深度解析拥有明星投资阵容的Movement

作者：河马投研

#### 在讲Movement之前，我们先熟悉一下当今加密领域最主流的智能合约编程语言：

1. Solidity：最常用的智能合约编程语言，专为以太坊平台设计，它是一种高级面向对象语言，语法类似于JavaScript，Solidity是编写以太坊上智能合约的首选语言。

2. Rust：用于编写Solana区块链上的智能合约，Rust是一种系统编程语言，以高性能和内存安全为特色，Solana上的智能合约称为“程序”，用Rust编写后编译成WebAssembly（Wasm）。

3.Move：最初由Facebook（现为Meta）团队开发，用于Libra（后改名为Diem）区块链开发的智能合约语言。Move专注于安全性和可验证性以防止常见的智能合约漏洞。

4.Vyper：也是为以太坊设计的智能合约语言，相较于Solidity更加简洁和安全。Vyper避免了一些Solidity中的复杂功能，以减少安全漏洞的风险。

5.Cairo：用于StarkNet上的智能合约编写，Cairo是一种支持零知识证明的语言，专注于扩展性和隐私保护。

6.Tezos Michelson：一种为Tezos区块链设计的堆栈语言，虽然比较低级，但提供了强大的形式化验证支持，使得编写安全的智能合约更加容易。

7.Clarity：用于Stacks区块链（与比特币集成）的智能合约语言，Clarity是解释性语言，不支持图灵完备，旨在增强合约的可预测性和安全性。

#### 以上众多的智能合约编程语言各有特色，其中以太坊的Solidity编程语言作为智能合约开发的主要语言，尽管在区块链开发领域广泛使用，但仍存在以下痛点：

1. 安全性：Solidity智能合约的安全性是一个主要的痛点。由于智能合约一旦部署就不可更改，代码中的漏洞可能会被恶意利用，导致资金损失。历史上，像The DAO等安全事件就是因为智能合约中的漏洞被攻击者利用，每年被黑客攻击导致资金损失的项目不计其数。

2. 开发调试难度：Solidity的开发和调试过程较为复杂。由于区块链的不可变性和去中心化特性，开发者很难在主网环境中直接调试合约。虽然有诸如Remix和Truffle等开发工具，但调试仍然需要一定的技巧和经验。

3. 学习曲线陡峭：对于传统的Web开发者来说，Solidity的学习曲线较为陡峭。Solidity是一个类似于JavaScript的编程语言，但它引入了区块链特有的概念，如Gas费、合约状态等，这使得初学者需要花费更多时间来掌握。

4. 合约升级困难：Solidity智能合约的升级是一项挑战，因为合约一旦部署到区块链上就不能修改，所以在合约需要功能更新或修复错误时，开发者往往需要使用代理模式等复杂的设计模式来实现合约的升级，这增加了开发的复杂性。

5. Gas成本优化：Solidity代码的执行会消耗Gas，而Gas的成本直接影响用户的使用体验和开发者的成本控制。编写高效的Solidity代码以减少Gas消耗是开发者必须考虑的问题，但这往往需要对EVM（以太坊虚拟机）的深入理解。

6. 合约复杂度管理：随着智能合约功能的增加，代码的复杂性也会增加，管理复杂合约变得更加困难。复杂合约容易出现意外行为，难以测试和维护，这对开发者提出了更高的要求。

7. 工具和生态系统不够成熟：尽管以太坊有一套相对完整的开发工具链，但与传统开发生态系统相比，Solidity及其相关工具仍有较大的改进空间。一些工具可能功能不全或存在兼容性问题，影响开发效率。

#### 这些痛点使得Solidity开发需要开发者具备较高的专业技能，并且在开发过程中需要谨慎处理，以避免潜在的安全风险和高额的Gas消耗。幸运的是Move语言因其独特的优势，可以解决Solidity语言中存在的很多问题，比如：

1.安全性高：Move语言专注于资源安全管理，设计时就考虑到了防止常见的区块链攻击，如重放攻击和双花攻击。它通过类型系统和资源模型来确保资产的安全管理，使得资源只能以特定方式创建、销毁或转移，避免了不安全的操作。

