基于区块链的零知识位置证明方法研究

余荣威[①②] 周博孝*[①②] 王丽娜[①②] 朱欣焰[③] 谢辉华[①②] 谢红军[④]

[①](武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)

[②](武汉大学国家网络安全学院 武汉 430072)

[③](测绘遥感信息工程国家重点实验室 武汉 430072)

[④](矩阵元技术(深圳)有限公司 深圳 518000)

摘 要：地理位置虚拟软件泛滥、民用卫星定位信号易模拟或篡改，致使地理位置可信认证难以实现。针对已有位置证明方案采用中心化架构存在单点失效和易引起集中攻击等安全风险，该文引入去中心化范式思路，利用区块链具有的去中心化、不可篡改、可追溯等特点，并结合零知识证明协议，提出了基于区块链的零知识位置证明方法，实现了以去中心化、保护隐私、高度准确、审查抵制的地理位置认证服务，从而确保用户所提供位置的准确性。该方法不仅能消除中心化位置证明的弊端，确保位置数据的机密性，而且被证明位置数据一旦上链后不可篡改，实现了不可抵赖性。测试分析结果表明：完整的证明流程(包含证明生成验证和上链全过程)实际测试每次平均用时约5 s，其中证明生成和验证的总耗时是50.5～55.5 ms。因此，算法具有较好的性能开销，可满足实际应用需求。

关键词：位置证明；区块链；零知识证明；智能合约

中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)09-2142-08

DOI: 10.11999/JEIT191054

Zero-knowledge Location Proof Based on Blockchain

YU Rongwei[①②] ZHOU Boxiao[①②] WANG Lina[①②] ZHU Xinyan[③]
XIE Huihua[①②] XIE Hongjun[④]

[①](*Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education*, *Wuhan University*, *Wuhan* 430072, *China*)

[②](*School of Cyber Science and Engineering*, *Wuhan University*, *Wuhan* 430072, *China*)

[③](*State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing*, *Wuhan* 430072, *China*)

[④](*Juzix Technology*, *Shenzhen* 518000, *China*)

Abstract: Due to the proliferation of geographic location virtual software and the easy simulation or tampering of civil satellite positioning signals, it is difficult to realize the trusted authentication of geographic location. In view of the security risk of single-point failure in the existing location certification scheme using centralized architecture, a zero-knowledge location certification method based on blockchain is proposed, combining with zero knowledge certification protocol, to achieve a decentralized, privacy protected, highly accurate, review offset geographic location certification service, so as to ensure the accuracy of the location provided by users. This method not only ensures the confidentiality of the location data, but also proves that the location data can not tamper once it is linked. The results of the test analysis show that the average performance of the whole proving process is about 5 s/time, and the total time of proof generation and verification is 50.5～55.5 ms. Therefore, the algorithm has better performance overhead, which can meet the actual application requirements.

Key words: Location proof; Blockchain; Zero-knowledge proof; Smart contract

收稿日期：2019-12-30；改回日期：2020-08-10；网络出版：2020-08-19

*通信作者： 周博孝 boxiao@whu.edu.cn

基金项目：国家自然科学基金(U1836112, 61876134)

Foundation Items: The National Natural Science Foundation of China (U1836112, 61876134)

1　引言

随着导航定位技术的成熟发展，位置设备或装备(如智能手机、智能机器人等)得到了广泛的实际应用，定位方式也得到不断拓展，比如卫星定位、WiFi、基站等。但民用卫星定位信号未加密验证，地理位置虚拟软件泛滥，无线定位威胁频发，使其变得可欺骗和可更改；此外，在室内、地下室或城市高楼密集区定位几乎不能获取精确位置信息，且基于WLAN或基站的定位精度较低但速度较快卫星定位，使得定位能力覆盖有限。因此，如何实现覆盖外的位置可信性验证成为了当前信息安全领域的技术难点。位置证明[1,2](Proof of Location, PoL)是审查抵制的地理位置可信认证服务，验证所提供位置的准确性。文献[3–6]主要采用中心化体系架构来实现位置可信性认证，从而解决位置数据易欺诈、卫星定位覆盖有限、无线定位威胁频发等问题，但中心化架构存在节点失效等安全风险。Khan等人[7]设计的方案是采用中心化设施的典型，其中用户与见证者通信需要名叫位置权威的基站，所有的通信都需要通过该基站，位置证明成功后该基站给用户颁发证书。

