从模块化的角度讨论 Rollup 和应用链选择

崔晨

Rollup 概念由以太坊扩容兴起，下一阶段的以太坊主网升级也将围绕增强 Rollup 扩容效果的主题。自 Rollup 诞生后，应用无需部署在公链上，而可以选择手续费更便宜的 Rollup，应用链也可以不再以侧链的形式与底层链相连，而是采用独立 Rollup 的形式以实现定制化的功能。本文将借助模块化区块链的概念，以模块化的角度讨论 Rollup 和应用链可选择的形式。

一、Rollup 的种类

（一）模块化概念

Rollup 的扩容方式简单理解为将交易的执行放到链下，再将交易结果传回链上，传回链上的数据和结果是可用且可验证的，以保证 Rollup 中交易的真实性。由于 Rollup 链下数据可用性和状态转换结果发布到底层链上，所以底层链能够对其进行验证，因此在理想情况下，Rollup 执行交易不仅可以实现扩容，还能与底层链捆绑安全。

在区块链模块化概念中，Rollup 等 Layer 2 的扩容方案是将区块链的执行层独立由单独的项目实现，减轻了区块链的工作。随着模块化概念的发展，区块链的每个模块组件越来越专业化，并且产生了对应的辅助工具产品，增加了区块链的可组合性，能够更便捷地生成一些定制化功能的区块链。Rollup 的种类也不止于独立执行层这一种，而是衍生出多种形式。在介绍 Rollup 种类之前，首先要理解模块化的概念。

模块化公链以 Celestia 为代表，其模块化概念将区块链分为四层：数

据可用层（Data Availability）、共识层（Consensus）、结算层（Settlement）、执行层（Execution），这四种模块分别代表了交易在被记录在链上所经历的过程。数据可用性简称为 DA，用来保证交易信息在链上可用，即数据被发布到链上，让所有人接触。共识层中节点需要对区块中交易记录的顺序达成一致。结算层用于处理争议和保证交易结果的最终性，例如为执行交易提供了验证证明和欺诈证明。执行层用来执行交易并实现状态正确更新。在单一的公链上，这四部分在同一区块链上实现，加重了公链的负担，因此无法负载大量应用，将区块链进行模块化分类可以让各专业化工具辅助区块链实现更多功能和扩容。

（二）Rollup 的组合

Rollup 等 Layer 2 视为执行层为公链提供可扩展性时，会被要求将数据可用性传回底层链（Layer 1）上，并且由底层链实现结算和共识。不难发现，Rollup 的扩容效果存在短板，如果底层链的数据可用性、结算或共识速度和资源不足以维持 Rollup 时，就会限制 Rollup 中的交易速度。底层公链自身也需要同步为执行层优化，例如以太坊在区块上增加 Blob 空间，是为了增加 Rollup 的数据可用性空间和降低 Rollup 使用 Layer 1 的成本。

为了保证 Rollup 上执行结果是正确的，Rollup 可以分成 Optimistic Rollup 和 ZK Rollup 两条路径，这也是早期对 Rollup 的分类方式。现在可以由 Rollup 所选择的模块化组件进行分类，不同的模块化选择让 Rollup 具有不同特性。

例如，在 Delphi Digital 对 Rollup 的解读中，Rollup 被划分成下图的形式。在区块链被抽象出模块后，出现了针对模块的基础设施，因此 Rollup

