Blockchain Hw 5

16340041 陈亚楠

区块链技术拥有去中心化、不可篡改、可编程等特点，这使得其在数字支付、分布式存储、征信、供应链、金融等领域中拥有广泛的应用前景．然而当前的区块链系统存在严重的可扩展性瓶颈，主要为交易吞吐量不足和链与链之间的资产（数据）难以交互两方面，都限制了区块链技术的应用。

当前针对区块链性能提升的主流方案主要包含 3 类：

（1） 链下支付网络技术，涉及经典闪电网络及其相关改进方案：链下支付网络通过将大量交易离线处理，同时将区块链作为仲裁平台，处理通道支付过程中的异常情况，如双方对通道的状态有分歧等，其间接地提升了系统的交易吞吐量。 闪电网络是最早的通过链下支付通道形成支付网络、提升区块链交易吞吐量的方案。闪电网络主要包含 2 个协议 RSMC 和 HTLC。其相关其他方案主要是在 2 个协议上进行修改，针对闪电网络的改进主要包含效率、支付成本、通信开销、可持久化、寻路算法等，包含 Duplex 支付通道协议、Raiden network、Sprites 以及可持久化机制 4 种方案。

（2） Bitcoin—NG 方案：将原先比特币中的共识过程拆分成记账人选取和交易排序 2 个阶段，通过记账人选取阶段保证区块链安全性，在交易排序阶段由记账人进行大量交易数据的处理。其在保证了分布式一致性的基础上，提升了一轮共识过程中的交易确认数，从而在区块链上增加交易吞吐量。

（3） 分片机制：通过将全网节点划分成不同的集合，每个集合并行地进行共识，确认交易，从而使得系统的交易吞吐量随着全网中参与共识节点的增加而近似线性地增加 。

侧链技术是一种可以使数字资产在多条区块链之间安全转移的技术。当数字资产在主链上被锁定时，该资产可以在侧链内自由转移，不需要与主链进一步交互，从而减少对主链存储与计算资源的使用。

数字资产从主链转移到侧链的过程依赖于一种多重签名交易脚本。多重签名交易脚本通过记录 N 个公钥实现锁定，该脚本至少需要得到与公钥对应的 M 个签名才可以满足解锁交易的条件。M 是使多重签名生效的签名数阈值。执行签名的成员称为公证人，而区块链矿工负责执行脚本。

数字资产转移过程中，主链上的一个节点通过执行脚本发送带有IV名公证人公钥的锁定交易，锁定交易使得该交易所包含的数字资产不再进入其他智能合约的流程。侧链矿工等待一个确认期，确保锁定交易得到足够多的确认，用以验证其真实存在。在验证锁定交易真实存在后，执行多重签名交易脚本。当其中 M 个公证人执行签名后，数字资产得以解锁并发送给侧链上的数字资产持有人。如果需要将数字资产返回给主链上的节点，则由侧链上的数字资产持有人发送锁定交易，经过同样的过程完成转移。