



(12) 发明专利申请

(10) 申请公布号 CN 115664749 A
(43) 申请公布日 2023. 01. 31

(21) 申请号 202211274486.9
(22) 申请日 2022.10.18
(71) 申请人 东南大学
地址 210096 江苏省南京市玄武区四牌楼2号
(72) 发明人 李必信 何嘉昊 胡甜媛
(74) 专利代理机构 南京众联专利代理有限公司
32206
专利代理师 杜静静
(51) Int.Cl.
H04L 9/40 (2022.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 67/10 (2022.01)

权利要求书3页 说明书8页 附图1页

(54) 发明名称
一种基于可信执行环境的Fabric数据隐私
保护方法
(57) 摘要

本发明涉及一种基于可信执行环境的Fabric数据隐私保护方法,具体如下,首先,根据可信执行环境机密以及不可篡改的特性,通过可信执行环境完成用户节点交易会话密钥的生成,同时,使用用户节点的公钥对会话密钥加密,以保证除用户节点外其他节点无法获取交易会话密钥。其次,通过对称加密的方式实现用户节点与可信执行环境之间交易数据的安全传输,使用三个以上的可信执行环境对交易进行模拟执行保证了背书过程不会因拒绝服务攻击而中断。最后,交易数据中包含的随机数可以用作合约正确执行的验证。该方案提出基于可信执行环境进行智能合约的模拟执行,能够保证Fabric交易数据的全过程隐私,保证了可信执行环境的可用性。