可以借助不同的工具进行排列组合，以适应 Rollup 中的应用。Rollup 可以在四个模块中选择不同的组件，尤其体现在执行层和数据可用层。

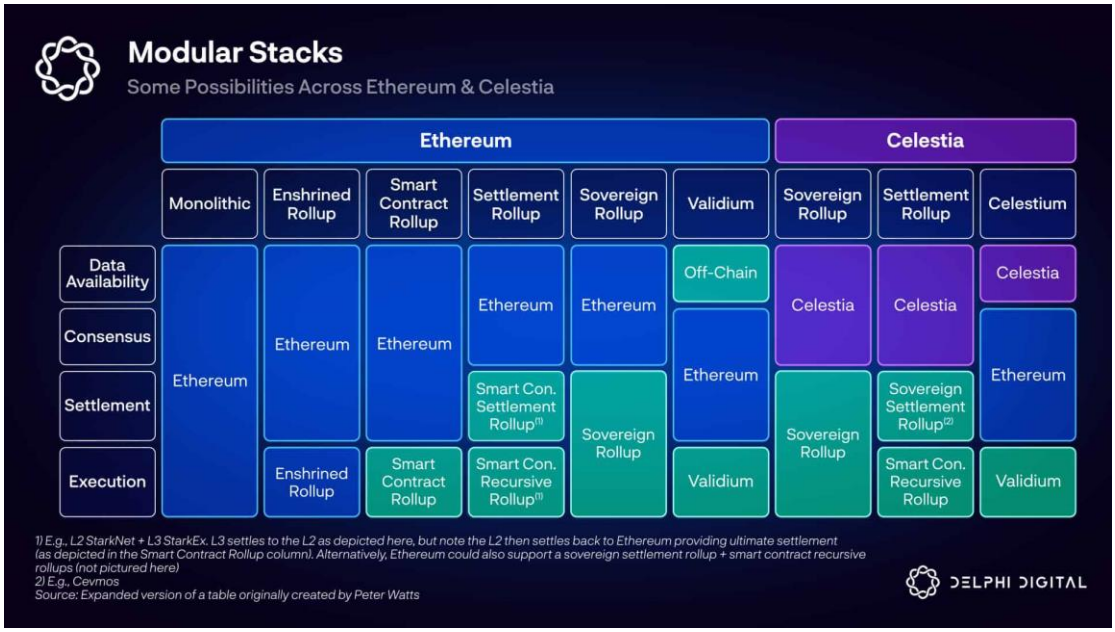

图 1：Rollup 的模块化组件，资料来源：《The Complete Guide to Rollups》

（三）Rollup 的模块化选择和特征

下表展示了不同种 Rollup 所借助的模块组件特点。

表 1：各种 Rollup 特点

	单层区块链	智能合约 Rollup	嵌入式 Rollup	结算 Rollup	主权 Rollup	链下 DA
数据可用层	独立	底层链	底层链	底层链	底层链	链下
共识层	独立	底层链	底层链	底层链	底层链	底层链
结算层	独立	底层链	底层链	独立	独立	底层链
执行层	独立	独立	与底层链一起	其他 Rollup	独立	独立

1、单层区块链（Monolithic）

对于单层区块链来说，这四种模块由同一区块链完成，因此负担较重，应用部署在单层区块链上的费用也较高。例如以太坊中的节点需要执行交

易、更新以太坊状态、验证交易和状态，还需与其他节点达成共识。因此单层区块链上的交易费用相对较高，速度较慢。

2、智能合约 Rollup（SC Rollup）

智能合约 Rollup 通过在底层链上部署智能合约来接受和验证交易，也是经典 Rollup 的形式。当 Rollup 中执行交易后，Rollup 会将数据可用性传回底层链上，并由智能合约呈现状态更新结果。除了执行外，智能合约 Rollup 中交易确认的其他步骤由底层链实现。智能合约 Rollup 主要分为 Optimistic Rollup 和 ZK Rollup 两类，他们的区别在于对执行结果的验证方式分别为欺诈证明和零知识证明。

3、嵌入式 Rollup（Enshrined Rollup）

嵌入式 Rollup 的执行层不独立于底层链架构，而是作为底层链的一部分存在。在以太坊中，嵌入式 Rollup 主要围绕 ZK 方向，目的是向以太坊网络提供 zkEVM 功能，以降低以太坊上的验证成本，现在仍处于开发状态。与其他种类 Rollup 相比，嵌入式 Rollup 更像是一种分片，其中的交易会随区块结算，交易速度等性能方面相对处于劣势。

