EiChain:全链资产质押再收益

释放闲置资产价值 & 新业态共享经济安全

EiChain 团队

Version 1.0: 2024-03-13

摘要

EiChain，一个针对全链资产质押共享经济安全再收益的连接器。作为 L1 层的区块链，EiChain 允许任意链的资产质押者选择加入验证加密经济生态系统上创建的新服务。我们提出了“全链资产权益质押”的理念，让持有者把所有高价值闲置资产质押，在增加 PoS 共识的安全性同时，全链资产拥有者还获取了收益。EiChain 提出了“全链资产质押再收益协议”，该协议让任意区块链上的资产去中心化的跨链数据交换，实现不同网络的资产、数据和流动性的统一高效管理；此质押无需把资产跨链到 EiChain，就可以提供通过惩罚销毁质押权益的安全保证；该协议以模块化设计，质押者可以验证包括共识协议、数据可用性层、虚拟机、维护者网络、预言机网络、桥接、阈值密码学方案和可信执行环境等多种类型的服务，在不分散服务之间安全性前提下，实现跨所有服务共享全链资产的安全性，进而增加了依赖这些服务的去中心化应用程序（DApps）的安全性；此外，比特币市值达 10,000 亿美元，以太坊市值 4,000 亿美金，大部分资本是闲置的，全链资产的质押者可以通过这些多样化服务产生新的收益机会，释放空闲资产的价值。我们提出了一套系统架构 -- 将 EiChain 作为核心枢纽，让众多资产链与基于 PoS 共识的创新服务同步，使得该协议具有很强的扩展能力，从

而惠及千千万万权益质押者和加密生态服务。EiChain 开创了一个无需许可的创新新时代：创新者不需要构建自己的信任网络来实施新的分布式验证服务，而是可以依靠资产质押者通过 EiChain 的提供来获得安全性和去中心化。

1 问题：去中心化信任很难产生和维护

共识机制是加密经济中核心内容之一，其安全由为之提供的资源来决定：PoW 由硬件算力来保障，但是缺少罚没机制；PoS 由质押的“资本”来决定。

比特链基于 PoW 开创了去中心化信任的时代，成为最安全的区块链。但是其资产仅限于链上转移。

而更多的公链都是使用 PoS 共识机制。特别是以太坊，其引领了模块化区块链时代。由以太坊网络为所有数据可用层提供安全服务：开发者只需要关注创新，不必为其安全性和活跃性分忧，这成为加密经济的关键驱动力。

但是，随着加密经济生态进一步的发展，存在更多涉及处理来自链外部的输入的服务。这些创新的服务不能在区块链上部署或验证，无法享受链协议提供的内在验证，需要自定义的分布式验证语义（称之为 AVS）。而这些服务要么由他们本地代币保护，要么由中心化上经过许可。

目前，对于 AVS 生态存在如下几个严重问题：

a. **新创造的 AVS 启动难。**为了建立一个新的信任网络以获得安全，就必须开始吸引大量资产质押。但是这往往是难以达到的，为了吸引此类资本，必须采取高通胀来提供高质押收益，而这胀阻碍了区块链的长期发展。
b. **资本成本的负担。**为了保护新 AVS，质押的验证者必须承担资本成本，即相当于与在新系统中质押相关的机会成本和价格风险。因此，AVS 必须提供足够高的质押回报以覆盖这一成本。对于目前运行的大多数 AVS

来说，质押的资本成本远远超过任何运营成本。例如，考虑一个有 100 亿美元质押保护的 AVS，假设质押者期望的年化回报率（APR）是 5%。这个 AVS 每年需要至少向质押者支付 5 亿美元，以补偿资本成本。这比 AVS 的运营成本要大得多。

c. **DApps 的信任模型降低。**当前的 AVS 生态系统产生了一个非常复杂的安全动态：DApp 可能依赖多个 AVS 服务，而这些 AVS 服务可能是攻击的目标。根据木桶原理，DApp 的 CoC 成本通常是其中依赖服务的最低成本$CoC = \min\{CoC_J\}$。在一个应用程序依赖于一个关键模块，如一个只有少量质押保护的预言机服务，即使区块链提供的强大的经济安全保证可能也没有太大意义，因为攻击预言机的成本远低于攻击区块链的成本。

