无界协议

RISC零团队

抽象的

我们建议*无边无际*，一个去中心化的市场、聚合和智能合约结算协议，旨在为每个链扩展 ZK 驱动的可验证计算。

在 Boundless 中，GPU 和其他商用硬件的运营者被称为“证明者”，他们通过高效开放的市场竞争“请求者”发出的链上或链下零知识证明请求 。此类请求可能出现在“现货”市场，也可能作为“服务协议”合约的一部分发生。无论哪种情况，付款都会在请求者指定的目标链上验证证明的同时进行结算。

我们描述了以下贡献：*可验证工作量证明*这是一种用于衡量零知识证明的复杂性（以及因此而产生的相对成本）的反欺诈和反垃圾邮件机制，Boundless 使用该机制通过向参与有用的“ZK 挖矿”的证明者发放代币奖励来激励证明；*计算金融化*利用加密经济激励机制，为匹配证明者和请求者的问题提供可靠、资本高效的解决方案；*无边无际*，一个基于这些想法而建立的实用系统。

内容

1 介绍

计算资源可以交易的想法与计算行业本身一样古老。几十年来，出现了几种不同的模型，最终形成了云计算和链上执行等现代方法。

然而，尽管云计算享有出色的规模经济，但链上执行却并非如此。

区别在于信任。云服务的用户默认信任服务提供商会忠实地执行计算。相比之下，区块链的用户不信任任何特定节点，而是信任协议，因为协议设置了应对不诚实节点的缓解措施。然而，这些缓解措施的运作机制（由持怀疑态度且受激励的验证者重新执行）必然会对链上可执行的计算量施加限制。对链上计算的需求超出了这些限制，并且

因此，区块链必须有另一种机制来决定执行哪些请求的计算。在以太坊和其他网络中，这由 Gas 市场决定，Gas 市场只是简单地拍卖链上有限的计算资源。虽然这种机制有很多优点，但它并没有解决根本问题（链上计算资源的稀缺性）；相反，它“定价”了所有请求，只留下利润最高的请求，实际上是牺牲一个工作负载来满足另一个工作负载，而不是同时满足两个工作负载。

基于零知识证明 (ZKP) 的现代方法提供了更好的解决方案。ZKP 通过允许节点证明给定计算会产生给定输出来改变信任动态。这使得用户或其他观察者即使不信任执行该计算的节点，也能信任计算结果。通过这种方式改变信任动态，ZK 消除了怀疑性重复执行的需要，从而开辟了一条通往可扩展、去信任化、去中心化计算的道路。

1.1 ZK 的采用之路

尽管上述论点已为人所知一段时间了，但直到最近，现实世界对 ZK 的采用才受到限制。

在零知识证明的早期发展中，它包含各种各样的专门技巧，每种技巧都能够解决特定类型的问题。RSA 和 ECDSA 等公钥数字签名方案或许是这一早期阶段最具代表性的例子。

随着时间的推移，计算复杂性理论的进步，特别是在概率可检验证明的研究中，为 ZK 应该能够执行通用计算提供了强有力的理论证据。实用算法

——以及图灵奖——很快就随之而来。

然而，这些算法虽然实用，但离易用性还相去甚远。就其本质而言，只有精通应用密码学且对前沿理论成果有深入理解的人才能掌握。尽管如此，2016 年 Zcash 的推出证明了这项技术的可行性。这引发了旨在提升 ZK 性能、功能、安全性和易用性的大量研究。

由此催生了诸如 Bulletproofs（2018 年）、Circom（2019 年）、Halo（2019 年）等新技术。与此同时，STARK 的开发以及 2020 年 CairoVM 的发布表明，ZK 无需可信设置即可实现安全性和可编程性。

