区块链

通往 Web3.0 的入口：零知识证明与 EVM

增持（维持）

Web2.0 通向 Web3.0 征程中，有哪些实用的入口技术？

在 Web2.0 向 Web3.0 演化的过程中，数据、资产账户互通和应用程序的互操作是两个尤为关键的问题。前者涉及到不同生态之间的共识传递，这里包括了链上、链下共识传递；后者则是程序应用部署过程中的务实问题。虽然 Web3.0 世界如星辰大海般的浩渺，Web2.0 向 Web3.0 进化过程中需要在实用技术、信用传导机制方面不断探索。

目前，零知识证明和 EVM 是当下非常实用的的两种技术，成为 Web2.0 向 Web3.0 演化的两个重要入口。零知识证明提供了一种方便实用的验证方法，使得在 Web3.0 之外（链外）的数据/账户能够方便取得链上验证，获得 Web3.0 生态的信任，为数据/资产互通提供可能。同时，目前所谓的 Web3.0 生态，主要基于以太坊构建，对接以太坊生态流量成为进入 Web3.0 世界的重要入口。因此，EVM 成为极为实用的基础设施和技术。Web2.0 生态也可以通过兼容 EVM，尝试与以太坊对接，实现应用程序的互操作。

零知识证明可以分担计算功能，链上只负责安全和验证。将零知识证明和区块链的一致共识结合起来，则可以降低网络成本，一台设备即可运行计算，链上用密码学的方法验证其可靠性而非重复参与计算，并且在成本昂贵的区块链网络上，验证计算的正确性要比重复计算便宜得多。因此，区块链只负责网络的共识和安全，而一些计算的工作则可以交给零知识证明，在区块链网络外部完成。整体上，不仅提升了扩展性，这种方法依旧有着区块链网络的安全性和共识。这一点在我们的《Web3.0 程序该跑在哪里？》报告中有所详述。零知识证明应用方面的代表项目包括 zkSync、Mina 等。

由于以太坊强大的生态，其他公链来若想部署原以太坊生态应用（如 DeFi 应用协议），部署 EVM 则成为最快捷的路径。以太坊的资产账户、合约程序执行、ERC 系列代币（包括 ERC20 标准代币和 ERC721 标准的 NFT）等都依赖于 EVM。一个部署了 EVM 的平台，则在代币标准、合约程序等方面对接了以太坊。这意味着，原以太坊生态应用协议可以无缝平移到新的公链部署，对于其用户来说，EVM 也是的在其他公链体验 Dapp 是无感的，与在以太坊上操作差不多。可以这样说，部署 EVM 成为大多数公链的标配。

对于实际应用程序部署，EVM 不光为非以太坊公链提供了一个“偷懒”而实用的入口，同时，我们不禁设想，Web2.0 生态能否通过部署 EVM，在数据状态、资产账户和合约程序等方面与以太坊无缝对接？能否想象这样的场景，股票交易所通过部署 EVM，实现与以太坊甚至其他 Web3.0 生态之间的资产转移和互操作？类似 Synthetix、Mirror、UMA 这种区块链合成资产平台，相当于在 Web3.0 世界制造 Web2.0 资产的影子、映射。能否通过 EVM，使得 Web2.0 资产直接、正面进入 Web3.0 世界？**例如，直接通过邮箱、手机号直接获得 Web3.0 世界的通行证？无论如何，EVM 都是一个非常务实的基础设施应用。**

风险提示：区块链商业模式落地不及预期；监管政策的不确定性。

行业走势

作者

分析师 宋嘉吉
执业证书编号：S0680519010002
邮箱：songjiaji@gszq.com
分析师 任鹤义
执业证书编号：S0680519040002
邮箱：renheyi@gszq.com

相关研究

1、《区块链：李宁联名无聊猿意味着什么？》2022-04-26
2、《通信：关注通信出口产业链与一季报超跌机会》2022-04-24
3、《区块链：元宇宙的九宫格框架：从 What 到 How》2022-04-19

内容目录

图表目录

1. 核心观点

当前，国内对 Web3.0 的关注度日益提高，除了认识到其开放、共享、隐私等特征外，如何基于现有的应用场景和开发能力向 Web3.0 迁移成为重要议题。Web3.0 并非空谈，而有很多底层的逻辑和技术需要理顺。

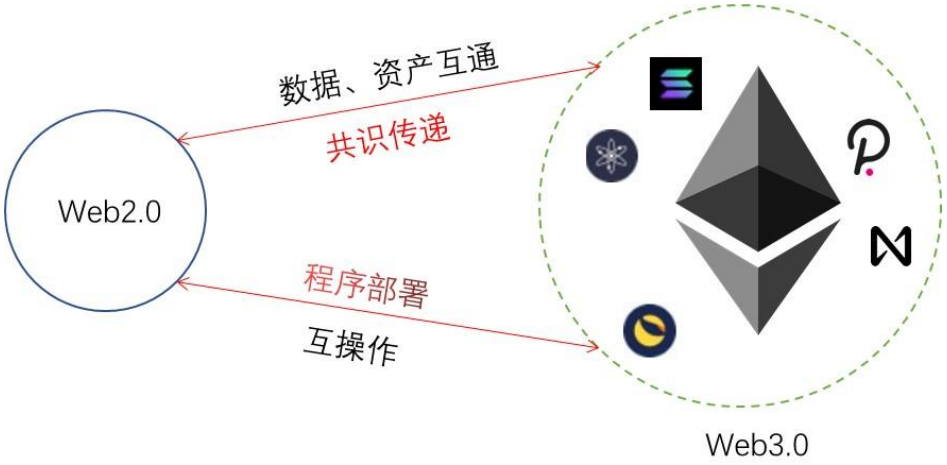
在 Web2.0 向 Web3.0 演化的过程中，数据、资产互通和应用程序的互操作是两个尤为关键的问题。前者涉及到不同生态之间的共识传递，这也包括了链上、链下共识传递；后者则是程序应用部署过程中的务实问题。虽然 Web3.0 世界如星辰大海般的浩渺，Web2.0 向 Web3.0 进化过程中需要在实用技术、信用传导机制方面不断探索。

