DOI: 10.54254/3050-2187/2025.22124

基于零知识证明的隐私增强型数字资产交易机制

韦 甜

（商洛学院，陕西省商洛市，726000；1908790127@qq.com ）

摘 要：区块链技术广泛应用于数字资产和电子交易等行业。针对数字资产中的数据隐私性和数据资产交易的资金安全性难以保证的问题，传统区块链交易公开透明，与数字资产匿名性需求矛盾。本文提出一种基于零知识证明的区块链数字资产隐私访问策略。在数据层解决了用户的隐私信息被第三方泄漏风险和权限控制传递不明确的问题。该访问策略包括用户注册、数据上传和验证、数据处理和访问控制三个阶段。用户注册阶段，以数字签名来确认所属关系，以避免将个人信息与账户相关联，从而降低关联泄露风险。在数据上传和验证阶段，采用 BGN 算法对原始数据进行加密，并用零知识证明验证数字资产的所有者。在访问控制阶段，为解决数据细粒度共享问题，提出一种基于 Shamir 的零知识密钥分配方案，并提高信息分割部分的安全性和个人隐私信息管理的效率。并从一致性分析、隐私性分析证明了所提系统的安全性。最终实验分析了该系统的各个参数对运行时间的影响。

关键词：数字资产；隐私访问控制；零知识证明；区块链

引言

数字资产的隐私访问是安全使用数据的前提。由于在数据交易过程中的每一个环节都需要数据承载，只有在保证数据访问完整性和安全性的前提下，才能使得数据交易的这一系列流程真实、可靠和有效。数据访问策略不仅可以实现数据确权、高效管理，还可以防止数据泄露和伪造。

目前研究者们采用数字签名、混币、同态加密和零知识证明等方式[1, 2]解决区块链的隐私访问。因为区块链的交易信息是公开的，仅仅依靠区块链技术难以实现有效的信息管理和保护。现有的基于区块链技术的数字访问策略中，主要存在身份验证不够便捷、数据访问权限粗粒度以及资产所属性不够明确等问题。GaBa 等人[2]提出基于零知识证明的身份验证密钥协议（Authentication and Key Agreement, AKA）方案。ZKP-AKA 保持数据完整性、机密性、匿名性。Gabay 等人[3]借助 Zk-SNARK 协议，确保车主身份验证过程中的隐私保护和匿名性。Feng 等人[4]提出在工业互联网数据共享中解决数据隐私和安全问题的方案，方案包括六个实体，数据所有者、云服务、半可信云服务器、私钥生成器、智能合约和区块链，使用零知识证明（ZKP）技术、智能合约和代理重新加密技术保证隐私的安全性。零知识证明是属于区块链中的一种安全技术路线，核心是采用零知识验证进行链下的安全运算，然后再将计算结果交给链上的智能协议验证，以建立链下计算链上验证的隐私防护系统。

随着互联网技术的发展，移动设备的普及间接导致个人隐私等信息频繁泄露和滥用。此外，小型物联网设备的计算能力和存储能力有限，这也使得管理员难以使用复杂的、资源密集型的安全协议。针对上述问题，本章节结合同态加密 BGN 提出了一种基于零知识证明的区块链数字资产隐私的访问控制方案（ZKP-BGN），保证了数字资产可用可信不可见。本部分主要工作如下：

首先构建用户数据和用户资产的关联，以确保其安全性，然后采用零知识证明（ZKP）技术实现用户数字资产识别的隐私性和灵活控制性，使用者拥有完全去中心化的数字资产的控制访问权，使数字资产的属性唯一。

（1）本节提出一种基于零知识证明的区块链安全分散数据共享方案，结合安全多方协议 BGN，在云服务器上对数据高效计算的同时保证数据的隐私性。

该方案利用了 Zk-SNARK 协议，用户可以以此证明自身满足有效通信的某些要求，且不暴露身份。此需求由中心节点设置，并保存在一个智能合约中，合约中用户构建了一个零知识证明，并将其提交给区域总节点验证。一旦验证通过，用户便能够开始与其他节点通信；

（2）本节主要对所提方案进行一致性、安全性和隐私性分析。然后实现区块链上交易效率的性能评估，对比本文所提方案与其他方案在数字内容保护功能，通过理论分析以及详细的实验结果分析，证实该方案可以实现用户和数据的安全性和隐私性。

