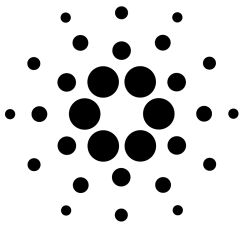

为何我们正在建立卡尔达诺

CHARLES HOSKINSON

<Charles.Hoskinson@iohk.io>

<C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66>

中文翻译：Hsinying Lin

1. 绪言

动机

卡尔达诺是一项从2015年开始的项目，旨在改变加密货币的设计和开发的方式。超越一系列创新的总体，重点是提供一个更加平衡和永续发展的生态系统，更佳地描述其用户以及其他寻求整合系统的需求。

本着许多开源项目的精神，卡尔达诺并没有从全面蓝图开始，甚至没有一个权威的白皮书。相反地，它包含一系列的原则，工程最佳实践和探索途径。这些包括以下的内容：

- 将会计和计算分为不同层次
- 在高度模块化的功能代码中实现核心组件
- 小组学者和开发人员与同行评审研究进行竞争
- 大量使用跨学科团队，包括早期使用InfoSec专家
- 迅速的迭代发生于白皮书，实施和需要通过审查期间发现问题进而更正的新颖研究
- 建立具有在不破坏网络环境下进行升级部署后系统的能力
- 制定未来运作所需的分散资金机制
- 通过长期观点改进加密货币的设计，以便它们在移动设备上运行时，具有合理和安全的用户体验
- 让利益相关者更加接近他们所拥有的加密货币之运营和维护
- 承认需要对同一个分类帐中的多项资产负责
- 交易包括可选元数据，以更佳符合传统系统的需求
- 通过从将近1000种的山寨币中学习，含括其有意义的功能
- 采用由互联网工程任务组启发的标准驱动流程，使用专门的基础来锁定最终的协议设计
- 探索商业的社会元素
- 为监管机构寻找一个健康的中间环节，与商业活动进行互动，并且不会影响从比特币继承的一些核心原则

从这个非结构化的想法，投身于卡尔达诺的负责人员开始探索密码学文献，并建立一个抽象的工具集。本研究的结果是，IOHK广泛的论文库，许多研究调查的结果，如最近的脚本语言概述以及智能合约本体论和Scorex项目。经验教训让我们欣赏到加密货币行业的独特性与其有时也会适得其反的增长。

首先，与成功的协议（如TCP / IP）不同，加密货币的设计几乎没有分层。 一直渴望保留一个单一的共识概念—可在单个分类帐中记录事实和事件，而不管它是否可行。

例如，以太坊陷入了巨大的复杂性，试图成为一个世界通用电脑的同时，却受困于一些琐碎的考量—可能会破坏该系统具有价值存储的能力。是否每个人的计划应该是一流的公民，而不顾其经济价值，维护成本或是监管后果？

第二，对主流加密研究的早期先前几乎无感激之意。例如，Bitshares授权的权益证明可以轻松可靠地产生随机数字，使用抛硬币确保输出交付，这是自80年代以来已知的技术（参阅Rabin和Ben-Or的研讨论文）。

第三，大多数的山寨币（除了一些显着的例外，例如Tezos）没有为未来的更新提供任何适应性。成功推动软叉或硬叉的能力对于任何加密货币的长期成功至关重要。

以推论而言，企业用户无法为协议提供数百万美元的资源，因为协议本身的蓝图和其背后扮演的角色是短暂的，轻率的或是激进的。需要有一个有效率的程序，通过这个程序，社会共识可以围绕着基础协议演变的愿景而形成。如果这个程序非常繁重，那么分裂则可能会破坏这整个社区。

最后，金钱终究是一种社会现象。为了尽力地匿名和中断中央角色，比特币及其同辈人也放弃了在商业交易中需要的稳定身份，元数据和声誉。通过集中式解决方案添加这些数据，以删除审计性，全球可用性和不可变性 — 这是使用区块链的重点。

诸如由SWIFT，FIX和ACH构成的传统金融系统，丰富了交易的元数据。不仅了解帐户之间的价值转移还不够，监管往往需要参与者的属性，合规信息，报告可疑活动以及其他记录和行为。在某些情况下，元数据甚至比交易更为重要。

因此，可以合理推断操控元数据，可能带来与伪造货币或重写交易历史一样的伤害。对于想自愿参与这些领域的人们造程不便，仿佛与主流和消费者保护适得其反。

旅居的結束

于加密货币空间聚集我们的原则探索是协议的两个集合，分别地，一个根据加密货币的可证安全权益证明(Proof-of-Stake)[1][2]，称为卡尔达诺结算层(CSL: Cardano Settlement Layer)；和一组协议称为卡尔达诺计算层（CCL: Cardano Computation Layer）。

我们的设计重点是为了适应加密货币的社会面，通过将价值核算分离于复杂计算的层次构建，并在几种不变原则的范围内解决监管机构的需求[1]。此外，明智的是我们试图通过同行评审和对正式规范的检查代码来审查所提出的协议。

权益证明

于加密货币中使用权益证明，是一个激烈辩论的设计选择，但是由于权益证明添加了导引安全投票的机制，且具有更多的扩展能力，并允许更多异域的激励计划，所以我们决定采用它。

我们的利益证明协议被称为乌洛波罗斯，它是由五个学术机构中[2]，非常有才华的密码学小组设计而成。由爱丁堡大学的Aggelos Kiayias教授带领。它使用严格的加密模型,已予证明安全的核心创新是一种模块化和灵活的设计，允许许多协议的组合来增强其功能。

这种模块化允许诸如授权，侧链，可订阅的检查点，轻型用户端的更佳数据结构，不同形式的随机数生成以及甚至不同的同步假设特征。随着从数十亿甚至数千亿用户的网络发展，其共识算法的要求也将发生变化。因此，至关重要的是要有足够的灵活性来适应这些变化，进而使加密货币的核心具有未来保证。

货币的社会元素

加密货币是货币社会组成的一个主要例子。当将纯粹地分析仅限于技术时，比特币和莱特币之间几乎没有区别，而以太坊和以太坊经典之间的差异更小。然而，莱特币和以太坊经典都拥有庞大的市值，强大的动态社区以及其本身的社会责任。

可以认为，一个加密货币的大部分价值来源于其社区，它使用货币的方式和参与货币演化的程度。进一步思考，像达世币这样的货币，甚至可以将其系统直接整合到协议中，让社区决定其应该优先开发和资助的项目。

[1]参閱監管部分

[2]康涅狄格大学，大学雅典大学，爱丁堡大学，奥胡斯大学，东京理工大学

加密货币的广泛多样性也为其社会元素提供了证据。关于哲学，货币政策，甚至核心开发商之间产生的分歧和分散。然而，与加密货币对等物不同的是，超级大国的货币政策往往试图不要引起任何货币危机或是大规模的货币流失，进而能够幸存于其政治转变和地方分歧。

因此，似乎有一些保留系统的元素从加密货币领域中遗失。我们认为 - 并且已经渗透到卡尔达诺蓝图中 - 一个协议的用户需要激励机制以了解其协议背后的社会契约，并且拥有自由以积极的方式提议改变。这种自由扩展到价值交换系统的各个方面，从决定市场应该如何管理到应该资助哪些项目。然而，它不能通过集中的行动者来斡旋，也不需要一些特殊的凭证，这些凭证意指资金充足的少数人之共同选择。

卡尔达诺将实施一个基于卡尔达诺结算层(CSL)的覆盖协议系统，以适应其用户需求。

首先，不管众筹如何成功地引导发展，最终资金将消散。因此，卡尔达诺将包括一个分散信托[3]，由单调递减的通货膨胀和交易手续费提供资金。

任何用户都有资格通过投票系统向信托机构申请资金，并且由卡尔达诺结算层(CSL)的股东投票表决谁成为受益人。该过程已在其它具有财政/信托系统的加密货币中可见，通过开始谈论关于应该和不应该资助谁，创建一个积极的反馈循环，如Dash。

资金谈论迫使建立一个长期和短期目标的关系，加密货币的社会契约、优先事宜和具有具体建议的价值创造信念。这个谈论意味着社区可不断地评估和辩论其信念，反抗可能的蓝图。

第二，我们希望卡尔达诺最终将在软叉和硬叉含括一个正式的、基于区块链的系统来提案和投票。比特币有其区块大小的争论、以太坊有DAO分叉，此外许多其他加密货币，长期以来，并且经常对代码库的技术和道德面的争议是尚未解决的。

它可以而且应该被认为，许多这些分歧，以及在采取行动时产生的社会破裂，是由于缺乏辩论变革的正式进展的直接结果。

哪里说服比特币用户采用隔离见证？以太坊的核心开发人员应该如何衡量社区的情绪来拯救DAO？如果社区发生破裂，则该加密货币的损坏将无法修复？

在最坏的情况下，行为的道德权力可直接转移至任何拥有开发商、基础设施关系和金钱的人，而非绝大多数社区的最佳期许。更进一步，如果大部分的社区由于不良的激励机制而无法参与或脱离[4]，那么人们如何真的得知他们的行为是否合法？

[3]也称为财政系统

[4]请参阅理性的无知

提案的加密货币如Tezos提供了一个有趣的模型，以检查一个加密货币协议如何被处理，例如包含三个部分（交易、共识和网络）的宪法，以及一套正式的规则和过程来更新宪法。然而，仍然有许多工作要进行的激励措施，以及如何用正式语言来建模和更改加密货币。

正在探索使用正式的方法、机器可理解的规范，并将财政与财务奖励的过程相结合，作为可能的灵感途径。最终，只要能够以透明、基于区块投票的免审查方式提出协议变更的能力，那么应该可以改进流程，即使无法设计更简练的解决方案。