具有去中心特点的区块链技术为位置证明提供了一种新的途径。区块链[8]是分布式数据存储、点对点传输、共识机制、加密算法等新型应用模式，在多方共享、统一维护、数据沿袭和追踪审计等方面有着明显优势。近年来，区块链技术引起了各国政府的高度重视，比特币[9]、以太坊[10]、EOS[11]和矩阵元[12]等区块链平台也逐步在行业得到应用。目前，国外初创公司正在创建位置证明区块链，通过发布加密货币鼓励用户参与，一些发达国家在此方面取得了一些初步成果，而国内尚处于起步阶段。国外的XYO[13]和FOAM[14]方案是与基础设施相关，在确定的地理位置安放地理标签，但是通过设置地理标识有很大的局限性；而与基础设施无关的方案则不需要提前构建位置证明的基础环境，提供位置证明服务时仅依靠证明者周边的信息确认地理位置，Nasrulin等人[15]提出在位置证明协议中通过访问控制模型的实现进行检测，并利用一组验证规则来创建和验证时空数据点，目前该方案只处于概念验证阶段，离成熟商用还有很长的一段距离。

分析发现，目前这些方案大多基于硬件设备，虽然它们通过经济奖励机制来鼓励用户安装硬件设备，但要做到大范围密集部署与管理这些设备，仍然是一个很大的挑战。本文引入去中心化范式思路，利用区块链具有的去中心化、不可篡改、可追溯等特点，并结合零知识证明协议[16]，提出了基于区块链的零知识位置证明方法，满足位置可信的地理位置认证，具有去中心化、保护隐私、高度准确和审查抵制等属性。该方法不仅能消除中心化位置证明的弊端，确保位置数据的机密性，而且被证明位置数据不会被篡改，防止否认历史位置数据，实现了不可抵赖性。

2　系统模型

本节将讨论系统的威胁模型和整体的协议流程。其中本文设计的系统结构如图1所示，手机APP通过位置证明请求与区块链进行交互。证明者是发起位置证明请求的用户，而见证者为参与位置证明的用户。证明者首先发起请求，证明者和见证者分别

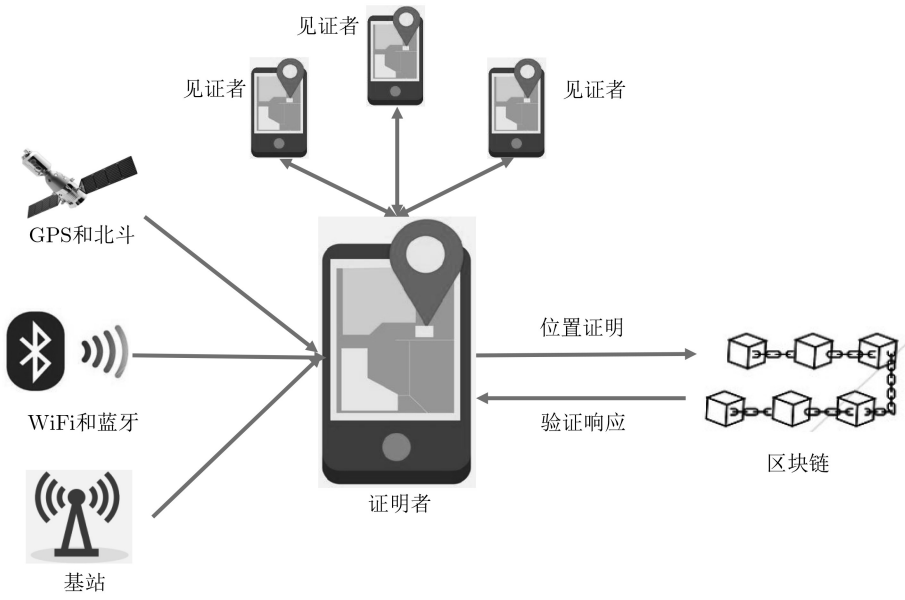

图 1 系统结构图

根据多源定位获取位置信息，其获取方式可包括：GPS、北斗卫星、WiFi、蓝牙和基站等，证明者的位置证明请求通过调用智能合约来处理和计算数据。

2.1 威胁模型

对于基于区块链的位置证明，任何人均可以通过公开的接口查询区块链数据和开发相关应用，因此已有的网络攻击都可能发生，例如DOS攻击、利用协议漏洞获取控制权等。此外，位置证明服务提供商可能利用用户历史位置数据，在用户不知情的情况下，私自用作其它用途。针对网络攻击已有大量研究工作，本文不做赘述。本文为构建合理的威胁攻击模型，现作如下假设：

