Computer Science and Application 计算机科学与应用, 2021, 11(2), 400-409
Published Online February 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.112040

Hans汉斯

面向边缘节点的分布式可信系统研究

陈雨晴，郑朝晖

苏州大学，江苏 苏州
Email: 448084942@qq.com

收稿日期：2021年1月22日；录用日期：2021年2月17日；发布日期：2021年2月24日

摘　要

随着物联网和5G的兴起，许多数据密集型的应用也随之发展了起来，如VR，高清视频。物联网终端之间的信息不互通且设备的数据安全性是一个亟待解决的问题。同时，针对移动物联网用户，基站往往会出现数据供应不及时，定位不准确等问题。由此，本文提出了一种基于区块链和边缘计算的分布式可信认证系统，旨在提高物联网终端节点的认证效率以及网络边缘数据的卸载效率。本系统由物理网络层，区块链边缘层和区块链网络层组成。通过区块链网络，设计优化了拜占庭容错共识算法，构建用于存储可信数据和日志的联盟链。此外，物联网边缘节点提供基于智能合约的域名解析和可信认证服务。同时，设计了一种非对称加密方法，以防止节点和终端之间通信时受到非法攻击。我们提出的认证机制是在通信和计算成本方面进行评估的。仿真结果表明，节点认证的时间被控制在一定时间内，本系统可广泛应用于基于不同形式的边缘计算网络，提供安全可靠的边缘缓存卸载服务。

关键词

5G，边缘计算，联盟链，可信认证机制

Research on Distributed Authentication of an Edge Computing System

Yuqing Chen, Zhaohui Zheng

Soochow University, Suzhou Jiangsu
Email: 448084942@qq.com

Received: Jan. 22nd, 2021; accepted: Feb. 17th, 2021; published: Feb. 24th, 2021

Abstract

With the development of the Internet of Things and 5G, many data-intensive applications have

文章引用: 陈雨晴, 郑朝晖. 面向边缘节点的分布式可信系统研究[J]. 计算机科学与应用, 2021, 11(2): 400-409.
DOI: 10.12677/csa.2021.112040

appeared, such as VR and high-definition video. The information between the terminals of the Internet of Things is not interoperable and the data security of the equipment is an urgent problem to be solved. Therefore, this paper proposes a distributed trusted authentication system based on blockchain and edge computing, which aims to improve the authentication efficiency of IoT terminal nodes and the offloading efficiency of network edge data. This system consists of a physical network layer, a blockchain edge layer and a blockchain network layer. Through the blockchain network, the Byzantine fault-tolerant consensus algorithm was designed and optimized, and a consortium chain for storing trusted data and logs was constructed. Simulation results show that the time for node authentication is controlled within a certain period of time. By deploying UAVs to assist edge node caching, this system can be widely used in edge computing networks based on different forms to provide safe and reliable edge caching offloading services.

Keywords

5G, Edge Computing, Consortium Blockchain, Trusted Authentication Mechanism

1. 引言

5G 和物联网的迅速发展已普及到千家万户[1]。传统的物联网平台通常采用云计算来处理各种终端产生的数据信息[2]。然而，这些中心式架构导致了用户彼此信息孤立和数据不兼容等问题。此外，一旦受到攻击，用户隐私就会很容易地暴露。边缘计算作为近年来的热点议题，相对于云计算，将网络资源卸载至用户附近，即网络边缘，为用户的体验感和网络延迟的控制做出了杰出贡献，然而，安全性也是边缘网络所存在的亟待解决的问题。因此，实现分布式和可信认证迫在眉睫。为了建立可信的物联网平台和支持统一的接入模型，区块链作为一个安全统一的分布式账本，对于物联网安全性和分布式特点都有很好的帮助，从而引起了学术界和工业界的广泛关注。

区块链是中本聪在 2008 年提出的，作为一个点对点(D2D)网络平台，区块链一直是被大家讨论的热点技术之一，同时，物联网研究专家也对区块链的安全可信等特征进行了一定的研究[3]。最初区块链通过工作量证明的方法(PoW)来确认网络的完整性和有效性。现有的区块链需要大量的计算和存储资源。例如，一种数据可信度评估的可信系统，算力很强的移动交通工具——汽车充当了矿工[4]。Dorri 等人选择网关作为智能家居的矿工。事实证明，边缘计算应用于区块链边缘节点，可以提高其计算和存储能力。同时，在各种物联网场景中采用区块链的现有工作有许多，如智能交通[5]、智能电网[6] [7]、智能医疗[8]等，主要是为了系统安全或隐私而设计的。很少有研究侧重于不同平台之间的高效认证和协作共享。