1 隐私访问策略

1.1 隐私访问策略系统结构

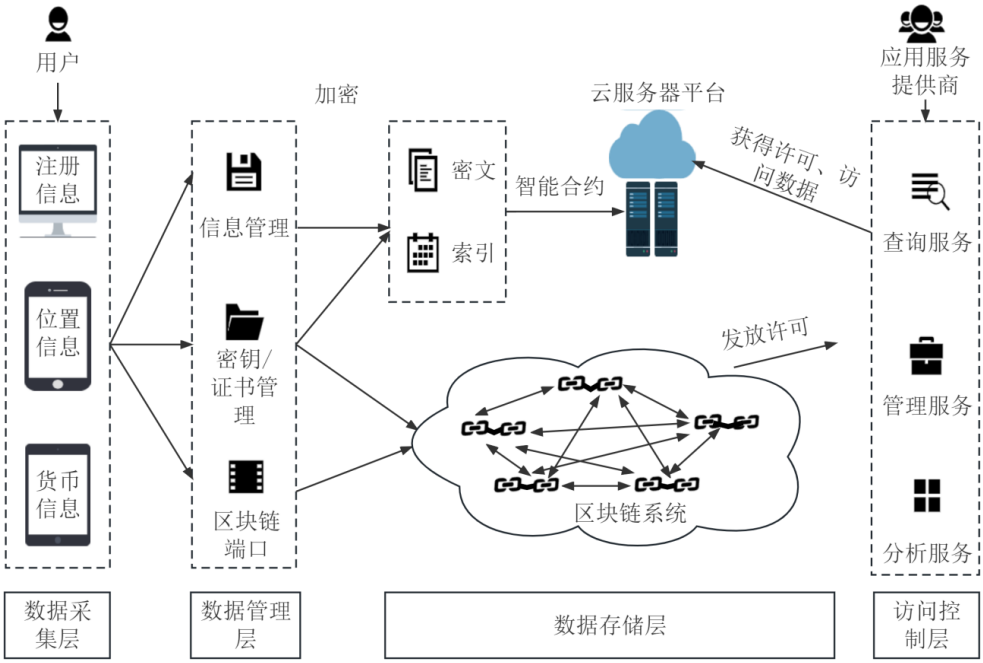

图 1 访问控制框架图

用户个人信息、位置信息、搜索记录、行为数据、健康数据和财务数据等敏感信息往往容易被暴露。应用区块链技术保护数字资产隐私时，一个主要的挑战是，确保使只有拥有相应资产的人才能访问这些资产，与相应资产无关的人员无法得到访问。即使允许其他人访问私有数字资产，访问记录也应该被数据所有者知晓。本章方案基于区块链技术的去中心化、分布式特点实现数据的可追溯性和不可篡改性，并采用零知识证明技术实现数据的隐私权限管理。本章的主要技术框架如图 1 所示，隐私访问策略分为以下四个部分：数据采集层、数据管理层、数据存储层和访问控制层。数据采集层负责收集用户个人信息，例如注册信息、位置信息等。数据管理层用于分配权限、上传数据至区块链等。数据存储层负责数据的持久化存储，同时需要考虑数据的访问权限和可扩展性，以满足不同场景下的数据需求。数据访问层是需求者与系统交互的接口，负责判定需求者是否拥有数据访问的权限。

1.2 攻击模型

在本小节采用 Dolev-Yao（DY）威胁模型[5]验证隐私访问策略系统的安全性。在 DY 模型中，攻击者可以读取、监听和修改不同实体之间的交易信息，并且拦截消息，提取用户身份、密钥、隐私数据等。一方面，这可能会危及用户私人数据，利用用户私人数据对用户造成严重的身体或者精神伤害。另一方面，入侵者还

可以通过修改时间戳来获得系统的非法访问权限，进而注入恶意软件，扰乱市场操作。入侵者主要的攻击行为如下：

（1）主服务商攻击：基于 ZKP-BGN 的数据匿名化隐私访问策略（DA 隐私访问策略）通过零知识证明对数据拥有者的身份隐匿化处理，从而降低主服务商攻击的风险。

（2）中间人攻击：数据拥有者将公钥加密的秘密信息发送到区块链网络中后，即便此信息包被中间人拦截，数据资产的具体内容也不会被暴露。而且，DA 的标识具有匿名性及动态性，可以保护信息隐私。例如，主服务商被黑客攻击后，可以获得 DA 的上传时间和属性内容，但是不能获取 DA 身份，也因此不能控制 DA 后续的交易流程，因此中间人攻击无效。

（3）重放攻击：通过在认证生成阶段添加一个时间戳作为输入，来防止证据被重播。时间戳是一个公共输入，因此在验证证明时，它会被提交给智能合同，然后身份验证合同验证当前的时间。如果当前时间在证明有效期内，则该证明有效。否则，它将被拒绝。

（4）拒绝服务攻击：在基于令牌的方法中，数字资产可以频繁交易。然而，交易需要提前支付押金费用，而且会被写入收费代币，所以对手必须限制其调度请求。基于此，DoS 试图进行虚假的调度将是不现实的。对于攻击者来说成本较高，因为计划收费的付款是在认证和承诺期间提前发送的，过度的调度将会导致花费大量的成本。

1.3 安全目标

基于上述安全威胁，本章将提出了一种基于零知识证明的区块链安全分散数据共享方案，其需要满足以下的安全目标：

（1）数据的一致性。区块链是一个去中心化的结构，可能会出现冲突交易、数据资产访问前后不一致等问题，本文所提出的方案需要确保 DA 的不可重写性、确定性。对于不可重写性来说，当交易被创建时，假设 DA 在时刻的稳定状态为，那么后续的状态必须在时刻的基础上创建。

（2）数据隐私性分析。基于零知识证明的区块链数字资产隐私访问策略需要确保攻击者无法获得有关于用户的任何 DA 信息，也就是说 DA 需要保持隐匿。此外，该方案还需要考虑一个更实际的问题，即多方攻击者合谋，企图窃取用户的数据，因此需要确保和保证云存储服务器上的数据隐私性。

（3）数据安全性。在基于零知识证明的区块链数字资产隐私访问策略中，区块链技术被用于提供安全可靠的 DA 信息管理，其中 DA 信息会被整合到一个区块交易，并通过哈希计算上传到区块链。由于区块链上的交易信息是公开透明的，攻击者可能会直接从区块链获得密钥信息，进而获得 DA 信息。因此本方案需要确保有权限用户才能访问区块链上的交易信息。

2 策略实现

2.1 符号描述

本节所涉及到的数学符号和含义，如表 1 所示：

表 1 数学符号和含义

符号	定义
ID_d	用户的身份信息
$< P, pk >$	<公钥，私钥>
Q_d	服务器生成公钥的值
Q_a	用户生成公钥的值
$S_a = S_b$	共享秘钥
$D = \langle d_1, d_2, \cdots, d_n \rangle$	注册阶段用户收集的信息
σ	挑战值