(1) 本文主要研究位置证明协议，假设证明者和见证者设备本身是可信的；

(2) 证明过程中所需的见证者通过安全随机方式选取，是诚实的；

(3) 证明人对自己的设备有完全控制权，可对设备上存储的数据做任何操作，包括删除、修改、插入等，假设证明人用户可能是恶意的，如位置虚拟软件篡改；

(4) 假设证明者和见证者能访问所有彼此的公钥。

2.2 协议流程

流程中负责生成零知识生成和区块链交互的被称为验证者。位置证明流程分为10个步骤，如图2所示。

第(1)步搜索见证者：若证明者和见证者同时处于同一局域网下，可通过WiFi或者P2P等方式进行通讯；否则通过服务器转发消息或蓝牙P2P通讯的方式进行。在同一局域网场景下，当证明者需要证明自己的位置时，首先搜索到与自己在同一局域网下的所有见证者；若不在同一局域网下，则需要通过服务器来转发消息的方式来通知其他见证者，以达到搜索的目的。于是证明者搜索见证者并发送请求准备和见证者保持通信。查询请求如式(1)

$$\mathrm{SR} =< \mathrm{TS}, \mathrm{ID} > \tag{1}$$

式中，请求中包括时间戳TS和身份标识ID，标识包括设备的信息与加密后的用户信息等。

第(2)步见证者的回应：见证者接收到请求，并回复是否愿意保持通信，见证者回复的结果存在R中，回应如式(2)

$$\mathrm{SRp} =< R > \tag{2}$$

式中包含回应结果R。

第(3)步位置证明请求：如果有多个见证者能够通信，证明者采取一定的策略来挑选见证者，并向它们发送位置证明请求。位置证明请求如式(3)

$$\mathrm{LR} =< \mathrm{TS}, \mathrm{ID} > \tag{3}$$

式中包含时间戳TS和身份的标识ID等。

第(4)步见证者返回位置信息：见证者收到位置证明请求后，首先对证明者的身份进行验证，若验证通过，则根据多源定位的方式获取自身位置。当在室外时，可以通过GPS获取自身位置。当在室内时，可先尝试用GPS获取位置，当GPS信号较弱

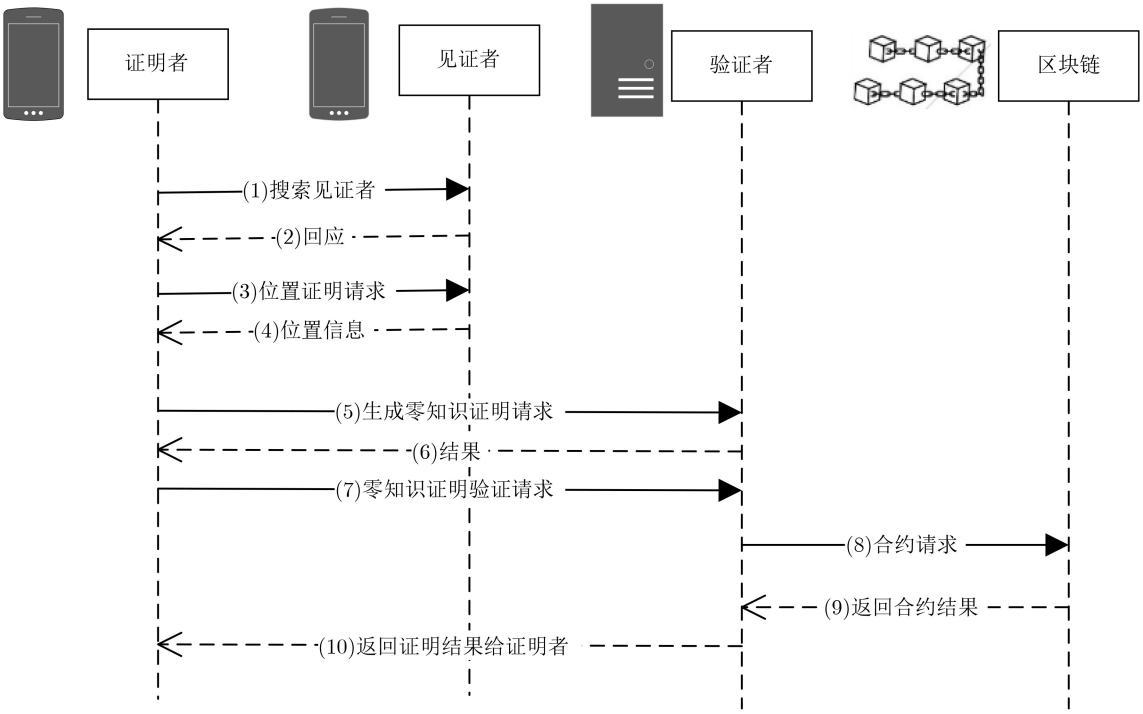

图 2 位置证明时序图

时，可通过室内布设的WiFi、蓝牙设备获得自身位置。然后使用私钥将自身的位置进行签名返回给证明者，否则返回验证失败信息。位置证明回应如式(4)