2022 年，RISC Zero 发布了 zkVM，这是首个基于标准架构 (RISC-V) 的通用零知识虚拟机。zkVM 彻底改变了整个行业：此前，零知识的采用需要使用一些特殊的编程语言或电路语言，而 zkVM 则使得使用任何支持 RISC-V 的编程语言成为可能。其中尤其值得一提的是 Rust，它拥有优秀的工具和库生态系统，并在区块链和其他行业中得到广泛应用。

一年后，RISC Zero 发布了首款“Type 1” zkEVM Zeth，展现了 zkVM 的强大功能。Zeth 震惊了整个行业。此前，传统观点认为 zkEVM 的构建需要数年时间。Zeth 的出现，证明了一个 3 人团队可以在一个月内完成。这种颠覆性创新，加上 zkVM 自发布以来不断提升的性能，引发了整个行业项目路线图的变革：Zk 不仅切实可行，而且使用 zkVM 构建起来也更加快速便捷。

1.2 最后的挑战

遗憾的是，采用 ZK 绝非像编写一些 Rust 代码并在 zkVM 中运行那样简单。真正的采用必然会面临最后一个挑战：端到端集成。挑战的本质在于，链上计算的 Gas 市场已被纳入链协议，而 ZK 证明的访问权限却并非如此。因此，寻求采用 ZK 的团队必须构建自己的证明流程。这是一个不小的挑战，包括缺乏合适的去中心化基础设施、标准链上执行和 ZK 驱动执行之间的控制流差异、激励管理，以及与引导和保留证明容量相关的问题。

zkVM 彻底改变了人们编写 ZK 的方式

应用程序。我们需要的是其部署和集成方式的类似革命。

2 *无边无际*

为了解决与 ZK 采用相关的挑战，我们建议*无边无际*，一个完全去中心化的 ZK 驱动协议，包含智能合约、新型加密原语和链下基础设施，其无许可市场通过以下方式促进任何协议或区块链的安全、高效和可靠执行：*计算的金融化*：

- 其核心是通过部署在任何兼容区块链上的智能合约来实现的。[1]每个部署都是独立的，并继承其所部署链的属性，包括去中心化、活跃性和加密经济安全性。
- 它使基础设施提供商能够同时无缝地参与所有这些部署，确保有足够的*证明流动性*跨越所有链条。
- 它利用了*零知识证明*和*可验证工作证明*实现无需信任的计算支付交换。
- 它是一个*市场*它通过将基于 ZK 的可验证计算视为可直接交易的商品（在*现货市场*）或间接地（通过*服务协议*）。
- 其计算能力与证明器操作的计算资源成线性比例：硬件加倍，容量加倍。

2.1 计算的金融化

在本节中，我们将解释 Boundless 背后的基本思想：（1）可验证计算可以被视为一种商品，（2）可验证计算的证明工作使得该商品能够以无需信任的方式计量和交易。Boundless 依托这些特性，利用市场力量来促进无需许可和无需信任的交易以及可验证计算的利用——从而为上述端到端集成挑战提供高效可靠的解决方案。

2.1.1 丰富的商品

ZKP 技术已经发展到可以在 MacBook Pro 和游戏 PC 等消费级现成硬件上生成非平凡的 ZKP 的阶段。此外，用于生成非平凡 ZKP 的软件是免费开源的。由于门槛如此之低，预计可验证计算将像一种丰富的商品一样普遍存在。

对于用户和协议来说，这意味着以稳定的价格简单、可靠地访问可验证的计算。

对于工业验证者来说，这意味着通过资源管理、容量规划、定价和可靠性来增加价值；通过销售服务协议和其他差异化产品；以及通过管理或协调住宅/业余验证者池。

最后，对于交易者来说，这意味着通过促进价格发现和提供允许市场参与者对冲波动的工具来增加价值（见*服务协议*以下）。

2.1.2 去信任交易

与实物商品不同（几乎所有的争议都归结为*同时观察的主体间真理*），所有关于 ZK 驱动的可验证计算的相关信息都属于*具有有限不确定性的客观真理*(即在标准密码学假设下的概率健全性。通过正确实现电路和软件（以及选择合适的密码学参数），这实际上与*客观真理*，这就是为什么 ZKpowered 可验证计算非常适合在无信任环境中使用的原因。[2]