层次设计 -卡尔达诺结算层

当设计出很好的协议和语言时，应该不要期待未来，而是回顾过去。历史提供了一系列在纸面上完美的伟大想法的例子，但不知何故还没有幸免于难，如开放系统互连标准。历史还提供从TCP / IP到JavaScript的愉悦偶然。

从历史观点汇整的一些原则如下：

1. 你不能预测未来，所以只能建立在摆动的空间中
2. 复杂性在纸面上表现很好，但通常胜出的是简
3. 人多手杂反坏事
4. 一旦标准被设置，它可能会不断持续下去，而不论其是否因应环境仍是最佳的
5. 若有意愿，坏的想法实际上可以演变成相当不错的想法

卡尔达诺是一个接受社会性质的金融体系。将非常需要灵活性和解决特定用户交易中任意复杂性的能力。若成功，将需要巨大的计算、存储和网络资源来容纳数百万个并发交易。

然而，我们没有一个数字的，分散的罗宾汉从丰富的节点中获取，并给穷困的，以实现一个公平的网络。我们也不相信人类利益，为了更大的网络利益而牺牲自身利益。因此，卡尔达诺的设计借鉴了TCP / IP分离关注的概念。

区块链最终是对事实和事件的数据库进行排序，保证了时间戳和不变性。在金钱的背景下，它们命令资产的所有权。通过存储和执行程序来增加复杂的计算是一个正交的概念。我们想知道有多少价值从爱丽丝转移到鲍勃，还是想要弄清楚交易背后的整个故事，然后决定发送多少价值？

如以太坊所做的，因为它更灵活，所以选择后者是非常诱人的，但它违反了上述的设计原则。了解整体故事意味着单个协议必须能够理解任意事件、撰写任意交易、允许在欺诈的情况下进行仲裁，甚至在新信息可被创造时可能进行逆向交易。

然后，必须对每个交易存储的元数据做出困难的设计决策。爱丽丝和鲍勃交易背后的故事有哪些元素是相关的？它们是永远相关的吗？什么时候可以丢掉一些数据？这样做是否违反了一些国家的法律？

此外，一些计算本质上是隐私的。例如，在计算办公室工作人员的平均工资时，我们不一定需要泄漏每个人的工资。但是如果每个计算都是公开的呢？如果这种宣传偏袒执行令危害结果怎么办？

因此，我们选择了将价值的会计与价值被移动的故事背景分离的立场。换句话说，将价值与计算的分离。这种分离并不意味着卡尔达诺无法支援智能合约。相反地，通过明确地分离，允许在智能合约的设计、使用、隐私和执行方面有更大的灵活性。

价值分类帐称为卡尔达诺结算层（CSL）。为了解释价值，蓝图有以下目标：

1. 支持两套脚本语言，一种用于移动价值，另一种用于增强覆盖协议支援
2. 提供对KMZ侧链的支持[5]链接到其他分类帐
3. 支持多种类型的签名，包括用于更高安全性的量子阻抗签名
4. 支援多用户发行的资产
5. 实现真正的可扩展性，意味着随着更多用户的加入，系统的功能也随之增加

撰写

从脚本语言开始，分类帐中的地址之间的交易需要某种形式的脚本来执行并被证明是有效的。理想的情况下，没有人希望以芙能够介入爱丽丝的钱，也不希望设计不好的脚本意外地将价值发送给一个无效地址，从而使资金无法回送。

诸如比特币等系统提供了一种极僵化和严厉的脚本语言，难以对定制的交易进行编程、阅读和理解。然而，诸如Solidity之类的一般可编程性的语言在系统中引发了非常多的复杂性，并且对于只有较小的一组参与者是有效的。

因此，我们选择设计一种称为Simon的新语言[6]，以纪念其创始人Simon Thompson和Simon Peyton Jones的启发思想的创造者。 Simon 是基于*构成合约：金融工程的冒险*之撰写的领域专用

[5]即将在Kiayias，Zindros和Miller发布的一篇文章中

[6]具体内容将在即将发布的规范中公布，2017年第四季的“雪莱卡尔达诺结算层版本”将支持该语言

语言。

主要的想法是，金融交易通常由基础元素的集合组成[7]。如果有一个组合元素的财务周期表，那么可以为任意大型的复合交易提供支援，这些复合交易将覆盖大多数，若不是全部，那么常见的交易类型则不需要一般的可编程性。

主要优点是可以极为了解安全性和执行性。可以编写证明来显示模板的正确性，并排除有问题的交易事件的执行空间，例如从稀薄的空气或交易可扩展性创建新的货币。第二，如果需要新的功能，可以通过软叉分离扩展来添加更多的元素。

也就是说，必须总是将卡尔达诺结算层连接到覆盖协议、传统金融系统和专用服务器。因此，我们开发Plutus作为通用智能合约语言和DSL专用的相互操作。

Plutus是基于Haskell概念的类型函数语言，可用于编写自定义交易脚本。对于卡尔达诺结算层，它将被用于我们需要连接的其它层次的添加支援所需的复杂交易，例如我们的侧链方案。

侧链

对于侧链，卡尔达诺将根据以前的工作证明结果支援Kiayias，Miller和Zindros（KMZ侧链）开发的新协议。具体设计超出了本文的范围; 然而，该概念允许从卡尔达诺结算层到任何卡尔达诺计算层或支援该持协议的其它区块链的资金的安全和非交互式移动。

KMZ侧链是封装复杂性的关键。具有监管要求、隐私操作、强大的脚本语言和其他特殊问题的帐本，实际上是卡尔达诺结算层的黑盒子，卡尔达诺结算层用户将获得关于会计的一些保证，以及在计算完成后召回资金的能力。

签名

为了安全地将价值从爱丽丝转移到鲍勃，爱丽丝需要证明她有权移动资金。完成此任务的最直接且可靠的方法是使用公钥签名方案，爱丽丝的资金连接到公钥，而爱丽丝控制相关联的私钥。

有数百种可能的方案具有不同的安全参数和假设。一些方案依赖于连接到椭圆曲线的数学问题，而另一些则使用网格连接到异乎寻常的概念。

[7]项目ACTUS有一个深入的阐述

抽象的目标总是相同的。现实存在一个难以解决的难题，除非有一个秘密的知识。据说这一知识的持有者是钥匙配对的所有者，应该是有能力使用它的唯一实体。

在选择签名方案时，有两组关于安全性的问题。首先，方案本身具有长期的安全性。 70年代和80年代使用的一些加密方案，如DES已被破解。此超越该方案应该有效的期间必须被决定。

其次，有很多企业、政府和其他机构倾向于或在某些情况下要求使用特定的方案。例如，NSA维护Suite B协议集。 ISO，甚至W3C加密工作组都具有其标准。

如果一个加密货币选择一个单一的签名方案，那么在未来的某个时间点被强制接受该方案可能会被破坏，则至少有一个实体由于法律或行业限制而不能使用这种加密货币。然而，一个加密货币不能支援每种签名方案，因为这将需要每位客户了解和验证每种方案。

对于卡尔达诺，我们决定从使用椭圆曲线密码学开始，特别是Ed25519曲线。我们还决定通过使用Dmitry Khovratovich博士和Jason Law的规范增加对分层确定性钱包的支援[8]。

可说卡尔达诺将来会支援更多的签名方案。特别是，我们有兴趣将BLISS-B整合到我们的系统中添加量子计算机抵抗签名。我们也有兴趣含括SECP256k1以增强与传统加密货币（如比特币）的相互操作性。

卡尔达诺已经设计了特殊的扩展，将允许我们通过一个软叉增加更多的签名方案。它们将根据需求和在蓝图计划中的主要更新一起添加[9]。

用户发行资产（UIAS: USER ISSUED ASSETS）

早期的比特币历史，协议很快开发出来，允许用户发行搭载比特币会计系统的资产，以便同时跟踪多种货币。这些协议本来不是比特币协议所支援的，而是通过聪明的黑客实施的。

在比特币覆盖如彩色币和万事达币（现称为全方位）的情况下，轻型客户被迫依赖可信赖的服务器。还必须在比特币中支付交易费用。这些属性与单一管道结合进行交易审批，使比特币未达适合多资产会计的最佳标准。

[8]这是卡尔达诺的分层确定性电子钱包的实施文档，我们相信卡尔达诺是第一个支援Ed25519分层确定性钱包的加密货币

[9]请参阅cardanoroadmap.com

在以太坊中使用ERC20标准，功能丰富度更高。但是，仍然需要交易费用。此外，以太坊网络难以扩展到所有已发行的ERC20令牌的需求。

基本问题可以分为三个部分：资源、激励措施和关注。在资源方面，向同一分类帐增加一种全新的货币意味着有两个独立的UTXO（未用的交易输入）集合共享带宽、内存池和区块空间。负责嵌入这些货币交易的共识节点需要执行的奖励措施。并不是每位加密货币的用户都可以或应该关心特定实体的货币。

鉴于这些问题，效益是非常巨大的，因为多重分类帐的主要标志可以有效地用作允许分散市场化的桥梁货币。可以发行特殊目的资产，以提供额外的实用工具，如价值稳定的资产，像是可用于贷款和汇款申请的Tether或MakerDAO。

对于这些挑战，卡尔达诺采取了务实的方法来实现多重会计。第一个挑战是设计必要的基础设施，以支援数千个用户资产发行的需求。亦即以下进步是必须的：

1. 特殊用途的认证数据结构，可以追踪非常大的UTXO（未用的交易输入）状态
2. 拥有一个分布式内存池以容纳一大批待处理交易的能力
3. 区块链分区和检查点允许一个巨大的全球区块链
4. 奖励共同节点的奖励方案，包括不同的交易集合
5. 一种订阅机制，允许用户决定他们要追踪的货币
6. 强大的安全保障，用户发行资产享有与本地资产相似的安全性
7. 支援分散化市场，以改善用户发行资产与主要标志之间的流动性