2.资源模型：Move使用了独特的资源模型，将资产（如代币）视为“不可复制和不可丢失”的资源。这意味着资产在转移时只能从一个所有者转移到另一个所有者，消除了重复创建或意外丢失资产的风险。

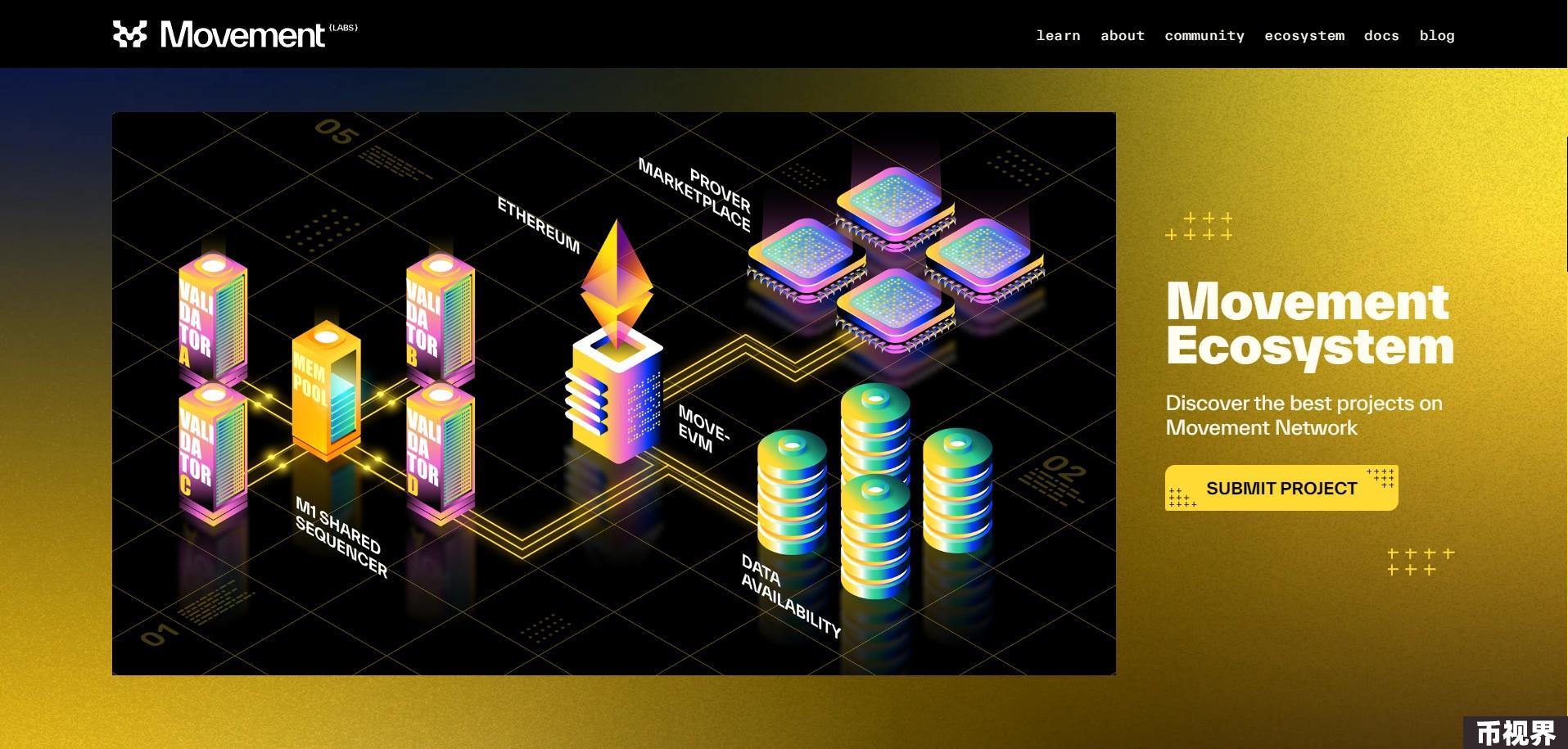
3. 灵活性和模块化：Move语言支持模块化设计，使得开发者可以重用代码，创建更加复杂和可扩展的智能合约。此外，Move的类型系统允许定义自定义的资源类型，使得开发者可以构建复杂的金融和商业逻辑。

