(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113726733 A
(43)申请公布日 2021.11.30

(21)申请号 202110815893.5

(22)申请日 2021.07.19

(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
代理人 杜静静

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/62(2013.01)
G06F 21/60(2013.01)

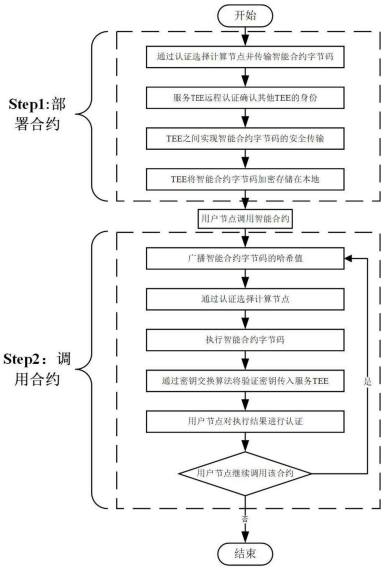
权利要求书3页 说明书10页 附图1页

(54)发明名称

一种基于可信执行环境的加密智能合约隐私保护方法

(57)摘要

本发明公开了一种基于可信执行环境和加密的智能合约隐私保护方法,包含合约部署与合约调用两个步骤。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智能合约字节码的加密部署,同时通过认证中心确认不同计算节点上可信执行环境的身份是否合法,在两个合法的可信执行环境之间实现智能合约字节码的安全传输。其次,智能合约字节码的执行也是发生在可信执行环境中,通过密钥交换算法实现用户节点与可信执行环境之间验证密钥的安全传输,可信执行环境使用验证密钥对执行结果进行签名,用户节点通过签名确保合约执行的正确性。该方案解决了之前方案中存在的智能合约代码隐私泄露以及计算节点承载TEE的身份不合法的问题。



CN 113726733 A