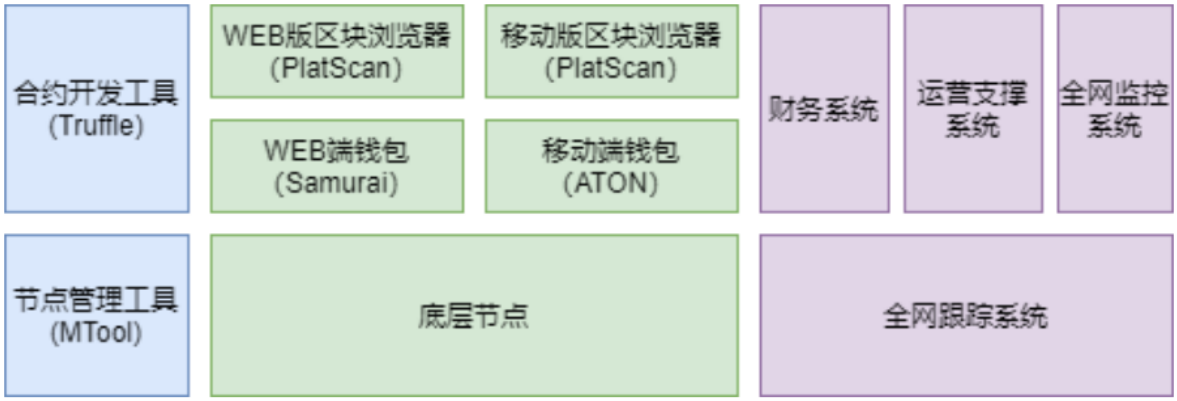
PlatON上线进展和后期规划

PlatON主网进展

PlatON产品架构如下：



PlatON的特性跟Alaya一致，主要在一些参数上存在差异：

1. 按PlatON经济蓝皮书，在Token总量、增发比例等经济参数与Alaya不同
2. 扩大了候选验证人数量和共识节点数量，修改为排名201成为候选验证人，并每次从中随机选取43个作为共识节点
3. 为增加网络安全性提高作恶节点的成本，相对于Alaya，PlatON增加了零出块处罚的数量（相当于10000LATs，此参数可通过治理调整）
4. ATON和PlatScan增加NFT的支持

目前主网上线技术工作进展如下：

1. 各产品版本已经完成开发，并完成详细的功能、性能、安全测试，钱包和底层请外部安全公司进行安全审计

   Truffle、Samurai、运营相关系统（财务系统等）还在进行测试，计划正式上线前完成
2. 开发者和用户使用手册完成，并邀请社区进行review和试用，进行持续优化
3. 正在进行第四轮整体上线演练，演练过程也邀请部分社区节点参与
4. 目前所有技术准备已完成，定于在北京时间4月25日 中午12点29分正式启动上线