[1]出于教学原因，本文将注意力集中在以太坊及其基于 EVM 的 L2 上。

[2]我们借此机会呼吁在各个层面更多地采用形式化验证——从底层理论的属性一直到现实世界的保证

但仅凭这一特性，可验证计算量还不足以实现高效的交易。为此，还需要一种无需信任且安全的方式来计量投入特定任务的计算量。在 Boundless 中，这种计量是通过以下方式实现的：*可验证工作证明*这是一种简单但强大的机制，除其他功能外，它允许证明者揭示特定证明所需的工作量。

这些属性——结果的客观性以及可验证工作证明所报告的指标的完整性——使得可验证计算的无信任交易成为可能。

2.2 可验证计算的现货市场

我们先从一个简单的例子开始。Alice 想要使用一款需要她提交零知识证明 (ZKP) 的链上应用。任何拥有足够计算资源并能访问必要数据的人都可以生成零知识证明。Alice 不想自己生成零知识证明，所以开始寻找可以代为生成和提交零知识证明的人。Bob 和 Charlie 都有兴趣为 Alice 生成零知识证明，只要她愿意支付足够的费用来支付成本并获得合理的利润。

Alice 能够描述所需的计算，并且 Bob 和 Charlie 可以根据该描述估算出满足她的请求所需的工作量。[3]因此，从市场角度来看，唯一的问题是：谁愿意/能够以最低的价格做到这一点？

无限市场通过促进*反向荷兰式拍卖*在反向荷兰式拍卖中，价格发现的运作方式如下：

1. 请求者（Alice）在一个公共论坛（无界市场），无论是链上还是链下。
2. 最初，请求者并不愿意支付太多费用来满足他们的请求。他们愿意等待一段时间，看看是否有人愿意以低价满足他们的请求。
3. 随着时间的推移，如果请求没有得到满足，请求者就会增加他们愿意支付的金额。
4. 最终，要么：
   （a）价格上涨到某人（鲍勃、查理或其他人）愿意满足该请求的水平；或
   （b）价格持续上涨，直至请求者不愿继续上涨。如果仍然无人接单，则请求无法完成。

这种方法有几个好处：

- 一旦第一个出价得到确认，荷兰式拍卖就会结束。[4] 此特性使得荷兰式拍卖特别适合低延迟情况以及链上实现。
- 拍卖的“逆向”特性使得协议比“普通”拍卖更简单。在“普通”拍卖中，证明者需要公布其价格和容量。以一种无需信任的通用方式做到这一点并不容易。而逆向拍卖则避免了这些挑战。
- 逆向荷兰式定价法展现出理想的效率和稳定性。至关重要的是，它能让 Alice 以较低的成本获得尽可能低的价格。

因此，当 Alice 需要 ZKP 时，她会向 Boundless Marketplace 发布一个包含以下数据的请求：

实施——并感谢 Nethermind、Veridise、Runtime Verification 和以太坊基金会的合作伙伴在这一领域做出的重大贡献。

[3]他们可以通过获取必要的数据并在非证明执行器中运行请求的计算来实现这一点。这样做成本相对较低，通过确保给定的数据确实能够成功实现结果来降低请求的风险，并准确地告知他们生成证明所需的工作量。

[4]要了解原因，请注意价格函数是单调非减的。这意味着第一个出价保证是最低的，因此请求者没有理由考虑任何后续出价。

- 她需要生成的 ZKP 的机器可读描述（以及满足请求所需的任何其他元数据）。[5]