表 1 （续表）

$data_{enc}$	加密后的信息
H_{rec}	数据文件
s	数字资产数据
H_{rec}	数据文件
U_d	密钥分发者
U_r	密钥持有者
m	消息

2.2 策略流程

具体实现方法如下：

阶段一：用户注册。传统的注册系统采用个人信息进行注册，在注册过程中难免泄露个人信息。为避免用户在注册过程中个人信息的泄露，本文采用基于零知识证明的隐私保护方案。当用户进行注册时，服务器会生成一个随机的挑战值，要求用户使用自己的私钥对该挑战值进行签名。用户完成签名后，将签名结果发送给服务器实现验证。服务器只需通过验证签名的有效性来确认用户的身份信息，不需了解用户的具体身份信息。具体过程如表 2 所示，时序流程对应图 2。

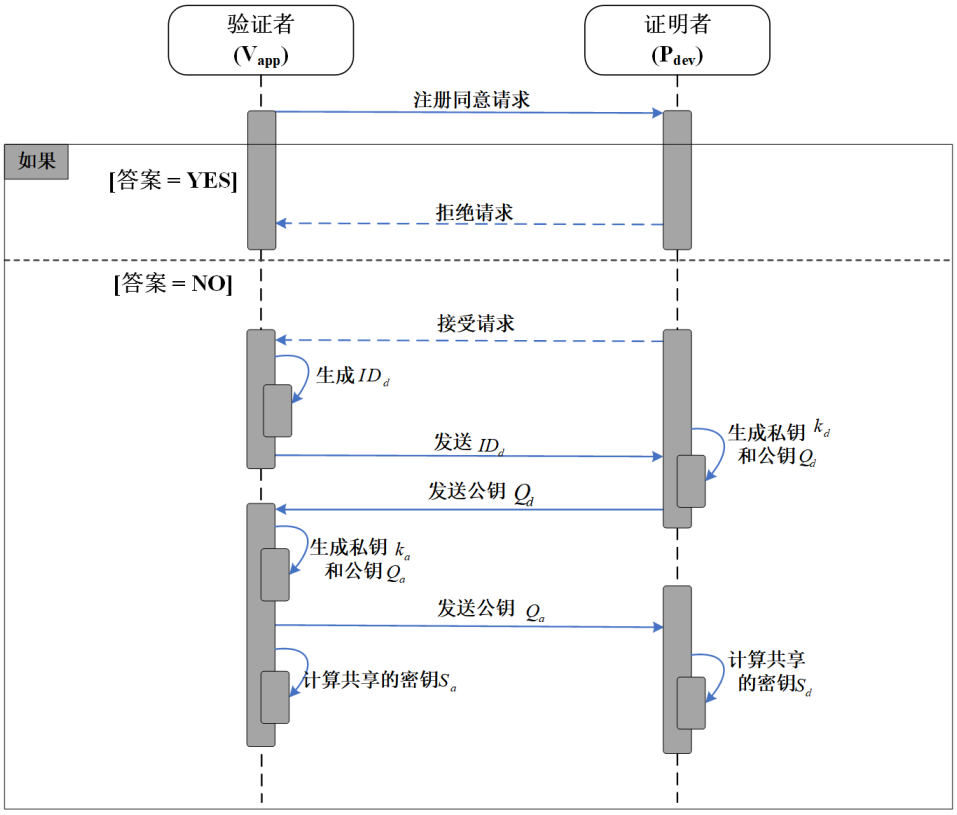

图 2 注册阶段

表 2 协议 1 注册阶段

协议 1：注册阶段
1.若用户（验证者V_{app}）已注册，注册请求拒绝 2.若用户未注册，生成ID_d给用户

表 2 （续表）

3.服务器（证明者P_{dev}）通过一个整数$k_d \in F_p$生成私钥pk，通过$Q_d = k_d G$且$Q_d \in E$（F_p）生成公钥P
4.服务器发送Q_d给用户，用户可通过Q_d计算分享密钥
5.用户通过一个随机数$k_a \in F_p$生成私钥，通过$Q_a = k_a G$且$Q_a \in E$（F_p）生成公钥P
6.用户发送Q_a给服务器
7.用户计算$S_a = k_a Q_d$，服务器计算$S_d = k_d Q_a$，Then$S_a = S_b$