4.形式化验证：Move语言支持形式化验证，这使得开发者可以在代码部署之前验证智能合约的正确性，进一步提高了安全性。通过数学证明的方式来验证智能合约行为，可以减少智能合约的漏洞和错误。

5.并发处理：Move设计中考虑了并发执行的需求，支持多个交易的并行处理。这对于区块链网络的性能提升至关重要，能够显著提高区块链的吞吐量。

6.适应性强：虽然Move最初是为Libra/Diem设计的，但由于其独立于具体区块链的特性，Move可以适配到其他区块链平台上。已经有多个区块链项目（如Aptos、Sui）开始采用或探索使用Move语言。

#### 这些特性使得Move语言在开发安全、高效、灵活的智能合约时具有显著优势。而EVM在当今加密领域的地位几乎无法撼动，那么有没有一种既能利用Move语言的优势又能将EVM连接打通的方案呢？这就是今天的主角Movement的诞生背景。



### 什么是Movement？

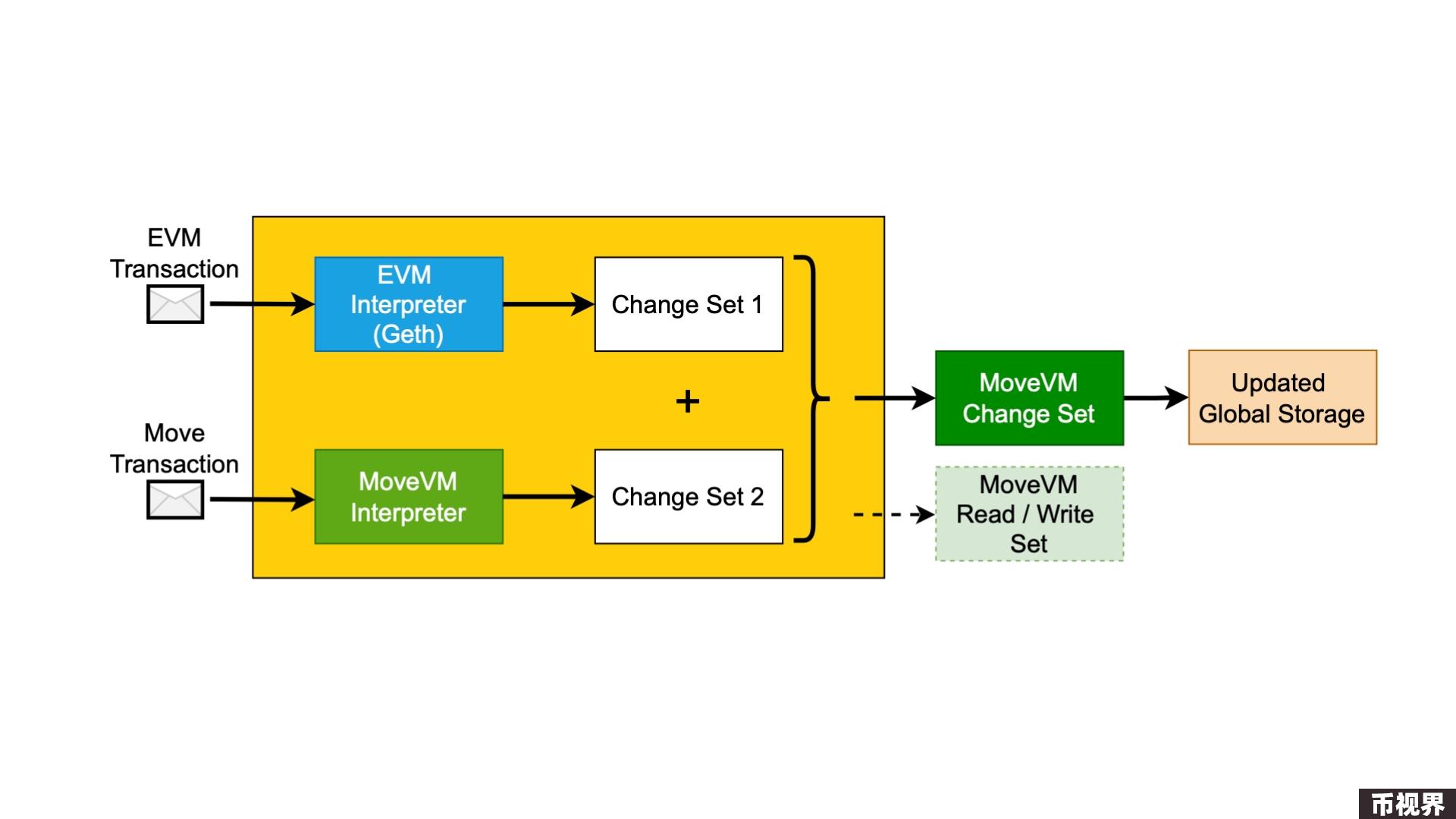
简单的来说Movement就是要将安全高效的MOVE语言引入EVM生态，Movement由M1和M2两个核心组件构成，通过M1和M2的结合，提供了一个安全、高效、去中心化的区块链生态系统。Movement 是一个模块化框架，用于在任何分布式环境中构建和部署基于 Move 的基础设施、应用程序和区块链。团队正在构建一套产品和服务，使非Move协议能够利用Move编程语言的强大功能，而无需编写一行Move代码。团队的第一个版本 M1 将 L1 重新定义为可垂直组合和水平可扩展的第1层框架，该框架与 Solidity 兼容，连接 EVM 和 Move 流动性，在如今的加密市场中，公链开发的技术层面已经相当内卷了，吸引足够多的用户和资金入场才是公链能否持续生存的关键因素，而Movement另辟蹊径，打通与EVM的流动性，使其生态可与EVM取得互操作性，从而可直接获得EVM所带来的用户和资金。