- 指示拍卖预计开始时间的时间戳。

- 单调、不递减的价格函数（以 ETH 或 ERC20 计价）。

- 可选债券（由寻求锁定请求的证明者质押）。

- 到期日/最后期限。

选择好请求参数后，Alice 便可以发布她的请求。为此，她有以下几种选择：

- 她可以将她的请求发布到 Boundless Marketplace 合约上（在她选择的链上）。

- 她可以签署她的请求并将其发布到一个或多个单独的协议（第三方八卦协议、交易所、列表服务等）。

无论哪种情况，她的请求最终都将通过她请求指定的链上的 Boundless Marketplace 合约来满足。

Alice 的请求发布后，Bob 和 Charlie 都会开始评估完成该请求所需的工作量。他们会根据以下因素评估请求：请求的描述（参见脚注 3）、到期日/截止时间、他们当前的工作量、市场上的其他机会、他们期望的利润率、是否有人愿意以更低的价格完成任务的可能性等等。[6]

基于这些因素，他们都选择了一个高于他们愿意履行合同的价格任务。不失一般性，假设查理选择的价格比鲍勃低。[7]

随着时间的推移，如果请求仍然有效，价格会根据价格函数以编程方式上涨。最终，价格会接近 Charlie 的门槛。当价格达到这个门槛时，他有两个选择：

1. *立即满足请求*查理可以通过在价格上涨到一定程度以吸引竞争之前争相生成证明并满足请求来做到这一点。

2. *立即锁定请求*此操作赋予 Charlie 完成请求的独家权利。这种锁定使他能够专注于生成证明的任务，而不必担心竞争对手会在最后一刻突然出现并完成请求。为了确保这种独家权利，他必须锁定一些权益。如果他未能在规定的期限内完成请求，他将失去这些权益。

在某些情况下，Alice 可能希望禁用锁定。她可以在请求中明确说明这一点。在这种情况下，上述路径 (2) 将被禁止。

当 Charlie 满足她的要求时，他通过程序获得了报酬*证明人费用*，等于 *请求的价格*减去 *市场费用*(由市场决定*接受率*，并归入市场 *保险库*）。请求的价格由锁定时（如果 Charlie 在执行前锁定了请求）或执行时（如果未锁定请求）的价格函数决定。为了节省与证明验证相关的 Gas 费用（如果 Alice 的请求允许），Charlie 可以将证明作为聚合批次的一部分进行交付。

2.2.1 履行保证

当一切顺利时，Alice 会支付最低的价格，在指定的时间内收到她的证明

[5] 为了节省链上数据成本，请求元数据可能包含对链下数据的引用，例如磁力链接、IPFS 链接、HTTPS 链接、S3 链接、DA 平台链接等。通常不需要长期数据可用性；在现货市场中，预计潜在的证明者会在尝试锁定或证明请求之前尝试获取数据。

[6] 这种评估可以通过使用模型来实现自动化
els。

[7] 也许鲍勃的成本基础比查理更高，又或许他只是追求更高的利润率。也许鲍勃并不指望查理会选择更低的价格，又或许鲍勃认为即使以最高价出售，该请求也无法盈利。接下来，鲍勃选择比查理更高目标价的原因将不再重要。

截止日期。但是，如果有人锁定了她的请求，但未能在截止日期前完成（可能是故意的）怎么办？

如果 Charlie 锁定了 Alice 的请求，但错过了截止日期，那么他将失去他的质押，而 Alice 的质押金将被退还。接下来会发生什么取决于 Alice 如何配置她的请求：

- 在最简单的情况下，丢失的股份被发送到市场合约（在那里可以通过积分机制分配给代币持有者），并且请求的生命周期被视为完成。

- 或者，如果 Alice 的请求允许，则该请求进入“重试”阶段。在此阶段，锁定将被禁用，证明者将获得原始证明者损失的质押金的一部分作为奖励（剩余部分将发送到市场合约）。假设 Alice 适当地调整了质押要求，证明者将识别出提供的溢价，并竞相满足她的请求。

