文章编号:1671-4598(2020)12-0248-05 DOI:10.16526/j.cnki.11—4762/tp.2020.12.051 中图分类号:TP311.5 文献标识码:A

基于区块链技术的网络终端鉴权认证方法研究

叶海明[1]，徐晓东[2]
(1. 中国人民解放军95910部队，甘肃 酒泉 735000；
2. 中国人民解放军94456部队，山东 威海 264200)

摘要：随着部队作战任务的需要变化，原有的基于有线网络固定终端的网络终端安全认证机制的性能瓶颈逐渐显现，针对存在有线无线网络终端并存、授权认证节点设备易损毁等近似实战情况下入网终端的安全认证要求无法提供低成本、高可靠性的解决方案；为解决上述问题，基于区块链技术的去中心化、防篡改、自动协商的特性，提出高兼容、自适应、抗损毁的网络终端安全认证方法；利用区块链对终端信息进行分布式存储并记录，通过ASE对区块信息进行加密，防止敏感信息泄漏，并利用终端信息对终端进行基于身份的安全认证的方法，经实际应用满足网络终端的权限认证及安全管理需求。

关键词：网络终端；安全认证；区块链；对等网络

Research on Authentication Method of Network Terminals Based on Block Chain Technology

Ye Haiming[1], Xu Xiaodong[2]
(1. 95910th Unit of PLA, Jiuquan 735000, China; 2. 94456th Unit of PLA, Weihai 264200, China)

Abstract: With the development of battle requirements, traditional client authentication based on central station authentication system by wired network can't meet the need of current demands, which are authentication of both wired clients and wireless clients by internal network having some destroyed network devices. In order to overcome these problems, a new authentication solution is designed based on block chain technology which has features including decentration, consensus mechanism, tamper—proofing and so on. And AES is used to encrypt classified information. Final the result is proved to be valid.

Keywords: network client; authentication; blockchain; P2P

0 引言

随着部队作战任务需求不断变化，作战样式及地域持续扩展，从原有的固定训练靶场向山林、丘陵、沙漠等真实作战环境延伸，部队内网从有线网络为主转向有线无线网络混合发展；数据传输类型从原有的语音通话、态势信息，逐步转换为语音、视频、数据多种内容的交互共享发展；数据交互范围从原有的小范围通信，逐步转换为跨区域、跨部门、跨业务领域的交互。作战保障网络终端（简称网络终端）类型从原有的基于有线网络的电脑终端，逐步转向为电脑终端与无线手持终端的混合使用；网络终端部署的要求也发生了变化，布设从原来的小范围单建筑单体布设，向大范围、多区域、快速布设转变，突出特点为网终端设备的稀疏分散，独立作战单位的各类型网络终端可能分布在十几平方公里内以多个节点进行接入，各网络终端之间需保持数据交互。上述变化让网络终端管理工作的难度进一步提升，对网络终端的身份识别及安全认证（简称鉴权认证）提出了更高的要求。

传统的网络终端鉴权认证方式是基于中心式的集中授权，网络终端通过证书、口令、硬件信息等方式，通过网络访问授权中心获取授权，验证后进行服务访问或数据利用，但该授权认证方式与作战实际需求存在差异，在鉴权认证的有效性和稳定性方面存在短板。

集中鉴权认证方式可以较好地满足有线网络、固定终端的鉴权认证需求，但无法满足当前近似作战环境下多种网络结构并存、多操作系统、多类型硬件设备、多种授权方式下手持终端和PC设备混合组网的终端入网鉴权认证需求，尤其是基于有线网络和无线网络业务互通的端到端的服务鉴权认证机制还不完善，单个鉴权服务器的故障即可导致鉴权体系的失效。在作战期间，任何可疑终端的违规接入，非法进行数据交互、对高密级业务的越权访问都会造成不可估量的损失。

为解决该问题，提出基于区块链技术，利用其中心化、分布式存储及信息无法篡改等特性，设计区块体数据结构，实现网络终端信息的分布式存储，并利用AES算法对敏感数据进行加密传输，实现网络终端设备的鉴权认证，满足作战保障对网络终端设备鉴权所需的低成本、抗损毁、高兼容性要求。

