购买 Celo 黄金，为 Celo 黄金提供初始价值，并将其他加密资产引入准备金。此外，Celo金币持有者在供应紧缩或储备减少的情况下承担一定风险：如果储备比率低于目标储备比率，则收取转移费用，如果对Celo稳定货币的需求长期萎缩，Celo金币的价值可能会下降。Celo金币持有者因以下两种方式担任这些角色而获得奖励：首先，由于对Celo稳定货币需求的增加，将会有更多协议导向的Celo金币购买行为，从而增加了对固定供应的需求。其次，如果准备金率高于目标准备金率，那么持有 Celo 黄金长期股权的 Celo 黄金持有人将获得部分区块奖励（前提是他们参与交易验证的共识达成，在被选中时发送验证消息，并参与谢林点投票以进行价格发现）。这些奖励按照持有的Celo金币数量和持有剩余时间的比例支付。

4.3 扩充系统用户群和提高使用频率

活跃用户（使用付款协议、通过移动钱包参与电话号码验证以及维持Celo金币的名义份额的人员）将通过区块奖励获得奖励。实际上，这减少了活跃用户的交易费用。（人们甚至可以想象这样一种场景，即以在单位时间内对稳定货币的一定数量交易免除交易费的方式发放这些区块奖励，通过以部分区块奖励来支付用户的交易费用，设置一定的费率以确保一定的交易速度，并根据其持有数量确定优先顺序。）

4.4 改进协议

最后，协议的不断发展需要激励和治理方案来改进协议。

4.4.1 技术改进

对于协议的技术改进，任何人都可以按定期周期投入一笔抵押保证金，提出有偿实施的技术方案[9]。提案将由长期利益相关方投票，类似于含Dash主节点[8]的投票方案，其投票权由其持有数量和通知期间加权而得。未在特定周期中分配的资金将添加到准备金中。

4.4.2 引入区域货币和扩大准备金基础

随着时间的推移，它还将改进协议，引入更稳定的价值货币，并扩大准备金。如果适当引入新的稳定价值货币，它们可以增加协议的有用性，促进货币需求的长期增长，并减少总需求波动。如果正确选择新的加密资产，可以降低准备金波动性。两者都具有进一步稳定协议所支持货币的效果。 这些引入的管治程序类似于围绕技术改进的管治。

按定期间隔，任何Celo金币持有者都可以通过一定数量的Celo金币来提出引入新的稳定价值货币的提案（指定挂钩）。当期Celo金币持有者按照拥有的Celo金币数量和持有剩余时间的比例投票。如果达到某个投票阈值，则在共享准备金中引入新的稳定货币。

[9] 这种机制也可以应用到其他类型的建议，例如营销提案。

同样，任何 Celo 黄金持有人都可以通过一定数量的 Celo 黄金，提出向准备金引入新的加密资产的建议（通过指定未来准备金中将分配给该资产的建议购买百分比）。长期Celo金币持有者按照持有的Celo金币数量和通知期限时间量的比例投票。如果通过某个投票门槛，那么未来对准备金的购买将包括新的加密资产，其配额为所有投票的中位百分比（所有其他资产的分配按比例稀释）。

评估这些提议的标准是它们在货币的长期稳定性方面会起多少促进作用。向储量引入加密资产可以增加准备金的预期升值，并降低准备金的波动性，这将对长期货币稳定性产生积极影响。推出新的稳定价值货币，增加长期总货币需求，减少货币需求总体崩塌的可能性，也增强了货币的稳定性特征。

4.4.3 Futarchical 管治

未来，我们可能会将市场预测作为一种补充形式的管治——预测市场也会考虑准备金构成的变化或稳定币组合的构成是否会长期加强或减弱货币的稳定性。在 futarchical 管治范式中，甚至有可能直接以预测市场作为表决机制[11]。这是将来工作的方向。