4、结算 Rollup（Settlement Rollup）

结算 Rollup 是具有结算功能的 Rollup，这一概念常常与 Rollup 之上的扩展层相关联，例如 Layer 3 概念。在这种情况下，位于 Layer 2 的 Rollup 将成为 Layer 3 Rollup 的结算层。Layer 3 最常见的形式为智能合约 Rollup，因此结算 Rollup 需要具备智能合约功能。

5、主权 Rollup（Sovereign Rollup）

主权 Rollup 是相较于智能合约 Rollup 区别的主权，重点体现在分叉

方面。在智能合约 Rollup 中，分叉规则由智能合约决定，进行分叉只能升级智能合约，因此智能合约无法修改时默认 Rollup 没有分叉的能力。在主权 Rollup 中，规则由客户端决定。虽然数据可用性是发布在底层链上的，但对数据可用性的解读由客户端完成，因此结算功能也由主权 Rollup 负责。

这一过程类似于以太坊的共识转换过程，当以太坊转为 PoS 机制时，节点需要下载 PoS 客户端用于共识，原有的 PoW 客户端会升级去掉共识层的功能。虽然理论上节点可以选择不升级，继续通过旧的 PoW 客户端挖矿，但在难度炸弹之后 PoW 挖矿的经济收益微乎其微，并且不受以太坊基金会支持，所以没有节点坚持 PoW。在主权 Rollup 中，数据会发布在底层链上保证可用性，但用户可以通过不同客户端对 Rollup 进行分叉，并且不会影响其他客户端版本解读的内容。

6、链下 DA

Rollup 将数据可用性传回链上是保证其安全的重要步骤，但链上成本阻碍了 Rollup 降低成本和提高效率，于是有些项目将数据可用性放在链下保管以节约成本，例如 Validium。曾经 Validium 被视为一种特殊的 Layer 2，但由于默认以太坊 Layer 2 要与以太坊的安全性相一致，不在以太坊上传 DA 的项目很难确认其安全性的原因，以太坊基金会成员公开宣布不利用以太坊作为 DA 层的不会被视为以太坊的 Layer 2。

（四）关于开放 Rollup 和单一应用 Rollup

除了以模块化的分类方式外，Rollup 还能以承载应用来划分，这是更明显的区别，可以分为两类：开放 Rollup 和单一应用 Rollup，他们都可以通过以上文介绍的方式与底层链相连。开放 Rollup 中的功能更通用，会采

用 EVM 虚拟机、允许其他应用部署在 Rollup 上，例如 Arbitrum 和 zksync。而单一应用 Rollup 只为一个应用构建，例如 Loopring。单一应用 Rollup 的状态转换功能和虚拟机可以针对应用来定制，提高其性能并且避免不必要的资源浪费，需要高性能的应用更需要这类 Rollup。

应用成为独立 Rollup 与底层链的连接成本要远低于直接部署在底层链上，同时独立 Rollup 还能为应用实现定制化的设计。市场上也出现了针对构建单一应用 Rollup 的工具，帮助他们开发 Rollup，降低部署成本。有些应用还会选择成为 Layer 3，通过一条 Rollup 与底层链相连，这样成本更低。

二、Rollup 存在的问题

（一）Rollup 中的五种风险

Rollup 仍处于百花齐放的状态，针对 Rollup 名词、概念和所具功能依旧在发展。Rollup 起源于以太坊，但模块化让 Rollup 的功能和形式得到丰富，并且模块中专业化解决方案降低了 Rollup 部署成本。虽然 Rollup 的设定是继承底层链安全性且能扩容，但实际上 Rollup 的风险依旧存在。一些 Rollup 项目虽自称为安全性与以太坊绑定你，但事实不一定如此，开发者仍有很大权力修改 Rollup 中的交易。

参考 L2BEAT 的评级标准，以太坊上的智能合约 Rollup 存在五类风险。但这些风险是通用的，其他种类的 Rollup 也存在对应的问题，同时这些风险也需要有对应的解决方案。

