Layer2 扩容技术发展现状与展望

作者：Gate.io 研究院 Eric Fu，Guin Peng，Jill Chow

摘要

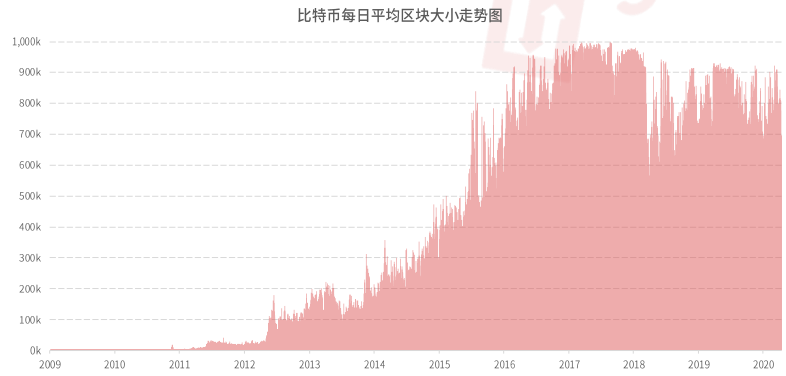
随着区块链技术在各行各业的应用扩张，人们对区块链信息处理速度的要求也越来越高，区块链扩容技术的关注度也逐渐增加，各种扩容方案相继被开发并完善。目前常见的扩容方案是从 Layer0、Layer1 和 Layer2 分别研发，不同的公链根据其自身发展需求选择不同的扩容方案。本文中 Gate.io 研究院通过对状态通道和侧链这两种主流的 Layer2 层扩容技术进行分析，并通过闪电网络与 Plasma 的对比对其未来发展前景进行探讨。

要点总结：

- 扩容技术的研发难点并不在于扩容本身，而是在“安全性”与“去中心化”同时被保障的情况下如何提高扩展性；
- 目前已有的 Layer2 层扩容技术如状态通道、侧链（Sidechains）、十倍协议（Tenfold Protocol）等均有各自针对的应用场景，但均未实现最为理想的状态；
- 闪电网络与 Plasma 分别是状态通道在比特币与侧链在以太坊上的扩容方案，达到扩容目的的同时均存在各自不同的问题；
- 对于闪电网络而言，如何平衡与比特币区块链安全性的关系将成为其未来发展道路上的重要研究课题之一，而如何实现便捷快速的支付则是比特币未来发展很重要的路线之一；
- 对于 Plasma 而言，力求实现无监管状态下链下交易的安全性，然而技术开发难度大，融合其他研发方案将有助于早日做出突破。

1 扩容技术各有千秋

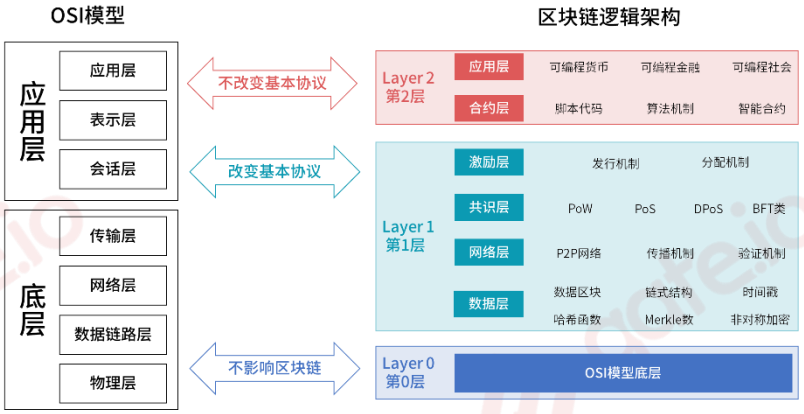
随着区块链交易的用户数量不断增加，区块链网络对系统吞吐量（TPS）的要求也越来越高。



来源：BitInfoCharts，Gate.io 研究院（截止至 2020-4-15）

以比特币为例，在 2017 年比特币区块便已趋近于 1MB *（比特币区块大小上限）*。同时，随着时间的发展，比特币交易量与交易频率加快，每秒仅能处理不超过 7 笔交易的系统已经远远无法满足交易量的需求。如何提高比特币的交易速度成为系统亟待解决的问题，很多扩容方案亦随之被提出。**虽然理论上，不同的扩容技术确实能缓和交易拥堵的现象，但始终是各有千秋，无法达到最理想的状态。**

