



多平台时代 的链下治理

Witness

去中心化治理



去中心化平台

Decentralized
platform



去中心化治理

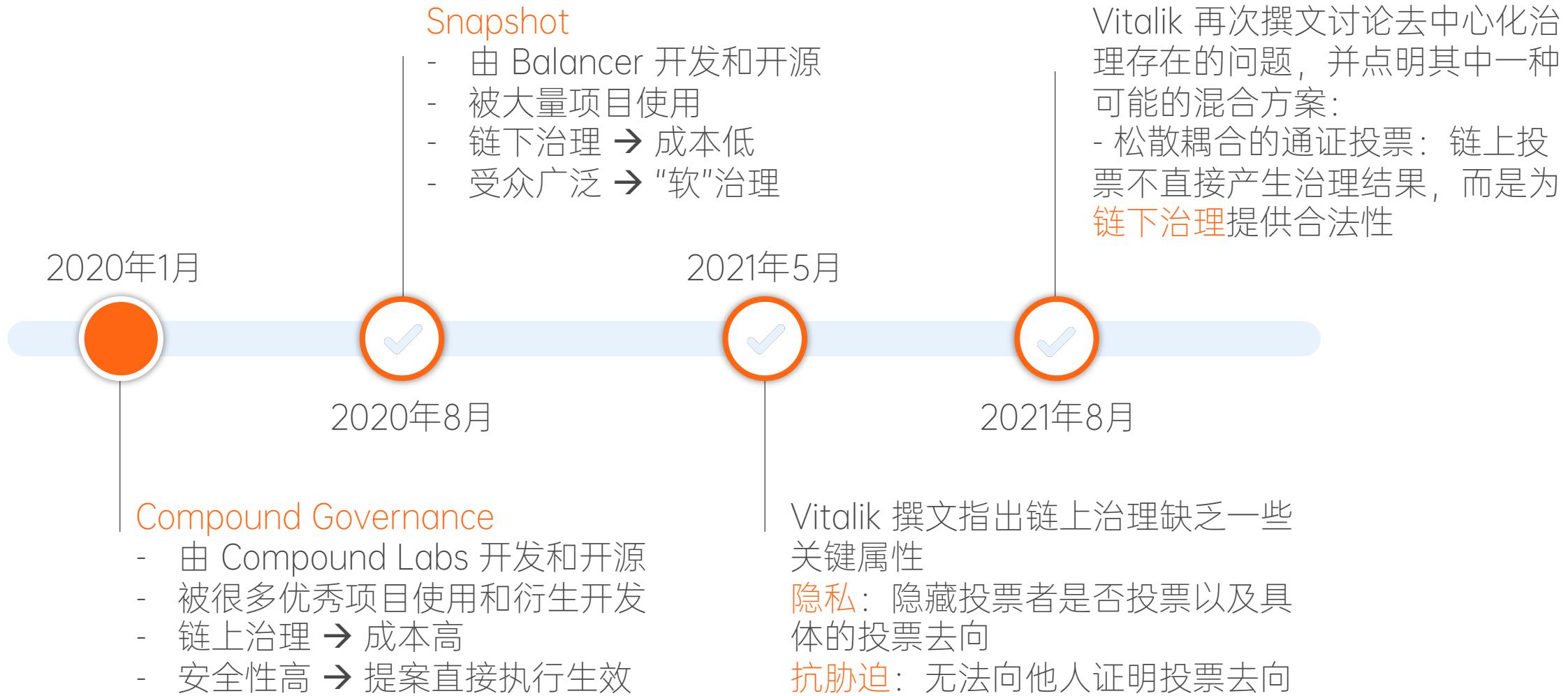
Decentralized
governance



去中心化自治组织

Decentralized
Autonomous Organization

发展与讨论



面临的问题

优点

链上投票

链上分布式化计算
无需依赖第三方组件
安全性保证

缺点

费用高昂

对小资产用户不友好
公平性有所损失
多平台聚合性差

共性问题

链下投票

投票低成本
公平性保证
通过去中心化存储来增加数据安全性

计算节点无监督

计算过程存在恶意篡改的可能

隐私、抗胁迫

Witness: 链下，隐私，多平台



链上存储

Workspace 和 Proposal 存储于合约中

链下计算

结合 Intel SGX 可信硬件和 Oblivious RAM 算法技术，
保证计算过程无法被窥探，计算结果不可被修改

链下投票

最终由可信节点把投票结果提交至合约中，实现用户零成本投票

隐私扩展

支持 Private Voting 和 Public Voting

多网络

支持常用区块链网络，如 Ethereum, BSC, Polygon, Darwinia, Astar 等

投票结果对应行为触发

支持对投票选项设定对应的 hooks 作为回调，自动执行投票结果

Witness: 链下投票治理



Witness: 链下投票治理



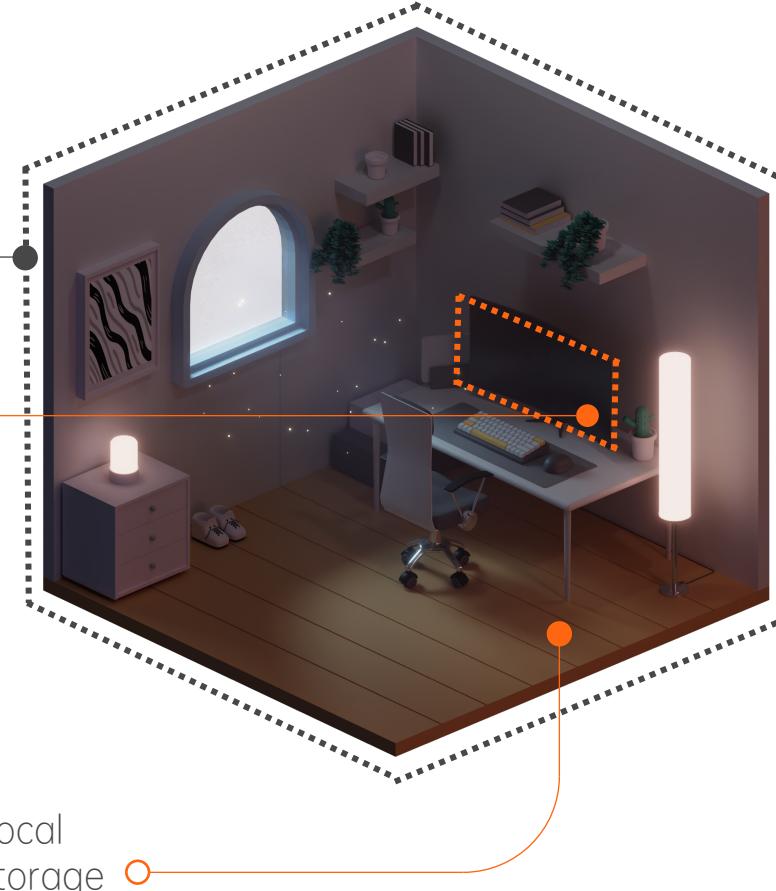
项目演示

Witness |

Witness 的技术基石: DRAM + TEE

TEE 创建了独立的可信执行环境, Enclave

Oblivious RAM 隐藏了Enclave到存储的数据访问模式



禁用未授权的访问

访问保护, 数据加密



Remote
storage



Local
storage

謝謝聆聽 欢迎提問
的鏈下治理