许可区块链网络中的数据动态存储方法

刘新璐[1]，闫皓楠[2]，张　平[1]，庄兴昌[1]，严　超[1]
（1. 中国电子科技集团公司第二十八研究所，江苏　南京 210023；
2. 中国人民解放军 96512 部队，宁夏　银川　750000）

摘　要：区块链技术是具有划时代意义的创新，一旦数据被录入区块链，就几乎无法被篡改或删除，这为重要信息的长期保存提供了可靠保障。然而，传统区块链节点间通信依赖直接连接，在面对链路变化时，会发生同步延迟，从而导致存储数据不一致。针对这一问题，提出了一种基于权威证明的许可链动态存储方法。在许可区块链网络中，节点需要存储大量的交易数据和区块信息，同时还需要保证链上数据的安全性和可靠性。为了更好地适应链路环境变化，该方法通过引入动态存储机制，更好地保证数据的安全性和完整性。实验结果表明，该方法可有效缓解时变链路环境中的数据不可用，并显著提高数据存储的安全性。

关键词：区块链；许可链；智能合约；时变链路；动态存储；区块链应用
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 02. 007
引用格式：刘新璐，闫皓楠，张平，等. 许可区块链网络中的数据动态存储方法［J］. 网络安全与数据治理，2025，44(2)：44 - 51.

Dynamic storage of data in permissioned blockchain networks

Liu Xinlu[1], Yan Haonan[2], Zhang Ping[1], Zhuang Xingchang[1], Yan Chao[1]
(1. The 28th Research Institute of China Electronics Technology Group Corporation, Nanjing 210023, China;
2. No. 96512 Unit of PLA, Yinchuan 750000, China)

Abstract: Blockchain is an epoch-making innovation that cannot be tampered with or deleted once the data is entered into the blockchain. This provides a reliable guarantee for the long-term preservation of important information. However, the communication between traditional blockchain nodes relies on direct connections, which can cause synchronization delays when there are changes in the channels. This leads to inconsistent stored data. To address this problem, this paper proposes a novel dynamic storage mechanism based on Proof of Authority (PoA) for permissioned networks. In permissioned networks, nodes need to store a large amount of transaction data and block information while ensuring the security and reliability of the data on the chain. To adapt to the time-varying channel, the dynamic storage mechanism is introduced to ensure the security and integrity of the data. Experimental results show that the method can effectively mitigate data unavailability in time-varying channels and significantly improve the security of data storage.

Key words: blockchain; permissioned blockchain; smart contract; time-varying channel; dynamic storage; blockchain application

0　引言

区块链技术[1]引领了划时代的数据存储和管理创新，其去中心化的特性确保了数据的安全性和永久性[2]。一旦数据被稳妥地录入区块链，便几乎无法篡改或删除，这为重要信息的长久保存提供了坚实的保障，例如交易记录、身份信息等。然而，区块链网络中的节点通信依赖于直接连接，因此在链路发生变化时，节点间的通信可能会中断，导致数据同步的延迟，甚至可能导致数据的不一致性。时变信道网络是指信道在时间上发生变化的无线通信网络[3]。面对时变信道环境，传统区块链在实现数据的安全可信存储方面显得捉襟见肘。

许可链是一种具备授权机制的区块链，参与者明确且彼此信任，其通常被设计为具有高吞吐量和高性能的系统，以满足各种实际应用的需求[4]。目前主流的许可链技术包括超级账本（Hyperledger Fabric）[5]和以太坊（Ethereum）[6]。其中，超级账本采用实用拜占庭容错

(Practical Byzantine Fault Tolerance, PBFT) 共识[7]。然而，PBFT 在通信开销方面较大，因此不适合时变信道的网络环境。以太坊提供工作量证明 (Proof of Work, PoW)[8]、权益证明 (Proof of Stake, PoS)[9] 和权威证明 (Proof of Authority, PoA)[10] 等共识机制。其中，PoA 由一组权威节点来维护区块链的安全，这些权威节点具有出块控制权，负责验证交易并创建新的区块。PoA 具有比 PoW 更快的交易确认速度和更高的吞吐量。由于权威节点的身份已经被信任和认证，因此，该共识具备比 PBFT 更高的安全性和抵抗恶意行为的能力。尽管 PoA 在许可链中得到了广泛应用，例如在 Goerli 测试链和 PoA Network[11] 中，但其仍然存在一些问题。例如，权威的节点进入与退出需要超过一半网络节点的投票确认，这会造成大量未确认的投票记录缓存在节点中，导致存储负担增加。此外，投票周期长不利于快速切换到下一个出块周期。