我们初步的努力是寻找正确的认证数据结构，由Leo Reyzin、IOHK和Waves共同开发的一种新型AVL + Tree。虽然需要更多的研究，但它将是一个基础的进步，其将被纳入卡尔达诺的更新版本。

分布式内存池可以使用斯坦福大学的RAMCloud协议实现。实验将于2017年第三季度开始，以研究其与卡尔达诺共识层的整合。

剩下的主题是相互关联的，并且由正在进行的研究所含括。在2018年卡尔达诺结算层发行Basho版的期间，我们期待 - 在研究成果的基础上，将协议纳入卡尔达诺的用户发行资产。

可扩展性

分布式系统由一组计算机（节点）组成，同时运行协议或协议套件来实现共同目标。此目标可能是由BitTorrent协议定义的文件共享或使用Folding @ Home的蛋白质折叠。

最有效的协议在节点加入网络时获得资源。例如，BitTorrent托管的文件，如果许多对等体同时下载它，它可以平均被更快地下载。速度增加，因为对等体提供资源同时也消耗它们。这个特征说明了分布式系统的尺度的典型意涵。

所有当前加密货币的设计所面临的挑战在于，它们实际上不是设计为可扩展的。例如，区块链通常是一个仅附加链接的区块列表。区块链协议的安全性和可用性依赖于具有区块链数据的完整副本的许多节点。因此，必须在N个节点中复制单个字节的数据。附加节点不提供额外的资源。

此结果对于整个系统中的交易处理和消息传递是相同的。向共识系统添加更多节点却不提供额外的交易处理能力。这只意味着需要花更多的资源来做同样的工作。更多的网络中继意味着更多的节点必须传递相同的消息，以保持整个网络与最新的区块同步。

鉴于这种拓扑，加密货币无法与传统金融系统相提并论。相比之下，传统基础架构是可扩展的，并且具有数量级以获得更多的处理和存储能力。增加一个特定点，比特币是一个非常小的网络相对于其支付对等体，但受困于管理其当前的负载。

我们对于卡尔达诺的可扩展性目标得到我们共识算法的极大帮助。乌洛波洛斯允许一种分散方式选择一个共同节点的法定人数，反过来又可以运行更多的传统协议，这些协议在过去20年中陆续开发，以适应大型基础设施供应商（如Google和Facebook）的需求[10]。

例如，选择一个纪元的法定人数意味着我们有一个值得信赖的节点集合来维持一个特定时间点分类帐。同时选举多个法定人数，并将交易划分到不同的法定人数，这是微不足道的。

类似的技术可以应用于网络传播，也可以将区块链本身分割成独特的分区。在我们目前的蓝图中，伸展方法将从2018年开始适用于乌洛波洛斯，并将继续成为2019年和2020年的开发重点。

[10]还有其他独立研究协议试图实现同样的目的，如Elastico和Bitcoin-NG

卡尔达诺计算层

如前述般，一个交易有两个组成部分：发送和记录令牌流的机制以及移动令牌后的原因以及条件。后者可以是任意复杂的，涉及到数兆位元组数据、多重签名和特殊事件的发生。后者也可以是非常简单的，使用单一签名将价值推送到另一个地址。

监控价直流的原因和条件所存在的挑战在于它们是用最不可预测的方式，由极为私人到实体的过程参与其中。我们从合约法中学到一个更有问题的景象，参与其中的角色本身甚至可能不知道交易与商业现实不符。我们通常把这种现象称为“语义差距”[11]。

为什么要建立一个追求无限层次的复杂性和抽象的加密货币？它似乎是永无尽头而又徒劳无功任务的天性，并且是实践中的天真。此外，每个摘要都拥有法律和安全的后果疑虑。

例如，在网上有许多普遍被认为是非法或蔑视的活动，如贩卖儿童色情物品或出售国家机密。通过部署强大的分散式基础设施，人们现在为这种活动提供了一个通道，与正常的商业交易具有相同的审查阻力。如果网络中的共识节点有动机随着时间的推移变得更联合，以提高效率，则在法律上不清楚是否会对它们所承载的内容负责。

起诉Tor经营者、对丝绸之路经营者的残酷待遇以及议定书参与者法律保护背后缺乏全面法律上明确的规定，造就了一条不确定的道路。不乏想象除了一个足够的先进加密货币之外还有什么可以将此付诸实现（请参阅“袭格斯戒指”）。迫使所有加密货币的用户支持或什至纵容这最糟的行为或是网络恶行，其是否合理？

不幸的是，没有明确的答案可以为加密货币的设计提供深刻见解。更重视的是选择职位，捍卫自己的荣誉。卡尔达诺和比特币的优势在于我们选择将问题用层次分离。就如同比特币有巴比特，而卡尔达诺有卡尔达诺计算层般。

这使得以前阐述的行为之复杂行为的种类不能在卡尔达诺上运行。它们需要运行以图灵完整语言编写的程序和某种形式的气体经济学来计算电脑能力。它们还需要共识节点愿意将交易包含在其区块中。

因此，功能限制可以合理地保护用户。至今，大多数建立完善的政府还没有采取表明使用或维护一个加密货币是非法行为的立场。因此，绝大多数用户应该舒适地维护与数字支付系统具有相当能力的分类帐。

[11] Loi Luu等人在最近关于使智能合约更智能的文章中讨论到这个差距

当人们想扩展能力时，有两种可能性。它是由一个私人集体志同道合的个人和短暂性功能（例如，一个扑克游戏）。或者，它是由与以太坊相似功能的分类帐所实现。在这两种情况下，我们选择将事件外包给另一个协议。

在隐私短暂事件的情况下，虽然完全避免区块链范式是合理的，但宁愿限制对一组特定参与者，当需要时可以调用特殊目的MPC协议库的努力。计算和活动在专用网络中进行协调，并在必要时将卡尔达诺结算层作为可信公告板和消息传递通道。

在这种情况下的关键见解是，同意、责任和隐私的封装。卡尔达诺结算层被用作用户的数字共识，以便用户进行会议和沟通，如在公园举办私人活动，但不提供任何特殊的住宿或设施。此外，使用专用MPC将能够实现低延迟交互，而不需要膨胀区块链。因此，它提高了系统的规模。

卡尔达诺对这文库的研究工作汇集于我们的东京工业大学实验室，并且拥有许多国外科学家的协助。在数学家们以及当代卡尔达诺的同伴下，我们称该文库为“塔尔塔利亚(Tartaglia)”，并预计在2018年第一季可以进行第一次迭代。

在第二种情况下，需要一个具有虚拟机的区块链、一组共同的节点和一个能够实现两个链之间的通信机制。我们已经开始使用K框架严格正式化以太坊虚拟机的过程[12]与伊利诺伊大学的团队合作。

该分析的结果将告知设计复制和最终分布式虚拟机的最佳方式[13]，具有明确的操作语义和正确实施规格的强大保证。换句话说，虚拟机实际上是执行的工作由代码告知，并将此工作的风险予以最小化。

还有一些由以太坊提出关于气体经济学尚未解决的问题，如何相关运作，诸如Jan Hoffmann等人的资源意识ML和为了计算的更广泛资源估算研究。我们也很好奇虚拟机的语言独立性。例如，以太坊项目已表达了渴望从目前的虚拟机转向网络配置。

接下来的努力是开发一种合理的编程语言来表达将被分散应用程序称为服务的有状态合约。对于这项任务，我们为低安全性的应用程序选择了支援传统智能合约语言的Solidity，然后为需要高度安全性的应用程序并开发了一种称为Plutus的新语言，以用于需要的正式验证。

如同基础扎实的Zeppelin项目般，IOHK还将开发Plutus代码的参考库，提供应用程序开发人员在其开发项目中使用。我们还将开发一套专门用于正式验证的工具，此验证受到UCSD Liquid Haskell项目的鼓舞。

[12]由Grigore Rosu教授等人发明，K是一种用于语言独立机器可执行语义的通用框架，在运用于我们的工作之前，已经用于模拟C、Java和JavaScript

[13]意指不同的共识节点运行不同的智能合约，也称为状态分片

根据共识，乌洛波洛斯设计的模块化模式足以支援智能合约评估。因此，卡尔达诺结算层和卡尔达诺计算层将共享相同的一致性算法。不同之处在于，可以通过令牌分配确认乌洛波洛斯允许有权和无权的分类帐。

通过卡尔达诺结算层，Ada已经通过令牌的形式发布给亚洲各地的买家，这些买家最终将在二级市场上转售。这意味着卡尔达诺结算层的一致性算法是由多样化和众多分散化参与组或其委托授权者所控制。使用卡尔达诺计算层，可创建一个特定目的的令牌，由该分类帐的授权者所持有，该授权者可以是受监管的实体，从而创建一个被许可的分类帐。

这种方法的弹性允许卡尔达诺计算层的不同实例通过关交易务评估的不同规则来实现。例如，赌博活动可能受到限制，除非KYC / AML数据被简易显示是通过将非属性交易列入黑名单。

我们的最终设计重点是将可信硬件安全模块（HSM）添加到我们的协议栈中。将这些功能引入协议时，有两个具大的优点。首先，HSMs提供大规模的性能提升[14]，而不会引起安全问题，超越信赖供应商。第二，通过使用密封玻璃证明（SGP），HSM可以保证数据可以被验证然后被销毁，而不会被复制或泄露给具有恶意的外部人员。

关注第二点，玻璃密封证明可能对法规产生革命性的影响。通常，当消费者提供个人身份信息（PII）来验证身份或证明参与权时，该信息将交给可信的第三方，希望第三方不会进行任何恶意行为。这种活动本质上是集中的，数据提供者失去对其个人身份信息的控制，也受到管辖权的各种规定所约束。