PlatON后期技术规划

PlatON底层上线后的主要技术规划是在以下四方面进行加强：

安全性

1. 增加验证人选取的随机性

   除了VRF，计划结合可验证秘密分享PVSS、BLS等密码算法增加随机性，方案还在调研设计中。
2. ATON和Samurai支持硬件钱包

   主要支持Ledger、Trezor两类主流硬件钱包，计划在上线后支持。

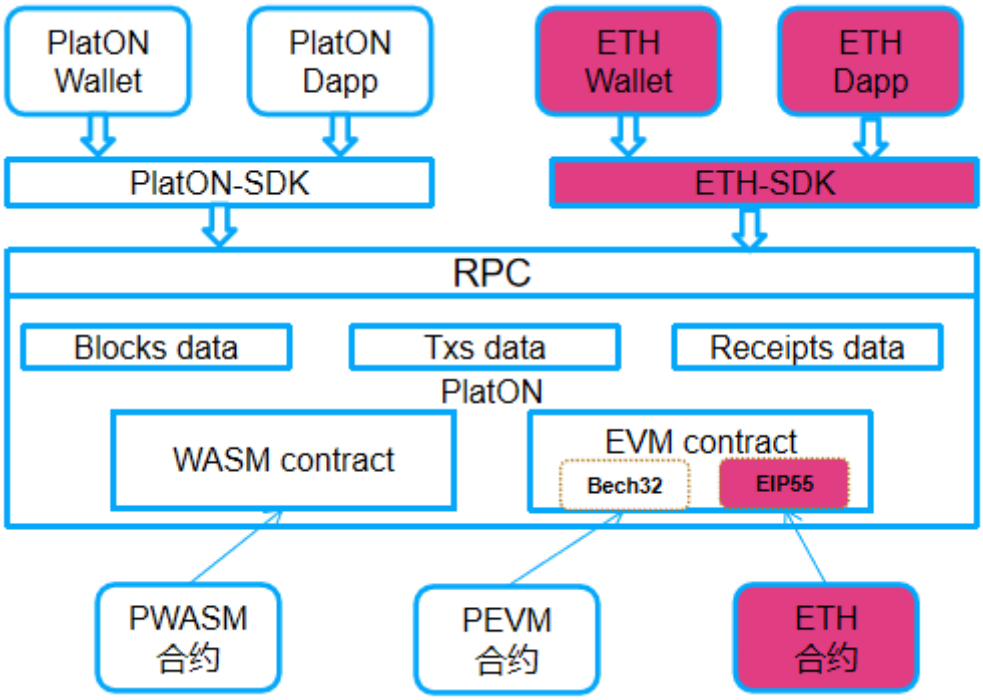
去中心化与性能

现在的机制是质押排名前201的成为备选节点（实际上这些节点都有机会选为验证节点），然后每8分钟左右从201中更换选取43个验证节点进行BFT出块。后续计划增加这两个数量：

1. 备选节点数量：计划支持10000个节点以上，计划修改为根据质押LAT数、交易数、出块率等因素动态调整备选节点数量，增加节点作恶成本，降低被攻击的风险
2. 验证节点数量：随着验证节点数量的增加，网络容错性和安全性相应增加，但是BFT共识的性能相应下降，目前我们在验证一个BFT共识的优化方案，在支持更多验证节点的情况下，性能没有明显的损耗，但是考虑到DDOS攻击的时间窗口，参与BFT验证节点数量不能太大，计划支持到200个节点

以太坊兼容

为吸引ETH/BSC上的生态项目，使得ETH/BSC上的项目和dapp可以无缝移植到PlatON，后期计划在地址和API接口上全面兼容以太坊，做以下修改：



1. EVM虚拟机

   EVM虚拟机的指令集计划定期同步以太坊，保持跟以太坊一致，目前已经支持到以太坊柏林版本。

   EVM中的地址计划同时兼容PlatON和以太坊的地址格式。PlatON的私钥和地址生成算法跟以太坊是一致的，主要是地址格式不同，PlatON用Bech32格式地址，以太坊用EIP55格式。

   以太坊合约如果需要迁移到PlatON，还会有很少部分（使用较少）需要调整或有影响：

   - Token单位：以太坊是ether/wei，PlatON是lat/von
   - 部分fake函数：因共识机制不同，block.difficlty、miner.setCoinbase等函数在PlatON为fake实现，使用到这些函数的合约可能不适合在PlatON上运行，需要进行相应调整，不过这些函数很少使用