1 网络安全终端认证的现状及需求

1.1 作战保障网络结构

随着作战保障需求的提高，要求作战保障网络能够实

收稿日期:2020-07-02； **修回日期**:2020-07-24。

作者简介:叶海明(1984-)，男，山东烟台人，硕士研究生，工程师，主要从事数据的获取采集及应用方向的研究。

现对所属战场环境的时间、空间信息实现实时采集、实时监测、作战信息的实时传输。能够为作战单元的指挥维修提供及时、有效、可靠的数据支撑。因此，原有的范围固定、功能单一的作战信息保障模式已经无法满足现有需求，作战通信网络已逐步由单一的数据传送网络或话音传送网络向数据、话音、视频和交互式多媒体等多种类型信息的综合传输服务演进，网络服务逐渐向多样化的方向发展，终端类型更加多样、网络结构也变得更加复杂，具备分散性、异构性、融合性的发展[1]发展趋势，网络结构可见下图 1 所示。网络终端类型更加多样，其服务内容逐渐向多样化的方向发展，更有效满足通信和信息获取的需求。主要体现在是在移动无线网络与固定有线网络的融合互通以及无线自组网设备的互联互通上。作战相关的信息保障任务主要是通过两类终端完成：1）基于有线网络的 PC 终端，用于态势数据的存储、计算及分析应用；2）基于无线网络的手持终端，用于现场的指挥调度、动态数据的采集存储及作战保障相关业务数据的访问。

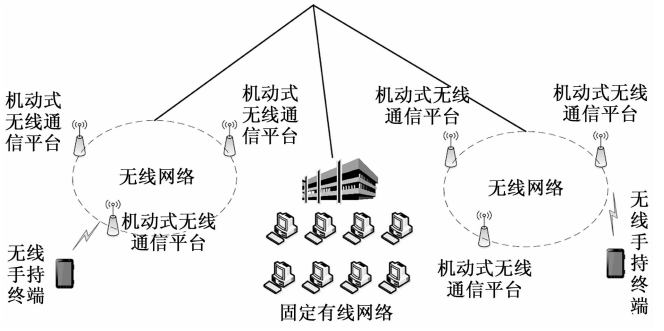

图 1　异构网络框架

1.2　网络终端鉴权的需求

新的网络架构及终端类型必然对应新的需求，网络终端的权限鉴别成为影响作战保障网络安全的瓶颈因素，由于网络规模庞大，终端设备从硬件类型到操作系统均有较大差异，如何能够进行统一的鉴权验证，确保入网终端的安全可靠是必须要关注的问题。作战保障网络对网络终端认证，在保证安全性的前提下，有以下几方面的需求：1）抗损毁效果好，稳定性强，单个或多个网络交换节点机鉴权认证设备的损坏不会造成重大影响；2）兼容性好，对终端设备的硬件类型、操作系统、业务应用有较好的兼容性；3）维护性强，运行维护成本极低，对维护人员及各种备品备件要求低，能够实现在野外等恶劣情况下的快速维修。

现阶段主流的网络终端鉴权模式还是基于同构网络的集中鉴权模式为主，实际上是基于中心式的 C/S 模式，实现方式为以下几种：1）基于网络接入设备或交换设备的硬件形式的鉴权认证，即采用基于网络硬件设备的 IP-SOURCEGUARD 授权认证方式；2）基于鉴权服务器的软件或加密卡等定制软硬件结合产品的授权认证方案，即采用星型、总线型的混合拓扑结构，通过集中安管设备进行接入终端的认证授权。

集中式鉴权验证模式针对使用相同技术体制、网络架构且终端集中部署的专网有成熟的解决方案及有较多的成熟产品，能够满足现有的民用需求。但考虑到实战过程中无法保证数据链路的稳定性，在实战环境下部分网络交换节点甚至包括核心交换节点均存在被破坏的可能性，一旦交换节点被破坏，基于集中式的网络终端的鉴权验证就无法实现，会允许未经授权终端访问敏感数据，造成失泄密问题。为解决这一问题，现在主要的解决措施是在集中式鉴权验证的基础上进行分区域的多重多次鉴权，将多个在业务上较为独立的子网进行统一整合，在实现基层网络层互联互通的基础上，各业务的授权认证体系进行整合，形成多重授权的结构[2]。因此 A 区域终端访问 C 区域终端的拓扑结构可简化为以授权设备为核心的多个星型拓扑结构的连接，如终端 ClientA1 与 ClientC1 实现交互，必须通过 Authen A、Authen B、Authen C 三次授权认证通过后方可进行互联互通，如图 2 所示。