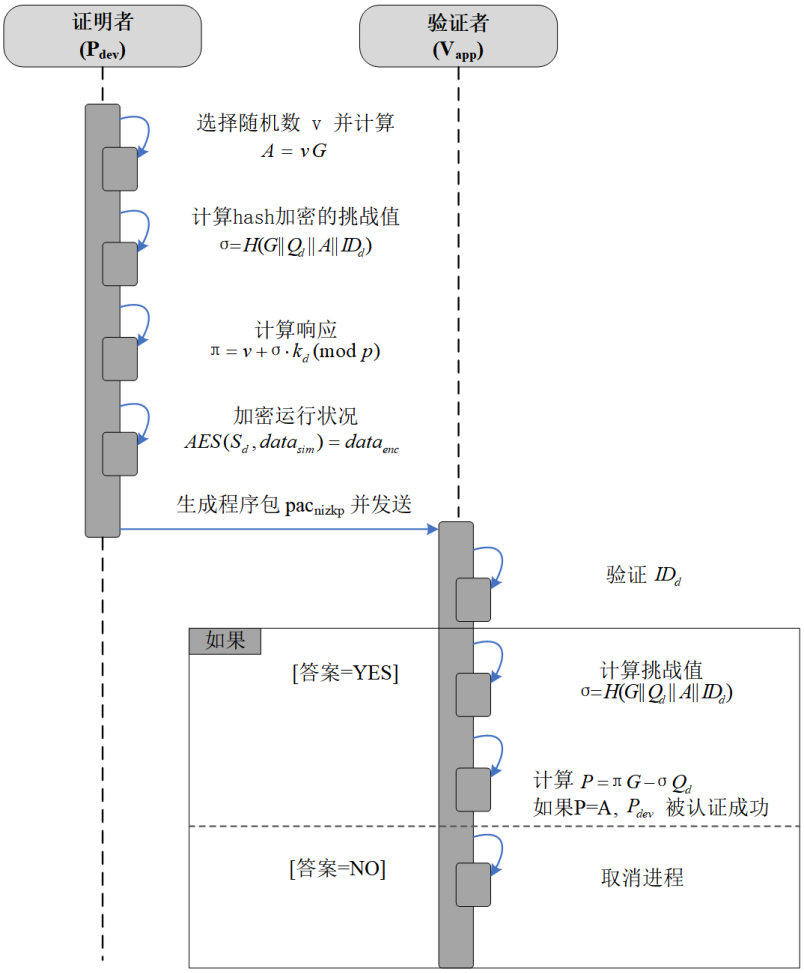

图 3 数据上传与认证阶段

阶段二：数据上传与验证阶段。分布式区块链允许多个节点协同管理数据，从而实现去中心化的数据存储和管理。其特点是数据分布在网络中的多个节点上，所有节点都拥有数据副本的全部内容，并且通过达成共识来确保数据的完整性和一致性。为了保证数据的安全性，本文采用了 BGN 算法进行加密。在 BGN 算法中，数据的加密和解密是基于一个大素数和一个多项式环实现的，这样可以保证数据的机密性和完整性。最终为保证数据的真实性和完整性，本文采用了零知识证明技术对数据拥有者进行验证。零知识证明是一种基于密码学的技术，它允许证明者证明某个命题的真实性，而不需要向验证者透露任何有关命题的信息。采用分布式区块链、BGN 算法和零知识证明技术可以有效地保证数据的安全性和可追溯性，从而为数据共享和授权提供了一个安全、可靠的平台。具体过程如表 3 所示，完整流程对应图 3。

表 3 协议 2 数据上传与验证阶段

协议2：数据上传与验证阶段
1.用户收集信息记为$D = \langle d_1, d_2, \cdots, d_n \rangle$
2.用户生成随机常数$v \in F_p$，并计算$A = vG$
3.用户通过哈希函数计算挑战值$\sigma = H$（$G \| \| Q_d \| \| A \| \| ID_d$）
4.用户计算相应值$\pi = v + \sigma \cdot k_d \, mod \, p$
5.用户通过 BGN 加密数据$D = \langle d_1, d_2, \cdots, d_n \rangle$并生成加密后数据$data_{enc}$
6.$Encrypt(PK, PK_u \langle d_1, d_2, \cdots, d_n \rangle) \rightarrow C_{PK_u}$其中$C_{pk_u} = \left(c_{pk_1}, c_{pk_2}, \cdots, c_{pk_n} \right)$
7.用户生成数据包，其中包含 A，π，ID_d以及加密数据$data_{enc}$并发至区块链
8.用户将数据信息的哈希值和数字签名存储在区块链平台上，如图1访问控制框架图所示
9.检查设备是否注册，若注册进行下一步
10.服务端使用公钥Q_d以及ID_d计算挑战，$\sigma = H$（$G \| \| Q_d \| \| A \| \| ID_d$）
11.服务端计算$P = \pi G - \sigma Q_d$并检查$P = A$若$P = A$则属于认证用户，若不属于不允许访问
12.若属于认证用户，可将区块链哈希值和数字前面保存至系统中。

阶段三：数据处理阶段。采用基于 Shamir 密钥共享的细粒度访问。Shamir 提出的（t, n）密钥共享方案是基于 Lagrange 插值公式构造的，描述如下（见表 4）：

（1）初始化阶段：密钥分发者U_d随机地从有限域$\mathbb{G}$中选取n个不同的非零元素$x_1, x_2, \ldots, x_n$标记共享密钥持有者$U_r = \{U_1 . U_2, \cdots, U_n\}$（$r = 1,2, \cdots, n$），公开元素$x_r$和其对应的$U_r$。

（2）共享密钥分发阶段：U_d分发的秘密为$s \in Z_q$其中q为大素数，在有限域$\mathbb{G}$内选择$t-1$个元素a_i（$i = 1,2, \cdots, t-1$）构成$t-1$阶多项式，如式（1）所示：

$$f（x） = \sum_{i=1}^{t-1} a_0 + a_i x^i \, mod \, p \quad （1）$$

其中p是一个大素数且$p > s$，秘密$s = f（0） = a_0$，U_d生成共享秘密s_r并发送给相应的共享密钥持有者U_r，见式（2）：

$$s_r = f（x_r） = \sum_{i=1}^{t-1} a_0 + a_i x_r^i \, mod \, p \ （r = 1,2, \cdots, n） \quad （2）$$

（3）秘密恢复过程：任何 t 个共享密钥持有者发送他们的秘密，然后使用拉格朗日插值公式还原。

表 4 算法 1：基于 Shamir 的零知识密钥分配方案

算法 1：基于 Shamir 的零知识密钥分配方案
1.将 DA 秘密s分成 n 个部分$s_1, s_2, \cdots, s_n$使用 Shamir 生成 n 个共享秘密分配给 n 个不同的共享密钥持有者
2.共享密钥持有者对每个共享秘密计算$y = g^{s_n}$
3.共享密钥持有者选择一个随机数v_n，并计算$t = g^{v_n}$
4.共享密钥持有者计算$c = H$（g, y, t）其中 H 是哈希函数
5.共享密钥持有者计算$r_n = v_n - cs_n$其中$n = 1,2, \cdots, n$
6.验证者检查是否$g^{r_n} y_n^c = t$，若验证通过则可以查看文件相应的部分内容。

Shamir 方案将原始信息分为多个部分，且每个部分的内容都是已知的，这意味着可以通过简单地收集和组合这些部分来恢复原始信息。由于每个部分的内容已知，访问其中任何一个部分，都可以获取原始信息的全部或部分内容。因此，在没有进一步的安全保护的情况下，Shamir 方案并不能有效地保护原始信息。为了

避免这种情况，需要采用更加安全的技术手段，本文对分割后的部分进行加密并结合算法 1 零知识证明技术来实现更高级别的安全保护，如表 5 所示，具体数据处理流程如图 4 所示。