目前常见的扩容方案从系统底层（Layer 0）、链上（Layer 1）或链下（Layer 2）三个层面进行研发。实际上这三层不同的扩容方案对应 OSI 模型[1]的不同层面进行优化来实现扩容。



来源：通证通研究院，Gate.io 研究院

如图所示，Layer 0 进行扩容实际上针对的就是 OSI 的底层协议（1~4 层）进行优化，Layer 1 和 Layer 2 的优化则是针对 OSI 模型中的高层协议（5~7 层）进行优化。虽然 Layer 1 和 Layer 2 同为针对 OSI 高层协议进行优化，但是二者侧重方向不同。前者属于链上扩容，对区块链中的数据层、

网络层、共识层以及激励层进行优化。Layer 2 扩容则是链下扩容，针对合约层与应用层的优化。

由于区块链体系中存在去中心化、安全性与扩展性的三角关系，三者很难同时实现。而比特币与以太坊最初选择以“安全性”与“去中心化”为基准，导致在扩展性方面存在局限性。换而言之，**扩容技术的研发难点并不在于扩容本身，而是在“安全性”与“去中心化”同时被保障的情况下如何提高扩展性。**

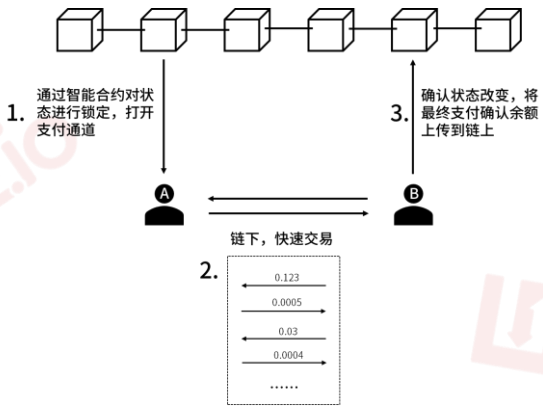
2 Layer2 层扩容技术

比特币是目前流通最广的数字货币，其采用闪电网络进行区块链系统的扩容；闪电网络则是区块链 Layer2 层扩容技术——状态通道的应用之一。除此之外，目前常见的 Layer2 扩容方案还有侧链（Sidechains）、Plasma 和十倍协议[2]（Tenfold Protocol）。由于各自技术特点的不同，各技术针对的应用场景与发展方向也有所区别。

2.1 状态通道

2.1.1 运作原理

从本质上说，状态通道在链下开通一个临时的点对点交易通道，交易双方通过状态通道进行交易时会在主链上分别锁定一定的余额并设定一个时限，该状态通道可以由任意一方主动关闭。交易双方基于特定的协议进行价值转移，当达到时限或某方主动向主链同步数据时，交易结果会被提交到主链上。



来源：nichanank.com，Gate.io 研究院

如图，A 和 B 之间有大量的小额交易往来，此时 A 和 B 可以在链下开通一条状态通道，在一定时间内进行点对点的快速交易。在交易完成之后，只需将最初的交易与最终的交易结果上传到链上即可。如此一来，将大大节省交易确认时间，交易性能也得到了极大的提升并具有极好的隐私性。

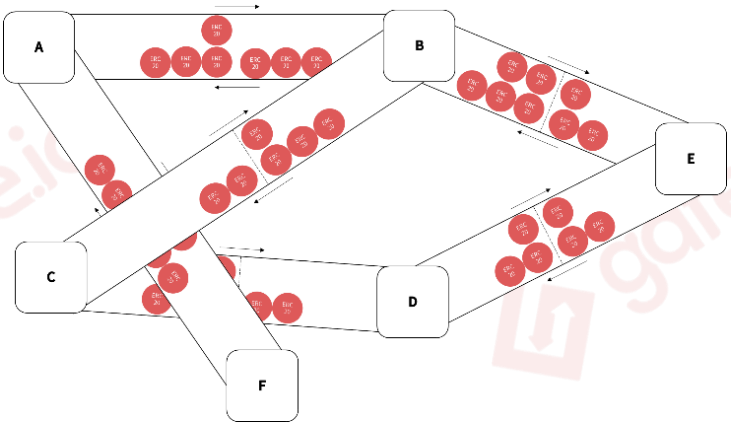
但这种链下点对点交易也存在着风险，为了防止作弊，状态通道严格要求交易双方的在线情况。同时，状态通道目前只适合进行小额的交易，即使网络发生故障，对交易双方并不会造成过大的经济损失。这种不适合大额交易的特性也限制了状态通道技术的扩展通用性和扩容效果。