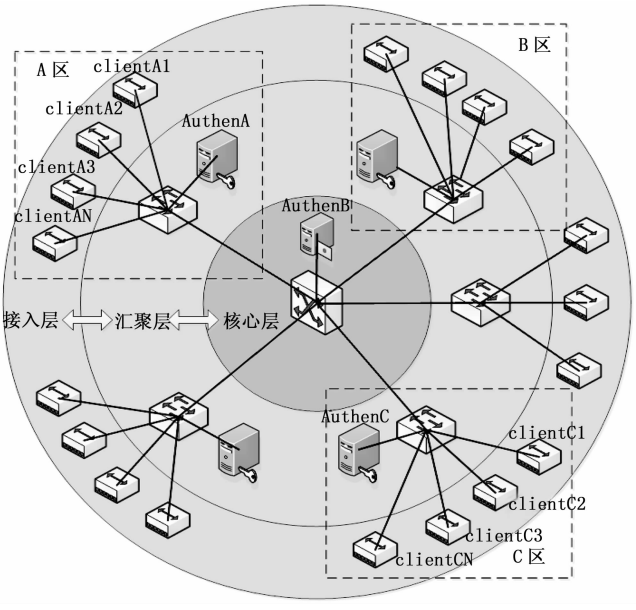

图 2　集中式授权拓扑结构图

该模式存在的缺点：1）抗损毁能力弱，该模式较单一网络授权认证设备的集中授权模式抗损毁性确有提升，但依赖单独授权认证设备的问题并未得到根本解决，要求任何一个业务区域必须存在授权认证设备，一旦该授权认证设备被损毁，还是会导致该区域无法实现网络终端鉴权；2）兼容性不理想，该方案纵向横向兼容性均不理想，不同业务子网的授权验证方式不同，有通过域安全授权认证、有通过基于硬件的 IPSOURCEGUARD 授权认证、有通过 RADIUS 方式授权认证，差异较大，会出现授权认证体系无法兼容导致情况；3）灵活性不高，授权方式固定，入网终端必须与授权设备联网后方可实现授权认证，且需要通过专用硬件实现，性能提升空间不大；4）成本偏高，作战

保障网络入网终端分布地域面积广、终端数量并不多，一个 C 类地址段可满足网络终端入网需求，如使用集中式鉴权模式，需配置大量的鉴权认证设备，维护成本高昂。因此，集中式网络鉴权模式很难满足作战保障网络终端鉴权的需求。

2 网络终端鉴权方案设计

2.1 网络终端鉴权体系框架

作战保障网络可进行简化，即各个业务子网中各终端可以互相访问也可通过汇聚交换机与其他业务子网中的终端进行访问，即可视为多个 P2P 网络组成的异构网络。因此，尝试通过使用区块链技术将集中式的 C/S 模式的入网终端认证模式，进行简化转变为基于 P2P 网络（Peer—to—peer networking，对等网络）终端鉴权认证模式[3]，不再依赖于单一的授权鉴权设备，而是实现每一台入网终端既访问数据也为提供入网终端的鉴权服务。

P2P 网络终端鉴权的技术特点体现在以下几个方面：

1）去中心化[4]，网络中的所有资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行，无需中间环节和服务器的介入。

2）可扩展性，在 P2P 网络中，随着终端的接入，不仅服务的需求增加了，系统整体的资源和服务能力也在同步地扩充，始终能比较容易地满足需要。

3）健壮性，P2P 架构天生具有耐攻击、高容错的优点，由于鉴权服务是分散在各个终端设备之间进行的，部分设备或网络节点遭到破坏对其它部分的影响很小。由于对等网络不需要专门的服务器来做网络支持，因此组网成本较低，维护性高。

4）安全性[5-6]，基于密码学技术保证，未经授权终端即使能够访问到区块链数据，但无法解析数据内容，能够确保数据的安全性。

2.2 基于区块链的网络终端鉴权工作机制

设计私有区块链[7-8]，区块链中的每个区块包含着终端详细信息及对应的权限限制，同时包含着前一数据块的哈希值，在网络中任意一台入网终端都能够访问，合法终端通过加密算法可以对区块链信息进行读取，从读取的信息中判断该终端的类型及访问行为是否合法。