2 EiChain：全链资产质押再收益

“全链资产质押再收益”创造了一个双边市场：一方是拥有资产并希望赚取收益的持有者，一方面是由安全需求并愿意付费的 AVS。而”全链资产质押协议”实现了双边市场的“共享经济安全协议”。EiChain 引入了两个新概念，汇集安全和市场治理，这有助于将底层的安全性扩展到其他任何系统，并消除现有僵化治理结构的低效性：

2.1、通过重新质押实现汇集安全性

EiChain 通过复投机制提供了一种新的汇集安全的方法：它允许 AVS 通过复投的资产篮子而不是它们自己的代币来获得安全性。特别是，全链资产的验证者可以将他们的资产质押到 EiChain，并选择加入在 EiChain 上构建的新 AVS。验证者需要下载并运行这些 AVS 所需的任何额外的节点软件。然后，这些模块有能力对选择加入 AVS 的验证者的质押资产施加额外的削减条件。

作为回报，验证者从提供安全性和验证服务给他们选择的 AVS 中获得额外的收入。当与链上可验证的削减机制结合使用时，这种复投机制允许深度转移加密经济的安全性。复投极大地扩展了可以汇集安全性的区块链应用的范围。因此，EiChain 将开放创新扩展到去中心化应用（DApps）之外，包括虚拟机、共识协议和中间件等，任何具有链上削减合约的自治验证系统（AVS）都可以由 EiChain 来保护。

2.2、开放市场

EiChain 提供了一个开放市场机制，该机制管理其如何运作。EiChain 充当一个开放市场：自治验证系统（AVS）可以在这里租用由资产验证者提供的汇集安全性。汇集安全性由验证者提供，并由 AVS 消费。验证者可以选择加入或退出在 EiChain 上构建的每个 AVS。各种 AVS 需要充分激励验证者将复投的资产分配给他们的 AVS，验证者将帮助确定哪些 AVS 值得分配这些额外的汇集安全性，考虑到可能的额外削减风险。

EiChain 的加入有两个重要好处：（1）核心区块链的稳定、保守治理与快速高效的自由市场治理结构相结合，用于启动新的辅助功能；（2）加入验证使得新的区块链模块能够利用验证者之间的异构资源，从而实现更好权衡。

EiChain 作为一个开放的市场，自治验证系统（AVS）可以在其中租用共享由全链资产验证者提供的汇集安全性。

EiChain 解决了上述 AVS 生态系统中的各种问题。

3. EiChain 全链资产质押：安全性

全链资产权益质押协议，具有三个重要的安全性质：

a. 全链资产跨链安全。

基于多方计算（Multi-Party Computation, MPC）的门限签名方案，任何单个验证者或少部分验证者以及外部行为者无法访问完整私钥，获得跨链极大的安全能力。

b. 质押者的安全性。

只要诚实地遵守 PoS 协议，每一位质押者都可以到期提取或提前解绑其质押的资产

c. 全面可罚没的 PoS 安全性。

一旦共识完好性遭破坏，则所质押资产必定会被罚减。只要所质押资产的三分之二诚实地遵守 PoS 协议，AVS 就能保持良好的活性。

4. 技术分析

4.1 去中心化跨链技术

跨链技术是指不同区块链网络之间实现互操作和数据交换的技术。跨链技术和跨链互操作性不仅依赖于跨链消息传递（CCMP），还涉及到如何在源链和目标链上进行有效的签名和授权，以确保资产的安全处理和交易的合法性。不同的跨链技术方案采用了不同的签名和授权机制，这些机制核心在于如何验证和执行交易的合法性，以及确保资产的安全转移。当前一些跨链技术在安全和体验方面都存在不同的问题，如跨链桥、公证人要么过于中心化存在不安全因素；HTLC、BoB 等机制，要么效率低体验差。

EIChain 采用把跨链消息传输规则和资产的签名授权规则写入到智能合约里面。跨链签名授权机制依赖于先进的多方门限签名方案（Threshold Signature Scheme, TSS），这种方案能有效地解决单点故障问题，增强整个系统的安全性：

(1) EiChain 基于多方计算（Multi-Party Computation, MPC）的 TSS，这种方案，允许多个验证器集体共同持有单一的标准 ECDSA/EdDSA 私钥、公钥和地址，用于与外部链进行认证互动。这种方式可以提供热钱包的便捷性和冷钱包级别的安全性。