目前而言，零知识证明和 EVM 是当下非常实用的的两种技术，成为 Web2.0 向 Web3.0 演化的两个重要入口。零知识证明提供了一种方便实用的验证方法，使得在 Web3.0 之外（链外）的数据/账户能够方便取得链上验证，获得 Web3.0 生态的信任，为数据/资产互通提供可能。目前所谓的 Web3.0 生态，基本上是基于以太坊构建的，对接以太坊的生态流量成为进入 Web3.0 世界的重要入口。因此，EVM 成为极为实用的基础设施和技术。Web2.0 生态也可以通过兼容 EVM，尝试与以太坊对接，实现应用程序的互操作。

2. 通往 Web3.0 的入口

毫无疑问，在通往 Web3.0 的路上，Web2.0 价值生态和数据会长期共存，并不断融合。那么，Web2.0 通往 Web3.0 的入口是什么？这里有两个关键问题：首先，明显壁垒存在的情况下，两个生态之间信用如何传递？例如，Web2.0 生态数据获得 Web3.0 链上的一致共识？Web2.0 资产如何与 Web3.0 账户打通？其次，两个生态之间的程序如果需要实现互操作，在实际应用部署中，不同的程序语言环境会带来很大的部署困难，这是落地过程中一个非常务实的问题。

图表 1：通往 Web3.0 的两个关键问题



资料来源：国盛证券研究所整理

零知识证明为第一个问题提供了一种简单有效的解决方案，零知识证明为 Web2.0 数据状态（可以推广到一切链外的数据状态）和 Web3.0 数据共享提供有效的状态证明；也就是说，通过零知识证明，Web2.0 和 Web3.0 之间可以彼此信任，来自前者的数据状态可

以有效地获得后者链上的共识。这一点类似我们在**《Web3.0 程序该跑在哪里？》**报告中提到的链上链下共识传递。

在目前所谓的 Web3.0 生态中，以太坊生态是绝对的主力。对接 Web3.0 生态，往往可以从对接以太坊生态入手。大量的非以太坊公链通过部署 EVM 从而分享以太坊是生态流量。对于实际应用程序部署，EVM 不光为非以太坊公链提供了一个“偷懒”而实用的入口，同时，我们不禁设想，Web2.0 能否通过部署 EVM，在数据状态、资产账户和合约程序等方面与以太坊无缝对接？能否想象这样的场景，股票交易所通过部署 EVM，实现与以太坊甚至其他 Web3.0 生态之间的资产转移和互操作？类似 Synthetix、Mirror、UMA 这种区块链合成资产平台，相当于在 Web3.0 世界制造 Web2.0 资产的影子、映射。能否通过 EVM，使得 Web2.0 资产直接、正面进入 Web3.0 世界？

零知识证明、EVM 是 Web3.0 生态中，非常实用的两种技术，也是有望在 Web2.0、Web3.0 之间架起“传送门”。

3. Web3.0 两个实用技术：零知识证明和 EVM

本章节分别就零知识证明和 EVM 做了介绍，零知识证明典型的案例包括 zkSync、mina 等项目，EVM 几乎成为非以太坊公链的标配，最近兴起的包括 Cosmos 生态的 EVMOS 和分布式存储项目 Filecoin 的 FVM 虚拟机，FVM 作为基于存储公链的虚拟机，还有着其他不一样的特点。

3.1. 零知识证明（Zero-Knowledge Proof）

零知识证明（也叫做最小泄露证明）无疑是近段时间最热门的区块链行业词汇之一，零知识证明最早由 MIT 教授和密码学专家于上世纪八十年代首次提出。零知识证明具体是指证明者可向验证者证明某个申明的真实性而不泄露任何其他信息。如今零知识证明主要被应用于区块链领域。其出色的数学特性可以被用在很多不同的场景中。零知识证明技术仍处在非常早期的阶段。

此生动的例子可以简单阐述什么是零知识证明：假设 A 有一个带密码锁的盒子，他想在不告诉 B 真正密码的情况下，又让 B 相信 A 知道这个盒子的密码。那么他要怎么做呢？

A 让 B 写了一个全世界只有 B 自己知道的秘密，B 写下了一张“我的小狗叫 Bob”的字条放入盒子中。A 通过正确的密码打开盒子后获取了此信息并告知 B。在这个交互过程中，B 并没有得知任何此前自己不知道的信息（盒子的密码），但 A 还是成功的让 B 相信了 A 知道密码。

最初人们认为证明是人们面对面沟通中的一种交互行为。随机性可以用来证明某件事听起来很反直觉。一个理想的证明不应该存在随机性和不确定性。零知识证明是对传统概念里“证明”的一次彻头彻尾的颠覆。在传统证明中，随机性完全有悖于证明者所努力的目标。证明者会努力公开全部信息流。但是一但颠覆观念，不再试图去暴露信息流，随机性所带来的负面影响就成了正面的，随机性可以被利用去隐藏想要隐藏的信息。

3.1.1 零知识证明（Zero-Knowledge Proof）原理

零知识证明（Zero-Knowledge Proof）是麻省理工学院研究人员在 20 世纪 80 年代提出的一种加密方法，是可信计算广泛使用的密码学算法之一。零知识证明或零知识协议是一种基于概率的验证方法，包括两部分：宣称某一命题为真的证明者（prover）和确