2.1.2 状态通道的应用——闪电网络

闪电网络是基于状态通道的应用之一，目前被应用在比特币区块链上。闪电网络有两个核心技术概念，分别是序列到期可撤销合约（Recoverable Sequence Maturity Contract, RSMC）和哈希时锁合约（Hashed Timelock Contract, HTLC）。

2.1.2.1 闪电网络的核心技术

序列到期可撤销合约（RSMC）要求交易双方都必须在支付通道中预存一部分资金作为保障金，由 RSMC 监管并判断双方的交易是否足以支持每次交易，一旦其中一方存在欺诈行为，那么将这部分保障金划归于对方，如此便保障了交易的有效性并降低欺诈风险。出于保障金的限制，闪电通道无法支持大宗交易，若交易额很高，那么对保障金的要求也很高。



来源：公开资料，Gate.io 研究院

虽然序列到期可撤销合约（RSMC）保障了两方交易者之间的链下直接交易，但有时候想进行交易的双方可能并不存在直接的点对点通道。如图所示，如果某个节点与状态通道网络中的另外一个节点之间并不存在通道（如 A 与 D 进行交易），那么便需要通过路由算法找到对应的路径完成价值转移。

此时哈希时锁合约（HTLC）便保障了任意交易双方的转账都可以通过一条支付通道来完成。通过让每一个周转点都可以得到一定的收益来保障交易顺利进行。

2.1.2.2 闪电网络的特性

通过闪电网络，比特币可以将高频、小额交易转移到链下进行交易，这样大幅提高了比特币系统的工作效率，但是目前闪电网络也存在它的局限性。

■ 交易效率提高，但仅满足小额交易

从交易速度上看，闪电网络支持快速支付，无需等待矿工打包、交易、上传区块便可直接使用进行比特币交易。同时也减少了比特币主链上的负担，比特币主链只需要对初始交易与最终交易进行记录便可。

目前闪电网络只能满足小额度交易。由于通道开启时，交易方需要将一定的资金作为保障金抵押在交易通道内，如果进行大额交易，首先保障金本身就是一笔很大的费用。其次，基于安全性上的考虑，一旦发生掉线、操作失误等错误时，交易用户会意外损失大笔资金。

■ 安全性受到影响

从闪电网络通道的安全角度分析，闪电网络只是一个临时通道，数据并不会永久保存。由于两个节点之间并不一定存在着交易通道，而是通过特定的路由算法来确定可行路径的方式创建合理的交易通道，**一旦通道上的某个节点掉线便会导致交易的失败。**

此外，基于闪电通道中的设计，如果一方出现欺诈行为，通道内的资金将直接划归于另一位交易方。某些时候交易用户并没有进行欺诈行为的意图，但**软件的错误以及备份故障等问题也存在造成交易用户经济损失的可能。**

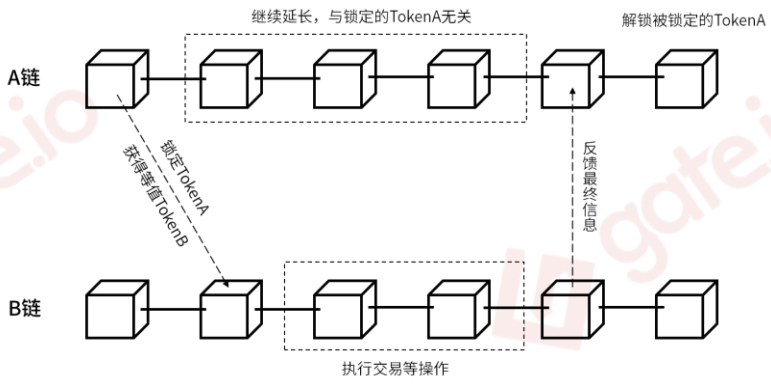
■ 存在节点中心化的潜在问题

闪电网络若要真正解决比特币交易速率的问题，除了需要保障矿工利益外，网络节点中心化问题也是需要注意的。一旦闪电网络愈发中心化而产生大节点出现问题，那么将很可能出现闪电网络崩溃的现象。