针对这些问题，本文将深入探讨在许可区块链网络中数据面对时变信道网络时的动态存储方式，并提出基于 PoA 的动态存储方法。本文的主要贡献如下：

(1) 通过上游节点灵活选择授权节点。在网络信道发生变化时，上游节点通过委托下一个出块节点变更权威节点列表，进入新的一轮出块周期，从而降低切换出块周期的时间。

(2) 设计存储数据的智能合约，提供高效的存储和检索性能。该方法提供数据存储和检索、授权节点更换和查询的远程过程调用 (Remote Procedure Call, RPC) 接口和 TCP 接口，便于二次开发。

1 许可区块链网络的数据存储机制

1.1 许可区块链网络的特点

许可区块链网络是公链的一种变体，它由一组经过授权的参与者组成，与公链相比，它具有更高的透明度和可追溯性[12]。许可链的性质更为集中，为数据存储提供了更多的控制和管理空间。

公链和私链的特性被融合到许可链中，这使得参与者能够拥有更多的控制权，同时保持了区块链的去中心化和透明性。只有经过授权的参与者才能访问网络，这为数据存储提供了更高级别的安全性。此外，许可链的可追溯性也为数据存储提供了更多的控制和管理空间，所有参与者都能够跟踪数据的来源和去处，从而增强了数据的安全性和可靠性。

1.2 许可链中的数据管理和存储方式

在许可链中，数据管理具有高效和可控的特点，这是因为数据的创建、传输和存储均由经过验证和授权的节点来执行[13]。这种机制确保了数据的准确性和完整性，避免了非法或未授权节点的干扰。为了实现这些目标，许可链采用了多种策略和技术手段。

在数据管理方面，许可区块链网络采用加密算法、访问控制和审计跟踪等。这些措施有助于保护数据的机密性、完整性和可用性，从而确保数据的安全可靠。

在数据存储方面，许可区块链网络通常采用分布式存储架构，这种架构将数据分散存储在多个节点上，提高了数据的可靠性和容错性。同时，为了确保数据的安全性，许可区块链网络还采用了数据备份和恢复机制，以应对意外情况的发生。

1.3 许可区块链网络中的数据动态存储需求分析

在时变信道网络中，信道状态会随着时间的推移而发生变化，这会导致数据传输的质量和延迟出现波动或不稳定。因此，为了确保数据传输的可靠性和稳定性，需要对时变信道网络环境进行监测和管理，并采取相应的措施来应对信道状态的变化。

1.4 数据动态存储的挑战

许可区块链网络中的数据动态存储涉及诸多挑战。首先，存储效率是首要考虑的问题，随着数据量的持续增长，如何更有效地利用存储资源、降低存储成本并提高存储效率成为了亟待解决的难题。其次，实时调整机制的设计也是一大挑战。由于网络环境的变化，数据的存储和访问需求也会随之改变。因此，需要设计一种实时调整机制，根据网络环境的变化动态地调整数据的存储和访问策略，以确保数据的可用性和可靠性。最后，数据一致性是许可区块链网络中数据动态存储的关键问题之一。由于网络中的多个节点可以同时访问和修改数据，因此需要确保数据在所有节点之间保持一致性。

2 系统模型

2.1 数据动态存储模型

图 1 所示的系统模型描述了一个涵盖多个层级和不同类型节点的通信网络。节点部分包括上游节点、目标节点和分布式节点。在上游节点向目标节点传送数据的过程中，为确保数据的完整性和安全性，目标节点在接收数据后会将其存储在由分布式节点构建的区块链系统中。每个节点都具备合法身份，并根据不同的权限对数据进行管理，如存储和查询等。这些节点间通过有线或无线的方式进行数据通信。

该模型借助智能合约技术，实现数据的存证、恢复及防篡改功能。在区块链初始化阶段，智能合约将得以部署，该智能合约在共识层之上运行，负责将来自上游节点的关键数据存储在区块链中。当授权节点有数据上