#### 工作原理

Movement网络有三个主要组件可增强其性能、安全性和互操作性：移动执行器、质押结算模块和去中心化共享排序器（M1）。每个组件在确保基于 Move的rollups 运行方面都发挥着至关重要的作用。

1.移动执行器

Move 执行器是 Movement-SDK 的核心组件，支持 MoveVM 和 EVM 字节码。这种双重兼容性提供了强大的执行环境，使开发人员能够利用 Move 语言的高级功能，同时保持与现有以太坊应用程序的兼容性。Move 执行器将MoveVM 的并行执行功能与现有的 EVM解释器集成在一起，确保了兼容性和可扩展性。



质押结算模块：质押结算模块旨在为 Move Rollups 网络内的交易提供快速终结性。通过利用质押资产来验证状态转换的证明者网络，该模块可确保较高的经济安全性并减少延迟。验证者质押资产并证明状态转换的正确性，将质押的安全性优势与快速交易终结性的效率相结合。

2.安全机制：

以太坊结算，验证者质押资产以提供经济安全，确保网络完整性中的重大经济利益。zk 和 Optimistic Rollups：zk-rollups 通过有效性证明提供安全性，而 Optimistic Rollups 则依靠挑战期来解决争议。这两种方法的延迟和计算成本都较高。

Staked Rollups：与 zk 和 optimism Rollups 相比，它能提供快速的终结性和较高的经济安全性，无需大量的证明生成或挑战期，从而减少延迟并改善用户体验。