$$\mathrm{LRp} =< s_{\mathrm{pk}}(f), h > \tag{4}$$

式中，见证者先取位置信息的哈希值h，然后用私钥对其进行签名。

第(5)步生成零知识证明请求：根据自身位置、见证者的位置和以见证者位置为圆心的阈值半径向验证者发送零知识证明生成请求，生成零知识证明请求如式(5)

$$\mathrm{ZKR} =< \mathrm{pl}, \mathrm{wl}, r > \tag{5}$$

式中包含两个位置pl, wl和一个阈值r。

第(6)步返回零知识证明：验证收到请求后计算零知识证明，并把结果返回给证明者，返回证明如式(6)

$$\mathrm{ZKR} =< \mathrm{zk} > \tag{6}$$

式中zk是零知识证明。

第(7)步零知识证明验证请求：证明者整合所有见证者的零知识证明，然后对零知识证明计算结果用RSA私钥签名，之后将签名后的信息转换为JSON字符串并用AES秘钥进行加密，再用验证者的RSA公钥对AES秘钥进行加密，最后把加密后的数据和秘钥与时间戳等信息封装成证书，然后向验证者发送零知识证明验证请求，请求如式(7)

$$\mathrm{VR} =< \mathrm{en}_k(d), \mathrm{en}_{\mathrm{pk}}(k), \mathrm{TS} > \tag{7}$$

式中包含数据d和秘钥k的密文和时间戳信息TS等。

第(8)步向区块链发送调用合约请求：验证者先获取证明者的公钥，再用私钥解密AES秘钥，用AES秘钥解密然后进行验证签名，如果验签不通过则返回错误给证明者，通过则解密数据获取证书中每个见证者的零知识证明，调用智能合约对每个见证者的零知识证明进行验证，向区块链发送请求如式(8)

$$\mathrm{BCR} =< \mathrm{zks} > \tag{8}$$

式中zks是关于多个见证者的证明集合。

第(9)步返回证明结果：验证者调用完智能合约后，合约返回证书的合法性，即证明是否验证成功，如果验证失败，则返回错误给证明者。向区块链发送计算请求如式(9)

$$\mathrm{BCRp} =< R > \tag{9}$$

式中，R是合约中存储的证书。

第(10)步返回结果给证明者：验证者将最后的验证结果返回给证明者，如式(10)

$$\mathrm{VRp} =< \mathrm{vR} > \tag{10}$$

式中vR是验证结果。

从第(1)步到第(10)步，一直成功执行就算完成了整个位置证明的流程，证明者收到最终的验证结果，见证者也获得了代币奖励。

3　零知识位置证明算法

零知识证明是一种协议，通过它可以简化数字身份验证过程，而不需要使用任何密码或其他有效数据。在证明者不对验证者发送或者传递任何有用的信息的情况下，验证者仍然可以进行验证，判断证明者发送的信息是否正确。本节要介绍的是应用于空间位置信息的零知识证明算法，算法对位置信息(经度、纬度和海拔)进行隐藏，并可以通过计算来验证信息的正确性。

3.1　零知识证明生成算法

算法结合离散对数问题(Discrete Logarithm Problem, DLP)[17]来保护位置隐私不被泄露。DLP令大素数p为群G的阶，群G的任意生成元q，对于未知$\forall g \in Z_p^*$，通过$gq \in G$计算g，该问题在任意的概率多项式时间(Probabilistic Polynomial Time, PPT)成功被解决的概率可以忽略。DLP是一种基于同余运算和原根的一种对数运算，当模N有原根时，设b为模N的一个原根，当

$$a \equiv b^x \mod N \tag{11}$$

$$\log_b a \equiv x \bmod \phi(N) \tag{12}$$

$\log_b a$为a以整数b为底，模$\phi(N)$时的离散对数值。

表1是零知识证明生成算法1，其把证明者的位置和见证者的位置和圆心的半径R作为输入。

在算法1中，通过挑选大数来保证了算法的可靠性，其中主要运算包含大数的模乘和模幂。在第(1)行中生成23个随机大数，第(2)行根据证明者和见证者的经纬度和海拔算出距离差值$\{\alpha_i | i = 1, 2, 3\}$，并计算两个位置的实际物理距离；第(3)行判断证明者是否在以见证者为圆心的圆里面，如果不在圆内则返回空集，在圆内则继续执行， 其中设置阈值半径R的目的是可以对应不同的通信方式来调整最佳的合适距离；接着第(4)行挑选两个大素数相乘得到N，并舍弃掉两个素数；第(5)行中运用了四平方和定理算出4个整数$\{c_i | i = 1, 2, 3, 4\}$，四平方和定理是指每个正整数均可表示为4个整数的平方和。第(7)行使用随机大数l_i等作为隐藏指数c_i的底，c_i作为指数隐藏了起来，再和b_4^k相乘混淆结果，如式(13)

$$b_4^k \prod_{i=1}^{4} l_i^{c_i} (\mathrm{mod} N) \equiv b_4^k l_1^{c_1} l_2^{c_2} l_3^{c_3} l_4^{c_4} (\mathrm{mod} N) \tag{13}$$