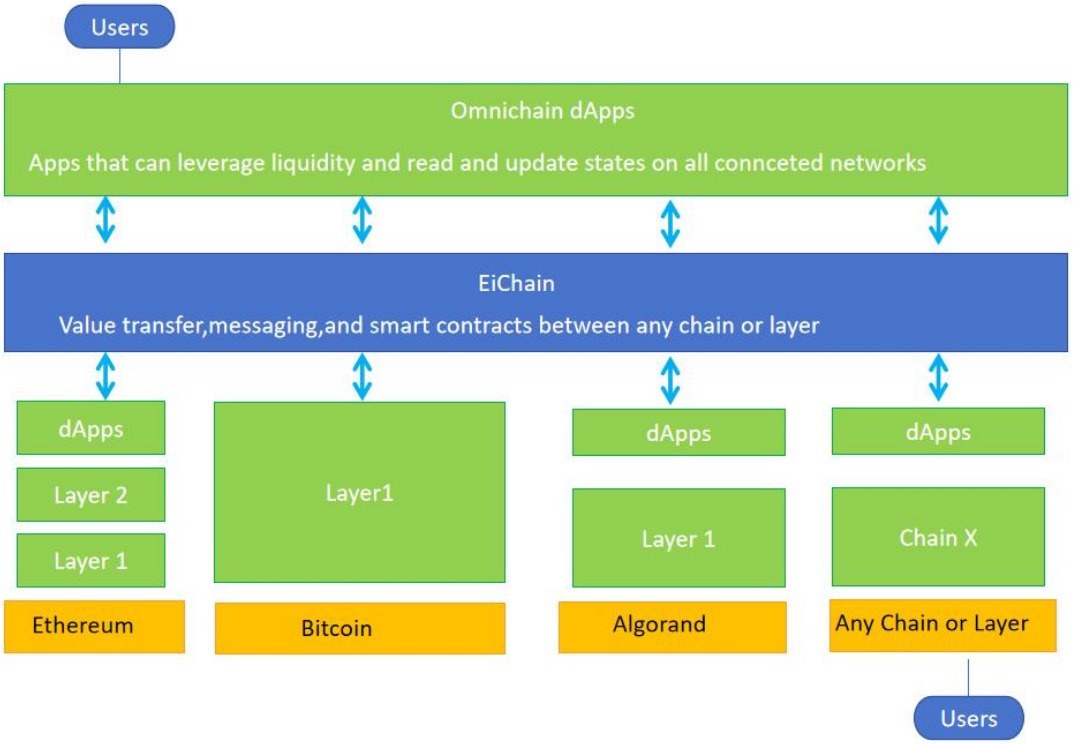
(2) EiChain 的 TSS 私钥是通过无需信任中介的方式生成的，没有任何单个验证者或外部行为者在任何时候都能访问完整的私钥，从而确保了系统的安全性。

(3) EiChain 的 TSS 是无领导的，即它通过分布式方式进行密钥生成和签名，这样可以保证在密钥生成或签名过程中不泄露任何私密信息。为了提高效率，EiChain 还采用了批量签名和并行签名技术，以提高签名者的吞吐量。

4.2 全链资产跨链技术

EiChain 保存 TSS 密钥和地址，所以能够支持管理连接链上管理本地资产池，使得用户可以把资产汇集在一起，让智能合约根据预设规则管理这些资产，如自动化市场做市商（AMM）池或借贷池等。

TSS 使得 EiChain 能够支持如比特币、狗狗币这样的非智能合约链，这实际上为这些网络添加了智能合约功能。 通过这种签名授权机制，EiChain 不仅能提供强大的跨链功能，还能确保交易的安全性和验证的去中心化，使其成为支持广泛数字资产管理和操作的强有力平台。