2.2 侧链

2.2.1 运作原理

侧链技术是相对较早的扩容方案，属于跨链扩容方案，通过侧链将主链上的数字资产转移到侧链上进行交易，待完成交易后再将资产重新转移回到主链上。



来源：公开资料，Gate.io 研究院

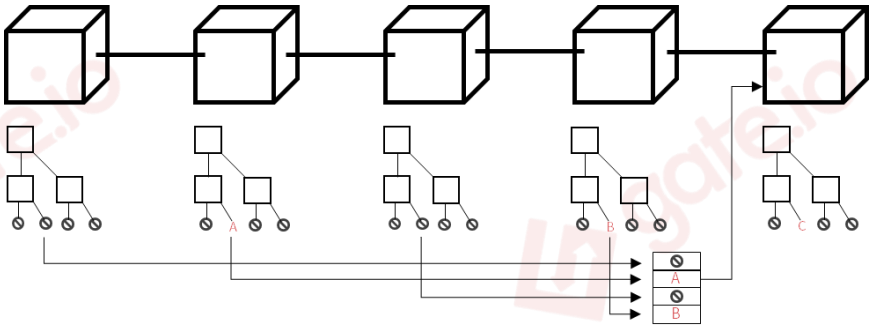
当主链 A 使用侧链 B 进行链下交易时，链 A 上的资产会被锁定，同时侧链 B 上会释放等价的资产用于交易，此时并不影响主链 A 的正常运作。当侧链 B 的交易完成后，侧链 B 上的资产会被锁定，同时主链 A 上资产会

被释放并完成交易。如此一来既减轻了主链上的负担，亦提高了交易速度，但由于主链无法完全验证侧链上的所有区块。如果有攻击者串谋发动无效状态攻击[3]，可能会造成用户的损失，侧链的安全性在无监管情况下将无法得到保障。

2.2.2 侧链的应用——Plasma

2.2.2.1 Plasma 的核心技术

Plasma 是侧链中的一种，与一般的侧链相比，Plasma 链的安全性更高。即使在无监管的情况下，所有验证者串通进行欺诈，Plasma 链上的资产依然是安全的。



来源：公开资料，Gate.io 研究院

如图所示，主链上每一个区块内都有一个默克尔树（Merkle Tree），记录着每一个代币的所有交易记录（比如一枚代币在 A 与 B 之间存在交易记录）。当使用 Plasma Cash *（Plasma 的其中一版迭代）*进行交易时，交易方需要将此代币的完整交易历史提供至 Plasma 链，Plasma 链将所有区块头[4]进行快照并发到主链上。此时 A 与 C 进行交易，C 通过验证所有默克尔证明与 Plasma 链发送给主链的快照是否相同判断交易是否真实，如果通过验证则此交易成功。

2.2.2.2 Plasma 的特性

Plasma 提供了更安全的链下交易机制，但由于向主链上传数据时需要提供所有交易数据，机制设计变得更为复杂。

■ 侧链安全性提高，退出机制变得复杂

Plasma 通过验证代币完整交易史的方式提高了侧链在无监管状态下的安全性，出现交易安全事故时，仍可保障用户可以安全的取回属于自己的资产，然而与闪电通道不同的是，Plasma 无法即时提款，也就是说并不是交易双方同意退出就可以很快提现。Plasma 扩容方案虽然理论上提高了交易安全性，但是退出机制相当复杂，用户需要等待挑战期结束才可以拿回资金。

■ 代币完成历史交易记录过长，迫使存储要求过高

由于 Plasma 的验证机制是验证代币完整交易历史，当恶意用户或攻击者挑战正常交易用户时，用户将不得不提供自己的验证证明，从长期来看，对用户的存储要求将越来越高。

2.3 Layer2 主流扩容方案对比

下表为主流 Layer2 扩容方案的简单对比：

扩容技术	优点	缺点
闪电网络	交易速度快；可跨链运作	无法进行额度过大的交易
Plasma	安全性高	退出机制复杂；完善难度大
十倍协议	扩容量大	存在 50%经济体攻击