表 1 零知识证明生成算法1

输入：证明者和见证者的经度、纬度和海拔、与以见证者位置为圆心的半径R，

输出：零知识证明结果pf；

(1) 挑选随机大数$a,b_1,b_2,b_3,b_4,b_5,e_1,e_2,e_3,e_4,f_1,f_2,f_3,f_4,k,l_1,l_2,l_3,l_4,n,q_1,q_2,s$；

(2) $\alpha_1,\alpha_2,\alpha_3 \leftarrow$经纬度海拔之差，$D \leftarrow \text{getDis}(\alpha_1,\alpha_2,\alpha_3)$；

(3) **if** $R^2 \ge D^2$ **do** //判断是否在圆内

(4) 挑选两个大素数，相乘得到N，并舍弃掉两个素数；

(5) $\sum_{i=1}^{4} c_i^2 \leftarrow R^2-D^2$；$d_1 \leftarrow \sum_{i=1}^{3} e_i^2+\sum_{i=1}^{4} f_i^2 (\text{mod}N)$；

(6) $d_2 \leftarrow \sum_{i=1}^{4} c_i f_i+\prod_{i=1}^{3} e_i\alpha_i (\text{mod}N)$；$m \leftarrow b_4^n \prod_{i=1}^{4} l_i^{f_i} (\text{mod}N)$；

(7) $g \leftarrow \prod_{i=1}^{4} b_i^{e_i} (\text{mod}N)$；$h \leftarrow b_4^k \prod_{i=1}^{4} l_i^{c_i} (\text{mod}N)$；

(8) $p \leftarrow b_4^{-d_1} b_5^{q_1} (\text{mod}N)$；$r \leftarrow b_4^{-2d_2} b_5^{q_2} (\text{mod}N)$；

(9) $x_i \leftarrow s\cdot\alpha_i+e_i (\text{mod}N)(i=1,2,3)$，$x_4 \leftarrow s\cdot a+e_4 (\text{mod}N)$；

(10) $\beta_i \leftarrow sc_i+f_i (\text{mod}N)(i=1,2,3,4)$；$A \leftarrow \prod_{i=1}^{3} b_i^{\alpha_i} b_4^a (\text{mod}N)$；

(11) $\gamma \leftarrow sk+n (\text{mod}N), \lambda \leftarrow sq_1+q_2 (\text{mod}N)$；

(12) $\text{pf} \leftarrow \{N,A,s,b_i,x_i,g,R,\beta_i,\lambda,p,r,\gamma,h,l_i,m\}$；

(13) **else**

(14) $\text{pf} \leftarrow \{\}$.

第(9)和第(10)行的x_i,β_i是对带有位置敏感数据α_i,c_i的混淆，第(11)行的γ,λ作为验证所需参数是由随机数运算得出，不带敏感数据。第(10)行中计算A使用随机大数b_i等作为隐藏指数α_i的底，由于α_i是经纬度和海拔等信息，这样位置信息就作为指数隐藏了起来，再和b_4^a相乘混淆结果，如式(14)

$$\prod_{i=1}^{3} b_i^{\alpha_i} b_4^a (\text{mod}N) \equiv b_1^{\alpha_1} b_2^{\alpha_2} b_3^{\alpha_3} b_4^{\alpha_4} (\text{mod}N) \tag{14}$$

第(12)行最后得出零知识证明pf，证明中包含$\{N,A,s,b_i,x_i,g,R,\beta_i,\lambda,p,r,\gamma,h,l_i,m\}$。虽然计算$A,h$中涉及位置敏感数据，但是通过指数隐藏了起来，$x_i,\beta_i$则是位置数据混淆后的结果，$R$是阈值半径，并没有涉及有关证明者和见证者的位置信息，其他元素则是随机数或者随机数之间的运算结果，所以可以推断整个证明pf中不包含任何有用信息，算法1可以断定为零知识的；第(14)行返回空集，说明零知识证明失败，证明者的位置不可以被证明。

3.2 零知识证明验证算法

根据上面零知识生成算法生成的结果，把证明作为验证算法的输入，输出即为证明是否正确。这个位置验证协议是以调用智能合约的方式来执行的，根据传入的参数计算出验证结果，验证通过则会把证书持久化存储在区块链的全节点上，算法2见表2。