#	NAME	STATE VALIDATION	DATA AVAILABILITY	UPGRADEABILITY	SEQUENCER FAILURE	PROPOSER FAILURE
1	Arbitrum One	Fraud proofs (INT)	On chain	~12d 9h or no delay	Self sequence	Self propose
2	OP Mainnet	In development	On chain	Yes	Self sequence	Cannot withdraw
3	Base	In development	On chain	Yes	Self sequence	Cannot withdraw
4	zkSync Era	ZK proofs	On chain (SD)	Yes	Enqueue via L1	Cannot withdraw
5	dYdX	ZK proofs (ST)	On chain	9d or 2d delay	Force via L1	Use escape hatch
6	Mantle	In development	External	Yes	Enqueue via L1	Cannot withdraw
7	Starknet	ZK proofs (ST)	On chain (SD)	Yes	No mechanism	Cannot withdraw
8	Immutable X	ZK proofs (ST)	External (DAC)	14d delay	Force via L1	Use escape hatch
9	Loopring	ZK proofs (SN)	On chain	Yes	Force via L1	Use escape hatch
10	Linea	ZK proofs (SN)	On chain	Yes	No mechanism	Cannot withdraw
11	zkSync Lite	ZK proofs (SN)	On chain	21d or no delay	Force via L1	Use escape hatch
12	Polygon zkEVM	ZK proofs (SN)	On chain	10d or no delay	No mechanism	Self propose
13	Metis Andromeda	In development	Optimistic (MEMO)	Yes	Enqueue via L1	Cannot withdraw
14	ApeX	ZK proofs (ST)	External (DAC)	14d delay	Force via L1	Use escape hatch
15	Scroll	ZK proofs (SN)	On chain	Yes	No mechanism	Cannot withdraw

图 2：Rollup 的风险 资料来源：L2BEAT，2023 年 10 月

1、状态验证（State Validation）

状态验证主要指 Rollup 中状态转换的正确性和完整性，Rollup 外的人需要能够验证 Rollup 中交易的正确性。在 Optimisic Rollup 中，状态验证采用的是欺诈证明，如果有人在挑战期内（一般为 7 天）发现 Rollup 上传了错误信息，则可以发送状态是错误的证明来阻止错误内容发布到底层链中，同时此错误状态后的内容回滚。欺诈证明分为很多种，例如 Arbitrum 采用的是多轮交互式证明。其他项目的欺诈证明仍在开发中，而欺诈证明上线前是允许错误状态更新的。

在 ZK 类型的 Rollup 中，状态转换证明由零知识证明提供，零知识证明主要有两种形式，zk-STARKS 和 zk-SNARKS。在生成的零知识证明被

底层链确认后，Rollup 的有效性随即得到确认。

这两种方式各有优劣，挑战期的要求会让 Optimistic Rollup 中交易得到最终确认的时间长于 ZK Rollup，但 ZK Rollup 中提交零知识证明的成本较高，并且不完全适用以太坊的 EVM。目前也有针对这两者的创新，例如将零知识证明融入欺诈证明中，减少挑战期的时间。

2、数据可用性（Data Availability）

数据可用性上传到任何人都能获取的地方，是验证状态有效性的基础，更重要的是，数据可用性发布到安全性更高的区块链中，可以借助区块链的安全性。当 Rollup 将数据可用性发布到以太坊上时，只有以太坊回滚时 Rollup 的内容才会回滚。虽然这不意味着 Rollup 中的内容无法更改（下文将详细介绍），但一般将数据可用性发布的场所可视为保证安全的基础保证。

对于以太坊上的 Rollup 来说，数据可用性占据了区块空间，DA 的花销成为 Rollup 最大的负担，以太坊也在着手解决降低 Rollup 成本的问题。EIP-4844 的提案通过给区块增加 Blob 扩大空间，将 Rollup 上传的数据统一放到更便宜的 Blob 中来降低成本。