该算法对在区块链交易算法的基础上进行了改进，取消了 POW 工作量验证机制及 transactions 交易机制，不需要重复挖矿、不设置 Proof 验证，避免挖矿导致的硬件资源大量占用的情况。具体步骤如下：

步骤 1：创建区块信息。合法网络终端设备通过一个公私密钥对与区块链网络交互，创建入网终端的区块信息。区块的组成内容包括加密后的基本信息及 hash 头两部分，基本信息包括该入网终端的 IP 地址、MAC 地址及访问权限；hash 头信息，基于入网终端基本信息，使用 sha256 算法进行封装生成 hash 头，可确保一旦区块中的信息被篡改，hash 头信息均会改变，该区块失效，确保在区块链中记录的信息无法被篡改。

步骤 2：形成区块链。通过 socket/http 端口向临近的对等终端进行组播，接收端对合法区块进行验证，验证后加入到区块链中，形成区块链如图 3 所示。

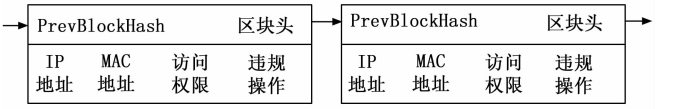

图 3 区块链组成图

步骤 3：形成共识。通过 socket/http 端口进行组播，网络内的对等终端电脑如出现区块认知冲突，则通过比较最长区块链获取共识信息，并通过该链识别网内终端电脑的授权是否合法，因此形成共识的工作分为两步，第一步将区块信息向专网内部所有终端以单播或广播形式发送；第二步，网内终端区块链信息不一致时，通过比较最长区块链获得共识信息，并以最长区块链为合法区块链。

步骤 4：全网终端授权鉴权完成。一旦有新终端入网则自动重复步骤 1～3，实现新终端的鉴权认证；

步骤 5：被访问设备监听访问消息，并从区块链数据记录中获取提交访问需求设备的信息，确定该设备是否能进行数据访问，并将上述内容添加到区块链中向全网进行广播。

步骤 6：网络内部任意终端设备受到广播消息后，验证消息是否有效，若无效则丢弃，有效则向其下一跳节点转发。最后，将有效的交易消息传播到整个区块链网络。

3 关键技术实现及效果验证

3.1 区块链实现

网络终端鉴权的区块链实际上属于私有链（private block chains），主要功能是对入网终端设备访问行为进行鉴权，如符合权限要求则允许进行数据访问；如出现越权访问请求则禁止数据交互行为并将该终端设备标记为非法终端，同时将非法终端数据添加到区块链里，禁止所有合法终端与该终端进行数据交互。

3.1.1 区块链设计

针对网络终端鉴权的要求，对区块的区块头及区块体进行设计，详情如表 1 所示，区块头由本区块的 hash 码、前一区块的 hash 码及本区块产生的时间戳信息组成；区块体由入网终端注册的 IP 地址、MAC 地址、访问权限及该设备的行为属性信息。最终，由上述区块组成一个完整的区块链。

区块体的代码实现如下：

```
def __init__(self):
self. chain=[]
self. hash = None
```

表 1　区块链数据结构

区域	字段名称	大小/byte	描述
区块头	this_hash	64	区块链 hash 头信息
	previous	64	区块链 hash 尾部信息
	timestamp	128	该区块产生的近似时间，精确到秒
区块体	IP	20	入网终端的 IP 地址
	MAC	20	入网终端的 MAC 地址
	level	20	入网终端的访问权限，默认值为 normal/high/administrator
	Action Attribute	20	入网终端的访问行为是否合法，默认值为 legal/illegal

```
self. previous_hash = None
self. timestamp = time. time()
```

如果还有其他的数据内容添加进来，则选取它的 hash 值作为本数据块的 previous _ hash，组建区块头

```
def link(self, block):
self. previous_hash = block['hash']
def create_block(self,data):
JsonData={
'timestamp':time. time(),
'data':data
}
```

生成区块链的哈希码

```
JsonData _ serialized = json. dumps (JsonData, sort _ keys = True). encode('utf-8')
JsonData_hash = hashlib. sha256(JsonData_serialized). hexdigest()
if len(self. chain)>0:
self. link(self. chain[-1])
```

构建区块信息

```
block={
'timestamp':time. time(),
'hash':JsonData_hash,
'pre_hash':self. previous_hash,
'data':data
}
self. chain. append(block)
return block
```