第(1)和第(2)行是通过运算来校验参数，如果数据无误则等式成立，其运算推导如式(15)

$$\begin{aligned} v_1 &= A^{-s}\prod_{i=1}^{4} b_i^{x_i} (\text{mod}N) \\ &= \left(\prod_{i=1}^{3} b_i^{\alpha_i} b_4^a\right)^{-s} \prod_{i=1}^{4} b_i^{x_i} (\text{mod}N) \\ &= \prod_{i=1}^{3} b_i^{-s\alpha_i} b_4^{-s\cdot a} \prod_{i=1}^{3} b_i^{(s\alpha_i+e_i)} b_4^{(s\cdot a+e_4)} (\text{mod}N) \\ &= \prod_{i=1}^{4} b_i^{e_i} (\text{mod}N) = g \end{aligned} \tag{15}$$

第(4)和第(5)行的运算推导如式(16)

$$\left.\begin{aligned} v_2 &= s^2R^2-\sum_{i=3}^{3} x_i^2-\sum_{i=1}^{4} \beta_i^2 (\text{mod}N) \\ &= s^2R^2-\sum_{i=3}^{3} (s\alpha_i+e_i)^2-\sum_{i=1}^{4} (sc_i+f_i)^2 (\text{mod}N) \\ &= -d_1-2sd_2 (\text{mod}N) \\ v_3 &= b_4^{v_2} b_5^{\lambda} (\text{mod}N) \\ &= b_4^{-d_1-2sd_2} b_5^{sq_1+q_2} (\text{mod}N) = \text{pr}^s (\text{mod}N) \end{aligned}\right\} \tag{16}$$

第(7)和第(8)行的运算推导如式(17)

$$\begin{aligned} v_4 &= b_4^{\gamma} h^{-s} \prod_{i=1}^{4} l_i^{\beta_i} (\text{mod}N) \\ &= b_4^{(s\cdot k+n)} \left(b_4^k \prod_{i=1}^{4} l_i^{c_i}\right)^{-s} \prod_{i=1}^{4} l_i^{(s\cdot c_i+f_i)} (\text{mod}N) \\ &= b_4^n \prod_{i=1}^{4} l_i^{f_i} (\text{mod}N) = m \end{aligned} \tag{17}$$

表 2　零知识证明验证算法2

输入：零知识证明pf，
输出：验证结果R；

(1)　$v_1 \leftarrow A^{-s}\prod_{i=1}^{4} b_i^{x_i}(\mathrm{mod}N)$;
(2)　**if** $v_1 != g$ **do**
(3)　$R \leftarrow F$；//返回验证失败
(4)　$v_2 \leftarrow s^2R^2 - \sum_{i=3}^{3} x_i^2 - \sum_{i=1}^{4} \beta_i^2$;
　　$v_3 \leftarrow b_4^{v_2} b_5^{\lambda}(\mathrm{mod}N)$;
(5)　**if** $v_3 != \mathrm{pr}^s(\mathrm{mod}N)$ **do**
(6)　$R \leftarrow F$;
(7)　$v_4 \leftarrow b_4^{\gamma} h^{-s}\prod_{i=1}^{4} l_i^{\beta_i}(\mathrm{mod}N)$;
(8)　**if** $v_4 != m$ **do**
(9)　$R \leftarrow F$;
(10)　$R \leftarrow T$；//返回验证通过。

在算法2中，运算主要涉及到模乘和模幂，计算之后判断值是否相等就可以得出最后的结果。根据算法1中得到的结果pf，去验证等式是否相等，3个验证等式全部相等则返回正确，反之则返回错误。

4　实验评估

在本节中通过实现原型系统来演示，包括前端APP和后端DAPP(Decentralized APPlication)，测试各个请求和回应的时间，零知识生成算法和验证算法的时间，以此来评估所设计的位置证明协议的性能。

4.1　协议实现

为了方便去评估协议，本文选择在手机Android系统上编写位置证明的应用，在手机上安装测试的APP，并在WiFi环境下测试。鉴于证明过程中存在合谋的行为，设置参与实验的手机数量不少于4个，其中1个作为证明者，剩下的3个作为见证者。攻击者必须控制一半以上的参与证明的见证者才能成功发动攻击。用户APP可以获取到每个用户包括自己的RSA公钥。鉴于区块链环境中的计算的要求，实验采用了4台服务器，其配置是Intel Xeon(R) E5-2687W CPU+32 GB内存，操作系统是CentOS Linux release 7.5.1804。另外区块链平台是基于以太坊客户端Geth进行改造的Jueth。

改造的内容主要是包含两部分：第1个是添加了智能合约的扩展调用功能，即合约可以调用用户自定义的动态库so文件；第2个是更改了共识算法，原本的以太坊客户端Geth使用的是工作量证明(Proof of Work, PoW)算法，PoW是系统为了达到某一目标而设置的度量方法，通过比拼算力获取记账权，而Jueth选用的是实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT), PBFT是一种基于消息传递的一致性算法，是基于原有的拜占庭协议的改进，把运行的复杂度从指数级别降低到了多项式级别。生成零知识证明算法是通过C++实现的，调用了开源的CryptoPP库，验证算法的实现则是依靠于智能合约编程语言Solidity和扩展库。