认该命题确实为真的验证者（verifier）。

顾名思义，零知识证明就是既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄漏出去，即给外界的 “知识” 为“零”。零知识证明有三条性质：
（1）完备性。如果证明方和验证方都是诚实的，并遵循证明过程的每一步，进行正确的计算，那么这个证明一定是成功的，验证方一定能够接受证明方；
（2）合理性。没有人能够假冒证明方，使这个证明成功；
（3）零知识性。证明过程执行完之后，验证方只获得了“证明方拥有这个知识”这条信息，而没有获得关于这个知识本身的任何一点信息。

零知识的形式定义必须使用一些计算模型，最常见的是图灵机的计算模型，而作为图灵完备的以太坊来说，与零知识证明结合就催生了 zkSync 这样的 L2 应用。

3.1.2 零知识证明（Zero-Knowledge Proof）的意义

从应用角度来说，零知识证明有两个非常重要的方向：
1）隐私性：零知识证明可以满足消息的隐私性。例如在区块链交易中，如果你需要证明你拥有某种尚未使用的资产，但同时又不想暴露资产的详细来龙去脉，零知识证明技术可以解决常见的区块链网络中因透明性所带来的消息泄露，例如地址和资产额度。

隐私计算是零知识证明的一个重要的应用领域。隐私是信息泄露所导致的问题，若想保护隐私，则必须通过密码学的解决方案对链上数据进行加密，让链上的不同交易之间找不出关联性。零知识证明可以验证计算而不会暴露有关输入和计算本身的任何信息，保证链上数据隐私。

在 Web3.0 中至关重要的一点是用户自身真正掌握身份和数据所有权。但当前区块链上所有的信息都是公开的，通过一些手段可以轻易得获取用户的信息(当然这本身也是区块链网络共识的特性)。虽然目前区块链用户尚没有广泛且强烈的隐私意识，但随着发展，这种需求在未来一定是更加迫切且长期存在的。所以要实现 Web3.0 的愿景，用户必须要有权力拥有自己的链上隐私。因此可以说隐私未必是必选项，但一定是可选项。

2）拓展性：若常用的区块链平台中产出新区块的验证时间很长，可直接更改为一人（节点）验证并生成证明，网络中的其他参与者都掌握快速验证该证明的方法，而不需要每个参与者都花费大量的时间来直接进行验证。

这涉及共识的成本问题，从经济学角度来看，例如以太坊，比特币等区块链网络交易成本高昂的原因在于：共识必须是昂贵的，廉价的共识一定程度上是不可信的。而其中的成本主要来自于区块链的一致共识下，若干台设备的重复计算。例如 POW 共识机制（如比特币、以太坊等）网络中，1000 台机器做重复的计算工作，效率不会大于一台计算机的效率，但成本可以简单认为是在一台设备上处理同样计算任务的 1000 倍。这是所有的主流共识协议，无论是 POW 还是 POS，为确保去中心化的共识所必须付出的成本。也就是不可能三角的束缚。

将零知识证明和区块链的一致共识结合起来，则可以降低网络成本，一台设备即可运行计算，链上用密码学的方法验证其可靠性而非重复参与计算，并且在成本昂贵的区块链网络上，验证计算的正确性要比重复计算便宜得多。

因此，区块链依旧负责网络的共识和安全，而一些计算的工作则可以交给零知识证明，在区块链网络外部完成。整体上，不仅提升了扩展性，这种方法依旧有着区块链网络的安全性和共识。这一点在我们的《Web3.0 程序该跑在哪里？》报告中有所详述。

3.1.3 零知识证明（Zero-Knowledge Proof）的技术及应用

zk-SNARKs（简洁非交互式零知识证明），zk-STARKs（简洁全透明零知识证明）和 BulletProofs（防弹证明）是零知识证明的 3 种常见技术。区块链项目应用的主要是其中两种：zk-SNARKs 和 zk-STARKs。

这两种技术均与 zk-Rollup 结合，zk-Rollup 搭建在 L1 主链之上。例如以太坊就是我们所说的“单一型”区块链。因为共识、执行和数据可用性都发生在同一区块链上。这也是为什么单一型的以太坊区块链无法扩展的原因，也就是我们常说的不可能三角问题。想要实现扩容，以太坊必须向“模块化”的区块链发展。这意味着只将区块链用于其最擅长的方面：共识。并将其他的工作执行和数据可用性“外包”给链下。

zk-Rollup 将多笔交易打包成一笔提交给主链（例如以太坊），通过零知识证明而被主链快速验证并且这个证明会被储存在主链上。因此可以继承主链的安全性同时将执行和数据可用性移植到 zk-Rollup 上。主链无需单独处理所有交易，这样每笔交易的大小会被压缩，同时验证成本会被分摊到所有交易上以节省 Gas 费和提高 TPS。其中 zkSync 和 Starkware 当属 zk-Rollup 中的佼佼者。这两个项目有着同样类似的架构：Rollup 智能合约被部署到以太坊区块链中，用来存储 L2 状态转换的 zk 证明。ZK Rollup 的本质是将链上的用户状态压缩存储在一个默克尔根（意思是 rollup 中包含了账户余额、合约代码等）中，并将用户状态的更新转移到链下来，同时通过 zk-SNARKs 的证明来保证该链下用户状态变更过程的正确性。在 Layer1 直接处理用户状态的更新成本是比较高的，但是仅仅利用主链(Layer1)上的智能合约来验证一个零知识证明的 Proof 是否正确，成本是相对低很多的。这也是零知识证明发挥的最关键作用。

zk-STARKs 代表项目 StarkWare:
StarkWare 发明了基于 STARKs 证明的密码学技术。同时它通过 Volition 系统解决 DA(数据可用性）问题。(DA 非常重要，有了它，用户才能在区块链浏览器上看到自己的交易具体是如何发生的）Volition 允许用户可以在 rollup 方案 (链上数据可用性，更昂贵) 和 validium 方案 (链下数据可用性，更便宜) 之间自由选择。在 validium 方案中，链下 DA 由中心化的 "数据可用性委员会" 提供保证，委员会由一些有声望的加密实体组成。虽然不够去中心化但费用更低。用户仍可自由选择，这其实是一个折中的方案。