3.1.2　共识算法实现

通过 socket/http 端口进行组播，通过比较最长区块链获取共识信息，并通过该链识别网内终端的授权级别及访问行为是否合法。形成共识的工作分为两步：

步骤 1：将区块信息向专网内部所有终端以单播或广播形式发送，区块信息网内广播。

```
def sendToNode(self,ip,block):
```

将区块信息向专网内部所有终端进行发送

```
sendSocket = socket. socket(socket. AF_INET,socket. SOCK_DGRAM)
sendSocket. sendto(msg,(ip,NETWORK_PORT))
def broadcastSync(self):
self. broadcastPacket(packet_sync_request)
```

以广播形式将区块信息向网内进行发送

```
def broadcastPacket(self,packet):
broadcastSocket = socket. socket ( socket. AF _ INET, socket. SOCK_DGRAM)
broadcastSocket. setsockopt(socket. SOL_SOCKET,socket. SO_BROADCAST,1)
broadcastSocket. sendto( packet, ( "255. 255. 255. 255", NETWORK_PORT))
```

步骤 2：网内终端区块链信息不一致时，通过比较最长区块链获得共识信息，并以最长区块链为合法区块链。

获得专网内部所有终端的 IP 地址信息，用于进行区块链共识比较

```
def register_nodes(self):
values = request. get_json()
nodes = values. get('nodes')
if nodes is None:
return "Error: 节点序列", 400
for node in nodes:
blockchain. register_node(node)
response = {"message":"新的节点已经被添","total_nodes":list(blockchain. nodes)}
return jsonify(response), 201
```

进行共识比较

```
def resolve_conflicts(self):
neighbours = self. nodes
new_chain = None
max_length = len(self. chain)
```

使用 http 端口从网内终端获取区块链，选最长的区块链为合法的共识链

```
for node in neighbours:
print('http://' + node + '/chain')
response = requests. get('http://' + node + '/chain')
if response. status_code == 200:
length = response. json()['length']
chain = response. json()['chain']
```

找到最长的区块链，进行替换

```
if length > max_length and self. valid_chain(chain):
max_length = length
new_chain = chain
if new_chain:
self. chain = new_chain
return True
```