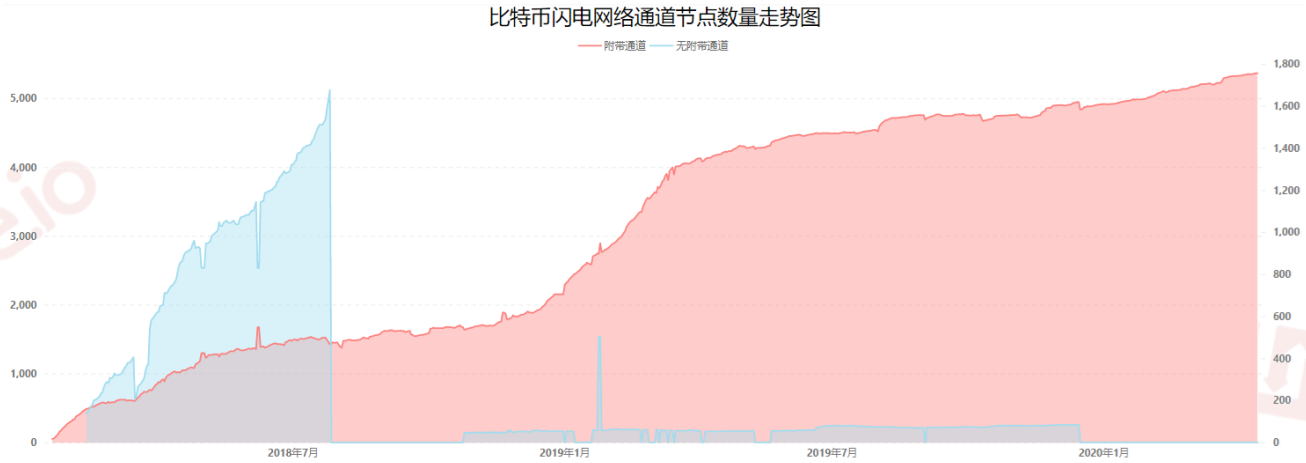
来源：公开资料，Gate.io 研究院

现阶段每一种扩容方案都有各自的优点以及需要解决的难题，不同扩容方案的差别大体上还是在对安全性、扩张性与去中心化上做权衡，**彻底解决扩容带来的种种问题还需要更多的研发时间。**

3 Layer2 扩容技术未来展望

3.1 闪电网络的未来憧憬

随着交易量的逐渐加大，比特币区块的大小严重限制了交易速率。虽然此后产生了很多不同的扩容方案，每个扩容方案依然有它的可行性与局限性，闪电网络也是如此。2017 年底上线至今，闪电网络为用户带来了很多的便利，如下图所示，**从上线到目前为止，闪电网络的节点数始终保持着增加的趋势。**



来源：bitcoinvisuals，Gate.io 研究院（截止至 2020-4-15）

对于用户来说，闪电网络解决了他们对于交易速率上的部分需求，但是对于比特币整个生态圈，闪电网络未来的发展之路可谓任重道远。**如何平衡闪电网络与比特币网络安全性的关系将成为闪电网络发展道路上的研究课题之一。**

比特币的交易速率是否提高、手续费的高低已经影响到了未来人们是否能够使用比特币购物消费犹如使用 VISA、支付宝一样便捷。虽然扩容方案很多，但是不同扩容方案适用的应用场景并不相同。对于一种货币而言，流通性决定了其是否存在价值。目前比特币的流通性是所有数字货币中最广的，也是最有可能率先成为人们日常支付手段的一种数字货币。基于这种情况，

如何进行便捷快速的支付是比特币未来发展很重要的路线之一。

相比于十倍协议更偏向于在游戏场景下进行发展，闪电网络的理念则是使比特币可以成为零售支付手段的长期解决方案。换言之，**闪电网络的扩容方案更适合于比特币作为日常支付方式的发展，随着闪电网络技术的成熟、未来对增加资金限制的一些协议逐步放宽，届时闪电网络对于比特币应用层面的扩展将会有更明显的作用。**

就目前而言，闪电网络支持拼接（Splice-in＆Splice-out）和双出资（Dual-funding)技术，使闪电网络的体验感得到了大大的改善。随着时间的发展，**闪电网络的安全性以及隐私性的逐步提高也将使闪电网络的使用更为便捷与普及。**

3.2 Plasma 的发展前景

由于以太坊的应用场景与比特币目前面临的发展路线并不相同，所以状态通道并不是最合适以太坊扩容的研发方向。

Plasma 的设计理念一度被认为是以太坊扩容的理想方案，既可以提高系统吞吐量，解决以太坊链上交易拥堵问题，同时还可以保障在无监管状态下交易方资金的安全性问题。Plasma 从最开始的 Plasma MVP 到 Plasma Cash 始终处于开发迭代状态。由于技术完善难度大，以太坊 2.0 也始终未上线。