优势是其中 T 代表 Transparent(透明)，这意味着无需信任设置。同时生成证明的速度更快。(有研究指出生成 STARKs 证明的速度最高可比 SNARKs 快 10 倍。）劣势是技术不如 SNARKs 成熟，同时如果它实现了图灵完备，就很难与 EVM 兼容。(StarkWare 创建了一种特定的编程语言来运行其支持的自主程序。目前 StarWare 正在创建代码转移器来讲 Solidity 无缝转换为其特殊的语言 Cairo 以便兼容 EVM。)它具有证明快、验证快，但证明体积大等特点。

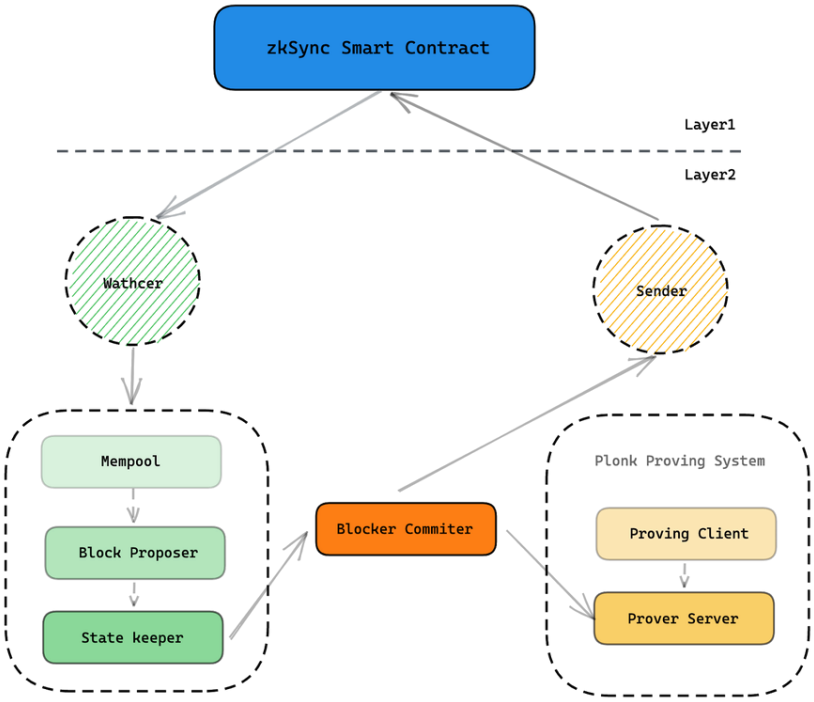
ZK-SNARKs 技术的代表项目 zkSync:
以太坊创始人 Vitalik 认为，“从中长期来看，随着 ZK-SNARK 技术的改进，ZK Rollup 最终将在所有场景中胜出。”可见，ZK-SNARK 有着明显的优点，但技术难度较大。这方面的代表项目是 zkSync。

zkSync 是基于 ZK Rollup 架构的低成本且无需信任扩容协议，用于在以太坊上进行可扩展的低成本支付。主要通过零知识证明和数据可用性保障用户资产安全来保证用户的资产安全。所有资金都由主链上的智能合约持有，而计算和存储则在主链外进行。为了提升效率，不是单独验证每个交易，而是将交易“汇总”到单个项目（汇总块，即 Rollup），然后对其进行验证，同时批准所有交易。

zkSync 的主要架构分为链上和链下，即 L1 和 L2；L1 的核心为 zkSync 智能合约，主要负责存款、提款、交易验证，也就是以太坊主链上账户的最终状态维护。L2 分为 L1

交互（Watcher、Sender）、L2 状态维护（Mempool、Block Proposer、State Keeper、Block Commiter）、零知识证明系统。

图表 2：zkSync 架构



资料来源：CSDN、国盛证券研究所

zkSzkSync 工作流程:
1. 用户签署交易并将其提交给验证者;
1. 其提交给验证者;
2. 验证者将数千笔交易汇总在一个区块中，并向主网上的智能合约提交新状态的加密承诺（根哈希）以及该新状态确实是该新状态的结果的加密证明将一些正确的事务应用于旧状态;
3. 除了证明之外，状态（指每笔交易的少量数据）在主链网络上以便宜的价格发布 calldata，这使任何人都可以随时重建状态;
4. 证明和状态由智能合约验证，从而验证区块中包含的全部交易的有效性和区块数据的可用性。

zkSync 在转账过程中，State Keeper 通知 Block Commiter 收集生成零知识证明所需信息，调用 Plonk Proving System 生成零知识证明后，借助 Sender 将存款和转账等交易数据，以及将对应的零知识证明提交到 L1 的 zkSync 智能合约验证；等待 L1 交易确认后，Watcher 会通知 L2 更新交易状态为最终确认。**由此可见，脱离了主链的 L2 通过零知识证明实现了与主链的共识传递。**

zkSync 优势是实现 EVM 兼容的方式要比 zk-STARKs 方案更自然。因为智能合约可以由 zkSync 编译器逐一转换操作码，而不需要一个中介语言或者专门的转译器。劣势则是生成证明的速度较慢。简单来说 zkSync 具有证明慢、验证快，证明体积小的特点。因此，zkSync 成为行业最为看好的 L2 解决方案，随着 2.0 版本的上线，其生态发展蓬勃发展。

