为何我们正在建立卡尔达诺

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，却受困于丨些琐碎的考量—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，丨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，是丨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。

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？

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。

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)

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。

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。

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。

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。

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

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。

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。

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

3: 也称为财政系统

4: 请参阅理性的无知

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

7: 项目 ACTUS 有一个深入的阐述

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

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

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

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

14: 请参阅 由康奈尔大学发布使用安全硬件缩放比特币

15: 请参阅 BIP39

16: 作为资本流动的对策的一个例子，参阅 Hawala 银行系统银行系统

17: 参阅预付费诈骗