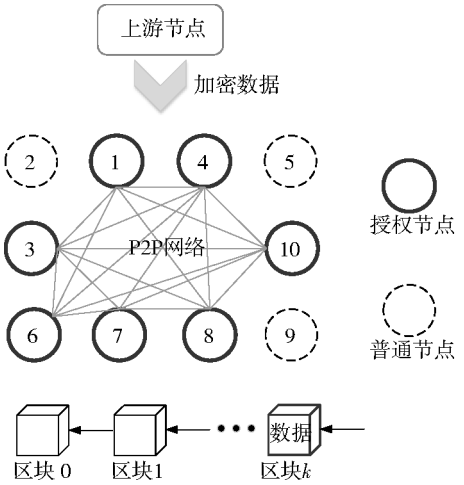

图 1　区块链动态存储系统模型

链需求时，它们会将数据封装在一个交易中，发送至智能合约的链上地址，从而触发数据上链存储操作。这些授权节点会通过共识协议执行上链操作。若某节点的数据发生损坏，可以通过从其他节点同步历史交易，重新将数据上链到该智能合约，实现数据恢复。同时，得益于区块链的链式结构、时间戳及共识机制，数据篡改得以有效防范。

2.2　数据动态存储功能模块

图 2 所示的功能模块包括：初始化模块、授权节点推荐模块、共识模块、智能合约模块以及通信模块。其中，初始化模块可实现智能合约部署和预设区块链参数的功能；授权节点推荐模块则根据上游节点的反馈信息，选取通信信道状态较好的部分节点作为授权节点参与共识；共识模块能够对存储数据形成共识以防篡改，实现分布式持久化存储；智能合约模块则能够实现数据存储和恢复功能。

初始化模块的核心目标是规划智能合约的执行逻辑和优化 Gas 开销，同时建立智能合约的链上链下存储机制。

授权节点推荐模块的设计理念是：上游节点可以监听任意分布式节点的信道状态，并推荐一组信道状况良好的授权节点组成委员会。一旦确定了授权节点名单，将由上游节点确定并公布。在每个纪元内，授权节点保持不变，协同参与区块的产生。如果信道状态发生变化，上游节点将公布新的授权节点名单，开启新的区块纪元。在授权节点内部，将按照共识协议的规则对未按时出块的节点进行剔除惩罚。

共识模块基于 PoA 协议，并对以太坊 Clique 共识进行优化。Clique 共识作为目前以太坊测试网络所采用的共识协议，其核心思想是设立一个由授权节点组成的委员会，协同合作来打包区块并维护区块链[14]。而其他节点则无权进行区块打包。在此基础上，本文所提出的方法进一步优化了适用于时变信道网络的共识机制——Cluster。与 Clique 共识相比，Cluster 共识在调整授权节点集合的组成时，无需冗长的投票周期，这有助于减少区块链节点的缓存数据量。

智能合约模块的设计目标是创建存储数据的合约，并实现将数据进行上链持久化存储。在合约设计实现时，需要考虑链上存储开销和计算开销对存储和计算的性能影响。因此，需要优化合约设计以降低存储和计算开销，从而提高智能合约的性能。

通信模块的设计将采用高效传输的广播协议，同时结合数据聚合与数据滤除技术。其中，数据聚合通过对共识协议相关的消息进行语义识别，将语义相关的消息聚合为一个通信数据包，然后交给下层通信协议栈处理和传输，以减少各层间的通信协议开销。

