计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190800147

基于 TBchain 区块链的高可信云存储模型

李 莹[1,2] 于亚新[1,2] 张宏宇[1] 李振国[1]
1 东北大学计算机科学与工程学院 沈阳 110819
2 东北大学计算机科学与工程学院医学影像智能计算教育部重点实验室 沈阳 110819
(liying1771@163.com)

摘 要 云存储中的数据可能会遭受非法窃取或篡改,从而使用户数据的机密性面临威胁。为了更加安全、高效地存储海量数据,提出一种支持索引、可追溯、可验证的云存储与区块链结合的存储模型 CBaaS(Cloud and Blockchain as a service),它可以增强云中数据的可信性。另外,区块链的协商一致协议导致交易的吞吐量低,处理速度慢,严重制约了去中心化应用的发展。基于此,文中实现了一个三层架构的区块链模型 TBchain(Three-tier architecture Blockchain),其通过分割区块链的一部分并将其锁定在更高级别区块链的块中提高区块链的可伸缩性,从而提高区块链中交易的吞吐量。此外,区块链由于去中心化的需求占用了海量节点的大量存储空间,这极大地限制了以区块链技术为基础的数据库系统的发展与应用。通过 TBchain 将一部分交易存储在本地,增加了区块链存储容量的可扩展性。云存储对象元数据中的 ETag 标示一个 Object 的内容,可以用来检查 Object 内容是否发生变化。将云存储中的对象元数据存储在区块链上,利用 ETag 值可以用于检查 Object 内容是否发生变化的特性和区块链上的数据不可篡改的特性来验证云上存储的数据是否安全,从而提高云上存储数据的可信性。实验结果表明,TBchain 模型提高了区块链的可伸缩性和区块链存储容量的可扩展性,CBaaS 模型也有效地提高了云上存储数据的可信性。

关键词:三层区块链;高可信云存储;可伸缩性;储存扩展性;元数据
中图法分类号 TP311

High Trusted Cloud Storage Model Based on TBchain Blockchain

LI Ying[1,2], YU Ya-xin[1,2], ZHANG Hong-yu[1] and LI Zhen-guo[1]
1 School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
2 Key Laboratory of Intelligent Computing of Medical Imaging, Ministry of Education, School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China

Abstract Data stored in the cloud can be illegally stolen or tampered with, exposing users' data to confidentiality threats. In order to store mass data more safely and efficiently, this paper proposes a storage model CBaaS(Cloud and Blockchain as a service) that supports the combination of index, traceability and verifiability of Cloud storage and Blockchain, which can enhance the credibility of data in the Cloud. Secondly, blockchain consensus protocol leads to low throughput and slow processing speed of transactions, which seriously restricts the development of decentralized applications. Based on this, this paper implements a three-tier architecture Blockchain model TBchain, which improves the scalability of the Blockchain and the throughput of transactions in the blockchain by dividing a part of the blockchain and locking it in the block of a higher level blockchain. Next, due to the demand of decentralization, blockchain occupies a large amount of storage space of massive nodes, which greatly limits the development and application of the database system based on blockchain technology. Part of the transaction is stored locally through TBchain, which increases the scalability of blockchain capacity. The ETag in the cloud storage object metadata is used to identify the contents of an Object and can be used to check if the contents of the Object have changed. By storing the object metadata in the cloud storage on the blockchain, the ETag value can be used to check whether the content of the Object changes and the data on the blockchain can not be tampered with to verify whether the data stored on the cloud is safe and improve the reliability of the data stored on the cloud. The experimental results show that the TBchain model improves the scalability and storage capacity scalability of the blockchain, and the CBaaS model also improves the reliability of data stored in the cloud.

Keywords Three-tier hierarchical blockchain, Highly trusted cloud storage, Scalability, Storage scalability, Metadata

---

到稿日期:2019-08-29 返修日期:2019-10-18 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61871106);基于自由曲面透镜衍射机理的超分辨率计算成像理论研究(61973059);国家重点研发计划项目(2016YFC0101500)
This work was supported by the National Natural Science Foundation of China(61871106), Research on Theory of Super-resolution Computational Imaging Based Optical Diffraction in Freeform Lens (61973059) and National Key Research and Development Program of China (2016YFC0101500).
通信作者:于亚新(yuyx@mail.neu.edu.cn)