表 5 协议 3 数据访问细粒度处理

协议 3：数据访问细粒度处理
1.通过 BGN 解密算法解密数据得到$data$并生成数据文件H_{rec}
2.采用 ABE 算法对文件H_{rec}进行权限管理，记为（H_{rec}, A） $= H_{recA}$
3.将（H_{rec}, A） $= H_{recA}$上传至区块链网络，并生成 hash 值
4.访问者需通过区块链进行交易，交易时会由区块链智能合约进行检查看是否拥有相应的查看权限
5.判定拥有查看权限，则生成交易记录，交易记录则是对每个信息的访问权限管理。

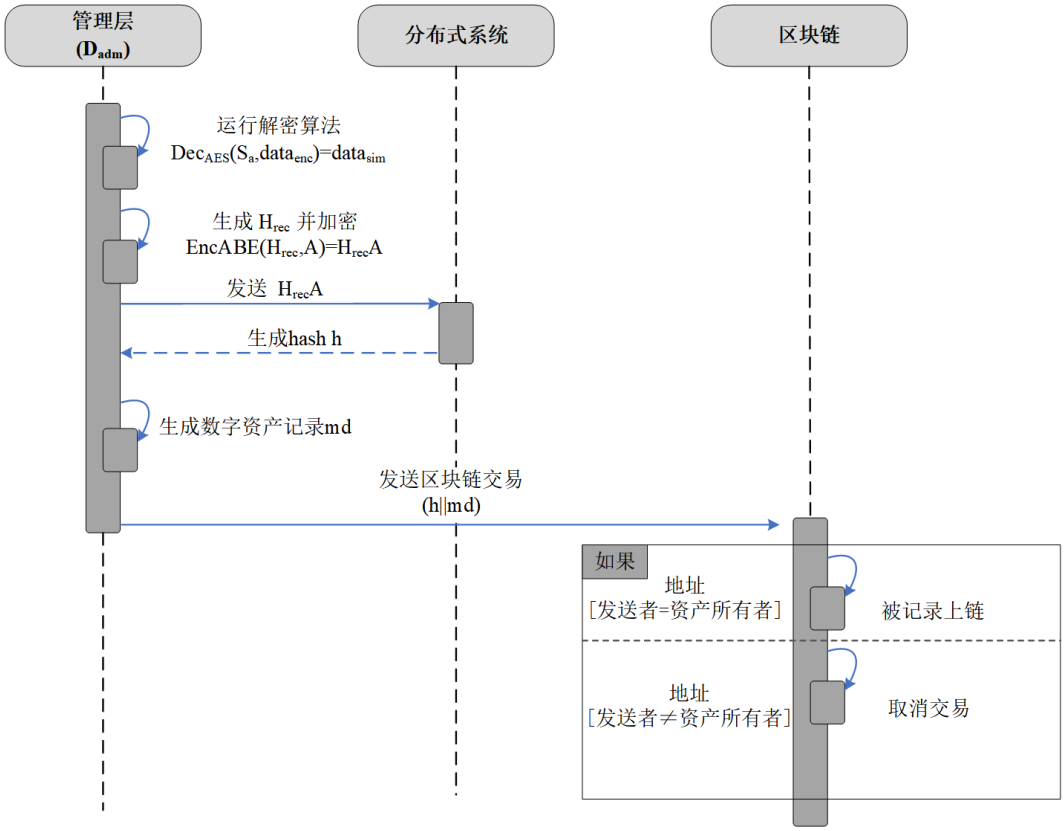

图 4 数据处理阶段协议 3

3 安全性分析

本小节对基于零知识证明的区块链数字资产隐私的访问控制方案的安全性分析主要包括一致性分析、隐私性分析和安全性。

3.1 一致性分析

Shamir 共享安全性分析：假设一个用户想要在消息m上获得签名，即计算m^d。需要将m发送至服务器计算签名片段并将计算结果，式（3）返回至用户。设$\Delta = n!$，在本场景中Δ是因子，以确保每个参与者生成的

签名分片是不同的，可以组合成有效的签名。具体而言，每个参与者分配一个唯一索引i，而其分享值$d_i = f（i）$。因此，对于任何不同的索引子集Y，对应差值的乘积都可被Δ整除。

$$s_i = m^{2\Delta d_i}（mod\, N）\tag{3}$$

假设现在用户从子集$Y = \{i_1, \cdots, i_t\} \subset \{1, \cdots, n\}$中获得了足够数量的签名分片。重组向量的定义由以下公式（4）给出。

$$r_{i_j,Y} = \prod_{i_k \in Y, i_j \neq i_k} \frac{-i_k}{i_j - i_k}\tag{4}$$

由于$i_j - i_k$可以整除Δ，可以得到$\Delta * r_{i_j,Y}$并推出公式（5）：

$$s' = \prod_{i_j \in Y} s_{i_j}^{\,2\cdot\Delta\cdot r_{i_j,Y}}\,(mod\, N) = （m^{4\cdot\Delta^2}）^{\sum_{i_j \in Y} r_{i_j,Y}\cdot d_{i_j}} = m^{4\cdot\Delta^2\cdot d}（mod\, N）\tag{5}$$

若需要恢复真正的签名，假设$e > n$且e为质数，此时意味e与$4\Delta^2$互质，因此可以通过扩展欧几里得算法，计算出整数u和v使得$u \cdot e + v \cdot 4 \cdot \Delta^2 = 1$。拓展拉格朗日算法是一种计算两个整数$a$和$b$的最大公约数，以及一组整数$x$和$y$使得$ax + by = gcd（a, b）$。其中，$a = e$，$b = 4\Delta^2$，$gcd（a, b）= 1$。签名计算如式（6）所示：

$$s = m^u \cdot s'^v（mod\, N）\tag{6}$$

此时可以验证密钥s是有效的签名，因为：

$$s^e = （m^u \cdot s'^v）^e = m^{e\cdot u} \cdot m^{4\cdot e\cdot v\cdot\Delta^2\cdot d} = m^{u\cdot e + 4\cdot v\cdot\Delta^2} = m\tag{7}$$