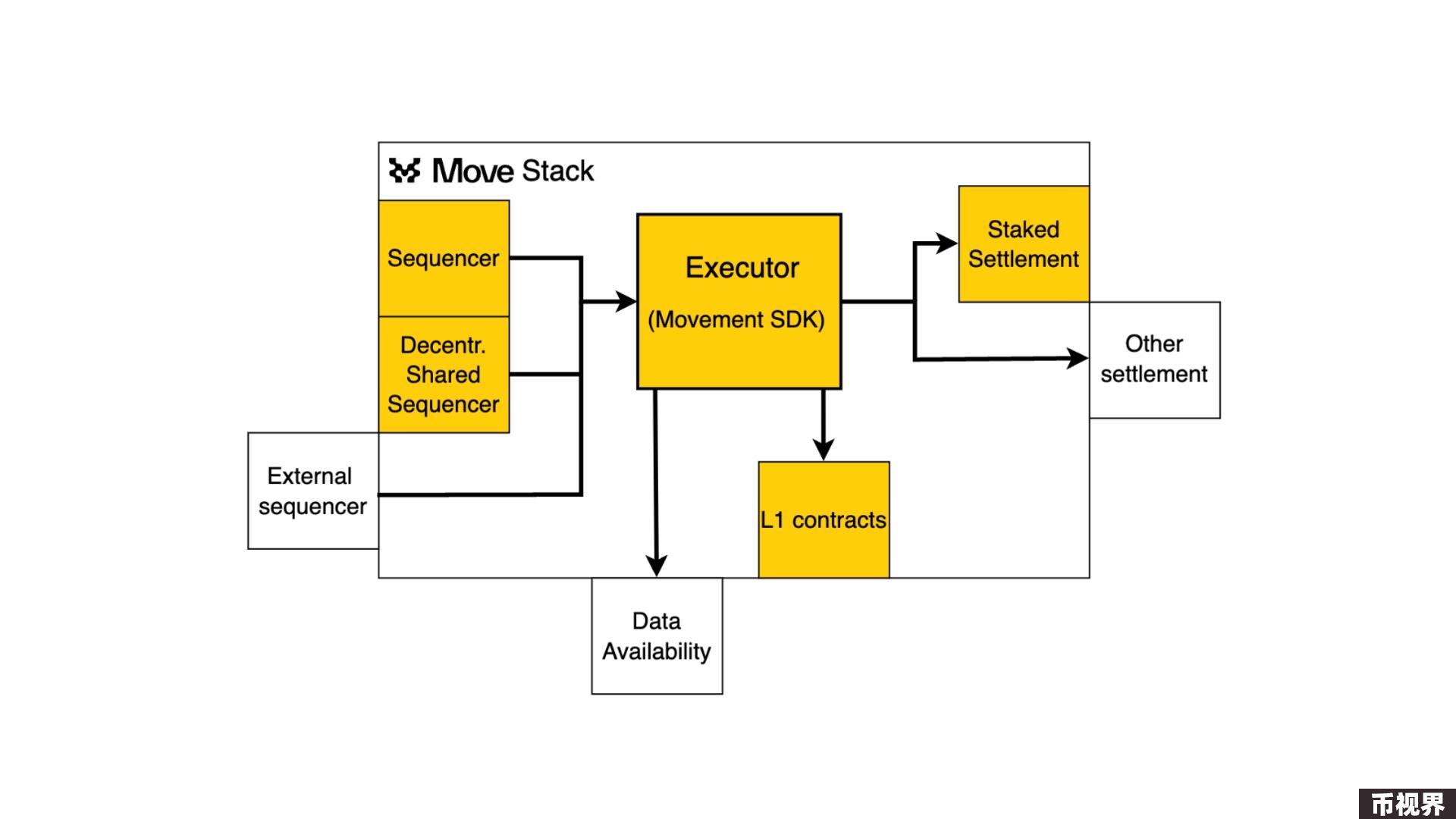
与其他Rollup:与 zk-rollups 不同，Staked Rollups 不需要昂贵的证明生成设备。

与乐观汇总和 zk-rollups 相比，Staked Rollups 显著降低了延迟，并在几秒钟内完成。

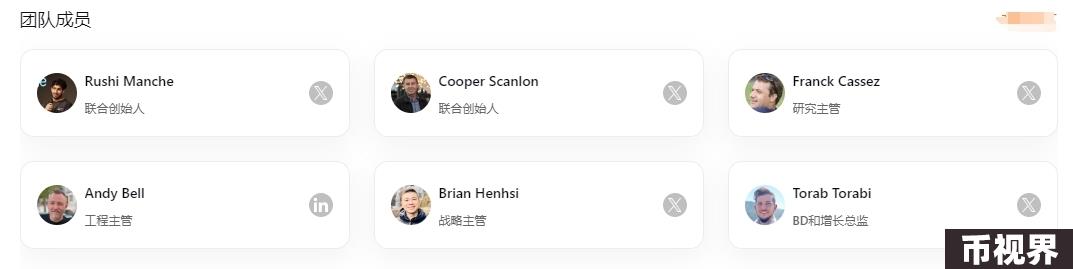
快速终结对于互操作性和原子跨 rollup 交易至关重要，这使得 Staked Rollup 成为许多应用程序的理想解决方案。