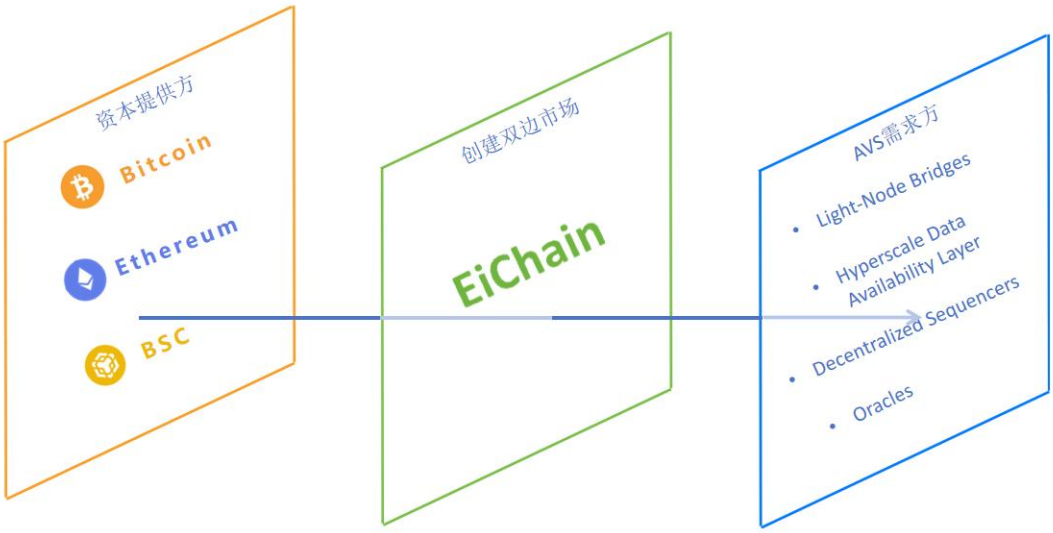
4.3 可问责性与可罚减性

PoS 共识协议具有一重要性质，即它们都可以将违反协议者以可证明的方式进行惩罚。由于 PoW 协议的矿工没有链上身份，因此 PoW 链不具备该性质。实际上“可问责的完好性（accountable safety）”这一性质（即当区块链完好性遭破坏时，有能力对三分之一的校验者实施问责并惩罚）是 PoS 的设计核心。然而，在可问责性与链上罚减之间还存在一道鸿沟—即依据破坏者对区块链协议的违规证据，在链上对破坏者的质押权益实施实质性的罚减。尤其是当链的完好性被侵犯时，说明该链已经有超过 1/3 的恶意校验者了。因此，这些恶意校验者拥有足以阻止证据上链的投票权，并可以藉此阻止罚减。在这种情况下，必须在区块链之外执行复杂的社区共识流程，以便能够罚减违规者的质押权益，并将其踢出校验者集合，其余这些诚实的验证人随即重启区块链。

5. 系统架构

全链资产质押协议的核心基础设施是 EiChain。该 EiChain 负责多种关键功能，包括：

- 为资产持有人提供资产权益质押服务；
- 为 AVS 方提供基于 PoS 共识的共享安全服务；
- 运行市场，匹配全链资产质押权益和 AVS，追踪权益质押和验证信息；



6. EiChain:削减分析

6.1 削减机制

密码经济学安全量化了对手必须承担的成本，以使协议失去所需的安全属性。这被称为腐败成本（CoC）。当 CoC 远大于任何潜在的腐败利润（PfC）时，我们说系统具有强大的安全性。密码经济学安全与仅在假设至少有一定阈值百分比的操作者具有利他主义并诚实行动的大多数信任安全保证系统形成对比。EiChain 的核心思想是通过各种削减机制提供密码经济学安全，这些机制征收高昂的腐败成本。

6.2 EiChain 上没有可替代头寸

EiChain 不发行代表重新质押头寸的可替代代币，因为每个重新质押者可能

选择验证不同的模块组合，因此面临不同的削减风险集。确保这些风险对可替代头寸持有者保持透明是棘手的，可能会在可替代头寸持有者和运行节点的操作者之间产生委托人-代理人问题。这需要仔细管理；因此，EiChain 不计划发行可替代头寸。

6.3 风险管理

EiChain 中的两类风险：（1）多个操作者可能串谋同时攻击一组 AVS；（2）在 EiChain 上构建 AVS 可能具有意外的削减漏洞 - 这是诚实节点被削减的风险。

6.3.1 操作者串谋

首先在理想情况下，如果所有操作者都重新质押到所有 AVS 中，那么在 EiChain 上构建的任何 AVS 的腐败成本现在与 EiChain 中的总质押金额成比例。这是在最大化腐败成本方面所能期望的最佳情况。然而，在现实情况下，只有一部分操作者选择加入给定的 AVS，那么存在复杂的攻击，其中一些操作者集可能串谋从一个 AVS 集中窃取资金。