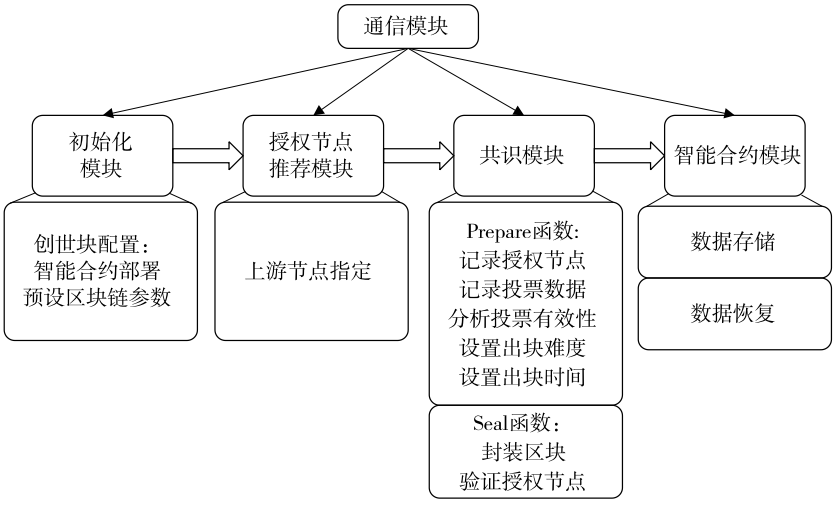

图 2　功能模块关系

2.3 数据动态存证流程

图3展示了数据动态的存证流程。授权节点推荐模块根据上游节点的反馈信息，推荐通信信道状态较好的部分节点作为授权节点集合，并将待上链数据发送至授权节点。授权节点将该数据封装至交易，并广播至其他授权节点。该交易用来调用数据存证的智能合约。其他授权节点收到交易后，利用本地以太坊虚拟机（Ethereum Virtual Machine，EVM）自动执行智能合约，并基于Cluster共识将交易中的数据上链。

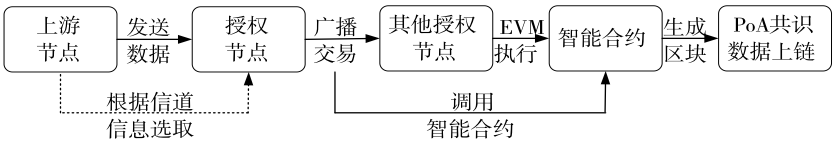

图3 基于Cluster的数据存证流程

3 数据动态存储技术实现

3.1 共识机制对数据动态存储的支持

图4展示了Cluster共识协议的核心思想是通过实时监测链路状态并调整授权策略，确保系统在面对时变信道时仍能保持高效运行。通信模块扮演着至关重要的角色，它不仅需要实时监测链路状态，还要将链路状态信息发送给Cluster。当链路状态发生变化时，通信模块会立即将最新的链路状态信息发送给Cluster。Cluster接收到链路状态信息后，会根据这些信息调整授权节点的授权策略。具体来说，Cluster会根据接收到的链路状态信息评估各个节点的通信质量，然后根据评估结果调整各个节点的授权策略。在面对时变信道时，这种调整策略尤为重要。由于信道状态是不断变化的，因此通信质量也会受到影响。通过实时监测链路状态并调整授权策略，Cluster共识协议能够确保在信道状态发生变化时，系统仍然能够保持高效的运行。

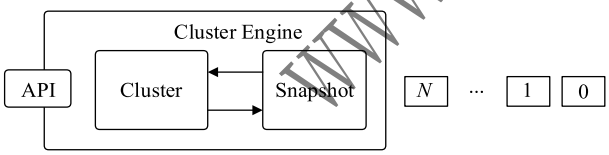

图4 Cluster模块示意

图5展示了Cluster共识的出块流程。Cluster的出块功能由算法1和算法2实现。在算法1中，授权节点提供区块头信息，包括轮转状态及Header.Time和Header.Difficulty字段等。算法2则通过本地签名认证创建已密封的区块，检测授权节点是否有打包区块（签名）的资格，并判断当前领导者是否已签名过区块。如果授权节点在最近签名集合中，将禁止再签名后续一定数量的区块，以防止恶意攻击者连续出块。此外，Cluster共识模块还通过投票（Vote）和计票（Tally）两个结构体，实现对引入和踢出授权节点的管理。这些机制共同保证了区块链的安全性和可靠性。

算法1 准备区块

输入：Number，Coinbase
输出：Header

```
if Number mod Epoch = 0 then
    Header_Extra ←Signers
else
    Header_Coinbase ←Coinbase
    Header_Nonce ←ChangeAuthorization
end if
Header_Difficulty ←inturn（Number，Coinbase）
return Header
```

算法2 签名区块

输入：Header
输出：Result

```
if Header_Coinbase ∉ SignerAccounts then
    return error
end if
if Header_Coinbase ∉ RecentAccounts then
    return error
end if
if Header_Difficulty = inturn then
    Delay←0
else
    Delay←FaxTime
end if
Sign（Header）
Wait（Delay）
return success
```

表1展示了Cluster共识算法所使用的关键字段。该算法通过复用当前以太坊区块头中可用的Extra字段，将授权节点列表和当前区块的授权者对该区块头的签名数据写入其中。为了更新一个动态的授权节点列表，复用区块头中的Coinbase和Nonce字段来创建投票方案。其中，Coinbase字段用于保持投票时被投节点的地址。创世块配置指定了出块时间，并预设了一组默认授权者。