选择独立于底层链的 DA 是另一种解决方案，例如使用 Celestia 或 EigenDA 来作为数据可用性的发布场所。但这对于以太坊来说数据被保存在链下，数据可用性是保证用户资金安全的基础，如果数据可用性不公开时，用户无法验证和保证交易的正确执行。因此对以太坊生态来说，一些使用独立 DA 的项目会因安全无法保证而不受以太坊承认为 Layer 2 项目。

3、智能合约可升级（Upgradeability）

智能合约 Rollup 依靠智能合约与底层链连通，如果智能合约是可升级的，意味着能够实现 Rollup 的关闭和分叉，不能完全保证 Rollup 中用户资金的安全。但是，如果 Rollup 智能合约不可升级，也会影响 Rollup 的功能。智能合约的部署可能存在各种问题，合约可升级意味着 Rollup 可修复潜在的 Bug，进行功能升级，以及阻止 Rollup 中的黑客攻击活动。在智能合约不能升级的情况下，Rollup 的功能升级只能通过创建新合约并进行用户迁移完成，较为繁琐。智能合约设置为延迟升级是折中的解决方案，但延迟升级不能阻止 Rollup 中可能的攻击行为。

可以看出，无论智能合约可升级或不可升级都存在固有的问题，现在大部分 Rollup 都会选择可升级。需要明确智能合约升级的控制权和触发升级的时点，代替社区表达和执行智能合约升级的角色一般为多签组织、开发团队、安全委员会、DAO 等。

Rollup 最便捷升级的场景发生在主权 Rollup，它开放了分叉 Rollup 的权力。如果社区对 Rollup 的发展出现分歧，可以通过使用不同客户端让 Rollup 走向不同道路，这两者会独立执行交易并向底层链上传数据可用性，不会互相影响。分叉出的两个 Rollup 不分对错，而是通过社区共识来区分。主权 Rollup 可以灵活地更新 Rollup 功能，是 Celestia 项目宣传的区别于以太坊经典 Rollup 的概念。

4、排序器（Sequencer）

排序器是 Rollup 的重要组件，负责在 Rollup 中排列交易，这是与 Layer 1 区块链所区别的地方，如果 Rollup 中以节点进行共识的方式对交易顺序达成一致，会阻碍交易的达成速度。排序器决定了 Rollup 的活性，如果排

序器停止运营，Rollup 中的交易内容无法发到底层链上来保证数据可用性，无法让用户证明其资金是最新状态。解决这一问题的简单方式是避免排序器的单点故障，开放排序器准入等，开放排序器还能保证 Rollup 上的交易避免审查。避免排序器问题，保证 Rollup 的活性的措施还包括让 Rollup 智能合约给用户开通“逃生通道”，让用户能够绕过排序器，强制将交易发送给 Layer 1 中的节点。

目前的 Rollup 上大多没有开放 Rollup 的排序器权限，而是自己组建，这种情况下能得到更多收益。除了 Rolllup 上交易手续费外，排序器还能得到跨层间的 MEV 收入。排序器的创新发展方向为去中心化排序器、共享排序器、跨层排序器等。

5、提案人（Proposer）

提案人负责将排序器已排列的交易上传状态证明到以太坊上，更新根节点的状态，在 ZK Rollup 中则是零知识证明。如果提案人全部掉线，Rollup 上的交易状态更新会停滞，可能导致用户无法提取他们在 Rollup 上的资金。解决方案和排序器类似，需要 Rollup 开放提案人准入，而非小范围的审核许可制。开放 Rollup 用户的强制提现功能，让用户可以自己发送证明到底层链上，避免 Rollup 审查也可以防止提案人的风险。

（二）总结

Rollup 能够受信任和保证安全性来自多方面，与公链的逻辑不同，不是排序器去中心化就能保护用户资金的安全。Rollup 与底层链相连，来自底层链上的资产是很重要的部分，要保证 Rollup 与底层链之间的桥连接安全，还需要让 Rollup 中的用户能够强制将交易发送给底层链节点，实现最