因此，我们提出了一种结合边缘计算和区块链的分布式可信认证系统，为智能终端提供高效的认证。系统由物理网络层，区块链边缘层，区块链网络层组成。区块链网络层作为底层支持层，使用优化的实用拜占庭容错(PBFT)共识算法存储认证数据和日志。区块链边缘层包含两种边缘节点，其中一类节点提供名称解析服务，另一类提供边缘节点认证服务。为了保证边缘安全，本文设计了一种基于椭圆曲线密码(ECC)的密码算法。

本文的主要贡献总结如下：

1) 提出了一种基于区块链和边缘计算的分布式可信认证系统。在区块链网络中，设计了一种用于存

储认证数据和日志的优化 PBFT 共识算法。它保证了可信认证，实现了终端的活动可追溯性。

2) 利用动态名称解析策略和 ECC 设计了分布式认证机制。采用名称解析策略，边缘节点可以及时同步终端数据。同时，密码学可以保持边缘节点和终端之间的身份保密性和通信安全性。

3) 提出了一种混合型边缘计算模型，结合无人机等小型基站的移动性等特点，提出了一种综合性缓存策略，以提高边缘节点的命中率，最小化传输延迟。与传统的不能处理移动终端的缓存策略相比，依靠智能合约的策略和无人机的特点，可以动态优化缓存空间的分配。

2. 理论基础

a) 边缘计算的发展

近年来，无线通信的发展导致了智能用户和移动用户的爆炸式增长。伴随着移动用户网络的发展，无线技术以及物联网发展出了许多移动应用和多媒体服务，如抖音 app，AR (虚拟现实)小游戏等。这些应用和服务大多依赖于高速数据服务和低延迟的传输，引发了移动网络中的重要挑战。如图 1 所示，传统的云服务是用户向附近基站发送请求指令，通过一系列的传输线路将请求发送至云服务器，云服务器根据请求将相应的内容通过回程线路传送给用户。边缘缓存通过在边缘设备中缓存内容来使内容更接近用户，并在回程中省略额外的延迟[9]，在基站和用户之间以及用户之间的延迟比云和基站之间要小得多，因此边缘缓存可以大大减少延迟。边缘缓存可以广泛应用在 5G 的场景中，满足低延迟要求。

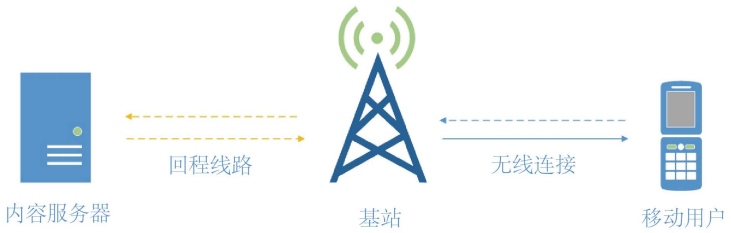


Figure 1. Delay problem between Clouds and mobile users
图 1. 云端回程线路延迟问题

同时，[10]使用移动缓存辅助缓存方案对边缘缓存命中率的性能进行了评估，该方案应用了车载系统充当缓存工具，随着车辆在道路上行驶的增加，可以利用更多的车辆缓存资源，并获得更高的缓存命中率，从而减缓延迟。如图 2 所示，本文提出了无人机辅助小型基站进行边缘缓存的系统，结合区块链架构，在保证安全性的同时，减少了因云服务端传送线路而带来的回程延迟。

b) 基于区块链的可信机制

一般来说，区块链的使用可以概括为三种类型：分布式账本，分布式存储，智能合约。在基于云的区块链网络中，认证效率是一个有待解决的挑战。Tselios 等人[11]认为区块链是基于软件定义网络(SDN)的云计算基础设施的重要安全因素。Ali 等人[12]专注于通过智能合约解决以云为中心的物联网网络中的信任问题。海鹏等[13]将云提供商和矿工之间的交互建模为 Stackelberg 博弈，以优化资源管理和定价问题。虽然这些工作致力于确保数据的有效性，但忽略了能源和计算资源的巨大成本。为了促进边缘处理，边缘计算被认为是一种新的计算范式。如图 3 所示，我们利用边缘计算的计算和存储能力，可以采用分布式方式操作固定和移动终端。