其中，$（N, e）$是公钥，d是私钥。

将上述协议应用至个人数据访问阶段，设访问者的共享值为式（8）：

$$\begin{cases} R_j（X）= v_j + r_{i,j}X^1 + \cdots + r_{t,j}X^t \\ S_j（X）= a_j + s_{1,j}X^1 + \cdots + s_{t,j}X^t \end{cases}\tag{8}$$

那么访问者将加密对$（u_{i,j}, w_{i,j}）=（R_j（i）, S_j（i）） \ 11 \le i \le n$发送至服务器，访问者所做承诺的内容是否与数据拥有者所提交的数据相符，验证过程见式（9）。

$$\begin{aligned} B_j \prod_{l=1}^{t} B_{l,j}^{\,i^l} &= B_{a_j}(v_j) \prod_{l=1}^{t} B_{sl,j}（r_{l,j}）^{i^l} = h^{v_j} g^{a_j} \prod_{l=1}^{t}（h^{r_l,j} g^{s_l,j}）^{i^l} \\ &= h^{（v_j + \sum_{l=1}^{t}（r_{l,j}）\, i^l）}\, g^{（a_j + \sum_{l=1}^{t}（s_{l,j}）\, i^l）} = h^{R_j} g^{S_j} = h^{u_{i,j}} g^{w_{i,j}} \end{aligned}\tag{9}$$

其中，$B_{l,j} = B_{s_{l,j}}（r_{l,j}） \ 1 \le l \le t$为访问者公开多项式承诺。

3.2 隐私性分析

3.2.1 零知识性证明：

本文在传递信息的过程采用了随机值v_n，如$（g^p）^{v_n}$。若攻击者需要提取知识，首先需要知道随机值v_n。具体来讲，验证者选择一个随机值，并对证明中的值求幂运算得到$（g^{p（s）}）^{v_n}$，$（g^{h（s）}）^{v_n}$，$（g^{\alpha p（s）}）^{v_n}$，然后将内容给验证者，$（g^{p（s）}）^{v_n} =（（g^h）^{v_n}）^{t（s）}$，$（（g^{p（s）}）^{v_n}）^{\alpha} =（g^{p'}）^{v_n}$，合并后得到$g^{v_n p} = g^{v_n t（s）h}$等式成立，从而保证了消息传递的零知识性。

3.2.2 多参与方串谋安全性证明：

假设 Alice 是共享密钥拥有者 A 选择随机数S_A和α_A，然后公开公共参考串 CRS（Common Reference String, CRS）=（$g^{s_A^i}, g^{\alpha_A}, g^{\alpha_A s_A^i}$）。Bob 是共享密钥拥有者 B 选择随机数$S_B$和$\alpha_B$。Carol 是共享密钥拥有者 C，选择随机数$S_C$和$\alpha_C$，然后通过同态乘法结合拥有者 A、B、C 的 CRS，如式（11）所示：

$$Alice \to Bob = （g^{（s_A^i）s_B^i}, g^{（\alpha_A）\alpha_B}, g^{（\alpha_A s_A^i）\alpha_B s_B^i}） = g^{（s_A s_B）^i}, g^{\alpha_A \alpha_B}, g^{\alpha_A \alpha_B （s_A s_B）^i} \quad （10）$$

$$Alice \to Bob \to Carol = （g^{（s_A s_B s_C）^i}, g^{\alpha_A \alpha_B \alpha_C}, g^{\alpha_A \alpha_B \alpha_C （s_A s_B s_C）^i}） \quad （11）$$

得到一个混合的$s^i = s_A^i s_B^i s_C^i$和$\alpha = \alpha_A \alpha_B \alpha_C$，这样避免参数的生成者不泄密问题，除非所有参与者串谋，否则参与者互相之间不知道其他人的秘密参数，只要有一个诚信参与者，就无法伪造证明。然而，仍然存在一个问题，即如何验证参与者在生成共识关键参数时使用的随机值是一致的。为解决这个问题，本文采用一种对原始密钥进行重新排列或替换的方法，以生成新的密钥，即 Alpha 变换技术，如式（12）所示：

$$e（g^{s^i}, g^{\alpha}） = e（g^{s^1}, g^{\alpha s^{i-1}}）\,|\,（i \in 2, \cdots, d） = e（g, g）^{\alpha s^i} \quad （12）$$

仅需要验证 Alpha 变换前后的值是否变化，即可知道 CRS 的值是否遭到篡改。

本节对零知识性以及多参与方串谋安全性进行了证明。多参与方串谋安全性证明保证了参与者之间的秘密参数不泄漏。而 Alpha 变换则解决了如何验证参与者在生成共识关键参数时使用的随机值是一致的问题。

3.3 安全性分析

本小节中，分析所提方案应对攻击模型中各类攻击的鲁棒性以及安全性，并通过“互联网协议和应用程序的自动验证（Automated Validation of Internet Security Protocols and Applications, AVISPA）”工具[6]验证。AVISPA 是一种安全分析器，经常被研究安全和认证协议的人员用来执行正式的安全分析。AVISPA 提供了四个后端，即动态模式检查器（On-the-fly Model-Checker, OFMC）、基于约束逻辑的攻击搜索器（Constraint-Logic-based Attack Searcher , CL-AtSe）、基于布尔满足性问题的模型检查器（SAT-based Model-Checker, SATMC）和基于树自动机的安全协议分析器（Tree Automata based on Automatic Approximations for the Analysis of Security Protocols, TA4SP）。