图表 3：zkSync 生态图景

资料来源：ZK Daily，国盛证券研究所

零知识证明所有特的隐私特性，可以有效地完成 Web2.0 与 Web3.0 生态之间的共识传递。例如对于传统市场的资产，并不能直接作为链上 DeFi 应用协议的抵押资产。但用户可以将自己的征信数据在本地生成证明并提交上链，可以在不泄露自身隐私数据的情况下，得到 DeFi 系统灵活的信贷服务；而传统的 DeFi 借贷服务都是需要以资产的超额抵押为前提。这个应用场景的意义在于，将多个生态的数据和应用实现快速对接，这些生态可以是区块链、也可以是链下生态。

无论是 L2 与 L1、链上链下、Web2.0 与 Web3.0，都可以利用零知识证明来传递信用，因此零知识证明作为一种有效的技术实现不同生态之间的共识传递，成为 Web2.0 通往 Web3.0 的入口技术。

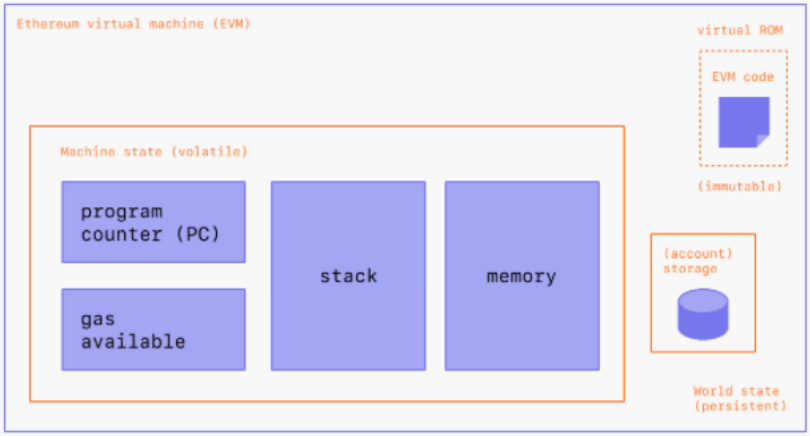
3.2. EVM：以太坊生态流量快车的秘密

EVM 全名是 Ethereum Virtual Machine，即以太坊的虚拟机。虚拟机是指能够通过软件模拟出具有完整硬件系统功能的运行在隔离环境中的一个完整的计算机系统。EVM 是一个巨大的虚拟机，允许部署和执行代码。用户只需安装必要的客户端软件即可访问 EVM，并使用它在以太坊上执行程序。由于以太坊是大量分散节点组成的“互联网计算机”，用户可以通过 EVM 在分散的环境中执行软件操作。EVM 是图灵完备的（简单说就是可以用来解决任何的可计算问题），因为它可以用于执行各种复杂度的计算，即通常所谓的执行智能合约程序。而比特币是图灵不完整的，限制了其功能开发。

我们可以将 EVM 理解为以太坊执行合约程序的平台或者环境，为用户提供了一个部署程序的应用环境平台。EVM 其实是作为一个单独的实体存在，由成千上万运行以太坊客户端的互相连接的计算机来维护。以太坊协议本身的存在唯一的目的就是保持 EVM 这个特殊状态机的连续、不间断以及不可改变的运行。EVM 是以太坊账户和智能合约赖以生存的环境。