3. 系统模型

本文提出了一个三层体系结构来处理信任和效率问题。该体系结构由物理网络层、区块链边缘层和

网络层组成。每个存储终端被设为$V=\{V_1,V_2,V_3,\cdots,V_M\}$，缓存节点和域名解析节点被定义为$B_c=\{B_{c,1},B_{c,2},B_{c,3},\cdots,B_{c,N}\}$，$B_r=\{B_{r,1},B_{r,2},B_{r,3},\cdots,B_{r,O}\}$。每层的方程式被定义如下：

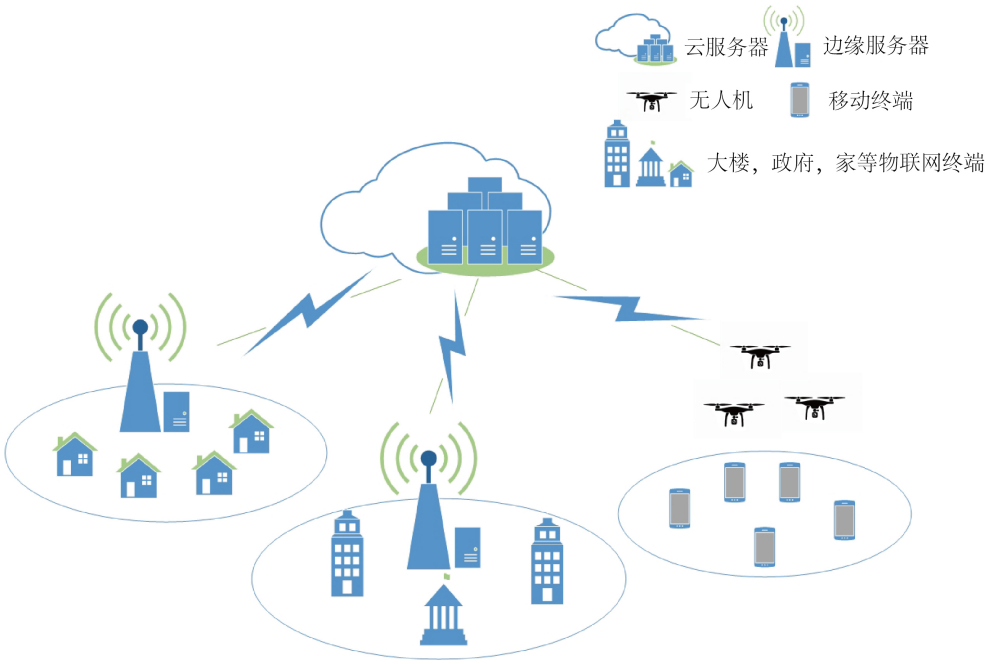


Figure 2. Edge computing structures
图 2. 边缘计算架构

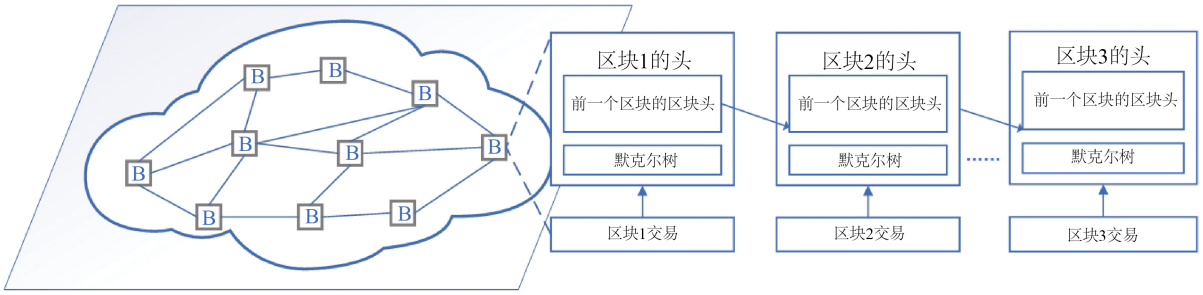


Figure 3. The blockchain edge layer
图 3. 区块链系统模型

1) 物理网络层：物联网采用大量的固定和移动终端，实现监控。本结构中，无人机以及小型基站配备了足够的缓存，负责收集数据并传输到其他层。由于边缘节点之间的移动性和不安全的访问控制系统，本结构提高了对实时响应和边缘安全性的高标准。

2) 区块链边缘层：区块链边缘层节点包含两种节点：缓存节点和域名解析节点。解析节点负责解析域名、验证交易并将块提交到区块链网络。缓存节点用于缓存终端所需的内容。通过认证系统，这些边缘节点可以提供边缘认证服务，并及时同步认证数据，以监测边缘节点的活动。

