

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2022/237558 A1

(43) 国际公布日
2022 年 11 月 17 日 (17.11.2022)

- (51) 国际专利分类号:
G06F 21/62 (2013.01) G06F 21/60 (2013.01)
- (21) 国际申请号: PCT/CN2022/089887
- (22) 国际申请日: 2022 年 4 月 28 日 (28.04.2022)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202110511543.X 2021 年 5 月 11 日 (11.05.2021) CN
- (71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。蚂蚁区块链技术 (上海) 有限公司 (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) [CN/CN];

中国上海市黄浦区外马路 618 号 8 层 803 室, Shanghai 200010 (CN)。

- (72) 发明人: 刘佳伟 (LIU, Jiawei); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。沈陈侃 (SHEN, Chenkan); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。金戈 (JIN, Ge); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。张翅飞 (ZHANG, Chifei); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。孔繁盛 (KONG, Fansheng); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。
- (74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市

(54) Title: BLOCKCHAIN-BASED USER ELEMENT AUTHENTICATION METHOD AND APPARATUS

(54) 发明名称: 一种基于区块链的用户要素认证的方法及装置

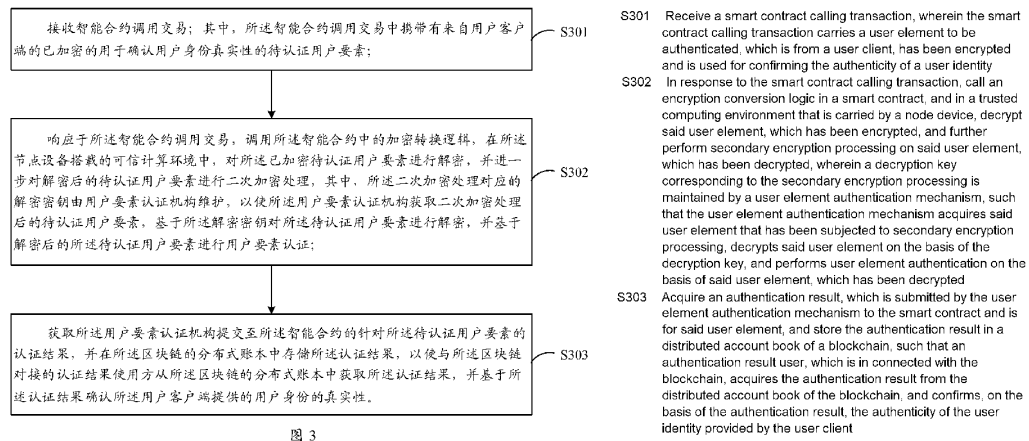


图 3

(57) Abstract: A blockchain-based user element authentication method and apparatus. The method is applied to a node device in a blockchain, and comprises: receiving a smart contract calling transaction, wherein the smart contract calling transaction carries a user element to be authenticated, which has been encrypted and is from a user client; in response to the smart contract calling transaction, calling an encryption conversion logic in a smart contract, and in a trusted computing environment, decrypting said user element, which has been encrypted, and performing secondary encryption processing on said user element, such that a user element authentication mechanism decrypts said user element, and performs user element authentication; and acquiring an authentication result submitted by the user element authentication mechanism, and storing the authentication result in a blockchain, such that an authentication result user party, which is connected with the blockchain, acquires the authentication result from the blockchain, and confirms, on the basis of the authentication result, the authenticity of a user identity provided by the user client.

[见续页]

海淀区上地三街9号嘉华大厦B座409,
Beijing 100085 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种基于区块链的用户要素认证方法及装置; 所述方法应用于区块链中的节点设备, 包括: 接收智能合约调用交易; 其中, 所述智能合约调用交易中携带有来自用户客户端的已加密的待认证用户要素; 响应于所述智能合约调用交易, 调用所述智能合约中的加密转换逻辑, 在可信计算环境中对所述已加密待认证用户要素进行解密并进行二次加密处理, 以使所述用户要素认证机构对所述待认证用户要素进行解密, 并进行用户要素认证; 获取所述用户要素认证机构提交的认证结果, 并在所述区块链中存储所述认证结果, 以使与所述区块链对接的认证结果使用方从所述区块链中获取所述认证结果, 并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。