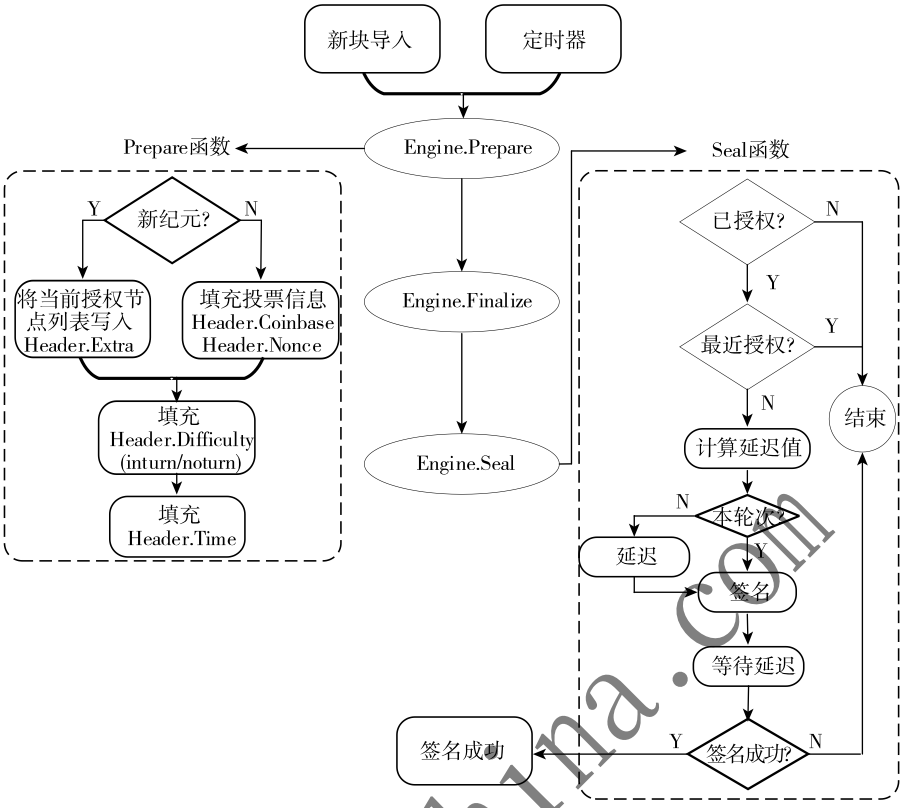

图 5　Cluster出块流程

表 1　区块数据中的关键字段

序号	字段	注释
1	Coinbase	出块授权节点的地址
2	Nonce	提名分类，添加或删除
3	Extra	在纪元内，存储当前授权节点集合
4	Difficulty	出块优先级

3.2　智能合约的应用与数据动态管理

3.2.1　智能合约模块实现

图 6 展示了智能合约模块的运作机制。此模块承担着管理账户私钥、数据存储合约的应用程序二进制接口（Application Binary Interface，ABI）与区块链动态存储软件之间建立 RPC 通信的任务。当智能合约模块接收到数据上链请求时，它会先将请求中携带的 Key 和 Value 值组装成一笔可执行的交易，然后将其发送至本网络的节点。随后，区块链节点的广播将这笔交易传播至整个网络。最后，出块节点将该交易打包进区块并广播该区块。区块链网络的其他节点会接收并验证这个区块，然后将其写入节点的数据库。

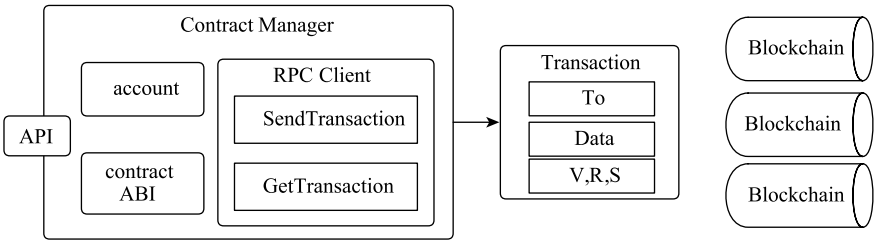

图 6　智能合约模块

3.2.2　智能合约调用流程

智能合约是在以太坊虚拟机上运行的一段代码，EVM 是一个图灵完备的虚拟机，是整个以太坊协议的核心[15]。图 7 展示了智能合约的创建和调用过程。Solidity 是一种专门用于此目的的高级语言。一旦完成了 Solidity 的编写并编译成字节码，就可以创建一个交易来将合约部署到区块链上。这个交易的“Data”字段会保存字节码，“To”的地址为一个空的账户。一旦这个交易被权