3) 区块链网络层：区块链网络提供分散的服务，通过 HyperledgerFabric 存储终端信息和创建智能合同。HyperledgerFabric 是一个可定制的区块链平台，有智能合同。作为一个分布式账本，Hyperledger 使用优化的 PBFT 算法有序地存储身份验证日志。分类账中的每个记录器充当时间约束和唯一的密码签名，实现终端的活动可追溯性。

我们对注册验证 ECC 加密结构，以及 PBFT 算法的优化如下：

a) 共识算法优化

本文采用联盟链建立可信认证系统。在区块链中，有不同种类的共识算法，如工作证明、利益证明(PoS)、委托 PoS (DPoS)、时间证明(PoET)和 PBFT [14]。通常，共识算法可以分为三个部分：验证身份，选择节点和同步区块链中的数据。为了满足高实时性的要求，我们采用了不需要令牌的 PBFT 算法。大多数政府和大企业在联盟链中是可信的，可以当做联盟节点。在这种情形下，我们提出了 PBFT 算法的优化去提高可信效率。此外，为了减轻区块链的存储和计算负担，由边缘节点执行解决和记录由多个终端生成的数据的任务。这样，共识算法只用于验证身份并将身份验证日志存储在区块链中，实现数据可追溯，防止数据篡改。

考虑到构成联盟链的大多数联盟对等点都是可信的，因此提出了一种优化的 PBFT 算法，其中主要联盟节点是通过循环选择的。联盟节点在收到认证结果后，通过优化的 PBFT 算法将认证日志写入分类账。假设有 N 个联盟节点。在每一轮达成共识的过程中，将选出一位同行作为演讲，而其他同行则作为候选节点。演讲节点对协商一致结果没有影响，允许主持协商一致进程 N 次。

演讲节点 Nx 由选择出，其中 h 是当前块高度。边缘节点可以向联盟同行广播认证结果。定义 t 以表示生成块的时间间隔。在 t 时间间隔后，Nx 给所有候选节点广播消息。v 表示身份标识，d 是消息摘要，Sigx 是演讲节点的摘要签名。在接收到 pre_prepare 消息后，候选者验证消息和签名，如果消息为真，Ni 将内容广播出去，让其余节点认证。如果这个消息超过 2f + 1 不同的候选节点接收到，则 Ni 广播消息，提交，女巫节点的数量不能超过 。当接收超过 提交消息时，演讲节点可以确认协商一致已经完成，并在区块链账本中生成一个块。认证日志在边缘节点中广播，并更新其分类账。如验证失败，则块将被丢弃，下一轮协商一致将被执行。

b) ECC

作为一种公钥密码学，ECC 确保了安全性，这取决于计算是随机点的点乘法，以及无法计算给定原始点的倍数曲线和积点[15]。

椭圆曲线 E 是在质数有限场 Ep 上的平面曲线，由方程定义 $y=x^3+ax+b$。在 E 上的所有点和无穷点 O 形成一个循环群 G。考虑两个相同质次的循环群 G_1 和 G_2，G_1 是加性循环群，G_2 是乘法循环群。定义 $e:G_1\times G_1\to G_2$ 具有双线性映射的基本性质。

非简并性：存在 $P,Q\in G_1$，使得 $e(P,Q)=1$。

双线性：$e(P+R,Q)=e(P,Q)\cdot e(P,R)$，

$e(aP+bQ)=e(P,Q)^{ab}$，$\forall a,b\in Z_q,\forall P,Q,R\in G_1$。

可计算性：$e(P+R,Q),\forall P,Q\in G_1$

为了保护终端和区块链边缘节点的身份私密性和通信安全性，本文设计了一种基于 ECC 的非对称密码算法。算法由四个步骤组成：设置、主体、签名和验证。

设置：假定一个安全参数 k，一个边缘节点选择两组数 G_1，G_2，排列顺序相同。然后，它选择一个数 $s\in Z_q^*$ 作为节点的私钥，计算主钥 $PK_{BE}=s\cdot P$,这个钥匙对被用来加密和解密消息，防止女巫攻击等恶意攻击。我们选择两个哈希对：$H_1:\{0,1\}^*\times G_1\to Z_q^*$，$H_2:\{0,1\}^*\times G_1\times G_1\to Z_q^*$

主体：根据智能合约，区块链分配一个唯一的 ID id_j 给 V_j，根据名称解析策略，V_j 可以在附近的缓存节点中进行身份验证 $B_{c,n}$。$B_{c,n}$ 会选择一个随机数 $r_j\in Z_q^*$。以下是可以计算用于产生主签名的公式：

$$R_j=r_j\cdot P$$

$$h_j=H_1\left(id_j\,\|\,R_j\,\|\,PK_{BE}\right)$$

$$\delta_{j1} = \left(r_j + \left(h_j \cdot s\right) \bmod q\right)^{-1} \cdot P$$