选择一组可信赖的证明者，然后在硬件地盘中存储个人身份信息，这意味着任何具有足够能力的HSM参与者将能够以不可伪造的方式来验证关于参与者的事实，而没有验证者知道此参与者的身份。例如，鲍勃不是美国公民。爱丽丝是一个认可的投资者。詹姆斯是美国纳税人，应该将应税利润纳入X帐户。

卡尔达诺的HSM策略将是在未来两年内使用Intel SGX和ARM Trustzone来实施特定协议。这两个模块皆已从笔记本电脑到手机装置，创建了数十亿个消费者设备，所以不需要消费者花费任何额外心力。两家公司也经过严格的审查、精心的设计，并且其发展基于一些最大和最优秀的硬件安全团队的多年迭代。

监管

[14]请参阅由康奈尔大学发布使用安全硬件缩放比特币

所有现代金融体系的惨痛现实面是，随着规模的扩大，它们累积了一种需求，或者至少是一种愿望。这是由一些参与者的疏忽或是参与者的阴谋在市场中盛行而导致的反复崩坏的结果。

所有现代金融体系的惨痛现实面是，随着规模的扩大，它们累积了一种需求，或者至少是一种愿望。这是由一些参与者的疏忽或是参与者的阴谋在市场中盛行而导致的反复崩坏的结果。

人们可以合理地辩论监管的需求、范围和效力，但不能否认其存在性和主轴政府执行的热忱。然而，随着世界的全球化和现金变得数字化，所有监管机构面临的挑战是双管齐下的。

首先，在处理司法管辖区的情况下，哪一套监管规定应该是至高无上的？威斯特伐利亚主权的过时概念在一分钟内触及三十个国家的单笔交易中就得以溶解。其是否应该成为最具地缘政治影响力的角色？

第二，隐私技术的改进创造了一个数字军备竞赛，越来越难以理解是谁参与了交易，更别说拥有一个价值的特定商店。在一个可以控制数百万美元资产的世界里，唯独秘密的持有一组12个字组，别无其它[15]，你该如何执行有效的监管？

像所有的金融系统一样，卡尔达诺协议在设计上必须拥有一个公平且合理的意见。我们选择在个人权利和市场权利之间进行分割。

个人应该永远独自拥有其资金，而不受强制或民事资产没收。这一权利必须得到执行，因为并不是所有的政府都能被信任，而且不滥用他们的主权权力，可以看见在委内瑞拉和津巴布韦，腐败的政客独占为其个人利益。加密货币必须被贯彻为回避矛盾而刻意简单化。

其次，历史不应该被篡改。区块链提供了不变性的承诺。阻碍历史或改变官方记录的权力引入了太多的诱惑来改变过去，使一位或多位的特定参与者受益。

第三，价值流动应该不受限制。资本管制和其他人造墙缩减了人权。在尝试无效果行动之外，强迫图执行[16]，在全球经济中，未发展国家的许多公民在其管辖范围之外流浪，以寻找生活工资，通常限制资本流动终究伤害世界上最贫穷的人口。

这些原则指出，市场与个人截然不同。卡尔达诺设计师虽然相信个人权利，但我们也认为，市场有权公开说明他们的条款和条件，如果个人同意在这个市场进行生意运作，那么他们必须遵守这些为了整个系统完整性的目标之标准。

[15]请参阅BIP39

[16]作为资本流动的对策的一个例子，参阅Hawala银行系统

一直以来的挑战是成本和执法的实用性。传统制度中的小型、多管辖权交易的成本太高，在发生欺诈或商业纠纷的情况下，提供高度的追索权。当某者将他们的电汇送到尼日利亚王子[17]时，通常想挽回自己的资金确需要更高的代价。

对于卡尔达诺来说，我们觉得我们可以在三个层次上进行创新。首先，通过使用智能合约，可以更好地控制商业关系的条款和条件。如果所有资产都是数字资产，只能用卡尔达诺结算层表示，就能取得强保无欺诈的商业行为。

第二，使用HSMs提供一个身份空间，其中个人身份信息不会泄漏，但尚未用于身份验证和证书参与者应提供给全球信誉体系，并允许进行更低成本管理的活动，例如具有自动化税收合规性的在线游戏或分散换汇。

最后，卡尔达诺的路线图是创建一个模块化调节DAO，可以客制化与用户编写的智能合约交互，以增加其可塑性、消费者保护和仲裁。这个项目的范围将在后续的文章中介绍。

所有的要点是什么？

卡尔达诺已经是一个马拉松项目，涉及来自隐私行业内外数百位最顶尖的人士予以反馈。它涉及不懈的迭代，积极使用同行评议，厚脸皮地窃取伟大的想法。

下的部分各自涵盖了我们决定的重点特定方面，这是我们项目的核心组成部分。有些被选中的是因为希望改善空间的整体最佳实践，而其它则是卡尔达诺进化的具体特征。.

虽然没有任何项目可以覆盖每个目标或满足每个用户，但我们的希望是提供一个愿景，此愿景是一个可以自我发展的金融堆栈，应该可应用于缺乏这些金融堆栈的管辖范围。加密货币的最终现实不是在于破坏现有的传统金融系统。传统的金融体系总是能够吸收变化并保持其形式和功能。

相反，人们应该看看部署现有银行系统太贵的地方，其中有许多人每天的生活可能花费不到几美元、没有稳定的身份和更不可能被挖掘的信用。

在这些地方，将支付系统、产权、身份、信用和风险保护连接到手机上运行的单个应用程序中的能力，并不仅仅是有用的，而是在于生活的变化。我们正在建设卡尔达诺的原因是，我们认为我们为发展中的世界提供或至少推进这一愿景是合法的。

如果我们可以改变加密货币的设计、发展和资助的方式，那将有很大的成就。

[17]参阅预付费诈骗

2. 科学与工程

迭代的艺术

加密货币是作为软件实现的协议。协议只是参与者之间的智能对话。软件最终是对数据操纵给予了一些目标。然而，坚实可靠的软件和有用的安全协议以及它们之间的区别是完全人性化。

良好的软件需要问责制、明确的业务需求、可重复的流程、彻底的测试和不懈的迭代。良好的软件还需要具有足够专业知识的合理能干的开发人员，以确切地设计一个系统，该系统可以完全解决他们正在尝试解决的问题。

对于有用和安全的协议，特别是涉及密码学和分布式系统的协议，它们从更偏向于学术和标准化过程。同行评审、无休止的辩论和坚定的权衡概念是确保协议有效的必要条件。然而，仅有这些是不够的，协议需要通过现实生活中的使用来实现和被测试。

加密货币领域的独特挑战是两个完全不同的哲学，在没有适当黑格尔合成的情况下被磨合在一起。我们的论点是由青春，贪欲和热情所驱动的“快速突破事件”的创业心态。对立面是一种缓慢，有条理和学术基础的手法，其动机是将我们的空间的创新融入一个良好的利基，享受充足的资金和声誉。

结果是，许多加密货币完全特定在白皮书上，只与CV相关，或者只是匆忙编写的代码。目前前按市值计算的十名加密货币[18]皆基于同行评议的协议。目前前十位加密货币中没有一个是由正式规范中实现的[19]。

然而，数十亿美元的价值受到威胁。一旦被部署后，一个加密货币是非常难以进行改变的。用户如何得知他们正在使用的是一个安全系统？用户如何知道营销声明是合法的？如果提出的协议永远不能达到其声称的呢？

这种缺乏合成和尊重过程是IOHK想要建造卡尔达诺的主要原因之一。我们的希望是开发一个提供大家参考的项目，作为一个以更有效、稳健和诚实的方式做事情的例子。

[18]参阅coinmarketcap.com按市值列出的广泛列表

[19]以太坊有一个称为黄皮书的半正式规范;但是，EVM语义没有被完全指定，也不足以完全实现该协议。

目标不是提出一种全新的开发软件和协议，而是承认确实有已经存在很好的软件和协议，然后我们可以模仿诱导其创建的条件。第二，尽可能使这些条件公开和开源，以便于整个领域皆可以藉由模仿这些条件而获利。

事实和意见

另一个问题就是事实的结束和意见的开始。有数百种编程语言、数十种开发模式和多种项目管理理念。学术界充满了自我挑战，源自于学术界与业务相关和实用性的距离。

对于卡尔达诺来说，我们首先试图捕捉明显的缺陷，从工程角度审视是普遍同意有用的。例如，密码学和分布式系统都是非常重要牵涉的主题，其中有太多的例子说明天真之手可以造成可怕的错误。因此，任何需要获得这些领域见解的协议，需要由公认的专家设计，并提交给其他专家进行审核。

乌洛波洛斯是我们这领域的第一个案例研究。它是由密码学家团队设计的，具有大量、多样和可公开验证的出版历史。它是根据标准密码学过程建立的，具有安全假设、对抗模型和证明。这些证明是通过提交会议进行审查[20]，也独立地由剑桥大学的一个团队以Isabelle编写的计算机予以证明[21]。

然而，这项工作本身并无法提供有用的保证 - 只是在一些假设情况下，通过严格检查的安全模型。为了确保其有用性，需要实施和测试协议。我们的开发人员在Haskell和Rust都进行了同样的过程。这项工作表明，需要更多的精力集中在同步模式上，这也引导了Ouroboros Praos的创立。

这个迭代的艺术造就了这伟大的协议，每一步引发了新的教训和必须重新验证先前步骤的正确性[22]。它是昂贵的、耗时的、有时是非常繁琐的，但是需要确保协议设计的正确性。

议定书 - 特别是数十亿人使用的议定书 - 并不是短暂的、快速演化的。相反，它们将被追溯至数十年。似乎完全合理的是，在世界承载新的金融体系之前，我们都要在未来的一百年中生存下去，我们想向设计这些协议的设计师，要求一些乏味和严谨。

