在今年 1 月，Partisia Blockchain
在参加了达沃斯世界经济论坛时，宣布推出一种全新的链上资产管理方案 MOCCA（MPC On-Chain Custody
Advanced），即多方计算链上托管高级解决方案。据悉该方案建立在 Partisia Blockchain
基础上，是一种以去中心化、可编程的、多链托管为特点的全新托管解决方案。而 MOCCA 方案的推出，进一步推动了 MPC 技术在资产管理领域的采用，并被行业解读为，是数字资产安全保护的格局以及资产管理领域的重新定义。

MOCCA：一种更具去中心化、可编程特性的全新管理方案

Partisia Blockchain 是一个兼具隐私、可互操以及高迸发特性的 Layer1 系统，其通过将区块链以及零知识计算（包括 MPC、零知识证明 ZKP 等）以协作的方式结合起来，并通过分片方案、Bring Your Own Coin（BYOC）功能和 Oracle 服务框架，构建一个更加安全的数字基础设施。

以 Partisia Blockchain 底层为基础，其进一步推出了基于 MPC 的 MOCCA 管理方案，该方案使用户能够在其首选区块链上桥接资产，并让数字资产的管理变得更加可信、安全，且兼具隐私以及可编程特性。

l 快速部署和成本效益

MOCCA 方案为部署者提供自定义模板和工具（Partisia Blockchain 的智能合约ID

E），部署者可以通过这些工具集低门槛、高效的部署，且不依赖于一些三方的托管供应商，减少了费用、实施时间，并确保了去中心化和灵活性。MOCCA 方案在易于部署上，与阈值签名（TTS）方案形成可鲜明的对比，后者在实施和维护方面更加复杂。

l 可编程性

MOCCA 方案以 MPC 为基础，提供了完全可编程的智能合约，允许使用 RUST 编写任意代码逻辑。模板合约包括经过安全审计的标准策略，涵盖常见的托管方案。MOCCA 的可编程性允许执行诸如添加或移除签名者、修改阈值签名方案和投票权、集成具有特殊权限的NFT、实施特定交易类别的特定规则等政策，并为部署者提供了更为定制化、个性化的包容性模块，与更多的场景进行适配。

l 高安全性

Partisia Blockchain MPC 的安全性来源于，其将 MPC 节点引入到链上，通过分布式的计算来为 MPC 的安全提供保障。Partisia 在网络中引入了 zk 计算节点，基于区块链网络共识驱动，具备计算能力的 zk 节点将以自发的方式，为网络中所需的零知识计算提供服务，并从网络中获取奖励。这种全新的集成，不仅简化了 MPC 的部署和管理过程，还通过利用区块链的特性，增强了整个系统的安全性和透明度。

在此基础上，MOCCA 方案能够通过在 Partisia Blockchain 底层引入了链下签名

功能的方式，进一步加强管理大量资金的机构用户的安全性。而这一功能也使离线设备能够生成密钥，并通过客户端参与链上协议。通过将特定密钥存储在 Partisia Blockchain 的去中心化 MPC 集群中，将进一步加强该方案的安全性。