考虑一个由 800 万美元重新质押的 EIC 保护的 AVS，其中包含 2000 万美元的总锁定价值。如果需要 50%的法定人数来捕获 200 万美元的锁定价值，那么应用似乎是安全的，因为成功的攻击至少会导致攻击者 40%的质押被削减。

然而，如果相同的质押者集也重新质押在其他 AVS 中，情况可能并非如此。在最简单的情况下，完全相同的一组重新质押者参与了其他 10 个 AVS，每个 AVS 都有 200 万美元的锁定资金。因此，腐败这组重新质押者的总利润是 2000 万美元，但总风险价值仅为 800 万美元，从而使系统在密码经济学上不安全。

一种解决方案是限制任何特定 AVS 的 PfC。例如，（1）桥接可以限制在削减期间内的价值流动，（2）预言机可以对期间内的总交易价值设定限制等。然

而，这个解决方案取决于这些 AVS 的设计者。另一个解决方案是 EiChain 可以积极增加腐败 AVS 的 CoC。在这里，有一个关于重新质押安全的通用分析，考虑任何一组质押者都可能串谋。如果该集合在某些 AVS 上形成一个多数法定人数，他们可能潜在地从这些 AVS 中提取 PfC。有一个机制来确定一个操作者或一组操作者，他们通过 EiChain 重新质押，是否可能通过某种串谋或不是来创建安全漏洞。通过创建一个开源的密码经济学仪表板，将允许在 EiChain 上构建的 AVS 监控参与他们验证任务的操作者集是否在许多其他 AVS 中根深蒂固。如果是这样，AVS 可以在其服务合同中放置一个规范，激励只参与少数 AVS 的 EiChain 操作者。因此，可以将 EiChain 视为具有弹性安全。

6.3.2 意外的削减

像任何发展良好的协议一样，构建在 EiChain 上的 AVS 的目标是一旦 AVS 经过实战测试，就逐渐固化。一旦 AVS 固化，假设意外的削减风险将最小化。然而，在 AVS 及其相关基础设施和合同经过实战测试之前，需要减轻 EiChain 中的各种削减风险，以避免风险连锁反应。一种风险是，AVS 创建时存在一个意外的削减漏洞（例如，编程错误）被触发，导致诚实用户的资金损失。

这里提出两道防线：（1）安全审计；（2）否决削减事件的能力。对于安全审计，认识到 AVS 代码库必须像智能合约一样进行审计。虽然 AVS 代码库可能比普通智能合约更复杂，但一个特殊情况是，与专注于保护消费者用户（普通大众成员）的智能合约审计不同，AVS 审计针对的是倾向于是区块链生态系统中更复杂的参与者的质押者和操作者。鉴于这种复杂性和风险/回报概况，期望适当的审计对于任何 AVS 获得质押者和操作者的加入是必要的。在 AVS 固化之前的第二道防线是，EiChain 中有一个由 EiChain 社区杰出成员组成的治理层，它

有能力通过多签否决削减决策。认为削减否决过程类似于辅助轮，最终将被移除。

6.4 治理

鉴于其拥有否决削减的权力，仔细考虑如何构成这个多签否决委员会是很重要的。选择这个否决委员会的一种方式是使用基于代币的法定人数。然而，使用基于代币的法定人数使治理容易受到中央实体购买大多数代币然后能够支配自己的规则甚至更糟糕，直接攻击系统的攻击。为了避免这种情况，我们使用一个基于声誉的委员会，由 EiChain 社区的知名人士组成。该委员会将负责启用对 EiChain 合约的升级，审查和否决削减事件，并允许新的 AVS 进入削减审查流程。请注意，否决委员会没有自己恶意触发削减的权力，任何对 EiChain 合约的升级都带有时间滞后。

这个否决委员会可以被视为新 AVS 加入 EiChain 的辅助轮。AVS 可以使用这个否决委员会来向 EiChain 重新质押者保证，他们不会受到恶意削减或由于错误而导致的不准确削减，因为总是有一个可以否决削减的委员会作为后备。与此同时，AVS 开发人员可以实战测试与 AVS 相关的代码库。一旦成熟并获得重新质押者的信任，AVS 可以停止使用否决委员会作为后备。使用否决委员会的信任假设是，AVS 必须信任否决委员会不会否决正确的削减，而重新质押在 EiChain 中的质押者必须信任否决委员会会否决 AVS 的任何不合理削减。