威节点打包并加入到区块链中，合约就被创建完成了，区块链上将出现一个与该智能合约相对应的合约账户，并拥有一个特定的地址，合约代码将保存在该合约账户上。

如表 2 所示，调用智能合约的交易数据包括以下核心字段：Nonce 字段记录了交易在调用节点的序列位置；To 字段记录了交易发送的目标地址，即智能合约的链上地址；Data 字段包含了通过合约编译生成的 ABI，也就是应用二进制接口，它编码了合约调用方法，具体指明了本次的调用方法，比如数据存储或恢复（store/retrieve），并列出输入参数列表；而 V、R、S 字段则包含了调用节点的数字签名信息，可用于查询调用者的地址。

表 2　调用智能合约的交易数据关键字段

序号	字段	注释
1	Nonce	该交易在节点账户的顺序
2	To	存储合约地址
3	Data	存储调用合约需要的参数
4	V，R，S	调用节点的数字签名信息

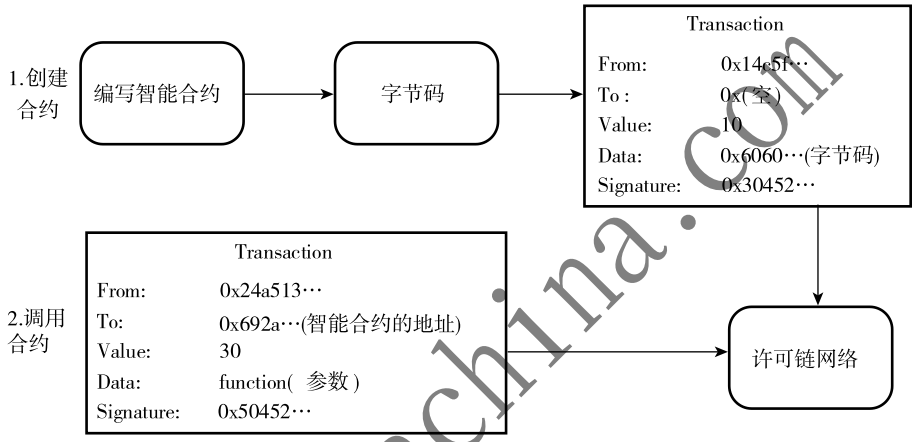

图 7　智能合约的创建与调用流程

3.3　授权节点动态变化的实现

Cluster 共识的权威节点选择包含两个主要步骤：首先，根据信道条件，上游节点会筛选出符合条件的授权节点集合 M 和备选节点集合，授权节点集合将组成 PoA 的委员会；然后，在该委员会内部，将按照 PoA 协议执行节点管理，即剔除当前的授权节点并从备选节点中选出新的授权节点。

如图 8 所示，授权节点的引入和剔除是由委员会内部授权节点的投票决定的。在每个纪元中，委员会内部授权节点会为某些备选授权节点进行投票。如果针对某个节点的投票超过了一个阈值，投票结果就会立即生效。系统会检查投票内容是引入票还是剔除票。如果是引入票，把该节点添加到委员会中；如果是剔除票，把该委员会的签名者移除出委员会。在这两种情况下，系统都会清理投票信息。

此外，在委员会授权节点内部，还会进行出块节点的选取。根据 Cluster 的规定，一个授权节点如果在当前轮次成为出块节点，那么在接下来的 $M/2+1$ 轮中，它就不能再次成为出块者。因此，在每一个出块轮次，系统会选择近期未出块的授权节点作为出块者。