利用非对称加密，区块链保证了广播中的数据完整性和安全性。V_j 可以确认接收到的消息的可靠性，并确保块记录信息在区块链网络中被“链式”记录。由于它们在生成终端签名和验证身份方面发挥着重要作用，这些参数应保持加密。

签名：当用户 V_j 进入缓存节点 $B_{c,i}$ 的覆盖范围时，DDNS 解析它的 IP 地址并更改认证节点。V_j 需要通过传递数字签名来获得身份认证。随机选取一个数字 $x_j \in Z_q^*$ 当做私钥，同时 V_j 计算相对应的公钥 $PK_j = x_j \cdot P$。给定消息 m 和公共参数，可以得出

$$X_j = H_2\left(id_j \| PK_j \| R_j \| PK_{BE} \| m\right)$$

$$\delta_{j2} = \left(X_j \cdot \left(r_j + h_j \cdot s \bmod q\right) + x_j\right)^{-1} \cdot P$$

验证。$\left(X_j, \delta_{j2}\right)$ 将当做签名被传至 $B_{c,i}$。当接到消息时，$B_{c,i}$ 会根据 $e\left(\delta_{j2}, X_j \cdot \left(R_j + h_j \cdot PK_{BE}\right) + PK_j\right) = e\left(P, P\right)$。若验证成功，$B_{c,i}$ 会传输可信结果在解析节点中，通过改进的拜占庭共识算法生成一个新区块。检验方程如下：

$$\begin{aligned} & e\left(\delta_{j2}, X_j \cdot \left(R_j + h_j \cdot PK_{BE}\right) + PK_j\right) \\ & = e\left(\left(X_j \cdot \left(r_j + h_j \cdot s\right) + x_j\right)^{-1} \cdot P, \left(X_j \cdot \left(r_j + h_j \cdot s\right) + x_j\right) \cdot P\right) \\ & = e\left(P, P\right)^{\left(X_j \cdot \left(r_j + h_j \cdot s\right) + x_j\right)^{-1} \cdot \left(X_j \cdot \left(r_j + h_j \cdot s\right) + x_j\right)} \\ & = e\left(P, P\right) \end{aligned}$$

正如[16]所示，区块链的分散性质可以使对特定实体的分布式拒绝服务(DDoS)攻击无效，因为每个联盟同行都形成了 CONSO 基于协商一致算法的 RTON 区块链可以验证数据的有效性。此外，随着智能契约中所提出的密码学定义，从终端或边缘节点发送的消息被加密。由于无法计算给定的 ECC 结果，使得攻击者几乎无法计算正确的数字签名。因此，系统是可信的。

4. 分布式验证机制(区块链流程图，如图 4 所示)

这是一种动态名称解析策略。作为域名系统(DNS)的基础，它提供边缘认证和数据同步服务。解析节点和缓存节点都维护本地 DNS 数据库，该数据库由终端 ID、公钥和 IP 地址组成。终端将通过相同的域名访问块链边缘节点。解析节点的域名解析器将域名转换为相应的 IP 地址并将其传递给附近的缓存节点。因此，终端可以直接在附近节点中获取证书，具有较低的交付延迟。一旦终端的身份被边缘节点确认，它就可以从一个认证中访问不同平台之间的所有资源，实现单点登录、身份和访问管理。

边缘节点通常为注册的终端维护本地 DNS 数据库，以加快验证速度。对于尚未注册的新节点，节点将在块链网络中提交块，获得唯一的 ID 和相应的公钥。为了避免重复记录，终端信息从缓存节点单向传输到域名解析节点。然后缓存节点以设定的间隔同步 ID 和缓存在域名解析节点中的账户。冗余日志将存储在域名解析节点中，以缓解区块链网络的存储压力，提高查询效率。