跟比特币的 UTXO 来维护账户余额不同，以太坊不仅能够维护账户的余额状态，还支持更强大的智能合约功能，以太坊实际上不光是分布式账本，而是分布式状态机。

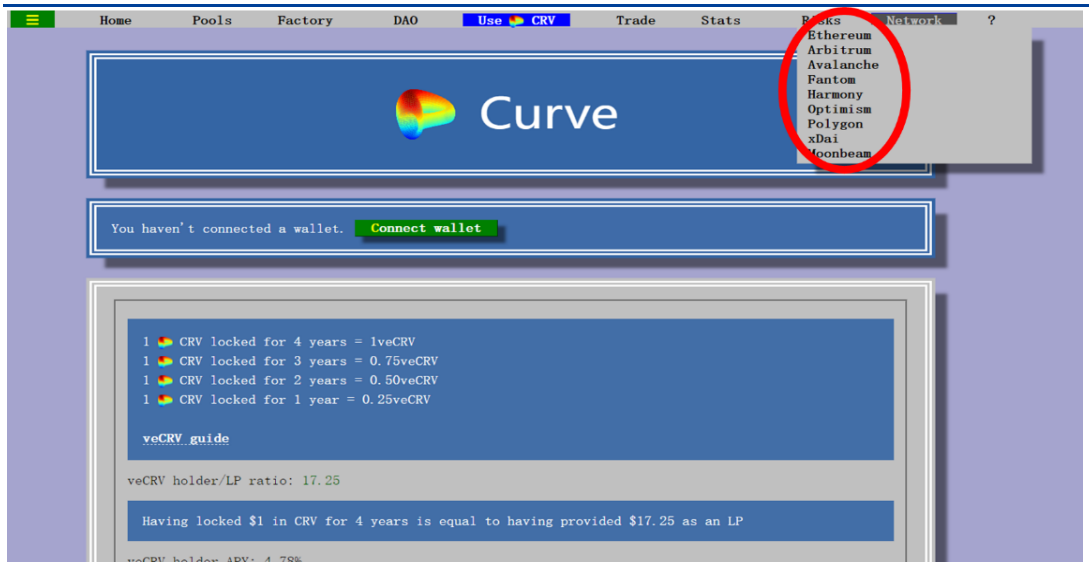
图表 4：EVM 基本构架



资料来源：ethereum.org，国盛证券研究所

更简单通俗地讲，发布到链上的智能合约代码，可以理解为一笔复杂的特殊交易（包含了可执行代码）。当某个智能合约需要被调用时，只需向智能合约的地址发送一笔交易。所有的节点都要安装以太坊客户端，而所有的客户端中又自带 EVM，当智能合约被链上交易触发时，智能合约的代码就会在 EVM 上执行。这种形式也实现了去中心化程序的部署和调用。EVM 是以太坊智能合约功能得以实现的最重要的组成部分。

图表 5：curve 平台可以无感地在多条主链/L2 网络之间切换登陆



资料来源：curve.fi、国盛证券研究所

资产账户、合约程序执行、ERC 系列代币（包括 ERC20 标准代币和 ERC721 标准的 NFT）等都依赖于 EVM。一个部署了 EVM 的平台，则在代币标准、以太坊合约程序等方面对接了以太坊。由于以太坊强大的生态，其他公链来若想部署原以太坊生态应用（如 DeF 应用协议），部署 EVM 则成为最快捷的路径。这意味着，原以太坊生态应用协议可以无缝平移到新的公链部署，对于其用户来说，EVM 也是的在其他公链体验 Dapp 是无感的，与在以太坊上操作差不多。例如，最流行的 DEX 协议 curve 目前已支持以太坊、Arbirum、Avalanche 等多条公链/L2 网络，同一套 UI 界面可以无感地在不同主网上登陆，因此，curve 长期位于 DeFi 协议 TVL（锁仓资产价值）排名榜前几名。

EVM 成为以太坊流量外溢最务实、快捷的入口。我们不禁设想，能否将 EVM 引入 Web2.0

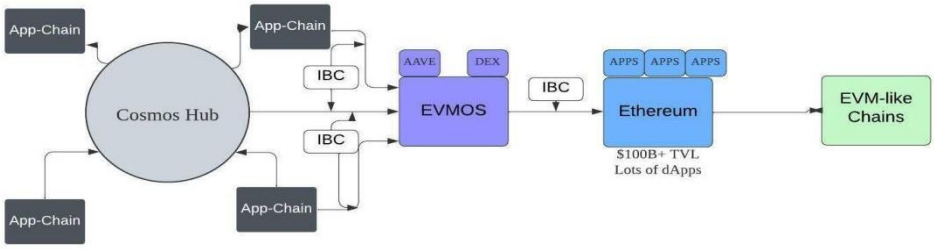
世界，如股票交易所等金融平台部署 EVM，打通与以太坊的连接，市场传统金融资产与 DeFi 金融资产的互通？从而推动传统金融市场与 DeFi 市场融合激发更多样的金融服务？目前用户习惯的 Web2.0 社交平台身份，通过部署 EVM 能否也可以直接登录 Web3.0 应用呢？例如，直接通过邮箱、手机号直接获得 Web3.0 世界的通行证？无论如何，EVM 都是一个非常务实的基础设施应用。

3.2.1 EVMOS：Cosmos 生态的 EVM 兼容链

Evmos 实现的是将 EVM 兼容链(不仅仅是以太坊)集成到 Cosmos 生态中。这意味着 Fantom、Avalanche 等 EVM 区块链可以通过 Evmos 将资产整合到 Cosmos IBC 生态系统中。也就是说，基于 EVM 的去中心化应用、代币以及 NFT 都可以连接到 Cosmos 生态，从而实现真正的多链生态群，用户和开发人员可以轻松地在多链之间进行资产转移和操作。Evmos 起源于 2016 年的 Ethermint，最初的目标是通过 Tendermint 共识协议来帮助以太坊和 EVM 应用实现扩容。

由此可见，EVMOS 将在 Cosmos 生态中具有不可或缺的独特地位。EVMOS 采取与 Terra(LUNA),Cosmos Hub(ATOM)相同的 Cosmos SDK 和 Tendermint 共识引擎开发，这些技术已经经过 2-3 年的稳定运行。Evmos 与 Cosmos 现有生态中各个链最大的不同就是在应用层引入了 EVM 兼容性，能够最大敏捷高效的部署使用 Solidity 语言所开发的智能合约，也就意味着以太坊上现存的成千上万个项目都可无缝移植。Evmos 还有一个特殊的 ERC20 的模块，旨在能够将基于 Cosmos 标准的代币转换为 ERC20，从而实现对以太坊生态代币的兼容。因此 Evmos 与以太坊几乎可以达到无缝衔接，互操作性极高。让以太坊上的庞大的资产能够流入 Cosmos 生态并能与其中优质的原生资产例如 ATOM，LUNA，OSMO 产生交互。以太坊上的资产通过 Cosmos 作为一个桥梁,可以不断拓展到整个 Cosmos 生态中。

图表 6：EVMOS 作为沟通 Cosmos 和其他兼容 evm 公链的桥梁



资料来源：DeFi 之道、国盛证券研究所

借助 EVM 的特性，EVMOS 的开发者可以直接利用以太坊上现存的大量应用，这意味着 EVMOS 可以更快速的引入一些 DeFi 的原生应用（债券市场、衍生品协议，DEX 等等），时间上将比 Cosmos 生态中的其他链要快非常多。这也可能成为其抢占市场的一大优势。