4.2　安全性分析

在本文的零知识证明算法中结合了DLP，其被求解的概率是可以被忽略的，这保证了算法的可靠性并保护了位置隐私。在运用区块链的技术的位置证明中保护安全性的有：第一是去中心化，独立不依赖第三方，用户的位置信息不会经过第三方或者中心化服务节点，从而确保隐私；第二是匿名，通信的匿名性，可以防止合谋；第三是共识算法，本协议运用共识算法PBFT。在区块链中最主要的时间消耗花在了共识上，共识算法给区块链的安全提供了保障，但是PoW需要消耗巨大的计算资源，PBFT不仅不需要比拼算力，而且也可以容纳将近1/3的错误节点误差，以此来确保安全性。

4.3　协议测试

本文着眼零知识证明生成和验证算法的性能来测试。其中零知识证明生成是使用链接成动态库的方式调用的，零知识证明验证是通过智能合约的方式进行执行的。图3中是对实现的零知识证明算法代码度量的执行时间，以100次为增量，每次在上一次的基础上多执行100次，一直到执行4000次，每次结果取平均值，可以观察到证明生成genProof执行的时间大约在50～55 ms之间(由于机器本身的型号规格不同会使结果产生一定的误差)，证明验证verifyProof执行时间大约在0.5 ms。

图4中的实验是不同的合约分别在Jueth和Ethereum上运行的时间比较，其中测得的是时间是运行10^4次的平均值。在Jueth上把PBFT算法共识时间设置为了1 s，在这1 s发生的交易都会打包进这个区块内。证书合约CertManager中的addCert添加证书方法中有持久化存储操作，即对应的字节码中有SStore指令，该操作会改变链上的世界状

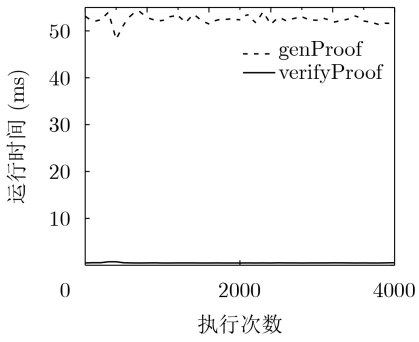

图 3 零知识证明算法代码执行时间

态。addCert方法执行时间约等于共识时间，即1 s。该合约方法在Etherum上的执行时间也大致约等于共识时间，即15 s。在图4中显示search查询和verify验证方法在两个平台上的执行时间则是大致一样，这是由于查询和验证不改变世界状态，不会引发共识，其中验证的时间是10～30 ms，在图4中几乎不可见。

图5中分别显示了零知识证明生成请求加响应ZKReq+Resp的平均时间花销是1.1 s左右，合约调用请求加响应BCReq+Resp的平均时间花销是3 s左右，验证请求加响应VerReq+Resp的平均时间花销是1 s左右，其中包含了少许的网络延迟，可得出3个操作的平均总耗时是在5 s左右。

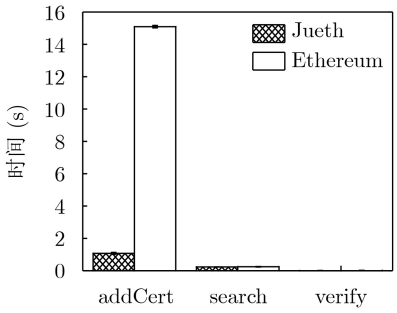

图 4 不同系统中不同合约的执行时间比较

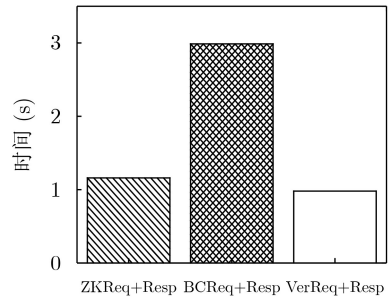

图 5 各个流程的时间花销

5 结束语

针对在威胁情境下位置数据隐私泄露和易被篡改的安全风险，本文提出了去中心化模式的位置证明方法。该方法采用区块链这一去中心化新型范式，解决了已有中心化架构存在的单点失效等问题，并结合零知识证明协议，满足了位置证明过程中位置数据的私密性要求。本文所提方法在实际测试结果表明：每次位置证明性能约5 s，其中包含证明生成验证和上链全过程，零知识证明算法生成和验证的总耗时是50.5～55.5 ms。因此，该算法具有较好的性能开销，可满足实际应用需求。下一步工作将重点研究基于区块链的空间位置查询，以适应位置证明的不同需求，并移植其他平台下进行实验测试。

参 考 文 献

[1] ZHU Zhichao and CAO Guohong. APPLAUS: A privacy-preserving location proof updating system for location-based services[C]. 2011 IEEE INFOCOM, Shanghai, China, 2011: 1889–1897. doi: 10.1109/INFCOM.2011.5934991.