3.去中心化共享排序器（M1）

M1 排序器是一种去中心化和共享的排序机制，可增强网络稳健性、公平性和抗审查性。通过提供可定制的交易排序，M1 支持 Move Arena 生态系统中的跨链原子交换和池化流动性。此共享排序器可确保所有参与汇总的交易排序公平高效。



#### 项目团队



1.Rushi Manche：Movement Labs 联合创始人，此前是 Aptos 软件工程师；

2.Cooper Scanlon 从范德比尔特大学退学后打造了一个 SPAC DAO 工具。完成该合资企业后，他与 Move 建立并审计了第一个收益聚合器。然后，他创立了 Movement Labs，这是一家下一代基础设施公司，将区块链环境与可组合的 Move 模板统一起来；

3.Franck Cassez 是 Movement 的研究主管，此前他曾是 Windranger Labs 的区块链研究主管，他还曾在 ConsenSys 任职。他拥有南特中央大学的计算机科学博士学位；

4.Andy Bell 是 Movement Labs 工程主管，毕业于诺丁汉大学，此前是 Biconomy 工程副总裁、Ajuna 首席技术官；

5.Brian Henhsi 是 Movement Labs 的战略主管，毕业于清华大学此前他曾在 Sui / Mysten Labs 和 Chia 任职。

#### 投资机构

1.2023年9月13日Movement Labs 完成 340 万美元的 Pre-Seed 轮融资，由Varys Capital、dao5、Blizzard The Avalanche Fund、Borderless Capital 及其专注于 Wormhole 生态系统的跨链基金领投；

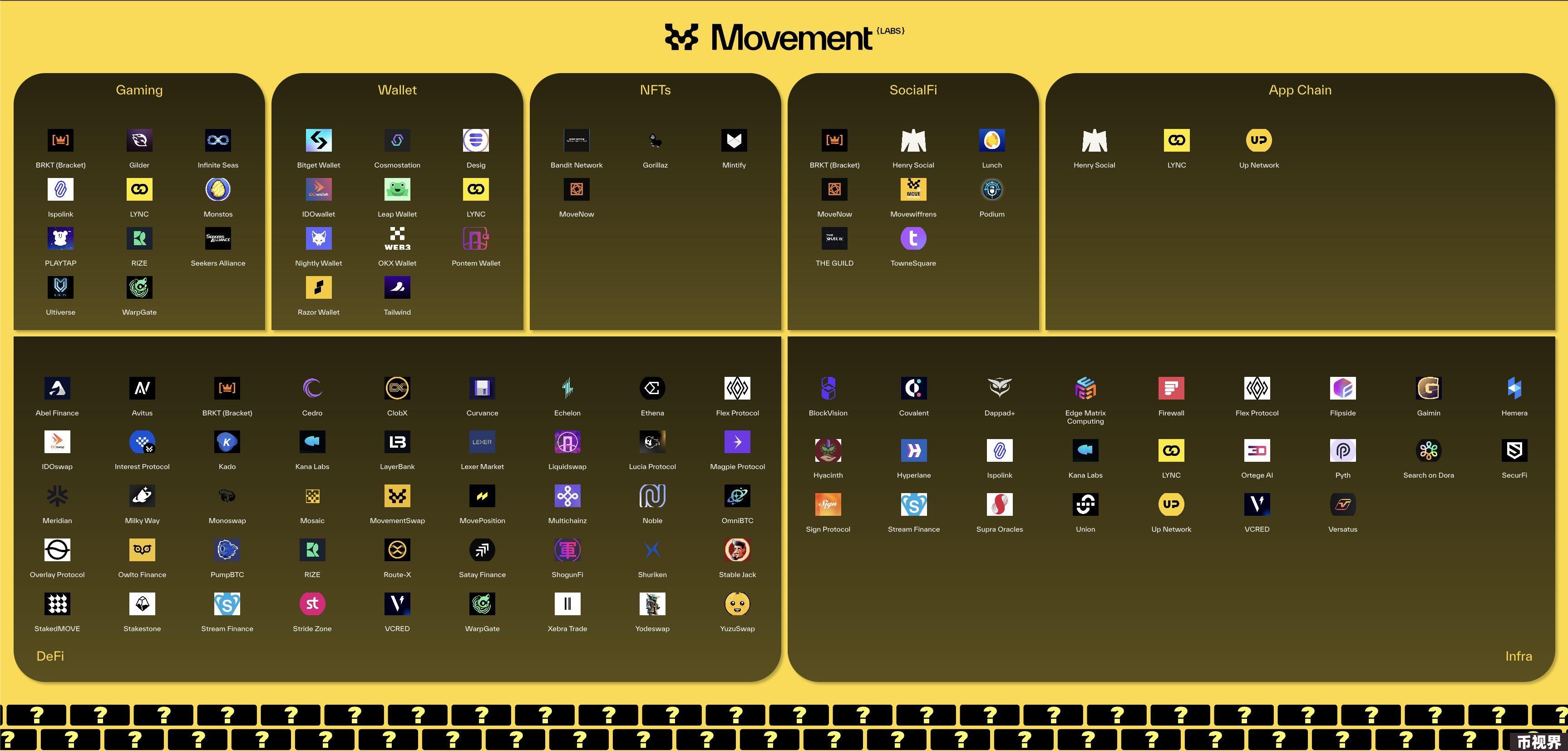
2.2024年4月25日Movement Labs 完成 3800 万美元 A 轮融资，Polychain Capital 领投，Hack VC、Foresight Ventures、Placeholder、Archetype、Maven 11、Robot Ventures、Figment Capital、Nomad Capital、Bankless Ventures、OKX Ventures、dao5 和 Aptos Labs 等参投；