Alice 还可以使用其他策略。例如，如果 Alice 需要证明*现在*她可以提交一个期限较短、禁用锁定且价格固定且较高的请求。当鲍勃和查理看到这个请求时，他们会意识到这个请求的溢价很高，于是争先恐后地去完成。

或者，假设 Alice 需要在 3 天内完成她的请求（即，这段时间大大超过了生成证明所需的时间）。在这种情况下，她可以提交一个截止时间更短的请求（例如，12 小时），初始价格合理，最高价格诱人，并且质押要求适中。如果她的请求没有引起任何兴趣，她仍然有充足的时间以更高的价格或不同的参数重新发出请求。

2.2.2 去中心化

大规模生成证明是一个工业过程，与其他工业过程一样，它具有规模经济效应。在其他条件相同的情况下，河边的数据中心能够以比家用游戏电脑池更低的成本生成更多证明。在

鉴于此，我们现在考虑以下问题：如何阻止垄断的形成？

为了回答这个问题，我们回到前面例子中的证明者 Bob 和 Charlie。

假设 Charlie 的规模超越了竞争对手，发展到可以承担绝大多数证明任务的程度。Bob 却很少能够锁定请求，实际上已经被挤出了市场。

如果查理继续以合理的价格满足请求，那么一切都很好。但是，如果查理开始提高价格或拒绝满足某些类型的请求，该怎么办？

当查理滥用垄断地位时，鲍勃开始看到机会。查理对市场的掌控并非绝对：他或许垄断了证明市场，但他并没有垄断证明所需的硬件。*从事*在证明市场中。事实上，Bob 已经拥有必要的硬件（MacBook Pro 或游戏 PC 即可）；如果机会足够大，他甚至可以启动一个云实例队列，以实现最大效果。该软件易于部署和运行。因此，如果 Bob 可以通过降低 Charlie 的价格或满足 Charlie 忽略的请求来获利，那么他就会进入市场并这样做。

在无边界市场中，目标是以低成本为用户提供可靠的服务。实现这一目标的方法是确保像Bob这样的人能够轻松利用他们已有的硬件加入并纠正市场。这种对市场力量（以及无需许可的区块链）的依赖是无边界去中心化的关键所在。作为证明者加入市场的门槛很低：该软件是开源的，并且可与商用硬件兼容，因此证明供应无需许可且无所有者。理想情况下，这将提供足够的“计算流动性”来纠正市场中的异常情况。因此，当至少有一方认为这样做有利可图时，向无边界市场发出的请求将以公平的价格得到满足。

2.3 代币

为了促进可靠、低摩擦的交易和无需信任的治理，无边界市场包括

一种名为 $ZKC 的新代币，具有以下属性：

- 总供应量上限。
- 可变的铸币率，最终由代币持有者通过链上治理控制，决定达到供应上限的速度。新铸造的代币将作为以下部分分配给证明者：*可验证工作证明*奖励机制（见下文）。
- 能够产生积分，从而获得市场收取的费用。
- 有能力参与现货市场和/或服务协议。
- 可变的奖励频率（由治理控制）决定了代币和积分的铸造/分配频率。

我们将在下面的部分中更详细地描述这些概念。

2.3.1 *可验证工作证明*

随着请求的满足，Boundless 市场会持续追踪与奖励分配相关的各项指标。具体来说，在每个奖励周期，Boundless 都会追踪：

- 市场收取的累计费用。这是衡量所提供价值的标准。
- 市场验证的累计循环次数。这是对已完成工作的衡量标准。

它还会逐个跟踪每个证明者的相关指标。因此，对于任何给定的周期，对于任何给定的证明者，都可以轻松计算出该证明者完成的请求所产生的费用百分比（即每个周期的费用）。

利用这些指标，Boundless 的智能合约会以程序化的方式奖励证明者，根据他们对市场的贡献比例向他们分配新铸造的代币。因此，市场为证明者提供了两种收入来源：他们在完成任务后从请求者那里收到的付款，以及可验证工作证明提供的本地奖励。