在 AVISPA 中定义三个主要角色，分别是用户设备、网关和应用服务提供商节点。其中，公开整体交易的组成，随后宣布全部节点，入侵各个用户节点。OFMC 后端的模拟花费不到 1 秒的时间访问 7 层深度的 65 个节点。同样，CL-AtSe 后端花费了 0.23s 的翻译时间和 0.02s 的计算时间来检验协议对网络攻击的健壮性。如表 6 显示，即使在被破坏的环境中经过多次迭代，AVISPA 也无法发现任何网络威胁或漏洞。因此，可以观察到本节所提策略可以保护信息安全性。

表 6 OFMC 和 CL-AtSe 的安全性分析表

后端检查器	运行环境	性能（搜寻 7 层 65 节点）	是否受到威胁
OFMC	安全	1.23s	否
CL-AtSe	安全	0.25s	否

4 实验分析

4.1 仿真实验

为了验证论文提出的 ZKP-BGN 算法的性能，本小节从验证算法的可行性和算法的实现效率分析。效率分析是指对算法的密钥生成、加解密过程和零知识证明密文合法性验证过程进行测试。

实验环境：使用 Python3.7。CPU 是 AMD R7 5800H（3.2Ghz）和 RAM 为 32GB。实验分析方案的时间成本，方案中共有三个变量：密文值大小 m、密钥位数 g 和验证轮数 n。

首先本文对密文大小以及时间成本之间的关系展开研究，分别设定密文大小为10^7、10^8、10^9、10^{10}进行初始化，其他变量保持一致，记录运行 100 次交易后的运行时间。由图 5 可知，密文的大小主要影响到密文的生成和签名的速度，因为它们需要使用密文进行幂运算这里的幂运算与图 3.5 之间的关系没有讲清楚。但在交易过程中，密文的大小不会对交易过程的速度产生明显的影响。即使增加密文至10^{10}，每次交易的时间也仅增加 0.09s。

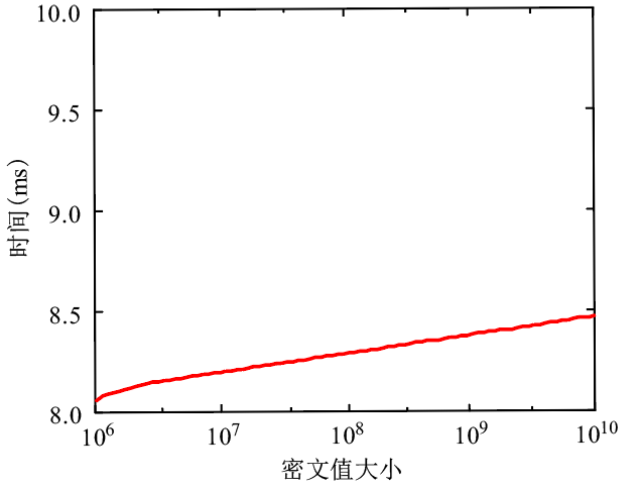

图 5 密文值集合的大小对算法效率的影响

其次，对密钥位数 g 与时间花费的关系分析，g 依次从 80、128、192、256 变化，设$m = 10^{10}$，记录运行 100 次交易后的运行时间。图 6 结果显示，密钥生成阶段的时间成本与密钥位数呈正相关，原因是在此阶段中，密钥生成需要在离散均匀分布器 Tug 中计算。因此在保证计算效率的情况下，尽可能使的密钥位数的最大可以保证数字资产的隐私，且不易被攻击。

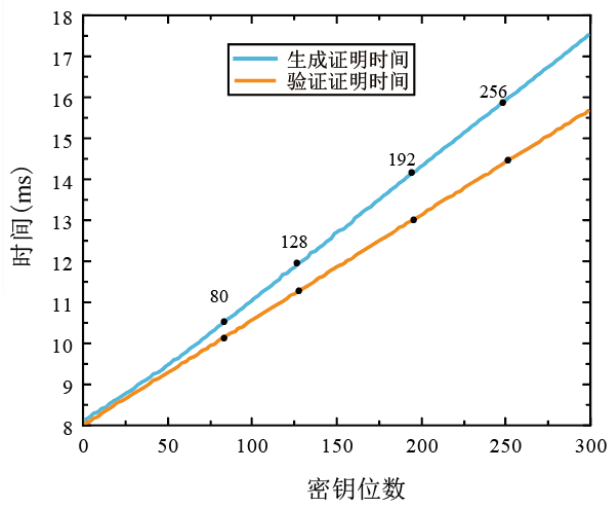

图 6 秘钥位数对算法效率的影响

在区块链中，为了确保交易的合法性，需要进行验证，而零知识证明可以用来验证交易的合法性，同时保护交易中的隐私信息。在验证过程中，增加验证轮数可以提高验证过程的安全性，但也会增加时间成本。因此，需要在时间和安全性之间进行平衡，设定合适的验证轮数。由图 7 所示，当验证轮数为 500 次时，每

次交易的时间是 0.08s，而当验证轮数为 1000 轮时，单次交易的时间为 0.16s，所以验证轮数的大小与验证时间成正比关系，所以在设定该参数的时候，需要同时考虑时间和安全性。