3.2024年5月7日Movement Labs完成了由Polychain Capital领投的3800万美元A轮融资，Hack VC、Foresight Ventures、Nomad Capital、Bankless Ventures、OKX Ventures等投资机构参投，同时Binance Labs也宣布投资Movement Labs。

我们可以看到Movement的明星豪华投资阵容非常强大，这种投资阵容项目的测试网我们尽量都去参与交互一下，后期应该会有不错的空投预期。

#### 项目发展

目前Movement上的生态项目已经达到了一百多个，涵盖Gaming、Wallet、NFTs、SocialFi、DeFi、Infra等多个板块，这对于一个仅仅在测试阶段的公链来说已经非常繁荣了，这也代表Movement团队的强大同时也表明其他项目对Movement的前景非常看好。



### 同赛道项目对比

#### Movement和Aptos以及SUI有什么区别？

1.Movement： Movement是一个新的区块链项目，旨在通过提供去中心化金融（DeFi）和去中心化应用（DApp）的解决方案来增强区块链生态系统的功能性和效率。

特点：可能包括高吞吐量、低交易费用和强大的安全性。

2.Aptos： Aptos是一个以开发高性能智能合约平台为目标的区块链项目。它是由前 Facebook 的 Libra 项目团队（现在称为 Diem）的一部分发起的。

特点：APTOS 注重于高性能、可扩展性和安全性，致力于解决传统区块链的扩展性问题，并支持复杂的智能合约和去中心化应用。

3.SUI： SUI 是一个相对较新的区块链平台，目标是提供一个去中心化、可扩展的网络环境，用于支持各种去中心化应用和金融服务。

特点SUI可能强调高吞吐量、低延迟和用户友好性，同时也可能提供支持创新功能的开发工具和平台。

#### 这三个项目各有其独特的设计理念和技术实现，适合不同的应用场景和需求。

### 总结：

Movement自身定位是第一个以太坊上的MOVEEVM的L2，其作为一个模块化的Move区块链框架，具有很大的发展潜力，Move作为一种新的智能合约编程语言，提供了更高的安全性和灵活性，Movement利用Move开发语言的先天优势，可能会吸引更多开发者和项目使用其框架。Movement的模块化设计可以提高区块链系统的灵活性和可扩展性，开发者能够根据需求选择和组合不同的模块，简化开发过程并提高效率。作为一个新兴框架，Movement 需要证明其技术的成熟性和稳定性，以赢得市场信任，区块链领域竞争激烈，其他框架和平台的创新也可能对 Movement 形成威胁，Movement 需要不断创新和优化，以保持竞争力。

我们期待 Movement 能够在未来带来更多的创新和突破，推动整个区块链行业的发展。