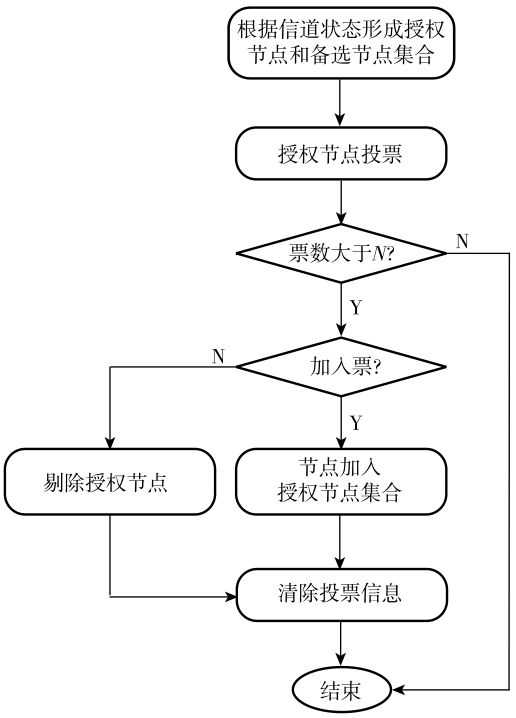

图 8　授权节点的选取与剔除流程

4　实验和分析

4.1　搭建区块链许可环境

表3 和表4 展示了搭建区块链网络的实验环境。本次实验共使用了4 台设备，其中环境1 和环境2 各使用了2 台设备。

表3　运行环境1

序号	环境条目	型号状态
1	CPU	国产飞腾多核处理器 FT1500A
2	内存	≥16 GB
3	硬盘	≥2 TB
4	网卡	≥1 000 Mb/s
5	操作系统	银河麒麟操作系统 V4. 0. 2

表4　运行环境2

序号	环境条目	型号状态
1	CPU	国产飞腾多核处理器 FT2000
2	内存	≥16 GB
3	硬盘	≥2 TB
4	网卡	≥1 000 Mb/s
5	操作系统	银河麒麟操作系统 V4. 0. 2

区块链账户是基于非对称加密算法的公私钥的抽象，它将公钥信息转换成20 字节的地址，作为用户的唯一标识[16]。而区块链动态存储软件的公私钥是在 secp256k1 椭圆曲线上随机选择一个点，然后将选择的坐标信息编码成64 个字符[17]。因此，账户生成流程包括两个步骤：产生随机的 secp256k1 曲线坐标和公钥信息序列化，具体为：

（1）通过以太坊客户端 Geth 生成加密账户，执行命令为：./geth --datadir./node account new。其中第一个参数 --datadir ./node 为账户密钥的存储路径；第二个参数 account 和第三个参数 new 表示创建新账户。

（2）导出./node/keystore 路径下账户的私钥文件。

分别在四台实验的机器上运行以太坊客户端，执行命令为：./geth --datadir "./node" --password "./passwd. txt" account import " ./node/keystore"。

运行区块链程序之后，四台节点组建许可区块链网络。

4.2　数据动态存储展示

为了更好地展示区块链动态存储软件，笔者开发了区块链浏览器 cluster-explorer，这是一个用于查看和分析区块链上交易和区块信息的工具或服务。cluster-explorer 基于 Angular 和 Node. js 开发，它提供了一个用户友好的界面，使普通用户能够轻松浏览和查询区块链的数据，包括交易历史、授权节点、区块高度等信息。此外，cluster-explorer 还提供了切换上游节点的功能，以及发送查询和存储数据请求的功能。

图9 显示了区块链的出块列表。根据图像，目前许可区块链网络中109 个区块达成了共识，每个区块的大小为606 个字节。

已达成共识的区块	区块的交易数量	区块大小(Bytes)	区块生成时间
109	0	606	2023-11-21 17:18:16
108	0	606	2023-11-21 17:18:06
107	0	606	2023-11-21 17:17:56
106	0	606	2023-11-21 17:17:46
105	0	606	2023-11-21 17:17:36
104	0	606	2023-11-21 17:17:26
103	0	606	2023-11-21 17:17:16

图9　出块列表

图10 展示了许可区块链网络的节点账户，其中序号1 的节点为授权节点。通过点击“切换授权节点”按钮，可以向区块链节点发送更新授权节点的请求。

节点数量：4　切换授权节点

序号#	节点账户#	授权节点#
1	0x2d951db6e953343343cadf39b16e7c546f51ee25	☑
2	0xd1ddb74ab75ee657792032436a531499bb8cf3d2	☐
3	0x72b2d2448f70c1b224bc4961fa6d8a7e5e4ed926	☐
4	0x4f7692d98ab4d3d529a96868f7967ed3740a4cc5	☐