Cosmos 生态中尚缺乏将一些优质的资产例如 ATOM 作为抵押资产借贷的方法，但 EVMOS 的到来很有可能改变游戏规则。因此在中短期内，EVMOS 的用户总数和活跃交易将可能迎来快速增长（类似 Avalanche C 链）以满足 Cosmos 生态中其他资产的持有者的各种各样的需求。这也是以太坊生态流量外溢的效应。

由此引发出一个问题，为什么原本想要成为以太坊杀手的公链都在争先恐后的拥抱 EVM？由于以运行以太坊虚拟机的低成本链（例如 Polygon,BSC,Fantom）都能在较短的时间获得成功以及相对繁荣的生态。其他更具特色的不同架构的公链不得不思考 EVM 对于他们各自发展的意义并加速拥抱。例如波卡上的 Moonbeam，Near 推出的的 Aurora 以及上面

提到的 Cosmos 中的 EVMOS 等等。

当这些不兼容 EVM 的链刚刚面世时，往往都声称自己拥有更卓越、更独特的设计和架构，以及支持一些主流编程语言或高速等特性。随着这些公链相继支持 EVM，似乎代表着他们已不太看重自己的技术优势， 而是更需要以太坊庞大的生态支持。通过兼容 EVM，这些链似乎已经回归初心，并不在叫嚣着成为“以太坊杀手”，而是构建一种更低成本的以太坊的替代方案以夺取市场份额，颇有些“打不过就加入”的感觉。

兼容 EVM 的优势在 EVMOS 的例子中已阐述清楚如成为资产涌入的入口；更为安全的 EVM 桥；将自己底层的原生资产链接到广泛的 EVM 生态等。但同样也存在着缺点例如这其实为以太坊生态的繁荣更加添砖加瓦，而高度同质化的用户体验也带来了恶性竞争，如果一个程序可以通过所有 EVM 和基础区块链来运行，那么想要把用户从他们原本的“温室”中吸引过来则需要一些切实的优惠或独特的优势，例如价格竞争、用户补贴、玩法创新等。

图表 7：几种公链兼容 EVM 方案对比

Base chain	Project name	Type	Tx fee token	Token use	Network architecture	TVL (USD)
COSMOS	Evmos	EVM+chain	EVMOS	Securing network	BFT, Tendermint PoS/ 150	Not launched
NEAR	Aurora	EVM	ETH	Governance	PoS, sharding/ Near validators	460m
SOLANA	Neon	EVM	NEON or any erc20	Governance	BFT, PoS/ Solana validators	Not launched
Polkadot.	Moonbeam	EVM+chain	GLMR	Securing network	PoS/32	190m

资料来源：Dose of DeFi、国盛证券研究所

一个通识的、被广泛接受的标准将提供更多的可组合型。由于共同的 EVM 标准，更紧密的联系可能引发未来更大的增长。EVM 是助推行业的繁荣或是限制技术的发展，未来会给出答案。但从目前几乎所有公链都在集成 EVM 的事实来看，EVM 兼容性将是其他公链必备的竞争力之一。

3.2.2FVM：存储+计算的探索

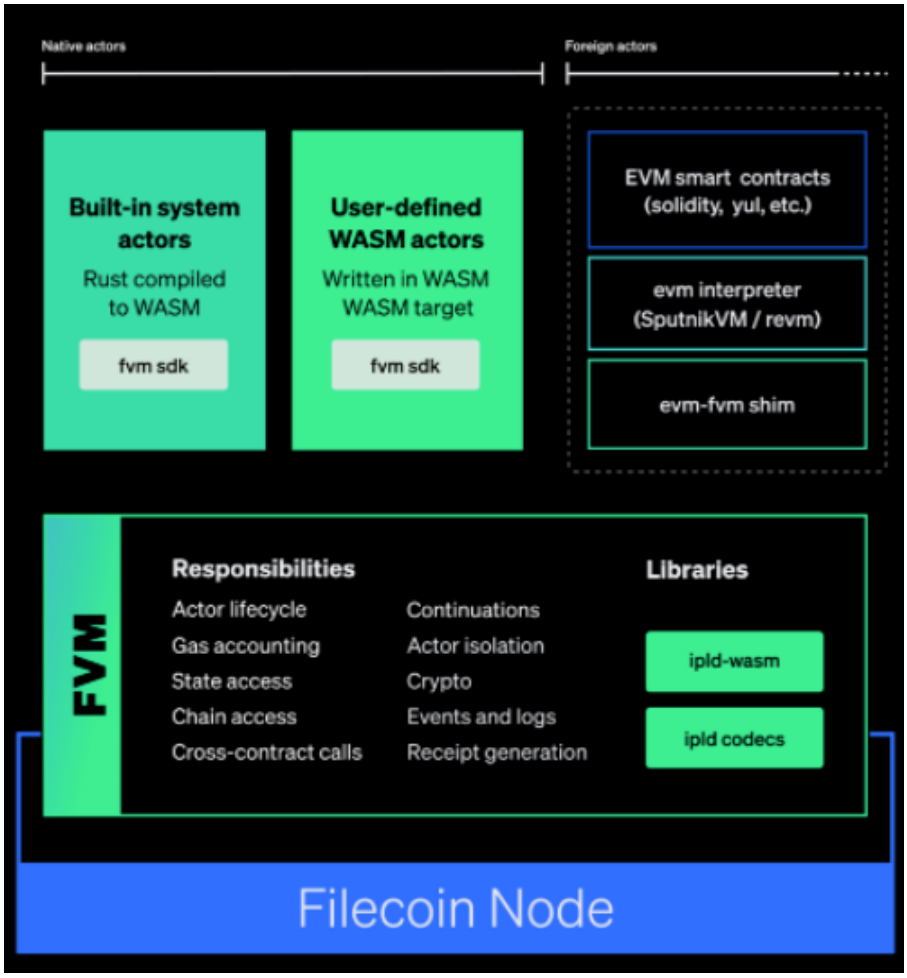
Filecoin 是一个分布式的数据存储市场，在遍布全球的存储空间提供者间分发内容寻址数据集，增加数据的冗余和弹性，这对于 NFT 等创新应用场景来说是必不可少的存储基础设施。**Filecoin 正在按计划推进逐步引入虚拟机（FVM），将存储和计算等基础资源进行整合，这将会为 Filecoin 生态带来全新的赋能。**