[20]加利福尼亚州IACR年度加密会议中受理的第71号文件

[21]由Lawrence Paulson教授监督下的Kawin Worrasangasilpa执行

[22]为了获得利益的一个切线，应该参考教授Halmo的讨论撰写的关于如何编写数学教科书的讨论。

功能性

进入更多的意见领域，软件开发中使用的工具、语言和方法，更多的是宗教信仰，而不是客观现实。源代码就像书写散文。每个人都持有什么是好的之意见 - 什么是已经被沟通的，有时，比起它如何被沟通更不重要。

我们必须承认，一旦选择接受了一方，那么至少在一个人的眼中会认为这是错误的选择。但是，至少有一个大型的论证主体存在我们选择的背后。该协议让卡尔达诺可在Haskell中实施。

用户界面已封装在Electron的叉子中，我们称之为代达罗斯(Daedalus)。我们选择在可能的情况下使用网络架构模型，对于我们的数据库，我们选择了使用RocksDB的键值范例。

从组件层面来看，这种摘要意味着更简单的维护，更好的技术可以在稍后的稍微地努力下被取代，我们的堆栈有一部份与Github和Facebook的开发工作相关。
使用WebGul可以让我们利用React和数十万JavaScript开发人员已理解的工具进行开发前端功能。使用网络架构，意味着组件可以被视为服务，且安全模型是明智的。

选择Haskell进行协议开发是最困难的选择。即使在功能世界，有更充足的选择。考量更灵活性和不透明面，有诸如Clojure、Scala和F＃之类的语言，它们受益于Java和.Net生态系的巨大文库，同时保留了一些功能编程的最佳特征。

有更多学术导向的语言，如Agda和Idris，与技术密切相关，可以强制验证正确性。然而，它们缺乏合理的文库，并且具有较低阶的开发经验。

对于卡尔达诺而言，选项剩下Ocaml和Haskell。 Ocaml是一个很好的语言，拥有一个庞大的社区、良好的工具、合理的开发经验和通过Coq的正式验证空间的伟大遗产[23]。那我们为什么选择Haskell呢？

为何选用Haskell?

[23]此外，IOHK实际上确实有一个项目在Ocaml中被称为Qeditas，是我们从匿名Bill White中继承的。

组合卡尔达诺的协议是分布式的，与密码学结合在一起，需要高度的容错能力。在最佳的日子里，仍然会有拜占庭式的参与者、格式错误的消息和错误的客户，于无意中在网络上造成某种形式的havok。

首先，我们需要一种具有强大类型系统的语言，让我们可以轻松地使用诸如Quickcheck等工具，和更精细的技术，如精简类型，同时对容错有合理的期许。 Erlang风格的OTP模型满足后者，而Haskell和Ocaml等语言则满足前者。

随着Cloud Haskell的推出，Haskell获得了许多Erlang的优势，而不是屈服于自身。此外，Haskell的模块化和可组合性使我们能够为卡尔达诺使用更轻量级的定制库，称之“Time Warp”。

其次，由于广泛的商业实体，如Galois、FP Complete和Well-Typed，Haskell的文库在过去几年中已经有很大的进展。因此，Haskell可用于编写生成应用程序[24]。

第三，PureScript的快速发展为JavaScript世界提供了一个非常需要的桥梁，类似于Clojurescript给予的Clojure。我们期待PureScript可在让卡尔达诺于浏览器中运作，并在开发手机钱包时尤为重要。

第四，于依赖解决方案方面，Haskell在过去几年中一直受到像Michael Snoyman这样的技术专家的技术支持，通过一个叫做堆栈的平台，这个平台很容易使用，并且得到了FP Complete的良好支援。

第五，除了足够的依赖解决方案之外，我们的目标是使我们的软件构建是可重现的。换句话说，使用相同的配置值和依赖性版本，它应该产生完全相同的构建工件。通过堆栈，我们一直在使用NixOps实现重现性，取得巨大成功。

最后，专业从事Haskell的开发人才库相当庞大，相当于同行 - 而且训练有素，具有相应的学术和行业资质。它也充当能力过滤器，因为在没有计算机科学的详细知识的情况下，找到经验丰富的Haskell开发人员是不太普遍的。

形式规范和验证

使用可证正确安全模型开发协议的主要优势在于它提供了对抗能力的保证限制。对于一份是合约，只要其协议遵循并且证明是正确的，那么对手就不能违反所声明的安全属性

[24] Bryan O'Sullivan在这里提供了一个关于Haskell工业用途的良好论述。

更深刻的反省使得先前的断言更加显着。对手可以是任意智能和有能力的。说他们仅通过数学模型被打败是非同寻常的。当然，这不完全是真的。

现实引发了阻止纯安全的乌托邦和现有的正确行为的因素和情况。实施可能是错误的。硬件可以诱发以前未经考虑的攻击向量。安全模式可能不足，并且不符合现实生活中的使用。

对于协议需要多少规范、多严格和怎么检查的判断是需要的。例如，像SeL4 Microkernel项目这样的努力是一个很好的例子，全面的歧义需要近20万行的Isabelle代码来验证少于10万行的C代码。然而，操作系统内核是关键的基础设施，如果没有正确实施，可能是严重的安全漏洞。

所有加密软件是否都需要相同的艰巨努力？还是可以选择一个没有那么吃力的途径，以产生相当的结果？如果协议是完美实现的，那么如果它运行的环境是非常脆弱的，如Windows XP，那有没有关系？

对于卡尔达诺而言，我们选择了以下的妥协。首先，由于密码学和分布式计算领域的复杂性，证据往往是非常微妙、漫长、复杂和有时需要相当的技术性。这意味着人为的检查可能是乏味且容易出错的。因此，我们认为，为了涵盖核心基础设施而编写的白皮书中，提出的每一个重要证据都需要进行机器检查。

第二，为了验证Haskell代码是否正确对应于我们的白皮书，我们可以选择两种流行的选项：通过LiquidHaskell与SMT验证器进行接口并使用Isabelle / HOL。

可满足的模理论（SMT: satisfiability modulo theories）求解器处理满足方程式或不等式的功能参数的问题，或者说可以不存在这样的参数。如De Moura和Bjørner所讨论的，SMT的用例是多样的，但关键是这些技术都是强大的，并且可以大幅减少瑕疵和语义错误。

另一方面，Isabelle / HOL是一种更具表现力和多样性的工具，可用于指定和验证实施。 Isabelle是一个通用的定理解算器，可以处理高阶逻辑结构，能够表示集合和其它用于证明的数学对象。Isabelle本身与Z3 SMT认证工具集成，以处理涉及此类限制的问题。

这两种方法都有价值，因此我们决定分阶段地含括这两种方法。人造书面证明将在Isabelle编码，以检查其正确性，从而满足我们的机器检查要求。我们打算逐渐将Liquid Haskell加入到卡尔达诺在2017年和2018年实施的所有生产代码。

最后一点，形式验证只能与可用工具集验证的规范相比。选择的Haskell的主要原因之一是，它提供了实用性和理论的平衡。从白皮书衍生出来的规范看起来很像Haskell的代码，连接这两个代码比用命令式语言更容易。

在获取适当的规范和更新规范时，仍然存在着巨大的困难，如升级，瑕疵修复和其他关注事项等需要做出更改;然而，这种现实并不能减弱总体价值如果在建立可证安全的基础上遇到麻烦，那么应该实施纸面提案。

透明度

在讨论开发一个密码学的科学和工程时，最后一个问题是如何解决透明度问题。设计决策不是布尔数学体系和飘渺的，给予开发人员梦想，然后突然变成榴弹炮。它们源于早期错误的经验、辩论和教训。

面临的挑战是，一个完全透明的发展过程可能会影响讨论变得更加戏剧化而不是基于证据的。Egos，企图夺取一个社区，害怕听起来很愚蠢，可能会使谈话变得无法适应，反而适得其反。

此外，外部人士也可以试图选择对话，努力强制其突变的话题成为唯一的相关话题。没有人会受到批评。

那么，如何平衡一个透明发展过程的需要，这个过程赋予一组核心开发者委托的社区，而无需担心言论自由呢？

于卡尔达诺中，我们决定采用标准化的过程，并进行指导监督。社区需要了解，科学和规范都是经过深思熟、检查并实际解决了开发人员声称的事宜。为此，同行审查应完全满足科学组成部分，因为它是为此而专门设计的，并给了我们现代世界。

对于代码，这个话题是更有争议的。对于卡尔达诺而言，我们委托卡尔达诺基金会担任IOHK执行工作的最终审核者。特别是被赋予以下职责：

1. 定期检查卡尔达诺Github中包含的源代码，以检查质量、测试覆盖面、适当的评论和完整性
2. 审查所有卡尔达诺文档的正确性和实用性
3. 验证科学家制定的协议是否得到充分实施的声明

为了完成这项任务，IOHK将定期及时向基金会及其委托人提交报告以进行审查。该基金会将至少在每季向卡尔达诺社区发布一份发展监督报告。

第一项工作主旨是就分散化项目，如何实现问责制开展更广泛的对话。来自可信赖第三方的开发监督，是确保开发人员正常进行工作的强大工具，但要完全保证项目始终可以实现是不够的。

因此，在资金融入卡尔达诺结算层之后，基金会将鼓励其开发团队，根据与IOHK共同制定的正式规范予以构建替代客户。发展多样性一直是以太坊项目使用的一个伟大技术，以避免在单一想法或开发人员周围形成单一文化。

对于规格方面，WC3和IETF所遵循的标准流程将有丰富的知识。最终，卡尔达诺集成的每个协议都需要独立于学术工作或源代码的规范。相反地，它需要使用合适的格式，如RFC。