5. 性能分析

在本节中，对第三节中定义的攻击模型进行了相应的评估和分析。安全分析中使用了以下前提条件。

1) 攻击者可能是可信认证系统中的合法对象，也可能是非法对象。

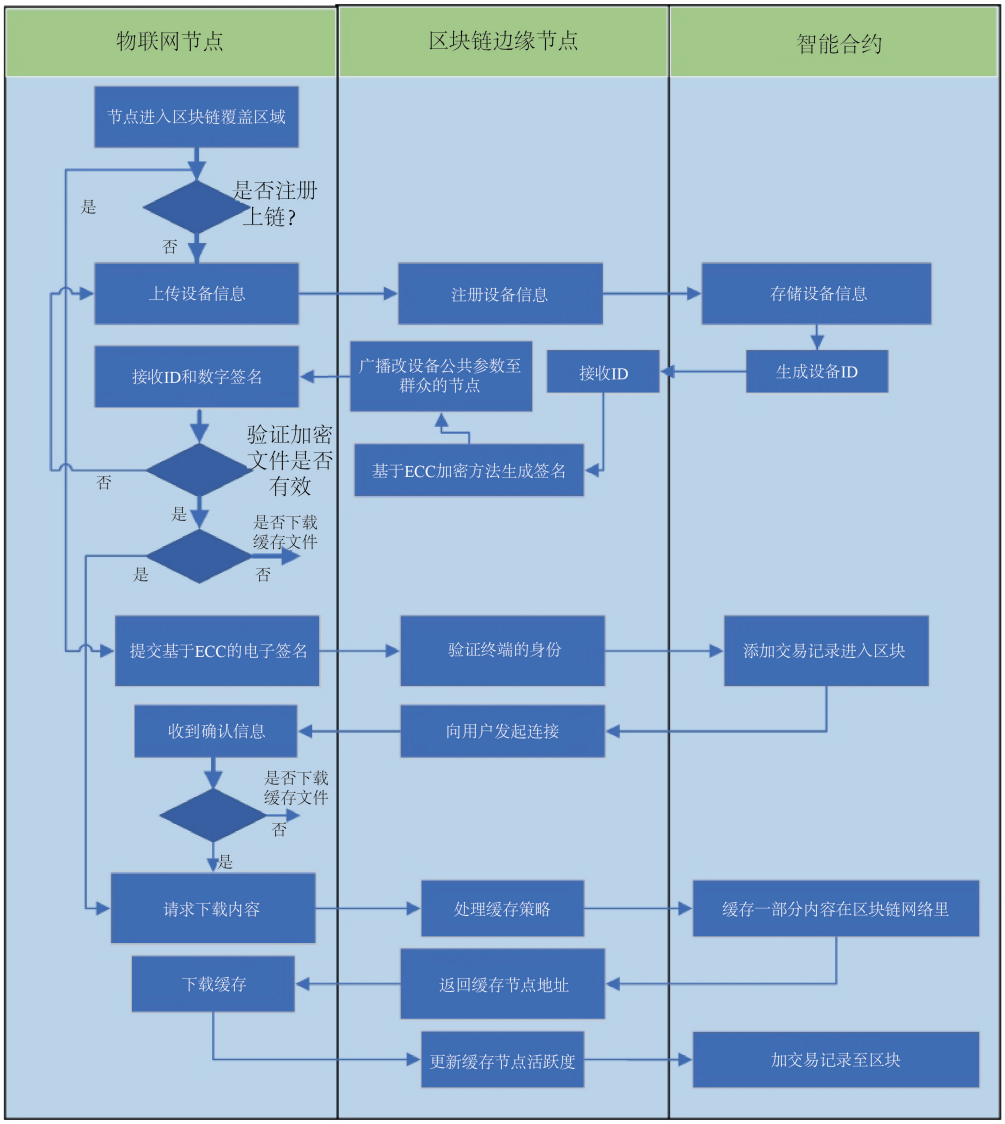


Figure 4. Dynamic caching flow chart
图 4. 动态验证缓存流程图

2) 对于任何 x，y，如果 x 或 y 中的一个未知，则 H(x|y)是未知的。

3) 任何私有信息，包括密码学中的安全参数、边缘节点之间共享的公共参数和 ECC 对，对于攻击者来说都是未知的。

4) 终端信息和数字签名对于攻击者来说是未知的。

根据名称解析策略，认证结果将在区块链边缘节点之间广播。如果攻击者阻止从区块链边缘节点传递到区块链的身份验证消息，并用假签名，联盟同行将检测污染消息，并使用优化的 PBFT 算法丢弃它们。在此之后，阻塞的消息将在下一轮中由随机分辨率节点重新提交，如果失败，协商一致算法可以执行 N 次。因此，只有当来自所有边缘节点的消息被阻塞时，具有假签名的 DoS 才能成为真，这是困难的，因为边缘节点是广泛的。因此，所提出的认证机制可以防止带有虚假签名的 DoS。