FVM 是基于 WASM 的多语言执行环境。WASM 全称 WebAssembly，是一种在基于栈的虚拟机上运行的二进制的指令格式，支持多种的现代编程语言例如 Rust，C++和 JavaScript 等等。WASM 原本是为浏览器所设计的虚拟机，不同的编程语言可以被编译成二进制文件的形式，在 CPU 上以近乎原生的速度运行。WASM 的主机独立性，沙盒安全机制和简洁等特性，使其比较贴合于区块链领域的需求，也使其成为智能合约理想的运行环境（runtime）。

FVM 主要目的是支持将其他编程语言编译成 WASM 格式的原生 Filecoin Actor（Actor 是 Filecoin 官方对于智能合约的另一种称呼）的运行，同时要为外部智能合约的运行环境（例如 EVM）提供支持。FVM 对 EVM 的兼容性通过模拟底层的字节码达到了开箱即用

的级别，也支持开发者使用他们熟悉的 Remix、Truffle、OpenZeppelin 等工具直接进行开发。绝大部分的智能合约移植到 FVM 上不需要任何更改。

图表 8：包含 FVM 的 Filecoin 节点说明



资料来源：fvm.filecoin.io，国盛证券研究所

FVM 赋予了生态参与者代理计算资源，激励计算执行，在存储提供者间分配工作任务以及证明计算结果的准确性的可能性。Filecoin 生态内的存储提供者（或者叫矿工）也可参与 FVM 的计算网络。计算客户端会将不同的计算任务分发给广大的计算资源的提供者，同时也引入或融合新的机制向这些参与者提供奖励。

由于距离真正上线还有一段时间，目前可获取的信息不算丰富，从官方的披露的文档和信息来看，本身 Fliecoin Layer0 的共识依旧是复制证明+时空证明的混合共识机制，而 FVM 则更有可能引入全新的独立的机制来保证计算资源提供者的奖励。FVM 的引入使得 Filecoin 从一个 Web3.0 的去中心化存储的基础设施而变为一条在链下数据可用性有着天然优势的公链。FVM 将首先为 Filecoin 生态内的一些活动提供更好的解决方案，例如：

1）数据进行去中心化计算：直接在 Filecoin 内存储数据的空间进行计算而无需移动；
2）智能弹性存储市场：按时间、需求、复制级别等条件更灵活的对存储费用进行动态定价；
3）存储衍生品（保险、抵押、贷款）：用户可以特定价格"预购"存储空间，数据生产者将预测他们在特定时间段内的成本。相反，通过让存储提供商对未来的存储空间进行投标，他们可以预先确定需求，从而有效地管理库存、硬件、运营和财务。或者是例如保险协议可以帮助存储提供商从投资者处为提供服务时所需的大量抵押物募资，或在更广阔的范围内分配风险。投资者也可通过收取日常费用来获得收入的现金流。

我们认为 FVM 的上线以及其积极兼容 EVM 将对 Filecoin 自身的发展带来许多巨大变革，由于 FVM 的支持，或许目前的很多 dApp 的形态包括 NFT 的应用又或是 DeFi 应用都将迎来变化，例如 NFT 应用不需要在自己运行 IPFS 节点，NFT 数据或可直接与交易挂钩，随时可验证且可靠性高，智能合约也可以引用这些数据以实现数据、计算、交易的统一。FVM 若需要异军突起，单纯的与其他链进行 TPS 性能的竞争似乎并非上策，而依旧发扬 Filecoin 本身作为存储基础设施在去中心化存储，存储证明及验证的优势进行差异化竞争或许能迸发出更多的可能性。

风险提示

区块链商业模式落地不及预期：Web3.0 基于区块链、密码学等技术，相关技术和项目处于发展初期，存在商业模式落地不及预期的风险。

监管政策的不确定性：Web3.0 实际运行过程中涉及到多项金融、网络及其他监管政策，目前各国监管政策还处于研究和探索阶段，并没有一个成熟的监管模式，所以行业面临监管政策不确定性的风险。

免责声明

国盛证券有限责任公司（以下简称"本公司"）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议,本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在 15%以上
		增持	相对同期基准指数涨幅在 5%~15%之间
		持有	相对同期基准指数涨幅在-5%~+5%之间
		减持	相对同期基准指数跌幅在 5%以上
	行业评级	增持	相对同期基准指数涨幅在 10%以上
		中性	相对同期基准指数涨幅在-10%~+10%之间
		减持	相对同期基准指数跌幅在 10%以上

国盛证券研究所

北京
地址：北京市西城区平安里西大街 26 号楼 3 层
邮编：100032
传真：010-57671718
邮箱：gsresearch@gszq.com

上海
地址：上海市浦明路 868 号保利 One56　1 号楼 10 层
邮编：200120
电话：021-38124100
邮箱：gsresearch@gszq.com

南昌
地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
邮编：330038
传真：0791-86281485
邮箱：gsresearch@gszq.com

深圳
地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
邮编：518033
邮箱：gsresearch@gszq.com