卡尔达诺基金会的核心原则之一是作为卡尔达诺协议专门的标准机构，并主持对话以更新、添加或更改与卡尔达诺相关的标准。如果通过IETF的互联网（标准的产物）能够对于使用什么核心协议达成共识，那么假设一个专门的机构可以促成相同的结果是完全合理的。

结语，有趣的是，将这些讨论转移到一个托管在一个区块链上的分散实体。这个概念被称为分散式自治组织（DAO; decentralized autonomous organization），初步工作正在该领域进行中。IOHK将开发一个提供参考的分散式自治组织模型，用于与卡尔达诺接口的实体使用，若需要，卡尔达诺基金会拥有此特权，表决是否根据其标准授权进行采纳。

3. 互操作性

视而不见

财务和更广泛的商业理念最终是人类的努力。存在着优雅的语言、非常精确的工具以捕捉意图，以及在不良后果和寻求贸易平等的数千年法律中，获得追求权利的无穷魅力。事实上，一些最早的写作形式是商业合约。

然而，无论是对逻辑、机器或是政府哨兵具有可怕的权限委托，都无能避免人为因素。其中存在加密货币的视而不见。他们大多是脱离人类的现实层面。

人们犯错。人们改变主意。人们并不总是完全理解他们已经同意且参与其中的业务关系。人们被误导和欺骗。当个人和国家层面的情况发生变化，则需要独特的解决方案。为此，大多数合约都包含不可抗力条款。

然而，加密货币设法丢弃人们的理解、同情和判断，以换取一个宪法漠不关心的数字评断，而没有考量其公平性或后果。鉴于人类一直以来，并且也会持续地为了自私的目的尝试改变规则，因此，实际上拥有不能被破坏的系统是令人耳目一新的

但是，当用户需要将这些新系统与传统的金融系统相融合时，会发生什么呢？当某人需要居住在这样的人世间，那会怎样呢？例如，土地登记等产权完全属于物质世界。即使标记土地仍然需要一些现任管辖权的承认。

提供另一论点，一条黄金无法移动自身。数字评断可以指挥其行动，但不能在没有使人们适应的情况下强迫执行它。因此，数字分类账可以从现实中摆脱。

因此，协议设计者需要决定在他的加密货币中应该允许多少的人类现实层面。灵活性越强，绝对的忠诚就越少。消费者保护越多，就必须存在越多的机制来提供反转、退款和编辑历史。

本节和下一章的监管涵盖卡尔达诺对这一话题的务实做法。在互操作性方面，有两个广泛的群体来讨论。首先，与传统金融系统（非加密货币世界）的互操作性。第二，与其他加密货币的互操作性。

遗产

金融科技不是由单一标准或通用语言组成。方法、负责转让和结算的实体、业务流程以及涉及会计、转换和价值变动的其他领域都有很大的差异。

仅因为一项技术是优越的，生态系统的其余部分将以某种方式承认失败和升级，这是不合理的建议。例如，许多人仍然使用着从初期发布至今已为期16年的Windows XP。这个令人感伤的事态就如同某人在西元2000年使用着西元1984年发行的Macintosh原始版。

除了消费者行为外，企业的升级周期通常更慢。许多银行仍然使用Cobol撰写的后端。一旦知道基础架构是可运行的，并且满足业务需求，那么为了超出合规和安全疑虑的消费者利益，进行升级或改进软件和协议的动机通常是很小的。

对于卡尔达诺来说，我们首先要建立什么是一座传统的桥梁需要涉及的？我们应确定哪些系统、标准、实体和协议，以确保互操作性的合理确定性？这些桥梁可以联合还是分散？或者像交易所一样，它们是否将成为黑客、恶意持有者或过度监管者的中心点？

有三项疑虑需要解决。首先，信息的表达并且相信其准确性。其次，价值的代表及其相关所有权。第三，实体的代表，以及特定用户与这些实体的总体信任水平。

为了实现有用性，信息和价值需要在传统金融世界和卡尔达诺之间自由地流动。然后，其结果是需要被建立和记录的，以构建正当理由和信誉的依赖。然而，这样的事宜自然地广泛涉及其参与者。将它们编码在区块链上，将使它们成具有全球性和永久性。

然而，传统世界的价值并不总是自由流动。禁运、制裁、资本管制和司法行动可能冻结资产。为了可互操作性，没有人可以创造一个永远的放出阀来泄漏价值。

最后，实体的品牌和声誉是商业关系的基石之一。每年花费数十亿美元用于建立、维护和维修品牌的营销活动。如果对个人或实体提出上诉、虚假或误导性的要求，则他们可以寻求法律追索权。然而，区块链试图永久保存历史。

像我们选择的编程语言一样，对于卡尔达诺而言，没有理想的解决方案以无所不在的准确性解决这些疑虑。想反，我们必须再次屈服于被支持的意见。

关于信息流动，该流动被称为可信数据馈送。它有一个来源和内容。消息来源有一些可信度和促使欺骗或保持诚实的动机。内容可被任意编码。

鉴于我们打算在协议栈中支持受信任的硬件，因此我们选择为Ari Juel等人的“城市公告协议”探索添加支援。假设这理存在一组可靠的数据源，城市公告允许安全地撷取网页内容以用于智能合约和其他应用程序。

Emurgo，IOHK和卡尔达诺基金会将提供引导程序来源的列表。之后，该列表单将被一个社区策划名单所取代，该个名单使用了卡尔达诺资金系统的机制。我们的希望是，声誉系统可以实现良好的数据馈送，从而创建一个积极的反馈回路，逐步提高可靠性和忠实度。

价值的表现是一个更复杂的话题。不同于信息，- 一旦建立了真实性、及时性和完整性，协议可以用可靠性和确定性的方式呈现 - 而价值确更加细腻。

一旦标记化，价值应该像是一个个唯一的对象。信息可以复制和传递，但是表示所有权（例如车辆号牌）的标记不能在两个不同的分类帐上复制和交易。这一行为将显著地破坏系统的完整性。

在处理标记化价值时，遗留互操作性的挑战是信任假设、可靠性和可审计性，这些随着分类帐之间的流动而发生变化。例如，如果鲍勃拥有一些比特币，然后将其存入交易所，那么鲍勃现在即是将他的比特币兑换成交易所的分类帐。在MtGOX的情况下，他们的分类帐不符合现实，导致用户失去了一切。

对于传统系统识别加密货币体系中的令牌的需求，这个问题更佳复杂。如前述，企业在历史上对升级软件和支持新协议有着抵抗性。这种情况使得很难看见明确的解决方案。

对于卡尔达诺而言，我们最佳期许是为用户提供一个选项，为他们的交易附加丰富的元数据，然后等待行业标准出现，以进一步和其融合和挂钩。 Interlerger工作组已经取得了一些进展，像是R3Cev这样的成就和国际授权来升级旧的财务协议。

然而，更大的挑战是定量和定性的价值从遗留系统发送到加密货币的分类帐。例如，如果鲍伯是一个银行的所有者和发行美元支持的令牌，那么他可以随时建立一个桥梁，将他的令牌发送给像卡尔达诺这样的分类帐，以作为用户发行的资产。

虽然卡尔达诺将精确跟踪所有权限，并提供我们所熟悉的所有功能，如时间戳和可审计性，但是没有加密货币可以驱使鲍伯成为一位诚实的银行家。他总是可以选择运行一个部分储备银行，而不是用真正的美元支持他所有的美元令牌。除非美元本身是由数字分类帐记录的令牌，否则这种欺诈是无法检测的[25]。

最后，在线实体的表现是可追溯到互联网初期的典型网络问题。大学、企业、政府部门和任意用户需要在某些时候建立自己的身份。

为此，已经实施了务实而集中的解决方案，如网络公钥基础设施和ICANN的DNS系统。鉴于我们享受着现代网络，这些解决方案既可扩展又实用。但是它们并没有实现一个更为商业化的可靠性，诚信和其他元特征的需求，以确定某人是否想要与该实体做生意。

像eBay这样的多边市场主持人已经构建了一个商业模式，提供一些元数据以及框架来完成交易。关于内容、事件和业务的质量判断，通常仅仅受到来自可信来源的在线评级的深刻影响[26]。

与卡尔达诺相关的一部分是声誉集中化的问题。卡尔达诺的目标之一是为发展中国家提供一个金融平台。这一努力的关键之一是与从未遇见的参与者建立信任的能力。

如果单个实体或实体联盟控制谁标记为好坏，而不是源于整个社区实际交互的有机过程，那么这些实体可以任意将任何人视为黑名单。这种权力是违反我们作为一个项目的价值观，并且阻碍将密码学使用于更广泛的领域。

幸运的是，用于投资国库券的相同机制，将资源添加到可信数据馈送的列表和分配协议中，可以重复使用以建立信誉空间。这是一个开放的研究领域，我们希望在更多的基础要素得到建立后，为2018-2019年分散的信誉网络提供覆盖协议。

加密货币互用性

从传统世界转移到分布式数字分类帐，互操作性变得更加简单。每个分类帐具有网络协议、通信标准和关于其一致性算法的安全假设。这些可以容易地被定量。

[25]另一方面，对于数字分类帐，已经提出了保留证据，作为一种保持诚实交换加密货币的聪明方式。

[26]这些评级甚至影响内容本身的创建，请参阅关于Rotten Tomatoes如何影响电影业的这有趣故事

通过连接到外部网络和翻译其信息建立信息的移动。价值的移动可以通过中继系统、原子交叉链交易或通过巧妙的侧链方案来实现。由于没有一个集中运营商，实体的一个代表性对开发商、矿工或其他一些掮客的信任限制更多。

对于卡尔达诺，我们正在整合由Kiayias、Miller和Zindros开发的新侧链协议。它提供了一种非交互式的方式，可以在支持协议的两条链之间安全地移动价值。这种机制将是卡尔达诺结算层和卡尔达诺计算层之间流动的主要途径。