最终用 MATLAB 和 HyperledgerFabric 对该系统进行了评价。

信任认证的 1) 性能评估：HyperLedger 织物使用码头容器技术用于运行包含系统应用程序逻辑的链

码本文中的验证环境是在 Ubuntu16 中的 Docker18.06 容器的 HyperledgerFabric1.4 版本中进行的。几个节点实际上托管在一个服务器机器上，充当联盟对等节点，并与 PBFT 协商一致算法达成协议。每个节点为 2.0 GHz 8-vCPUS。VM 是相互连接的通过 1 Mbps 虚拟局域网卡。使用了所提出的密码学，并将典型的定序器部署为单个排序服务。认证过程中的通信和计算成本如表 1 所示。

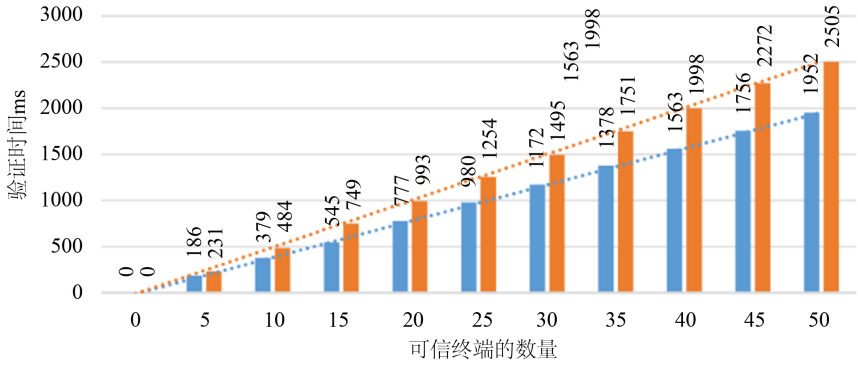
Table 1. Some data related to our work
表 1. 工作相关数据

可信模型参数	花费(单元)
随机数量创世区块(16 bits)	0.5 ms
哈希方程(SHA-256)输入(160 bits)	3 ms
ECC 加密对(176 bits)	10 ms
ECC 点乘法(160 bits)	4 ms
ECC 点加法(160 bits)	2 ms
节点认证	1 ms
PBFT 共识认证时间	11 ms

通信成本：在认证过程中计算通信成本。最初，终端计算哈希值，它需要 80 位(32 位标识，32 位节点数量和 16 位值)。然后通过哈希函数初始化事务，给出输出 160 位。而 ECC 配对产生的大小为 176 位。最后，最后的边缘终端的交易是使用 SHA-256 计算的，它输出 256 位的交易。因此，待认证终端的总体通信成本为 256，176，16，160 = 608 位，由消息摘要、ECC 配对、时间戳和交易组成。

计算成本：随机数发生器、哈希函数和 ECC 配对执行一次。对 ECC 点的乘法和加法进行了两次。当同行金额为 6 时，验证和 PBFT 共识算法承诺分别花费 1 和 15 毫秒。认证的总体计算成本约为 0.53104 × 22 × 211 = 37.5 ms。

在 6 个节点和 10 个节点请求缓存时，图 5 表明在部署的不同数量的对等点下，身份验证时间随着终端数量从 5 个增加到 50 个而增加。原因是，随着终端数量的增加，它们的身份验证等待更长的时间由边缘节点处理。



蓝色柱子代表 6 个节点，红色柱代表 10 个节点。

Figure 5. Delays among authentic terminals
图 5. 可信终端的数量对应的延迟变化

6. 结论

本文提出了一种结合边缘计算和区块链的分布式可信认证系统，以实现不同物联网节点之间的高效

认证和信息共享平台。在系统中，建立了由物理网络层、区块链边缘层和区块链网络层组成的分层认证体系结构。与优化的 PBFT 基于共识的算法，块链存储身份验证数据和日志，保证可信身份验证，实现终端的活动可追溯性。提供一种基于名称解析策略和 ECC 的分布式机制。对攻击模型的评价证明了该机制具有攻击预防和容错性。此外，我们提出了一种基于无人机部署的缓存策略，它可以实现边缘节点之间的协作，最大限度地减少下载延迟。在仿真中，对认证机制进行了评价通信和计算成本方面，证明了该机制是适用的。仿真结果还证明了所提出的缓存策略具有较高的命中率和较低的延迟。比其他基于流行缓存和随机缓存的缓存策略更有延迟。在今后的工作中，我们将将本系统应用于基于区块链的数据共享平台进行试点验证，以进一步优化性能和可用性。

致　谢

此项目是江苏高校优势学科建设工程资助项目。感谢支持。

参考文献

[1] Yang, X., Chen, Z., Li, K., Sun, Y., Liu, N., Xie, W. and Zhao, Y. (2018) Communication-Constrained Mobile Edge Computing Systems for Wireless Virtual Reality: Scheduling and Tradeoff. *IEEE Access*, **6**, 16665-16677. https://doi.org/10.1109/ACCESS.2018.2817288