低标准的同等安全。除此之外，数据可用性、状态验证证明等也是保证Rollup能实现与底层链同等安全的条件。

目前的Rollup多借助于辅助轮（training wheels）手段维持运转，意味着必须引入额外的信任假设才能认为现在运转的Rollup是安全的。例如有的项目提交证明的系统仍处于开发中，说明Rollup可能向底层链提交无效交易。Rollup 智能合约的升级是开放的，代表升级智能合约后可能盗取Rollup中的资金。还有排序器和提案者的许可制，存在用户交易和提现受到中心化审查的风险。辅助轮代表目前有些Rollup不是最小化信任的，仍需要用户相信Rollup的参与者们不会作恶。

总的来说，Rollup扩容工具受信任的基础来自上传到底层链中的交易执行结果保证是正确的，并且将资产转移到Rollup后，还能随时将Rollup上的资产提现到底层链上。在一些侧链类扩容项目中，用户需要先信任第三方，也就是侧链上的节点不会作恶，而且还要信任关联资产桥的安全，信任成本太高。这也是为什么Rollup要优于侧链，成为主流的扩容方式。虽然目前在Rollup发展早期，Rollup还存在不尽完美的地方，但在摘除辅助轮之后，Rollup需要各方面达到最小化信任的要求，例如完备的状态有效性证明方案、开通“逃生通道”、严谨的智能合约升级机制等。

三、应用链的选择

（一）应用链的趋势

公链为应用提供发展的平台，但同样在平台上也会制约应用发展。对于需要个性化功能的应用来说，公链不再是目的地，因此应用会选择独立成为应用链，将活动转移到应用链上进行。本小节将主要讨论以应用链形

式呈现的应用。

对于应用链来说，独立运营的优势体现在两个方面：

1、自成生态-功能平台化

应用能够围绕自己的主题，发展相关的生态，包括扶持有助于生态发展的项目。自成生态能够增加项目叙事，并且可以捕获额外的价值。

2、自我主权-减少负外部性

平台在发展到一定程度后，会暴露其负外部性问题，例如链上拥堵造成用户手续费过高，而独立应用链平台不需要与其他应用分享资源，可以尽可能地避免这些问题。

基于上述因素，独立成应用链往往是每个应用所设定的最终愿景，但在起步阶段，应用难以负担得起链的成本，并且完全脱离公链会让应用失去接触公链原生资产、导入公链用户的便捷性。部署链的前置条件包括更改开发环境、链的节点准备、共识机制选择等，需要链自身维护其账簿安全和节点共识。因此在应用发展中，独立成链往往作为最后一阶段实现，但在实际情况下，出于成本和应用发展的考虑，独立的应用链计划很难实现。

因此帮助应用构建应用链一直是区块链基础设施中的一类，致力于降低应用链部署成本。也可以看到，应用链从平行链、侧链发展到 Rollup 的形式，其中经历了几次叙事转换。在 Rollup 中，也存在最小（Micro Rollup）的概念，此 Rollup 专为应用准备，Rollup 中的功能和虚拟机的执行方式等也可以根据应用定制。

（二）应用链的权衡

对于第一节中讨论的 6 种模块化形式来说，适合应用链的是智能合约 Rollup（Layer 2 或 Layer 3）、主权 Rollup 和链下 DA 的形式。因为对于应用链来说，成立单层区块链的成本较高，Enshrined Rollup 的作用是给原本底层链带来更多功能。应用链可以作为结算层使用，以便扩大生态，需要具备智能合约功能。

对于应用链来说，既可以选择选择已有的 RaaS 工具或其他 Rollup 开放的架构，也可以根据模块化的角度，攒成一个 Rollup。明显地，应用链使用已有工具虽然能简化部署成本，解决排序器等问题，但已有的解决方案不如自己搭建 Rollup 灵活，能够自主决定 Rollup 的各组件以及表达的功能。