对于其他加密货币，联合桥梁应该随着卡尔达诺的价值和用户基础的增长而成形。为了促进加速增长，卡达达诺结算层支援Plutus的受限版本，用于互操作性脚本。新的交易将在Shelley版中添加，而在稍后发布的卡达达诺结算层专门用于满足这些需求。

代达罗斯的迷宫

互操作性的要点来自全球视野。特定的协议、新的交易类型，评估信任系统和信息动不能仅限于一个关守或用户。相反地，他们必须随时可让任何人在没有审查或收费的情况下所使用。

然而，当卡尔达诺不支持用户无法存在的协议、事务或应用程序时，会发生什么？我们是否应该超出范围？ 90年代，网络面临着类似的关切。

讽刺意味的是，网络提供了两种可以使用加密货币复制的解决方案。 JavaScript的引入为任何网站提供了可编程性，以增加任意的功能。引入浏览器插件和扩展程序为愿意安装它们的用户添加了自定义功能。这两种方法都给了我们现代网络以及其所有的安全恐怖。

以太坊采用了前一种方法，允许用户在以太坊区块链上的嵌入子协议，如智能合约。卡尔达诺通过卡尔达诺计算层范例支持此功能。但是自定义扩展程序呢？

一个明确的例子将是一个加密货币交易者。想象一下在一个称为Decentralized Marketplace 的分散市场中，支持一套不同的加密货币。一个交易者希望在分散市场上自动化操作运行他的策略。

在一个分散的生态系统中，交易者必须为每个加密货币安装数十个客户端，然后编写定制软件与每个客户端进行沟通，以协调自动交易。如果一个客户端更新，那么它可能会打破定制软件。此外，如果交易者想出售软件怎么办？

从扩展的网络模型中得到启发，如果将各种加密货币的接口拉入网络堆栈，那么交易者的任务将变得更容易。可以建立一个通用接口。安装是一键点击。软件分发可以在Chrome网上商店之后建模。

对于卡尔达诺而言，我们已经决定通过在Electron部署我们的参考钱包的前端，来实验这个范例。它是由Github维护的开源项目，它将Node和Chrome结合在一起。卡尔达诺的Electron建筑称为代达罗斯（Daedalus）。

代达罗斯的第一代[27]将如同分层确定性钱包运行，支持许多行业标准的预期会计和安全功能，例如支出密码和BIP39。在下一代的代达罗斯将发展成具有商店、通用集成应用程序编程接口(APIs: Application Programming Interface)和软件开发工具包（SDK: Software Development Kit)。

此关键的创新是易于开发，通过允许程序员使用JavaScript，HTML5和CSS3构建他们的应用程序和一座跨应用程序通信的统一桥梁。复杂的行为，如密码学、管理分布式网络和数据库机制可以被简化出来，从而让开发人员只需关注用户体验和应用程序的核心逻辑。

由于代达罗斯旨在成为一个通用的框架，其路线图和进化有些独立于卡尔达诺。在2017年期间，它们紧密耦合，但之后的卡尔达诺将只是代达罗斯用户使用中的一个应用程序。我们还打算探索非常独特的功能，例如在英特尔SGX上运行独立通用密钥管理服务。

最终，作为协议设计者，我们无法支援所有需求。我们的期许是，代达罗斯提供的灵活性将与卡尔达诺计算层上运行的有效智能合约相结合，该将满足从我们设计决策中所遗留的。我们也希望出现更好的标准来鼓励所有加密货币享受更好的互操作性和安全性。

4. 监管

虚假二分法

由于监管往往可以说是反覆无常且奥秘的，人们可以隐喻地推测一个贪污的优雅故事环节，而检举者们寻求正义。监管是法律执法者的工具包。但是如同所有的工具一样，它们可能是粗糙的、陈旧的或者简单地被滥用。

[27] daedaluswallet.io已经可以使用

加密货币并未改变人类的状况或故事环节。尽管有最佳的意图，但仍然总是有诈骗、不良行为和可怕的结局。虽然加密货币可以消除人们的判断，但它无法消除人们的行为。

一个加密或弊的设计师，他必须对为监管机构提供什么样的工具包来纠正这些不良事件。加密货币面临的独特挑战在于它们是监管和货币失败的产物[28]。

在文化上，许多加密货币认为政府行为是腐败的、不称职的或是无效的。所以它们无法尊重、有耐心或者愿意为一个监管机构或者一个律师提供一个特殊的后门来纠正这些错误。该行为，将导致所有加密货币的目的被可憎。

另一方面，计数交易失败和历史事件，比特币的百分之十以上已经从2009年1月3日开始，丢失或被盗。截至2017年6月30日，失去或被盗的价值超过 40亿美元。而这个数字还并未没有说明比特币和其他令牌对于诈骗和不良布局的ICO所造成的损失。

那么可以指明就是隐私问题。在宏观上，价值流经监管的专业渠道、丰富元数据，并得到执法机关、政府和国际监管机构的积极监督。这是一个很好理解的游戏，遗漏只会发生在现金方面，随着世界向数字货币的转移，金钱的遗漏则逐渐减少[29]。

如果加密货币不存在，这个范例似乎成为越来越把财物隐私视为社交媒体内容的世界。没有人，而人们也不能选择退出。因此，我们有一个困境产生了一个明显的二分法。

一个加密设计师可以将原则和产出屈服于其本地管辖权对其代码的任何要求，从而损害用户的隐私和完整性。或者他可以采取更有原则的、但是是无政府主义的，该与现行最佳实践和法律脱节的哲学。

对于卡尔达诺而言，我们觉得这种故事是由于缺乏想象力而带来的虚假二分法。实际情况是大多数用户并不关心市场规则。他们通常关心的是规则的突然变化，以使一位或多位参与者受益。他们担心缺乏透明性，让某特定人士获得特权。

我们需要区分个人和市场的权利。鉴于加密货币具有全球影响力，权利需要尽可能以用户为导向。

隐私应该是合理的，并且是在用户的控管下，而不是守门员。价值流动应该是无限制的。未经过同意，价值不得突然被没收。

---

[28]事实上，当Satoshi嵌入比特币创世区块时，2009年3月份的纽约时报揭开了此标题：为了银行次要紧急援助边缘的总理

[29]读者应考虑阅读David Wolman的“金钱结束”的复印版本，其中包括国际走向金钱消失的行动。

从市场的角度来看，市场对于数据的使用需要透明化，如何处理资金，并且每个人都需要通过相同的规则来执行。此外，一旦用户同意，那么用户不能因为自己的不便而突然改变主意。对方也需要确定性。

但是，人们该究竟如何从抽象移转到实际系统上呢？实践是怎么样？而法律又应该是什么样？我们将解决方案分为三类：元数据、认证与合规性，以及市场分散应用机构(DAOs': Decentralized Autonomous Organizations)。

元数据

某些东西的行为与围绕它的元数据相比之下，通常是比较无趣的。例如，从丹佛驾驶到博尔德是一种行为。驶着法拉利488，用平均每小时120英哩的速度从丹佛驾驶到博尔德是元数据。当然，这意味着与用平均每小时30英哩的速度驾驶丰田普锐斯，拥有着不同的体验。

金融交易没有什么不同。经济学家、税务机关、执法机构、企业和其他实体对他们的背景尤其重要。令人遗憾的是，对于我们目前的基于法定的系统中，大多数消费者从来没有看过他们的交易的元数据有多丰富，或者这些元数据与谁分享了[30]。

对于卡尔达诺而言，我们承认用户可能需要或依据法律要求，与某些参与者（如税务机关）分享交易的元数据。但是我们认为这种共享必须得到用户的同意。

我们也区块链系统具有庞大的力量，通过提供可审计性、时间戳和不变性来消除欺诈、浪费和滥用。因此，一些元数据应该被发布到卡尔达诺区块链上。

它非常难找到一个正确的平衡，让该平衡不会谴责我们的区块链大幅膨胀。鉴于这一问题，我们选择了一个务实的做法。

首先，代达罗斯将在未来的12个月内，支援大量的功能来标注交易和金融活动。这些元数据可以根据用户认为是必需的需求，进而导出或共享。此外，数据可以由三方应用程序操作，用于域特定目的（例如税务会计）。

其次，我们正在探索添加对可涵盖散列和加密字段的特殊地址的支援。这种结构将允许用户在我们的区块链上发布元数据，而不需公开揭示它。但是，如果她想要共享数据，那么它将具有交易享有的所有可审计性、不可变性和时间戳保证。

[30]在更宏观的规模上，作者Juan Zarate写道，美国财政部如何在财政战争中使用这些数据于恐怖主义战争。它提供了一个全面观，检视全球金融市场的现有结构如何被使用于地缘政治目标。

我们已经部署了一个包含属性领域的地址结构。它目前被用于存储为快速钱包恢复的分层确定性钱包之树结构的加密副本（参阅分层确定性钱包文档）。之后的版本将推广这个结构。

认证与合规性

与交易密切相关的主题是交易权和资金所有权。例如，虽然可能有足够的资金购买某物（例如酒品），但也有条件可能会限制其购买（如年龄要求）。

资金的所有权和来源通常是了解你的客户的规定。当银行或交易所的货币服务业务为新客户开立账户时，通常需要收集有关客户的基本情况以及获得资金的来源。

技术面的挑战是，在提交这种法律要求的信息过程中，发送信息的用户不能保证该信息将如何被使用、存储以及是否将被销毁。合规信息具有商业价值。在规定允许的情况下，可能发生身份盗用或信息转售。

对于卡尔达诺而言，我们希望尽可能地进行创新。在协议的软件方面，几乎接收方于合规信息中提供在行为范围内的行为保证。然而，在协议的硬件方面，使用可信硬件，可以利用英特尔SGX和其他的HSM来执行某些策略。

