



(12) 发明专利申请

(10) 申请公布号 CN 113469685 A

(43) 申请公布日 2021. 10. 01

(21) 申请号 202110815086.3

H04L 9/30 (2006.01)

(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 尹昊 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.

G06Q 20/38 (2012.01)

G06Q 40/04 (2012.01)

G06F 21/60 (2013.01)

G06F 21/62 (2013.01)

H04L 9/08 (2006.01)

权利要求书1页 说明书5页 附图2页

(54) 发明名称

一种以太坊交易金额加密和交易混淆的隐私保护方法

(57) 摘要

本发明公开了一种以太坊交易金额加密和交易混淆的隐私保护方法,首先,应用交易发送方的公钥对交易金额进行加密,使交易金额不在链上公开,保护交易金额的隐私;其次,通过随机选取混淆账户,生成的混淆交易形成一个环状交易组;最后,将原交易和混淆交易通过矿工打包上链。本方案运用以太坊固有的公钥和私钥机制,安全度高。混淆交易通过增加混淆账户,与原账户生成混淆交易,形成一个交易环,保证无关人员无法确定原交易。