无论是何种方式构建的应用链，运营者最关心的两个方面是可控度和应用运行成本。应用链对于基础设施的选择决定了其安全性和性能，也代表了应用对链的可控度，例如上文讨论的排序器和可升级智能合约等设置。而主权区块链的设定让 Rollup 分叉和主权选择更容易和灵活。DA 成本决定了应用的运行成本，一些新的 DA 解决方案能够在链下保管资料，成本远低于以太坊。应用链可以根据自身情况选择不同的方案，如下图所示。其中，链上 DA 和低可控度是 Rollup 最理想的情况。

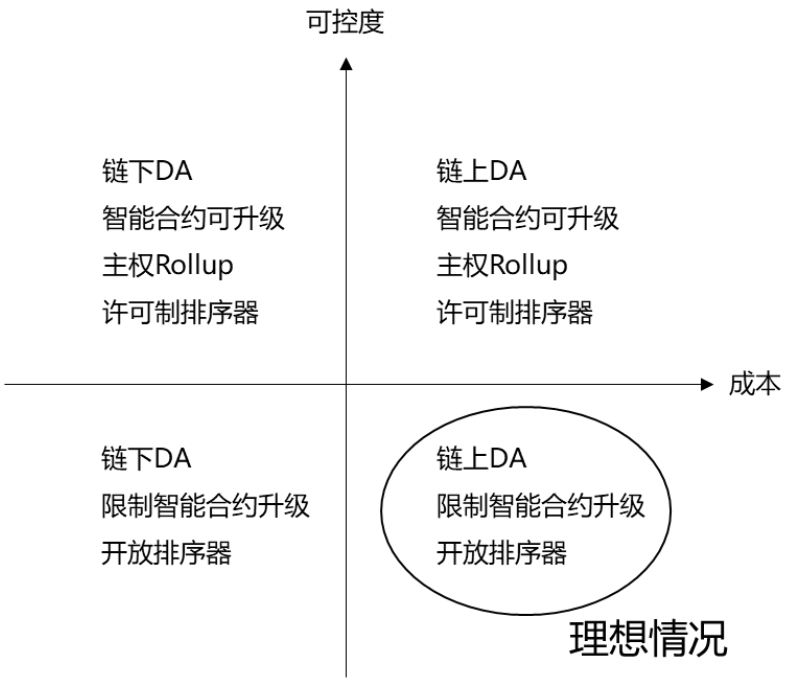

图 3：应用链考虑的两个角度

什么适合应用？这一问题需要应用自己解答，应用链的成本与实现底层链同等级别的安全性很难同时满足，那么根据应用自身所要实现的目标，在可控、安全、成本等方面做取舍。金融资产类应用和游戏类应用所选择的方式是不同的，Rollup 能够实现应用链所需要的组合性。

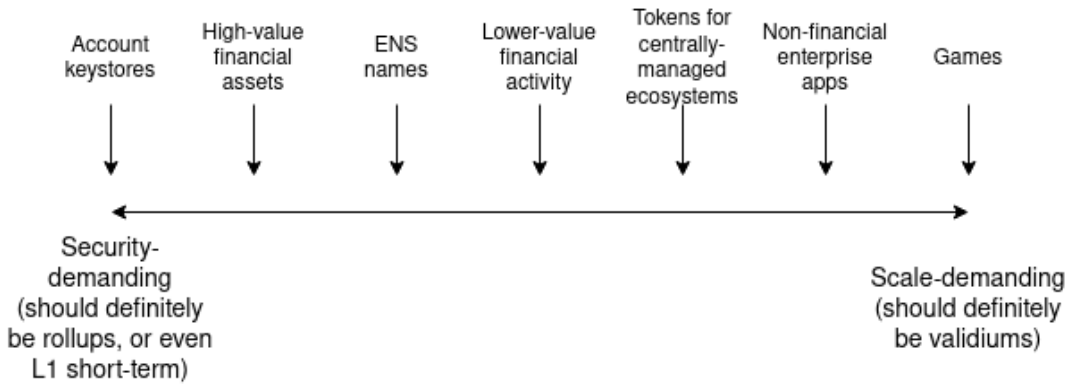

图 4：应用的权衡 资料来源：Vitalik Buterin 博客

（审核：邹传伟）