Open Storeman 方案节点恶意行为分析

Demmon 2020/4/20

作恶阶段	恶意行为	影响结果	解决方案
锁定账户建立阶段	不向合约提交多项式承诺	协议无法进行下去	1. 设置最大等待时间 2. 超时移出 Group 3. 对押金进行 slash 4. 启用候补节点，重启整个协议
	不提交加密数据到合约		
	向诚实节点发送错误加密数据	诚实节点将无法计算得到争取的私钥碎片	1. 数据接收方向合约进行接收数据合法性反馈 2. 允许重新提交数据 3. 超过最大提交次数，则进入挑战模式 4. 挑战模式中将暴露作恶者，对其本金进行 slash，并移出 Group 5. 启用候补节点，重启整个协议
	恶意节点合谋，互发错误数据，但是向合约确认数据合法	若私下传输正确数据，则只是合约内存了错误的加密数据，不影响锁定账户建立	——
		若私下未传输正确数据，则诚实节点不受影响，接收错误数据的恶意节点无法计算得到正确私钥碎片，因此永远无法参与跨链签名	1. 这种攻击无法鉴定 2. 通过增加基金会控制节点数量，来降低降低签名碎片不足的风险
	恶意节点合谋，选择随机数时候进行协商	合成锁定账户私钥部分信息被恶意节点掌握	1. 这种攻击无法鉴定 2. 保证诚实节点对锁定账户私钥的贡献即可
签名阶段	跨链交易信息的伪造，如金额、接收地址等	业务逻辑错误，资金丢失等	1. 跨链交易构造由 Leader 完成 2. Leader 从白名单中选取，为基金会控制
	构造跨链交易的节点宕机或者离线	跨链流程停滞	1. 白名单中有多个 Leader 节点 2. 第一个宕机后，后边进行替补，构造跨链交易
	恶意节点不发签名碎片	仍合成出完整签名，跨链不受影响	1. 未发签名碎片的恶意节点活性将会降低，影响其收益
		无法合成完整签名，跨链流程停滞	1. 对未发送签名碎片的节点进行 slash、 2. 提高基金会控制节点数量，降低此种情况发生概率
	恶意节点发送错误签名碎片	导致最终合成的签名错误	1. Leader 节点通过链上信息能够验证签名碎片的合法性 2. 发送错误签名碎片的节点会被 Slash
	Schnorr 签名过程中协商参数 r 时作恶，不发送或者发送错误数据	r 如果全部由恶意者贡献，会导致锁定账户私钥泄露，而恶意节点不发数据或者发送错误数据，会导致跨链流程停滞	1. 最终使用的 r 一定要有诚实节点贡献的部分!!! 2. 设立举报机制，如果节点可以将私下收到的错误数据向 Leader 举报，然后 Leader 验证后写入合约对发送者进行 slash 3. 关于 r 的决定方式，有两种思路：第一种是需要全部节点参与，这种方式逻辑简单，但是会导致跨链成功率低；第二种是只要超过门限数量的节点参与即可，其中要包括诚实节点，这种实现方式的难点在于如何在不同节点之间对这个集合进行统一一致
奖惩相关	故意不收集其他节点的签名碎片	导致其他节点活性下降，收益降低	1. Leader 负责签名碎片的收集，由基金会控制，不会出现恶意行为 2. 未来开放 Leader 节点后，这部分工作可以放到链上进行，但是要考虑效率
	作恶数据伪造	会对节点进行错误的 slash	1. 发送数据均需签名，防止伪造 2. 合约对作恶数据进行验证，通过后才会接收