[2] Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016) Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, **3**, 637-646. https://doi.org/10.1109/JIOT.2016.2579198

[3] Mao, Y., You, C., Zhang, J., Huang, K. and Letaief, K.B. (2017) A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Communications Surveys & Tutorials*, **19**, 2322-2358. https://doi.org/10.1109/COMST.2017.2745201

[4] Chen, M. and Hao, Y. (2018) Task Offloading for Mobile Edge Computing in Software Defined Ultra-Dense Network. *IEEE Journal on Selected Areas in Communications*, **36**, 587-597. https://doi.org/10.1109/JSAC.2018.2815360

[5] Mozaffari, M., Saad, W., Bennis, M., Nam, Y. and Debbah, M. (2019) A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *IEEE Communications Surveys & Tutorials*, **21**, 2334-2360. https://doi.org/10.1109/COMST.2019.2902862

[6] Li, B., Fei, Z. and Zhang, Y. (2019) UAV Communications for 5G and Beyond: Recent Advances and Future Trends. *IEEE Internet of Things Journal*, **6**, 2241-2263. https://doi.org/10.1109/JIOT.2018.2887086

[7] Chetlur Ravi, V.V. and Dhillon, H.S. (2016) Downlink Coverage Probability in a Finite Network of Unmanned Aerial Vehicle (UAV) Base Stations. 2016 *IEEE* 17*th International Workshop on Signal Processing Advances in Wireless Communications*, Edinburgh, 3-6 July 2016, 1-5. https://doi.org/10.1109/SPAWC.2016.7536859

[8] Cui, M., Zhang, G., Wu, Q. and Ng, D.W.K. (2018) Robust Trajectory and Transmit Power Design for Secure UAV Communications. *IEEE Transactions on Vehicular Technology*, **67**, 9042-9046. https://doi.org/10.1109/TVT.2018.2849644

[9] Islambouli, R. and Sharafeddine, S. (2019) Optimized 3D Deployment of UAV-Mounted Cloudlets to Support Latency-Sensitive Services in IoT Networks. *IEEE Access*, **7**, 172860-172870. https://doi.org/10.1109/ACCESS.2019.2956150

[10] Hu, X., Wong, K., Yang, K. and Zheng, Z. (2019) UAV-Assisted Relaying and Edge Computing: Scheduling and Trajectory Optimization. *IEEE Transactions on Wireless Communications*, **18**, 4738-4752. https://doi.org/10.1109/TWC.2019.2928539

[11] Tang, Q., Chang, L., Yang, K., Wang, K.Z., Wang, J. and Sharma, P.K. (2020) Task Number Maximization of Floading Strategy Seamlessly Adapted to UAV Scenario. *Computer Communications*, **151**, 19-30. https://doi.org/10.1016/j.comcom.2019.12.018

[12] Zhou, F., Wu, Y., Hu, R.Q. and Qian, Y. (2018) Computation Rate Maximization in UAV-Enabled Wireless-Powered Mobile-Edge Computing Systems. *IEEE Journal on Selected Areas in Communications*, **36**, 1927-1941. https://doi.org/10.1109/JSAC.2018.2864426

[13] Lakiotakis, E., Sermpezis, P. and Dimitropou-los, X. (2019) Joint Optimization of UAV Placement and Caching under Battery Constraints in UAV-Aided Small-Cell Networks. *ACM SIGCOMM*2019 *Workshop on Mobile AirGround Edge Computing*, *Systems*, *Net-Works*, *and Applications*, Beijing, August 2019, 8-14. https://doi.org/10.1145/3341568.3342106

[14] Khuller, S., Moss, A. and Naor, J.S. (1999) The Budgeted Maximum Coverage Problem. *Information Processing Letters*, **70**, 39-45. https://doi.org/10.1016/S0020-0190(99)00031-9

[15] Krause, A. and Golovin, D. (2012) Submodular Function Maximization. In: Bordeaux, L., Hamadi, Y. and Kohli, P., Eds., *Tractability*: *Practical Approaches to Hard Problems*, Cambridge University Press, Cambridge, 71-104. https://doi.org/10.1017/CBO9781139177801.004

[16] Caro, D.A. and Iovino, V. (2011) jPBC: Java Pairing Based Cryptography. 2011 *IEEE Symposium on Computers and Communications*, Kerkyra, 28 June-1 July 2011, 850-855. https://doi.org/10.1109/ISCC.2011.5983948