但这引出了一个问题：对市场“贡献”究竟意味着什么？虽然“贡献”的定义最终将由代币持有者治理，但在项目启动时将有两个关键指标：

- 交付的价值。按照这个指标，对市场收取的费用贡献较大比例的证明者应该获得丰厚的奖励。
- 已完成的工作。按照此指标，对大部分已证明循环负责的证明者应获得丰厚的奖励。

这些指标通过以下规则合成奖励：每个证明者根据其在市场收取的费用比例获得奖励[8]或其已证实的循环比例——以较小者为准。[9]

例如，假设Bob负责市场收取费用的25%，但只证明了10%的周期。在这种情况下，他将获得10%的新铸造代币。相反，假设Charlie负责市场收取费用的75%，但证明了90%的周期。在这种情况下，他将获得75%的新铸造代币。

在上面的例子中，我们看到 Bob 和 Charlie 承担了所有费用和周期，但最终只能获得 10% + 75% = 85% 的新铸造代币。剩余的 15% 则被直接销毁，从而降低了铸造率。

跟踪已证明的周期数的能力主要取决于 RISC Zero 的 zkVM 的一个独特功能，称为 *可验证工作证明*此功能使证明者能够在其证明中包含有关证明中所用循环次数的元数据。这些元数据是加密安全的。

[8] Boundless 支持 ETH 或 ERC20 代币付款。然而，就奖励机制而言，仅考虑以 ETH 计价的费用。

[9] 在治理将市场佣金率设定为 0% 的特殊情况下，费用比例将被忽略。在这种情况下，证明者将根据其证明的周期数获得相应的奖励。

这意味着证明者不能操纵或改变它，否则将导致证明无效。[10]并且还带有一个唯一的、不可变的值（*随机数*）来防止证明被奖励机制“重复计算”。

2.3.2 *保险库*

如上所述，市场会对所有已完成的请求收取费用。该费用按百分比计算（称为*接受率*请求价格的百分比。手续费由代币持有者治理配置。市场以这种方式收取的费用最终会分配给 $ZKC 持有者。在本节中，我们将描述实现这一过程的机制。

回想一下，市场部署在多条链上。每条部署都有自己的费用池，市场收取的费用都存入其中。

每个部署还具有*保险库*(由不可变的智能合约实现，其中包含已锁定的代币。$ZKC 持有者可以无权限地将其代币锁定在金库中。锁定期间，代币可赚取（不可转让的）积分，这些积分随后可被销毁，以从池中提取费用和/或解锁金库中的代币。提取/解锁机制基于比例：销毁 1% 所有未偿还积分的实体将获得池中 1% 的费用（销毁时）；同样，销毁 1% 积分的实体也可以选择同时解锁 1% 的代币。

除了生成积分外，锁仓中的代币还可以质押到服务协议中（见下文），或用于在现货市场锁定请求。与所有锁仓中的代币一样，以这种方式质押的代币将继续以编程方式生成积分。

[10]直观地讲，此功能通过向 zkVM 电路添加约束来实现，从而有效地实现一个单调计数器，其值与生成证明所需的 (ZK) 执行周期数相关。至于完整的细节，例如如何防止延展性以及如何核算不同电路的成本，则超出了本文的讨论范围。

2.4 可验证的服务协议

一个 *可验证的服务协议*是证明者和请求者之间的具有约束力的承诺，通常规定请求者可以要求证明者执行某些可验证工作的条款。

从机制上讲，服务协议由智能合约实现，这些智能合约利用了 Boundless 的市场、保险库、聚合、交付和奖励机制。Boundless 的设计理念是开放的：任何人只需部署兼容的合约，即可在无需许可的情况下将新型服务协议推向市场。这种灵活性使我们能够创建针对不同用例的定制工具，同时仍然享受 Boundless 市场提供的规模经济和内在奖励。