在 Plasma 难以做出突破的时，一种称作“rollup”的方案被 GitHub 的一名用户提出。随后 Vitalik 对这个方案称为“zk-rollup”。除此之外，Plasma Group 也基于此发布了“Optimistic Rollup”方案。就现阶段而言，以太坊的扩容方案发展与完善仍需较长时间。

4 总结

扩容是现阶段所有区块链系统都需要面对以及解决的问题，虽然不少研究者对此提出了很多扩容方案，但由于安全性、去中心化和扩展性的不可能三角存在，并没有一种扩容方案可以彻底解决区块链扩容问题。

状态通道和侧链都是目前常见的 Layer2 扩容技术，如基于状态通道的扩容方案闪电网络用于比特币扩容，使比特币的小额高频交易得以转移到链下，减少了主链上的负担。基于侧链技术的扩容方案 Plasma 链则用于以太坊扩容，是一套无监管状态下也能保证用户链下交易安全的方案。

作为目前流通性最广的数字货币，比特币最有望成为人们日常生活支付手段，但交易确认速度过慢限制了比特币在此方面的发展。对此，闪电网络将比特币区块链的部分链上交易转移到链下，减轻主链负担的同时亦给用户带来了便利。针对应用场景的不同，闪电网络的小额高频交易特性与比特币日常化发展路线更为契合，但闪电网络目前存在通道节点中心化导致网络安全性降低的风险。

而以太坊 2.0 目前还未上线，Plasma 作为以太坊链下扩容的蓝图目前仍在开发当中。Plasma 的尝试在于保障用户在以太坊链下交易的资产安全，然而尽管经历了多次迭代，始终还有很多技术难点需要克服。作为以太坊链下扩容的“先驱者”，Plasma 通过实践发现并解决了很多链下扩容需要面对的问题，这对以太坊未来的发展起到很重要的作用。

5 参考资料

5.1 参考资料

1. 曾帅, 袁勇, 倪晓春, & 王飞跃. (2019). 面向比特币的区块链扩容:关键技术, 制约因素与衍生问题. *自动化学报, 45*(6).
2. Khan, N. , & State, R. . (2019). *Lightning Network: A Comparative Review of Transaction Fees and Data Analysis. Blockchain and Applications.*
3. 喻辉, 张宗洋, & 刘建伟. (2017). 比特币区块链扩容技术研究. *计算机研究与发展*(10).
4. 常兴, & 赵运磊. (2019). 比特币扩容技术的发展现状与展望. *计算机应用与软件, 36*(03), 55-62.
5. Garza, M., & Andrés, J.M. (2018). The lightning network cross-chain exchange : a decentralized approach for peer to peer exchange across blockchain.
6. Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.
7. 第 0 层扩容，区块链扩容明日之星——区块链技术引卷之十二：https://www.chainnews.com/zh-hant/articles/539219822510.htm

5.2 名词解释

[1] OSI 模型：开放式系统互联通信参考模型（Open System Interconnection Reference Model），简称为 OSI 模型（OSI model），是一个由国际标准化组织提出的试图使各种计算

机在世界范围内互连为网络的标准框架，将计算机网络体系结构划分为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

[2] 十倍协议：区块链初创企业 Binary Mint 于 2018 年 8 月底发布的一项新型扩容方案，它用于安全地维持一个链下状态机，同时能在链上读取其状态。

[3] 无效状态攻击：侧链上超过 3/2 的验证者对认证进行篡改。

[4] 区块头：区块头负责储存区块头信息，包括默克尔树（Merkle Tree），哈希值（Hash）以及时间戳等。

声明

因出具该研究报告，特做出如下声明：

- 本研究报告是内部成员通过尽职调查和客观分析得出的结论，旨在对 Layer2 扩容技术进行分析总结，并不能完全以此来预测未来扩容技术的发展情况。
- 本研究报告非衡量研究对象本身价值、以及其发行代币价值的工具，不构成投资者做出最终投资决策的全部依据。

本研究报告中引用的项目资料来源自内部认为可靠、准确的渠道，因为存在人为或机械错误，信息均以获取时态为准。内部成员对研究报告中所依据的相关资料的真实性、准确度、完整性以及及时性进行了必要的核查与

验证，但对其不做任何明示或暗示的陈述或担保。