因此，我们正在探索使用密封玻璃证明以及分享政策，以便将合规信息安全传输给验证者，而该验证者又被迫遵守其传输的政策。我们认为，双方统一的标准可能会出现，而且这种方法可以通过防止黑客入侵所遗失的客户数据来降低验证者的风险。

为该努力的推论，我们为卡尔达诺从计算分离得到的价值之分层模型，也可以从这种方法中获益。如果计算层由受监管的实体（如交易所或赌场）运行，那么他们需要进行合规性的检查，并可能对用户实施税收政策。

使用统计生成程序(SGPs: Statistics Generation Programs)，用户可依照个人身份信息发送资金，而不用担心它会泄漏到更广泛的互联网中，或者被计算层的共识节点保留。此外，计算层将确定所有用户的交易都被认证且是合法的。

这种范式还允许受管制实体之间的客户携带性。交易所可以通过这些安全渠道立即转移客户的余额和账户，并且 - 在政策允许的情况下，与监管机构共享数据。

我们预计这项技术的第一次beta测试将在2018年中期进行，目的是依据该研究成果，在2018年底至2019年初期间将卡尔达诺集成。该时间表还含括与ARM和Intel合作的能力，以便获得在其硬件上运行的代码[31]。

市场分散应用机构

前两节介绍了假设存在一些外部系统的信息的产生和移动。为了确保传统的互操作性，这些功能将始终是必需的，但它们并未确立基于区块链的规则。

智能合约能够实现一种全新的商业系统，其关系是确定性的、自我执行的和无歧义的。反过来，它们可以用来制定市场规则，包括任意复杂的结构，如仲裁、事件驱使退款，以及给予特殊条件事实的揭示。

我们称这些智能合同执行结构市场分散应用机构。它们不需要特殊的协议支持，也不需要嵌入在分类帐中的可变性。事实上，它们可以使用相互依存的智能合同的集合以完全构建。

建筑概念是设计从合约法和商业最佳实践灵感的商业模式的集合。这些模板可以连接到开发人员的智能合约中，以便在市场上执行特定的标准。

例如，假设开发者希望在卡尔达诺计算层上发布ERC20令牌来进行众筹。市场分散应用机构可专门为众筹设立，其条款和条件参数化，甚至由志愿者或法律标准执行。诸如退款、重新分配资金或冻结付款等事项可以在开发商的ERC20合约中被继承。

这一努力使我们能够对于如何控制市场进行宏观的讨论，以确保消费者保护。第二，我们可以讨论如何建模交易，以自动确保特定司法辖区（如新罕布什尔州）的法律保护和权利。

于卡尔达诺基金会、IOHK和其它实体等的合作之下，卡尔达诺项目将建造市场分散应用机构的参考文库，以供智能合约开发人使用。我们的期许是，保险和监管市场可以围绕这些分散应用机构而形成，并且将根据其成果进行自我演变。

5. 永续发展

[31]请参阅英特尔SGX 商业许可证策略

沉浸于加密货币领域中产生许多概念上的矛盾。加密货币被设计成难以改变的，但如同所有技术一样，他们需要改变以解决设计缺陷和进步。区块链旨在防止集中化，但需要强大的参与者来引导变化或维护代码。

也许最令人沮丧的经历是，出现了大多数利益相关者都同意需要纠正的明显缺陷，但是在前进道路上，却并未出现共识。

比特币的区块大小争议现在已经是长达两年多的活跃问题。每日超过10亿美元的交易总额等待着，因为网络已达到其容量的高峰。

如果改变一个简单的参数 - 即使在临时解决方案的存在下- 其还是无法被协调的，那么企业和政府如何能够安心地在这些系统上投资数十亿美元，以建设基础设施呢？对于这个问题，任何企业如何赌注于无责任协议中的整合战略风险，而且这些协议又无法进行理性的设计升级？

回顾历史，互联网的演进也遵循了类似的模式，甚至是简单的改变，例如从IPv4到IPv6的过渡需要几十年才终于实现。然而，区块链技术和互联网之间存在强烈的对比，因为它们遵循非常不同的监护方式。

互联网是一个军事项目，从DARPA发展成为具有强大政府支持和一套明确定义的初始监护的学术界。互联网在非商业条件下成长，没有企业阴谋影响企图垄断网络。事实上，电子商务违反了NSF AUP，直至1992年将NSF AUP废除之前。

当企业拥有互联网商业化的光芒，早已有一套强大的标准、原则和传福音的信徒。这并没有阻止像美国在线和微软这样的公司，试图建造墙壁花园并创建像ActiveX这样的专有技术。谷歌基于其庞大的用户基础和资本，这个地基并没有阻止像Google这样的下一代参与者推出自己的议程。

通过一大群寻求租金的参与者[32]，从贸易商到矿工，加密货币是最终商业动机的生态系统。鉴于此基础，加密货币的监护管进化以藉由利己主义被优化。

例如，无效采矿开始更频繁地发生，因为它提高了矿工的利润率，但这完全无视采矿的整体目的和效用。集中化采矿已经发生，只有少数参与者控制了比特币的绝大分散列能力。

像互联网一样，加密货币需要共识来改变。但是，如果这种迅速集中权利发生在少数经纪人身上，那么当改变带给这些少数人不方便的时候，会发生什么呢？

与互联网不同，大多数加密货币的诱发不是通过无私的非商业或学术手段完成的。从一开始，一些集团力求获益，并且有权经纪人被分配来帮助确保这些获益。

[32]有关这一术语的更多信息，请参阅这里

资金集中化是每个密码学必须面对其演变的现实。我们不能完全逃避它，但至少应该设法逐步地分散集权。

对于卡尔达诺来说，我们仔细考虑了促进集权的因素，以及可以采用哪些技术来鼓励我们的协议逐渐成为像网络般的公共基础设施。

我们完全承认，全面分散化是不可能的，也许甚至适得其反。然而，某些因素可以被鼓励，来制定一个更加平衡的系统。

首先，群众资金的集中管理能够在初期灵活且快速地发展协议，但最终资金多样化，发展速度需要更系统化和更深思熟虑的步伐。接着，资金需要避免文化、语言和地理的偏见。

第二，随着社区越来越了解密码学技术的基本特性，也因此对于路线图的决策，无法集中在一组核心开发人员或基金会上。需要使用基于区块链的方法来提案、审查和颁布协议的更改。

第三，维护卡尔达诺结算层区块链的动机必须与所有用户的整体愿望直接相符。我们不允许一群具有独立意愿的大行社区的特殊参与者出现。

对于第一个原则，我们选择将财政系统整合到卡尔达诺。第二，我们将通过卡尔达诺结算层本身协调的系统，部署一个正式的过程来提出卡尔达诺的改进建议。第三，我们相信乌洛波洛斯提供了一个优雅的解决方案。

可以对上述主题提供更多细节，但是它们本身是广泛的，并且超出了调查文件的范围。机制设计是最复杂的，和相互依赖的学术领域之一，其理论不完整，而且没有坚实的规范模式。

相反地，我们在第二部分描述的科学驱使方法在这里为我们提供了良好的模式。 IOHK的Veritas团队正在与兰开斯特大学的一组研究人员合作，在Bingsheng Zhang教授的指导下开发卡尔达诺的参考财政模型。为了在2018年进行整合，我们预计到2017年底将有一份专门的同行评审刊物。

对于一个加密货币协议的修改的正式描述和审查，这个主题是最不被理解的，因为它需要本体论概念，和激励广泛参与的机制。也许某种形式的代议制民主过程可能出现，或使用液态反馈来提供更合理的投票。

我们预期这方面的研究将占有IOHK大部分正式参与卡尔达诺的开发[33]。作为一个起点，我们将在参考财政模型的基础上，部署几种机制来获得认可。需要进一步研究才能确定解决方案。

[33] IOHK将在2020年底之前保持建造卡尔达诺

最后，正由牛津大学的Elias Koutsoupias教授监督，进行为乌洛波洛斯提高激励措施的工作。在所有必要的可扩展性工作之结束后，乌洛波洛斯的加密基础得以巩固。将会进行对参考协议，增加对债券、惩罚和异国激励措施的更广泛研究。

6. 结论

一个加密货币远超出于其协议、源代码和实用程序的总和。它最终只是一个社会制度，来启发、实现和连接人们。对过去协议的许多折中办法、失败和破坏承诺感到沮丧，所以我们开始建立更好的。

这个过程并不简单，我们也不太相信能够完成它。随着人类和社会的变化，社会协议也持续无限地改变。为了是有用的，我们想嵌入进化的力量，并将其移植到卡尔达诺上。

进化不是靠单手或庞大的设计所引导。这是一个意外的过程，通过的无尽的错误和问题产生的灵感而启发。卡尔达诺致力成为这一过程的数字体现 - 足够能够在今天的市场中生存下来，并具有足够的自适应性，以适应未来的需求。

前面的章节简要地介绍了我们如何实现这一目标。我们勤奋地尝试了解认知偏见、从历史中学习，并遵循严格的过程。我们试图将快速发展的需求与传统上无法快速移动的正式方法相互平衡。

非常荣幸踏上这个旅程。在过去两年中，我们已经开发了一个可靠的权益证明协议，招募了一个Haskell开发人员的小团队，并使卡尔达诺的发展成为许多有才华的科学家所关注的焦点。

当我们从实验室迁移到野外布置系统时，会有越来越多的痛苦，但是我们希望卡尔达诺的未来可以被概括为一个单一的拟人化句子。卡尔达诺是一位务实的梦想家，从年长者那里学习，是社区内的好公民，并总是找到一个办法支付自己的账单。

我们无法得知未来，但我们很乐意为每个人做一件更好的事情。

谢谢阅读。