4.4.4 分割准备金

如果没有共享储备的支持，则引入新的本地货币不需要管治流程。人们可以推出一种新的本地货币，由自己的准备金支持，拥有自己的附属本地准备金货币，类似于单一的 Celo 美元和 Celo 黄金。在这些情况下，默认准备金将在其准备金中包括一篮子多样化的加密资产，包括 Celo 黄金、当地准备金货币和 Celo 美元等。

这样做带来很多可能性。首先，这些当地协议可以选择将一些本地准备金货币分配给所有当地居民，有效地创造社会红利，使当地居民能够从增加采用的当地货币中受益。

这些本地协议也可以选择以不同的方式实施转让费；当准备金比率较低时，他们可以选择通过定期地（而不是仅在保证金比率低于当地稳定货币的情况下）直接以当地稳定货币而不以当地准备金货币支付转账费用。这种滞期费的实施具有增加准备金和鼓励当地支付方式货币流通的效果，其代价是可能推动人们替换货币。尽管存在这个缺点，关于滞期费的文献（例如，参见 [9], [15]）表明值得对滞期费开展更多试验。

最后，随着越来越多的资产在未来被代币化，分割准备金机制允许准备金包括实际资产。这从稳定性的角度来看是有帮助的，并且还允许自然资本支持的支付方式货币（例如，由林地支持的货币），其中对这些货币的需求增长将增加支持它们的自然资本量。有关自然资本支持货币的详细讨论，请参阅[9]。

5 结论

我们引入了一种名为 Celo 的社会支付协议。Celo结合了基于地址的加密协议，允许发件人直接使用电话号码或电子邮件地址作为公钥，并通过储备支持的协议通过弹性供应规则将波动性降至最低。总之，这样可获得使用加密货币作为支付手段的无缝体验。此外，它们实现了由本地和区域货币、社会红利、滞期费货币以及未来的自然资本支持货币构成的一个货币生态系统。

参考

[1] Nader Al-Naji, Josh Chen, and Lawrence Diao. Basis: A price-stable cryptocurrency with an algorithmic central bank. 2017.

[2] Ferdinando M Ametrano. Hayek money: The cryptocurrency price stability solution. 2016.

[3] Eli Ben Sasson et al. Scalable, transparent, and post-quantum secure computational integrity. 2017.

[4] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001*, pages 213–229. Springer, 2001.

[5] Benedikt Bunz et al. Bulletproofs: Efficient range proofs for confidential transactions. 2017.

[6] Sanjit Chaterjee and Palash Sarkar. *Identity-Based Encryption*. Springer, 2011.

[7] Roman Croessman et al. An analysis of the stability characteristics of Celo. 2018.

[8] Evan Duffield and Daniel Diaz. Dash: A privacy-centric crypto-currency, 2014.

[9] Charles Eisenstein. *Sacred economics: Money, gift, and society in the age of transition*. North Atlantic Books, 2011.

[10] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. 18:186–208, 1989.

[11] Robin Hanson. Futarchy: Vote values, but bet beliefs. 2000.

[12] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification, version 2018.0-beta-20. 2018.

[13] Sepandar Kamvar. *Numerical Algorithms for Personalized Search in Self-Organizing Information Networks*. Princeton University Press, 2009.

[14] Sepandar Kamvar, Mario Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in peer-to-peer network. In *Proceedings of the 12th international conference on World Wide Web. ACM*. ACM, 2003.

[15] Bernard A Lietaer. *Mysterium Geld: Emotionale Bedeutung und Wirkungsweise eines Tabus.* Riemann, 2000.

[16] Bernard A Lietaer. *The future of money: A new way to create wealth, work and a wiser world*. Century, 2001.

[17] Robert Sams. A note on cryptocurrency stabilisation: Seigniorage shares. Technical report, Working paper, 2015.

[18] Adi Shamir et al. Identity-based cryptosystems and signature schemes. In *Crypto*, volume 84, pages 47–53. Springer, 1984.

[19] Maker Team. The dai stablecoin system. 2017.

[20] Lloyd Trefethen and David Bau. *Numerical Linear Algebra.* SIAM, 1997.

[21] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain, 2017.