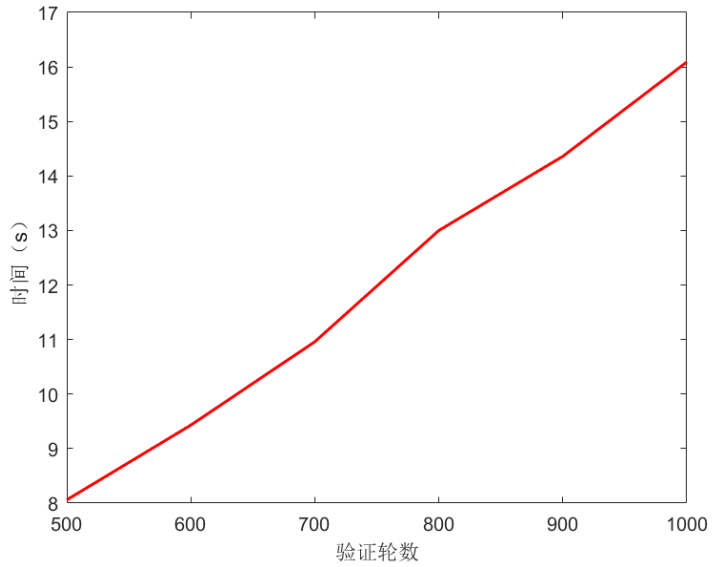

图 7 验证轮数对算法效率的影响

4.2 方案比较

文献[7]提出了一种利用区块链和智能合约等技术管理科研数据数字重用权的新方法，保证数据的合规性，但是数字内容访问未从加密角度保证数据隐私；文献[8]提出使用以太坊智能合约的数字资产买卖方案，但是算法都比较通用，在安全方面不能保证。文献[9]采用星际文件分布式的解决方案，实现数据交易安全，但是并未提及加密过程的详述。文献[10]由于 IPFS（Inter Planetary File System, IPFS）属于分布式区块链，会将数字内容拆分成不同的模快进行保存，数字内容未经过加密上传，可能会导致隐私泄露的风险增加；文献[11]使用秘密共享方案对数字媒体内容进行分割，然后将切割后的份额直接存储到 IPFS；文献[12]用区块链实现了版权的注册与版权交易，数字内容保护方案功能对比如表 7 所示。

基于零知识证明的区块链数字资产隐私访问策略采用同态加密技术，将数据加密后上传至 IPFS，以确保隐私数据在上传过程中得到保护。同时，在注册、上传隐私数据、验证访问者的过程中，采用零知识证明技术，确保数据访问者不会获取到隐私信息，提高了数据安全性。在秘密共享方案中，使用基于零知识的 Shamir 秘密共享算法，确保共享者无法勾结而推出目标秘密，进一步提升数据安全性。综上所述，本文方案考虑了多个方面的安全问题，采用了多种技术手段来确保数据的隐私性和安全性，具有较高的可行性和实用性。

表 7 数字内容保护方案功能对比

方案	是否基于区块链	是否支持访问控制	是否内容加密方式	是否支持零知识
文献[7]	是	是	否	否
文献[8]	是	否	是	否
文献[9]	是	否	否	否
文献[10]	是	否	否	否
文献[11]	是	否	否	否
文献[12]	是	否	否	否
本文方案	是	是	同态加密	是

5 结论

本文提出了一种基于零知识证明的区块链数字资产隐私访问策略，以解决数字资产在区块链中存在的隐私信息泄漏和权限控制传递不明确的问题。本文首先介绍了数字资产隐私访问策略的基本框架和实现方式，包括用户注册、数据上传和验证、数据处理和访问控制三个阶段。在这个基础上，本文采用了零知识证明来确保数字资产的隐私确权、存证和访问保护，增强数据的可信度和安全性。此外，本文还提出了基于 Shamir 的零知识密钥分配方案来提高信息分割的安全性和个人隐私信息管理的效率。从安全性分析的角度来看，本文提出的数字资产隐私访问策略在保证数字资产的可用性、可信性上具有显著的优势。通过采用数字签名确认用户身份、BGN 算法加密原始数据、零知识证明验证数字资产所有权等多种安全措施，有效地确保了数字资产的隐私性和安全性。此外，基于 Shamir 的零知识密钥分配方案也能够提高信息分割的安全性和个人隐私信息管理的效率。最终，本文通过实验分析表明所提出的数字资产隐私访问策略在不同参数设置下均具有良好的运行时间和准确性。这表明该策略可以在实际应用中有效地实现数字资产隐私访问控制和保护，提高数字资产的安全性和可信度。

参考文献

[1] 贺东博. 基于同态加密和零知识证明的区块链隐私保护研究 [D]. 华中科技大学, 2019.

[2] GABA G S, HEDABOU M, KUMAR P, et al. Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare [J]. Sustainable Cities and Society, 2022, 80: 1-12 .

[3] GABAY D, AKKAYA K, CEBE M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (6): 5760-5772.

[4] FENG T, YANG P, LIU C, et al. Blockchain data privacy protection and sharing scheme based on zero-knowledge proof [J]. Wireless Communications and Mobile Computing, 2022, 2022: 1-11.

[5] DOLEV D, YAO A. On the security of public key protocols [J]. IEEE Transactions on information theory, 1983, 29 (2): 198-208.

[6] ARMANDO A, BASIN D, BOICHUT Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications[C]//Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings 17. Springer Berlin Heidelberg, 2005: 281-285.

[7] PANESCU A T, MANTA V. Smart contracts for research data rights management over the ethereum blockchain network [J]. Science & Technology Libraries, 2018, 37 (3): 235-245.

[8] NIZAMUDDIN N, HASAN H, SALAH K, et al. Blockchain-based framework for protecting author royalty of digital assets [J]. Arabian Journal for Science and Engineering, 2019, 44: 3849-3866.

[9] HASAN H R, SALAH K. Proof of delivery of digital assets using blockchain and smart contracts [J]. IEEE Access, 2018, 6: 65439-65448.

[10] NAZ M, AL-ZAHRANI F A, KHALID R, et al. A secure data sharing platform using blockchain and interplanetary file system [J]. Sustainability, 2019, 11 (24): 1-24.

[11] KRIPA M, NIDHIN MAHESH A, RAMAGURU R, et al. Blockchain framework for social media DRM based on secret sharing [C]//Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 1. Springer Singapore, 2021: 451-458.

[12] 李莉, 周斯琴, 刘芹, 何德彪. 基于区块链的数字版权交易系统 [J]. 网络与信息安全学报, 2018, 4 (07): 22-29.