l 更加去中心化

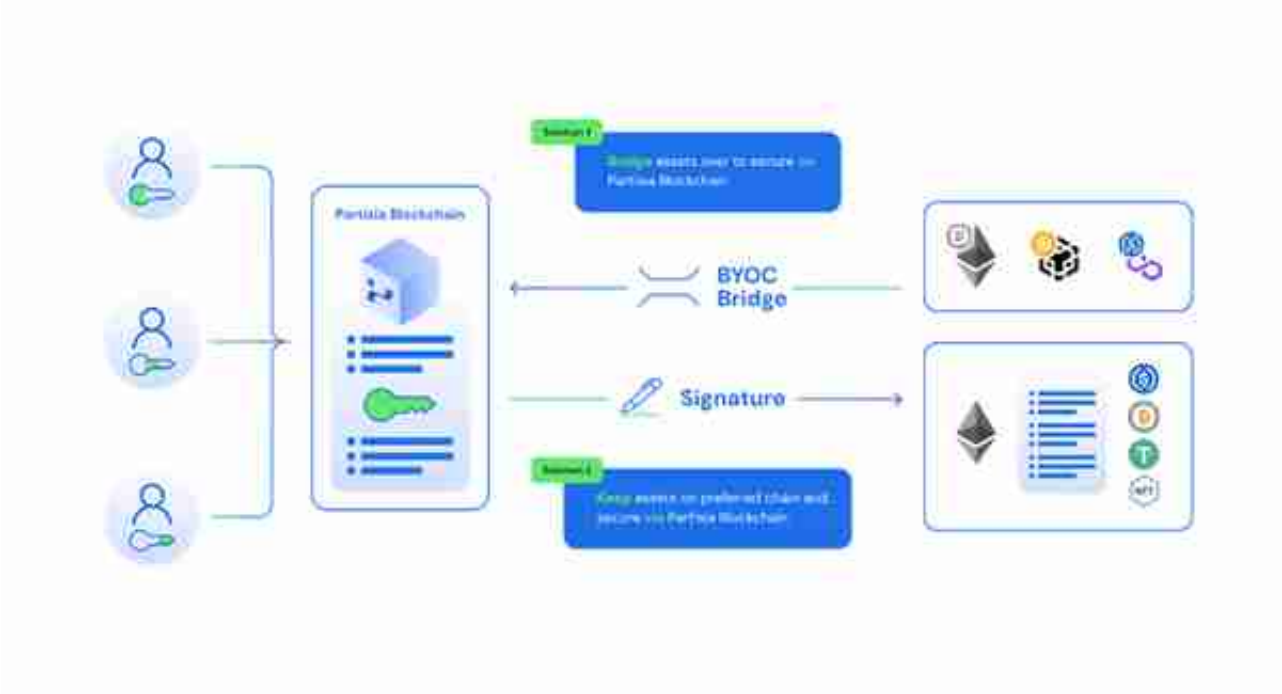
与其他解决方案不同，MOCCA 方案是直接部署在链上的，基于 MPC 方案，其要求每笔交易必须经过两方或以上的批准，并允许参与者积极参与治理并直接在链上签署交易。而这种方式在去中心化上，优于在链下生成签名的 TSS
协议，并提供了类似于公链的可修改性、可信协作平台。

l 具备隐私的合约功能

Partisia 通过通用隐私保护计算、智能合约自动化来实现以私有数字代理为基础的数据驱动型经济，让用户自主设定数据信息并提高议价能力，即智能合约可以被选择为隐私智能合约，或仅向某些账户披露信息的智能合约，以服务于某些私有业务。在这一模式下，任何开发者都可以轻松利用零知识证明（ZK）或多方计算（MPC）服务，同时也为链上隐私保护提供了一套完整的技术堆栈。

MOCCA 方案继承了该特性，即了零知识智能合约的概念，使得私有计算成为可能。这一独特功能确保了关于哪个密钥碎片启动了交易的保密性，并保持了治理投票的秘密输入，资产管理者也能够在不透露资产详情的情况下，开展一些业务交易，有助于保护大量资金免受潜在威胁。

此外，Partisia Blockchain 基于 Oracle 服务框架，具备原生的跨链互操作特性，能够进一步扩展区块链功能进行支持，使其与外部数据源交互，进一步加强了多链资产管理的适配。原生的跨链互操作特性，也为多链资产管理提供了可信、安全的支持。



Partisia Blockchain 首席技术官 Peter Frandsen 也表示：

“MOCCA 解决方案标志着去中心化托管演化的重要里程碑，它解决了传统智能合约和中心化的当前限制。MOCCA 为机构和组织提供真正的去中心化、先进的可编程性以及在多个链上保护数字资产的灵活性。得益于我们数十年在多方计算（MPC）方面的专业知识，这一产品体现了我们致力于提供重新定义安全性、合规性和区块链空间创新标准的前沿解决方案的承诺。”

在系列前沿技术的加持下，MOCCA 方案正在推动资产管理领域，从静态智能合约向去中心化、可编程托管方案的转变。在包括 MPC
在内的系列创新技术的保障下，确保了对多个区块链的无缝支持。MOCCA
有望进一步为包括 DAO、投资俱乐部、钱包提供商、交易所在内的各种实体，以及需要无信任协作的场景，寻求真正去中心化、安全、高效的定制化的资产管理方案。