	timestamp	this hash	previous hash	IP	MAC	level	Actio
1	158108074...	5847ed1b0023d2dab298f56c3a69525e591ead81ca153933d3ed1d84ac04b683	NULL	192.168.1.1	01-AF-3B-B1-DF-C3	normal	legal
2	158108074...	c1cefc158fc196005836bba24554b3c7a87dc3ea35a7c783a12e587d51cfe432	5847ed1b0023d2dab298f56c3a69525e591ead81ca153933d3ed1d84ac04b683	192.168.1.2	01-AF-3B-BA-CA-AC	normal	legal
3	158108074...	4da1ad009b8e4453a27c5958a4eeaba69af48dffa965dccd0b6d5a8113b76729	c1cefc158fc196005836bba24554b3c7a87dc3ea35a7c783a12e587d51cfe432	192.168.1.3	01-AF-3B-7C-57-CC	normal	legal
4	158108074...	745ebd65653de6ff2d908777ce3d9f40ac6fd0db11ce7a970dd368e5d44913a4	4da1ad009b8e4453a27c5958a4eeaba69af48dffa965dccd0b6d5a8113b76729	192.168.1.4	01-AF-3B-F0-38-63	normal	legal
5	158108074...	b3f8880b73dd9e9f5f7c76d6a9d2a5041bb16fd3ecff1955ffb12956dc5c6678	745ebd65653de6ff2d908777ce3d9f40ac6fd0db11ce7a970dd368e5d44913a4	192.168.1.5	01-AF-3B-0B-4D-AB	normal	legal
6	158108074...	8b46e67bab8618e5580f5a42e3876267e652cf85a2a1b36670beb5e2c982548a	b3f8880b73dd9e9f5f7c76d6a9d2a5041bb16fd3ecff1955ffb12956dc5c6678	192.168.1.6	01-AF-3B-7A-45-4A	normal	legal
7	158108074...	fe2443940ddc748e3718414fe332b29210ab2e748c302be00fb24754ddc37670	8b46e67bab8618e5580f5a42e3876267e652cf85a2a1b36670beb5e2c982548a	192.168.1.7	01-AF-3B-03-FE-F7	normal	legal
8	158108074...	2503a24e9cd959d838b610348d91f4c7ee09e8c99814e766dd5d65ced95128d6	fe2443940ddc748e3718414fe332b29210ab2e748c302be00fb24754ddc37670	192.168.1.8	01-AF-3B-01-CB-3F	normal	legal
9	158108074...	4f217b0d6bdc6bd7f572f26909075fe99b7870ec9c73394fbc1f2acb9d801485	2503a24e9cd959d838b610348d91f4c7ee09e8c99814e766dd5d65ced95128d6	192.168.1.9	01-AF-3B-DF-17-9F	normal	legal
10	158108074...	f1aa21b104bcc3ff43beaff2ada34cf171b10b43ec916cb7d06ae77b03ca428b	4f217b0d6bdc6bd7f572f26909075fe99b7870ec9c73394fbc1f2acb9d801485	192.168.1.10	01-AF-3B-AA-83-C8	normal	legal
11	158108074...	61a0ec81243de786bdde2a64b384b9c4454b8c271f58fe1f11d1fc2644fb82fe	f1aa21b104bcc3ff43beaff2ada34cf171b10b43ec916cb7d06ae77b03ca428b	192.168.1.11	01-AF-3B-6C-07-F8	normal	legal
12	158108074...	ead3987988dd4a63a334b7e846d0b6e50bca075127064204fc527cbb93e505c3	61a0ec81243de786bdde2a64b384b9c4454b8c271f58fe1f11d1fc2644fb82fe	192.168.1.12	01-AF-3B-30-CA-0A	normal	legal
13	158108074...	0d37294cc0376ea10f6d6a9835b940d4123fc096b40f3af8c7e57192b41d592b	ead3987988dd4a63a334b7e846d0b6e50bca075127064204fc527cbb93e505c3	192.168.1.13	01-AF-3B-AD-C2-68	normal	legal
14	158108074...	754d1284677cdcd0c5dcc1d298416505aeb05c77f6c83c664280d06f2e7d72c8	0d37294cc0376ea10f6d6a9835b940d4123fc096b40f3af8c7e57192b41d592b	192.168.1.14	01-AF-3B-9A-7A-E6	normal	legal
15	158108074...	597df3eebd3d0187e5ceba88d4e175b24e663dbb21f4387bcf8c0e529763cd7a	754d1284677cdcd0c5dcc1d298416505aeb05c77f6c83c664280d06f2e7d72c8	192.168.1.15	01-AF-3B-4D-3C-BC	normal	legal
16	158108074...	122621a5330fae0fede069c3d6a9746197503212e8c527de4ea6c49b102d34b6	597df3eebd3d0187e5ceba88d4e175b24e663dbb21f4387bcf8c0e529763cd7a	192.168.1.16	01-AF-3B-4F-C5-E6	normal	legal
17	158108074...	349a46b5214eea86086191b34cc72202bb15a26097097977c918b15b1bf1616f	122621a5330fae0fede069c3d6a9746197503212e8c527de4ea6c49b102d34b6	192.168.1.17	01-AF-3B-8D-A5-DF	normal	legal
18	158108074...	5ac04a8c940b5951ab35d932a16f14697e2b4f8ec0ccfcf4160656df644d633d	349a46b5214eea86086191b34cc72202bb15a26097097977c918b15b1bf1616f	192.168.1.18	01-AF-3B-46-CD-BA	normal	legal
19	158108074...	909d93762fc287e6cf6ba42bae5bc0383051d74ac34ead02edc12ce739d3e108	5ac04a8c940b5951ab35d932a16f14697e2b4f8ec0ccfcf4160656df644d633d	192.168.1.19	01-AF-3B-ED-C4-58	normal	legal
20	158108074...	1215db2ff88357fecdf5c43223345b785b4cc2055e68d43b446208f235173762	909d93762fc287e6cf6ba42bae5bc0383051d74ac34ead02edc12ce739d3e108	192.168.1.20	01-AF-3B-CE-10-A7	normal	legal
21	158108074...	897a3e858afe0161713a43f3ee2980f5aa088323332f1bf082a92f9d163b6c89	1215db2ff88357fecdf5c43223345b785b4cc2055e68d43b446208f235173762	192.168.1.21	01-AF-3B-C4-B5-CE	normal	legal