[2] ZHU Zhichao and CAO Guohong. Toward privacy preserving and collusion resistance in a location proof updating system[J]. *IEEE Transactions on Mobile Computing*, 2013, 12(1): 51–64. doi: 10.1109/TMC.2011.237.

[3] ZHENG Yao, LI Ming, LOU Wenjing, *et al*. SHARP: Private proximity test and secure handshake with cheat-proof location tags[C]. The 17th European Symposium on Research in Computer Security - ESORICS, Pisa, Italy, 2012. doi: 10.1007/978-3-642-33167-1_21.

[4] LUO Wanying and URS Hengartner. Veriplace: A privacy-aware location proof architecture[C]. The 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, San Jose, USA, 2010: 23–32. doi: 10.1145/1869790.1869797.

[5] SCHUMMER J and VOHRA R V. Strategy-proof location on a network[J]. *Journal of Economic Theory*, 2002, 104(2): 405–428. doi: 10.1006/jeth.2001.2807.

[6] LI Yi, ZHOU Lu, ZHU Haojin, *et al*. Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks[J]. *IEEE Internet of Things Journal*, 2016, 3(4): 563–571. doi: 10.1109/JIOT.2015.2481926.

[7] KHAN R, ZAWOAD S, HAQUE M M, *et al*. 'Who, When, and Where?' Location proof assertion for mobile devices[C]. The 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy XXVIII, Vienna, Austria, 2014: 146–162. doi: 10.1007/978-3-662-43936-4_10.

[8] 李佩丽, 徐海霞. 区块链用户匿名与可追踪技术[J]. 电子与信息学报, 2020, 42(5): 1061–1067. doi: 10.11999/JEIT190813.
LI Peili and XU Haixia. Blockchain user anonymity and traceability technology[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1061–1067. doi: 10.11999/JEIT190813.

[9] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. http://bitcoin.org/bitcoin.pdf, 2009.

[10] FOUNDATION E. Ethereum: Blockchain app platform[EB/OL]. https://ethereum.github.io/yellowpaper/paper.pdf, 2019.

[11] YOUSSEF J R, ZACHAREWICZ G, and CHEN D. Developing an Enterprise Operating System (EOS) - requirements and architecture[C]. The 25th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE),

Paris, France, 2016: 130–135. doi: 10.1109/WETICE.2016.36.

[12] PlatONE Corp. PlatONE_Whitepaper[EB/OL]. https://platone.juzix.net/static-new/pdf/zh/PlatONE_Whitepaper_ZH.pdf, 2019.

[13] TROUW A, LEVIN M, and SCHEPER S. The XY oracle network: The proof-of-origin based cryptographic location-network[EB/OL]. https://docs.xyo.network/XYO-White-Paper.pdf, 2018.

[14] Foamspace Corp. FOAM whitepaper[EB/OL]. https://www.foam.space/publicAssets/FOAM_Whitepaper.pdf, 2018.

[15] NASRULIN B, MUZAMMAL M, and QU Qiang. A robust spatio-temporal verification protocol for blockchain[C]. The 19th International Conference on Web Information Systems Engineering, Dubai, United Arab Emirates, 2018: 52–67.

[16] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014, 37(1): 246–258. doi: 10.3724/SP.J.1016.2014.00246.
FENG Dengguo, ZHANG Min, and LI Hao. Big data security and privacy protection[J]. *Chinese Journal of Computers*, 2014, 37(1): 246–258. doi: 10.3724/SP.J.1016.2014.00246.

[17] 曹素珍, 王斐, 郎晓丽, 等. 基于无证书的多方合同签署协议[J]. 电子与信息学报, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.
CAO Suzhen, WANG Fei, LANG Xiaoli, *et al*. Multi-party contract signing protocol based on certificateless[J]. *Journal of Electronics & Information Technology*, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.

余荣威：男，1981年生，副教授，研究方向为可信计算、区块链安全.
周博孝：男，1996年生，硕士生，研究方向为系统安全.
王丽娜：女，1964年生，教授，研究方向为可信计算、信息隐藏.
朱欣焰：男，1963年生，教授，研究方向为GIS、大数据安全.
谢辉华：男，1996年生，硕士生，研究方向为系统安全.
谢红军：男，1985年生，硕士生，研究方向为区块链.

责任编辑：马秀强