图10　切换授权节点

图11 展示了数据管理功能。上游节点调用 RPC 服务，往许可链写入数据，这些数据将被永久记录在链上。

图11　数据动态管理

5　结论

本文提出了一种基于 PoA 的许可链数据动态存储方法，首先，深入分析了许可区块链网络中数据动态存储

的需求与挑战；然后，详细设计了该方法的实施步骤；最后，在实验室环境中模拟了许可区块链网络，并开发了区块链展示程序以协助完成实验。目前，该方法主要基于 PoA 共识，在未来研究中，笔者计划引入分片机制以提高交易的吞吐量，并引入信誉机制以进一步提升网络的安全性。

参考文献

[1] NAKAMOTO S. Bitcoin：a peer-to-peer electronic cash system [EB/OL]. [2024－09－01]. https：//bitcoin. org/bitcoin. pdf.

[2] 袁勇，王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报，2016，42 (4)：481－494.

[3] SHAKKOTTAI S，STOLYAR A L. Scheduling for multiple flows sharing a time-varying channel：the exponential rule [J]. Translations of the American Mathematical Society-Series 2，2002，207：185－202.

[4] HELLIAR C V，CRAWFORD L，ROCCA L，et al. Permissionless and permissioned blockchain diffusion [J]. International Journal of Information Management，2020，54：102136.

[5] ANDROULAKI E，BARGER A，BORTNIKOV V，et al. Hyperledger fabric：a distributed operating system for permissioned blockchains [C]//Proceedings of the Thirteenth EuroSys Conference，2018：1－15.

[6] WOOD G. Ethereum：a secure decentralised generalised transaction ledger [J]. Ethereum Project Yellow Paper，2014，151：1－32.

[7] CASTRO M，LISKOV B. Practical byzantine fault tolerance [C]//Proceedings of the Third Symposium on Operating Systems Design and Implementation，1999，99：173－186.

[8] JAKOBSSON M，JUELS A. Proofs of work and bread pudding protocols [C]//Secure Information Networks：Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS’99). Boston，MA：Springer US，1999：258－272.

[9] KING S，NADAL S. PPCoin：peer-to-peer crypto-currency with proof-of-stake [J]. Computer Science，2012，19 (1).

[10] DE ANGELIS S，ANIELLO L，BALDONI R，et al. PBFT vs proof-of-authority：applying the CAP theorem to permissioned blockchain [C]//CEUR Workshop Proceedings，2018.

[11] SHAMILI P，MURUGANANTHAM B. Design and implementation considerations of POA network architecture in the Ethereum blockchain [J]. Webology，2022，19 (1)：5330－5352.

[12] POLGE J，ROBERT J，TRAON Y L. Permissioned blockchain frameworks in the industry：a comparison [J]. ICT Express，2021，7 (2)：229－233.

[13] AMIRI M J，AGRAWAL D，ABBADI A E. Caper：a cross-application permissioned blockchain [J]. Proceedings of the VLDB Endowment，2019，12 (11)：1385－1398.

[14] ISLAM M M，MERLEC M M，IN H P. A comparative analysis of proof-of-authority consensus algorithms：aura vs clique [C]//2022 IEEE International Conference on Services Computing (SCC). IEEE，2022：327－332.

[15] MA F，FU Y，REN M，et al. EVM：from offline detection to online reinforcement for Ethereum virtual machine [C]//2019 IEEE 26th International Conference on Software Analysis，Evolution and Reengineering (SANER). IEEE，2019：554－558.

[16] DHILLON V，METCALF D，HOOPER M，et al. Unpacking Ethereum [J]. Blockchain Enabled Applications，2021：37－72.

[17] NA J，KIM H Y，PARK N，et al. Comparative analysis of schnorr digital signature and ECDSA for efficiency using private Ethereum network [J]. IEIE Transactions on Smart Processing & Computing，2022，11 (3)：231－239.

(收稿日期：2024－12－01)

作者简介：

刘新璐 (1998－)，男，硕士，助理工程师，主要研究方向：大数据应用。

闫皓楠 (1993－)，男，本科，助理工程师，主要研究方向：大数据应用。

张平 (1987－)，男，硕士，高级工程师，主要研究方向：大数据应用。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部