22	158108074...	b58317d12d66e2670d551a11be2d312329be3bb601398b55595beaaac121736f	897a3e858afe0161713a43f3ee2980f5aa088323332f1bf082a92f9d163b6c89	192.168.1.22	01-AF-3B-E3-F0-5C	normal	legal
23	158108074...	8d3d5486d5470c0994755a23175fba0326b5999786160fef41bb900cb3b9661f	b58317d12d66e2670d551a11be2d312329be3bb601398b55595beaaac121736f	192.168.1.23	01-AF-3B-02-DE-94	normal	legal
24	158108074...	a04937a2d6c074cdbbd865c3fd95f6b71da8b94b24f76eb153871397d5eb3f32	8d3d5486d5470c0994755a23175fba0326b5999786160fef41bb900cb3b9661f	192.168.1.24	01-AF-3B-42-3E-A4	normal	legal
25	158108074...	6dd7ba9167cded3c56cd336db4e5b060912b63081fdac119ad1f25433db9ebd5	a04937a2d6c074cdbbd865c3fd95f6b71da8b94b24f76eb153871397d5eb3f32	192.168.1.25	01-AF-3B-E5-0E-DB	normal	legal
26	158108074...	4dc5e6aad0ddddf07e9ec16acadb8dc75fbe9fd829c7e43001d5c877cd02249e8	6dd7ba9167cded3c56cd336db4e5b060912b63081fdac119ad1f25433db9ebd5	192.168.1.26	01-AF-3B-A5-F0-79	normal	legal
27	158108074...	a851bfa07a3688dc0b907c1471c8b738424ff9bb67ef366e4300e0f26a6967cb	4dc5e6aad0ddddf07e9ec16acadb8dc75fbe9fd829c7e43001d5c877cd02249e8	192.168.1.27	01-AF-3B-AE-2E-8A	normal	legal
28	158108074...	afc2e30ed9a805af44bc021708b93f4a25017517e456a6d9de7de9562b215d4b	a851bfa07a3688dc0b907c1471c8b738424ff9bb67ef366e4300e0f26a6967cb	192.168.1.28	01-AF-3B-E5-CB-F6	normal	legal
29	158108074...	42dd6679adc7a85107d2e04a0410c59bbd97e8b363ad8e2b5d4fff7bfd7b81b8	afc2e30ed9a805af44bc021708b93f4a25017517e456a6d9de7de9562b215d4b	192.168.1.29	01-AF-3B-E8-CE-9C	normal	legal
30	158108074...	e0bc0db8b62b1f22c61673238fdede38e9afb82d83d1826410625137 52e0cf4e	42dd6679adc7a85107d2e04a0410c59bbd97e8b363ad8e2b5d4fff7bfd7b81b8	192.168.1.30	01-AF-3B-E9-4F-C5	normal	legal
31	158108074...	fbe0dc5faa509828d1b7f0632ef3761c7bc049b2a1a6d2f1238bc1b1030fc462	e0bc0db8b62b1f22c61673238fdede38e9afb82d83d1826410625137 52e0cf4e	192.168.1.31	01-AF-3B-A8-07-48	normal	legal
32	158108074...	fb34c2f27aee7777bf7ea46ada295132ba53e823a787481f0da64101415752e8	fbe0dc5faa509828d1b7f0632ef3761c7bc049b2a1a6d2f1238bc1b1030fc462	192.168.1.32	01-AF-3B-13-AD-76	normal	legal
33	158108074...	ada392280a44e76f9f9a44d4b7d1222e5387715a82127a73066bea22bf7dc73d	fb34c2f27aee7777bf7ea46ada295132ba53e823a787481f0da64101415752e8	192.168.1.33	01-AF-3B-6A-BA-C6	normal	legal
34	158108074...	96cb53326cff66ad94fffa09cf7e7e0df8cb864351e73045e5b80de1c19460e4	ada392280a44e76f9f9a44d4b7d1222e5387715a82127a73066bea22bf7dc73d	192.168.1.34	01-AF-3B-63-B2-A5	normal	legal
35	158108074...	657250eb94cfba3e84f3ee058901d63b35b5eb7acab482f450490f233e125402	96cb53326cff66ad94fffa09cf7e7e0df8cb864351e73045e5b80de1c19460e4	192.168.1.35	01-AF-3B-74-E6-9E	normal	legal
36	158108074...	2b291c05dbd4bf04b50fd06423ec606d78af0af0579cdfe0b1c24d0b267b60a8	657250eb94cfba3e84f3ee058901d63b35b5eb7acab482f450490f233e125402	192.168.1.36	01-AF-3B-85-F5-1C	normal	legal
37	158108074...	ea86620711bac53e6812c33eb5387ae60f1b462d11170a735109eb5309a3a7c8	2b291c05dbd4bf04b50fd06423ec606d78af0af0579cdfe0b1c24d0b267b60a8	192.168.1.37	01-AF-3B-0D-EF-BE	normal	legal
38	158108074...	3b43a02940f35c93c37a73730c98f3d4b586943a4f7684c1bd134dc674389125	ea86620711bac53e6812c33eb5387ae60f1b462d11170a735109eb5309a3a7c8	192.168.1.38	01-AF-3B-CF-5D-7E	normal	legal
39	158108074...	50cd74223ca9bc99dd8fcecfbe5f94ad21e9f038ac584580ff98965259706716	3b43a02940f35c93c37a73730c98f3d4b586943a4f7684c1bd134dc674389125	192.168.1.39	01-AF-3B-68-7D-B6	normal	legal
40	158108074...	47cf3ab87772a0ca897bb69767d31f6166c5093932a940e89c92fcea0d694d85	50cd74223ca9bc99dd8fcecfbe5f94ad21e9f038ac584580ff98965259706716	192.168.1.40	01-AF-3B-FD-6A-CF	normal	legal
41	158108074...	7d499af318bf54a70d737c7abc0b39e802f61a18092f3f5f5ffc09ac0597cb4e	47cf3ab87772a0ca897bb69767d31f6166c5093932a940e89c92fcea0d694d85	192.168.1.41	01-AF-3B-1B-CB-C8	normal	legal
42	158108074...	35f20595871f3d1c6ac99a930df7262d6aed1f63393e0a01ab42a4a44169d52b	7d499af318bf54a70d737c7abc0b39e802f61a18092f3f5f5ffc09ac0597cb4e	192.168.1.42	01-AF-3B-DF-3D-E8	normal	legal