我们通过两个例子来说明服务协议的实用性。

首先我们回到Alice和Charlie的案例。回想一下，Alice作为终端用户，利用现货市场从Charlie（证明者）那里购买了一份证明。她知道自己将来会提出更多请求，因此联系Charlie并提出了一项协议：她愿意预付一小笔款项，以换取在未来一年内以预定的价格，以有限的频率，一次购买100个类似的请求。他们通过一份智能合约（即服务协议）来记录这份协议，如果Charlie未能履行其承诺，Alice将获得无需信任、无需中介的追索权。

Charlie 喜欢这种安排，因为它与 Alice 建立了便捷的付款渠道，同时也有助于他进行长期容量规划。Alice 也喜欢这种安排。一方面，服务协议降低了她面临证明（现货）价格不可预测上涨的风险。另一方面，如果她没有像最初计划的那样发出那么多请求，那么她就损失了服务协议的成本，但无需为未使用的请求付费。此外，如果服务协议条款允许，她可以通过将服务协议出售给其他用户来收回部分成本。

但爱丽丝并非唯一寻求服务协议的人。第二个例子是帕姆，

一位协议开发者，希望确保其核心协议拥有充足的证明供应。具体来说，她正在寻找一份能够提供以下功能的服务协议：

- 明年将进行大量证明，可能会出现突然飙升，也可能在年底前出现显着增长。
- 及时提供证明（以确保协议顺利进行。）

帕姆联系查理，希望他能购买一份服务协议，但仅凭这一点还不够：无论查理过去多么可靠，无论他对这份合同投入多少精力，他总有可能无法履行自己的承诺。如果发生这种情况，帕姆可以选择现货市场作为后盾（第 2.2 节和 2.2.2 节）。然而，考虑到她工作量巨大，她更倾向于避免“按需”定价。

于是帕姆开始寻找像查理这样的人，也从他们那里购买服务协议。她*积累*将这些服务协议放入一个篮子里。这解决了她对可靠性的担忧：从结构上讲，没有任何单点故障能够阻止这个篮子提供证明。但这个篮子也相当大，可能比预期的工作量大几倍。因此，她采取了最后一步，*细分化*篮子。这使她能够出售过剩的容量，同时也让买家能够获得传统上只有大型协议才能获得的高端 SLA。

2.4.1 关于数据可用性的说明

如第 2.2 节所述，现货市场中的证明者自行决定处理请求，因此可以自由忽略数据不可用的请求（脚注 3 和 5）。

对于服务协议，情况可能更加微妙。例如，假设 Alice 从 Charlie 购买了一份服务协议，要求他满足她的请求（如果未能满足，Charlie 将被罚金）。如果 Alice 向 Charlie 发出请求，但未能提供完成请求所需的数据，会发生什么情况？一般来说，Charlie 无法*证明*那个爱丽丝隐瞒了数据，因此（在服务协议的智能合约中）Alice 发出了有效请求，而 Charlie 未能履行该请求。Alice 利用这一点，可以让 Charlie 在无辜的情况下被罚没。

为了避免这种情况，证明者在签订协议之前必须考虑协议中隐含的数据可用性要求。例如，如果协议仅适用于可以使用来自非许可来源（例如以太坊、EigenDA、Celestia 等）的数据来处理的请求，那么数据（不）可用性给证明者带来的风险相对较低。幸运的是，大多数去中心化应用程序应该自然满足此要求，因为数据可用性与进度之间的关系并非 ZK 独有。