想要在 EiChain 之上构建并使用否决委员会的 AVS 必须被否决委员会接纳。上船过程可能需要委员会成员进行安全审计和其他尽职调查，包括检查操作者为 AVS 服务所需的系统要求。

6.5 多代币法定人数

EiChain 为 AVS 提供了灵活性，以便它们可以定义自己的法定人数，以及包

括重新质押的 EIC 在内的法定人数，并要求对其验证任务的最终响应是来自每个法定人数多数响应的函数。例如，AVS 可以指定两个法定人数，一个是 EIC 重新质押者的法定人数，另一个是$AVS 法定人数（其中$AVS 是 AVS 的代币）。为了使 EiChain 上的任何操作者为这个 AVS 提供服务，他们要么必须重新质押他们的 EIC，要么必须质押$AVS 代币。AVS 可以将两个法定人数视为两个独立的法定人数，并使用 AND 子句来组合两个法定人数的多数响应。

定义多个法定人数的灵活性为 AVS 提供了一个机会，使其可以将自己的代币作为实用代币启动，并为其协议累积价值，同时使用重新质押的 EIC 法定人数来对冲其自身代币的死亡螺旋。

7.总结

a. EiChain 创建了一个由全链资产权益质押者提供给需要质押和验证服务的模块的去中心化信任自由市场。

b. 通过 EiChain 重新质押，全链资产质押者可以选择为他们选择的模块提供安全性和验证服务，无论是直接运行节点还是通过委托给其他 EiChain 操作者。

c. 可以在 EiChain 上构建各种轻量级和超大规模模块，这些模块可以设计为广泛地让单独质押者参与。

d. 服务还可以利用质押者之间的显著异质性，这些异质性可能在计算能力、风险/回报偏好和身份方面有所不同。

e. EiChain 旨在促进区块链上更敏捷、更去中心化和无需许可的创新。

参考文献

[1] Jae Kwon, and Ethan Buchman. “Cosmos: A Network of Distributed Ledgers.”

URL Https://cosmos.network/whitepaper. 2016。

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, page 21260, 2008。

[3]How does the avalanche bridge™ work? https://support.avax.network/en/articles/6349640-how-does-the-avalanche-bridge-work。

[4]Inter-blockchain communication protocol. https://ibcprotocol.org/。

[5] Mesh security. https://github.com/osmosis-labs/mesh-security。

[7] "Ethereum/BTCRelay." github.com/ethereum/btcrelay。

[8]The cryptoeconomics of slashing. https://a16zcrypto.com/the-cryptoeconomics-of-slashing/

[9]Rosario Gennaro, and Steven Goldfeder. "One Round Threshold ECDSA with Identifiable Abort." IACR Cryptol. ePrint Arch. 2020: 540. 2020。

[10] "Multi-Party Threshold Signature Scheme." https://github.com/binance chain/tss-lib.

[11] Caleb Banister Ryan Zarick Bryan Pellegrino. "LayerZero: Trustless Omnichain Interoperability Protocol." URL https://coinweb.io/files/Coinweb-Whitepaper.pdf. 2021

[12] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. arXiv:1710.09437, 2019。

[13]Phil Daian, Rafael Pass, and Elaine Shi. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In Financial Cryptography and Data Security, FC ' 19, pages 23–41. Springer, 2019。

[14] THORChain.org. "Decentralized Liquidity Network." URL https://github.com/thorchain/Resources/blob/master/Whitepapers/THORChain Whitepaper-May2020.pdf. 2020。

[15]Committee-driven mev smoothing. https://ethresear.ch/t/committee-driven-mev-smoothing/10408

[16]An incomplete guide to rollups. https://vitalik.ca/general/2021/01/05/rollup.html。

[17] Rosario Gennaro, and Steven Goldfeder. "Fast Multiparty Threshold ECDSA with Fast Trustless Setup." In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 11791194. CCS 18. Association for Computing Machinery, New York, NY, USA. 2018. doi:10.1145/3243734.3243859。