图 4 区块链数据内容

3.1.3 区块体数据加密实现

使用批量加密算法 AES 加密区块链信息，主要是对区块体中的 IP、MAC、level、ActionAttribute 等信息进行加密，确保只有合法用户才能访问区块链中的信息。

{

timestamp:1581080747.2656

this_hash:c1cefc158fc196005836bba24554b3c7a87dc3ea35a7c783a12e587d51cfe432

previous_hash:5847ed1b0023d2dab298f56c3a69525e591ead81ca153933d3ed1d84ac04b683

IP:192.168.1.201

MAC:01-AF-3B-BA-CA-AC

level:normal

ActionAttribute:legal

}

只对区块体数据进行加密，区块体经 AES 加密后，区块链数据如下所示：

{

timestamp:1581080747.2656

this_hash:c1cefc158fc196005836bba24554b3c7a87dc3ea35a7c783a12e587d51cfe432

previous_hash:5847ed1b0023d2dab298f56c3a69525e591ead81ca153933d3ed1d84ac04b683

IP:jfLJIMw0oL2UkkP2AZ0URQ==

MAC:CREbYAbe1sKN7jqbsvROMg7NNJpqWFF51d5qiBheVf4=

level:Fy1lCln1MqM2S5JmT4XvdQ==

ActionAttribute:0gy0FTQHOUxaGDUU84fXuQ==

}

3.2 区块链数据持久化

通过 sqlite 数据库对区块链中的区块信息进行数据进行存储，核心是将区块链信息转换为 JSON，并读取 JSON 中的数据内容存储至终端内部的 sqlite 数据库中，实现区块链信息的持久化存储[9]。对区块链信息解密后存储至 sqlite 数据库后数据内容如图 4 所示。

3.3 效果验证

使用基于区块链技术的分布式鉴权认证模式，可实现在网络状态不稳定、入网终端分散、维护力量薄弱的情况下实现入网终端的鉴权工作。基于区块链的分布式入网终端鉴权和集中式入网终端鉴权在安全性和性能方面的综合比较如表 2 所示。

表 2 性能对照表

方案名称	安全性	稳定性	维护性	成熟性
分布式鉴权	高	高	高	低
集中式鉴权	高	中	中	高

4 结束语

根据区块链的工作原理及技术特征，结合作战保障的

（下转第 257 页）