3 实施

Boundless 正在开放环境中构建。请参阅请求者、证明者和开发者文档以及代码本身，网址：https://beboundless.xyz。

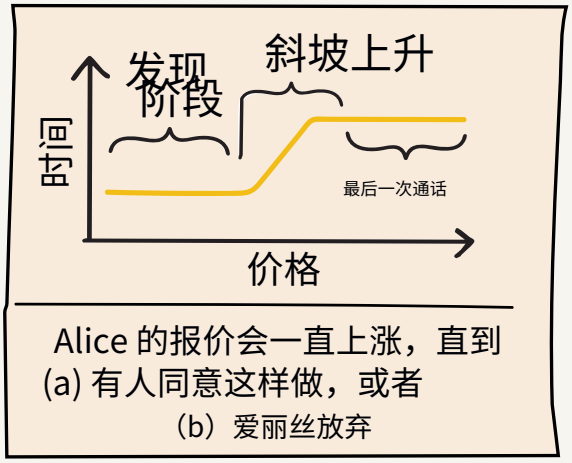
4 结论

自中本聪 15 年前发表他的 9 页巨作以来，很多事情发生了变化，但很多事情仍然保持不变。链上生态系统的大部分仍然植根于 20㊐世纪密码学。零知识证明的最新进展代表着向前迈出的重要一步，我们认为 Boundless 是实现其潜力的正确途径。

请求者

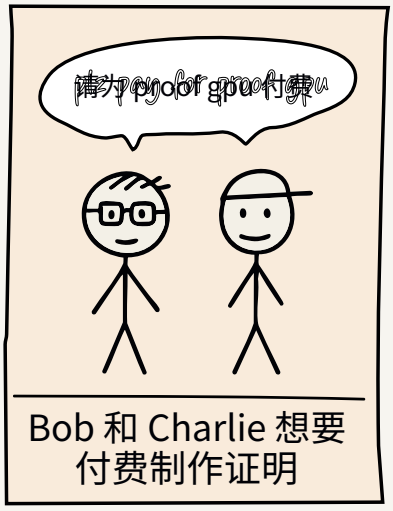
爱丽丝想要一个证明

为了与证明者相匹配，
她进行了一次逆转
荷兰式拍卖

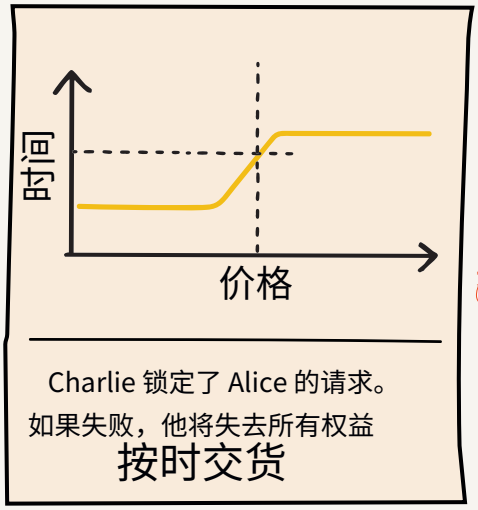


Alice 的报价会一直上涨，直到
(a) 有人同意这样做，或者
（b）爱丽丝放弃

证明者



Bob 和 Charlie 想要
付费制作证明



Charlie 锁定了 Alice 的请求。
如果失败，他将失去所有权益
按时交货

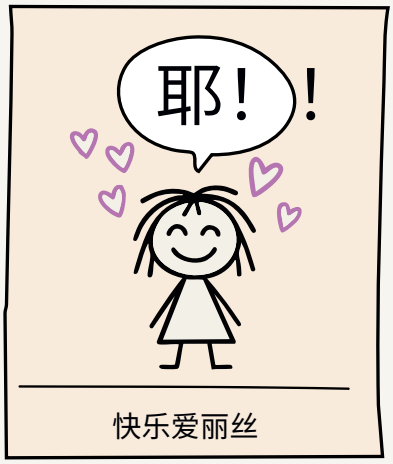
查理
错过了
截止日期

Charlie 错过了最后期限
Charlie 被削减股份；他的股
份被用来资助一场新的拍卖

结果

查理交付
准时

后备拍卖
成功



快乐爱丽丝