2. RPC接口

   RPC接口计划全面兼容以太坊协议，原有的以太坊钱包、DAPP等可以直接使用原有的以太坊SDK接入到PlatON。

3. PlatON-SDK

PlatON-SDK计划兼容以太坊的EIP55地址，钱包和DAPP等应用可直接使用以太坊地址调用PlatON-SDK接入PlatON。

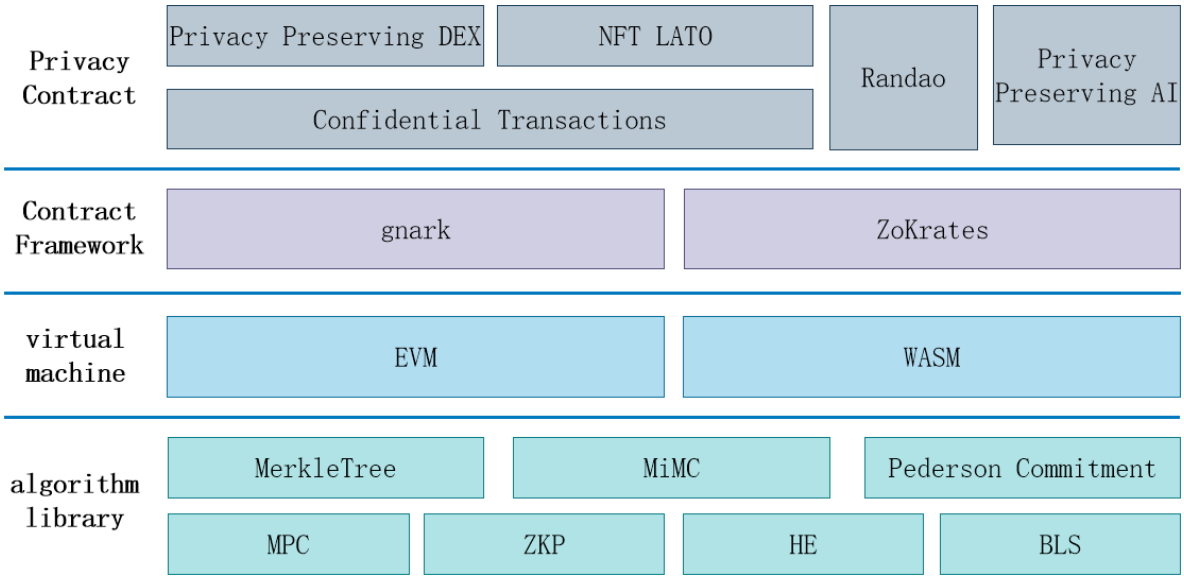
经济模型优化

目前计划还有几个经济相关的调整：

1. 解委托锁定：解委托不实时赎回，需要锁定一段时间后才能到账。
2. GPO（Gas Price Oracle）机制：对于预估交易Gas，PlatON和Alaya沿用了以太坊的GPO（Gas Price Oracle）机制，由于单个区块Gaslimit和出块速度不同，需要进行调整
3. 治理提案交易价格机制：PlatON和Alaya中的'提案'交易的价格不是通过GPO获取的，也不能由用户自定义，而是由系统固定限制的，这样做的目的是为了避免提案被恶意占位，但是可能交易成本过高，且极有可能对客户端估算gas产生影响，考虑增加一种提案白名单机制来替换当前任意节点可发起提案的机制
4. 默认的Gasprice：可能上线相当长时间内，由于有足够的出块奖励和Staking奖励，节点可能都不会调整Gasprice，因此默认的Gasprice直接影响交易成本，目前转账的交易成本0.000021LAT，相对于其他公链相对较低，但这也带来更大的DDOS攻击风险，后续需要进行调研分析并调整，长期上考虑参考stateless区块链等动态调整Gasprice的方案。

合约开发能力

主要计划在虚拟机底层集成更多的合约开发能力：



1. 安全随机数

   在虚拟机底层提供基于VRF的随机数，以及基于Randao基础合约的随机数。

   目前已经完成基于Randao基础合约的随机数，进一步测试后计划准备上线。

2. 隐私算法库

   在虚拟机底层集成ZKP/HE算法库，移植以太坊的gnark和Zokrates ZKP合约框架，并在基础上。

   目前已经开发完成，进一步测试后计划准备上线。

3. 隐私合约

   实现隐私交易以及相应的隐私Token、隐私NFT标准（隐私加强版的ERC20、ERC721）、隐私DEX。

   隐私交易及隐私Token标准已经开发完成，进一步测试后计划准备上线。隐私NFT、隐私DEX正在做算法和产品设计。

隐私计算网络

隐私计算网络为PlatON的二层网络，网络由数据节点、计算节点、服务节点、调度节点组成，构成去中心化的数据、算法和算力交易市场，隐私合约的输入数据保存在数据节点本地，由数据节点通过秘密分享给到多个随机计算节点，计算节点在链下以安全多方计算方式进行隐私计算，链上进行交易清结算、去中心化调度和全流程存证审计。

目前完成产品设计，正在进行技术架构设计和开发，计划在7月份发布网络，之前计划发布白皮书、demo和测试网络。

PlatON上线后的技术升级计划

升级策略

所有新技术特性都先在Alaya先行网升级验证，再升级到PlatON主网。

底层节点版本升级需要提案治理升级。

升级计划

初步规划升级计划如下：