1　引言

随着互联网技术的快速发展，具有高可靠、高性能、易扩展、数据优化、安全性强和易管理等特性的云存储成为了存储海量数据的必然选择。在云计算中，虽然云存储是分布式的系统，但是云存储服务还是由中心化的云服务商提供，存储在多个数据中心中的数据并不是完全分布的。这些数据仍然以高密度存储在几个数据中心，即使其中一个数据中心被破坏，也会泄露大量的数据；而且云服务提供商可以从服务端的平台中直接查看和删除用户上传的文件。这种管理机制导致用户的隐私容易泄露。2008 年，Nakamoto 发表了比特币白皮书[1]。区块链[2]是比特币的底层技术，具有去中心化、匿名性、可追溯以及数据不可篡改等特性，与云计算可信、可靠、可控制的长期发展目标不谋而合。云计算的一大特点是按需分配，而区块链本身就是一种资源，有按需供给的需求，是云计算的一个组成部分，因此云计算技术和区块链技术是可以相互融合的。云计算内存储的是一种资源，而区块链里存储的价值不在于存储本身，而在于相互链接的不可更改的块，是一种特殊的存储服务。本文以“平安城市”为背景，将区块链的存储服务与云计算的存储服务结合，让视频、语音、文件等作为公认有效的法律依据。

为了更加安全、高效地存储海量数据作为平安城市有效的法律依据，本文提出了一个云存储与区块链结合的存储模型 CBaaS。将平安城市中的视频、语音、文件等通过对象存储的方式存储在云上会产生该 Object 的元数据信息，元数据是对上传到对象存储的文件的属性描述。元数据中包含 Object 生成时会创建的相应 ETag（Entity Tag），ETag 用于标示一个 Object 的内容。对于 PutObject 请求创建的 Object，ETag 值是其内容的 MD5 值；对于其他方式创建的 Object，ETag 值是其内容的 UUID。MD5 是一种 Hash 运算，输入数据的稍微改变都会引起 Hash 运算结果面目全非，而 UUID 是一种通用唯一识别码。当 Object 内容发生变化时，ETag 中对应的 MD5 或 UUID 都会相应发生变化，因此 ETag 值可以用于检查 Object 内容是否发生变化。区块链具有不可篡改的特性，可以保证在区块链上存储的元数据不会改变。当需要验证云上数据是否被篡改时，将此时云上的 ETag 与区块链上存储的元数据中的 ETag 进行对比，两者相同则说明此时云上存储的内容没有改变，两者不同则说明云上存储的内容已经发生改变。

区块链的协商一致协议要求区块链网络中的每一个节点处理区块链中的每一个块，使得整个系统中的所有节点能够在去信任的环境中自由、安全地交换数据。但这也给区块链带来了可伸缩性[3]限制，导致区块链的交易吞吐量较低。为了克服区块链的协商一致协议带来的弊端，本文提出了一个区块链的三层架构模型 TBchain，它将一部分交易放在本地区块链上进行，既提高了云上存储数据的公信力和区块链的可伸缩性，又减小了基础层区块链的存储压力。

本文的主要贡献如下。

（1）提出了一个三层架构的区块链模型。通过分割区块链的一部分并将其锁定在更高级别区块链的块中，来克服区块链协商一致协议导致的可伸缩性限制，从而提高了区块链中交易的吞吐量。

（2）TBchain 模型提高了区块链容量的可扩展性[4]。将交易数据存储在本地节点上，多个交易数据组合生成的 hash 值存储在公共区块链上，减小了区块链的存储压力，提高了区块链容量的可扩展性。

（3）设计了一个将云存储与 TBchain 结合以提高区块伸缩性和云存储可信性的存储模型。基于区块链数据不可篡改和 ETag 值可以用于检查 Object 内容是否发生变化的特性，可以根据区块链上存储的相关元数据验证云上存储数据的完整性。

（4）实现了云存储与 TBchain 结合以提高区块伸缩性和云存储可信性的模型 CBaaS。CBaaS 存储模型由 4 层模块组成，分别是用户层、验证层、存储层和数据层。

2　相关工作

云存储可以为用户提供按需外包的数据服务，当前云存储的高可信能力是业界最为关注的问题之一。区块链的协商一致协议导致的可伸缩性限制使得区块链交易吞吐量低，能否提高交易吞吐量是区块链能否被广泛应用的关键问题。Otte 等[3]设计的 TrustChain 能够在没有中央控制的情况下在陌生人之间创建可信的事务，该方案提供了可伸缩性、开放性和抗 sybil 性，同时用一种建立事务有效性和完整性的机制替换了工作证明。Eyal 等[5]设计的 Bitcoin-NG 是一种区块链协议，具有良好的扩展性和拜占庭式的容错能力，抗极端波动能力强，并共享相同的信任模型，避免了质的变化生态系统。Sompolinsky 等[6]创建的 GHOST rule 提高了区块创建的速度，GHOST rule 是对比特币节点方式的一种修改构造和重组区块链。

Zhou 等[7]将信任与 RBAC 集成在一起，提出了两种概率模型，以提高云数据存储的安全性，但是这种模型容易受到共谋攻击。Uikey 等[8]提出了一种新的 RBAC 模型 Trust-RBAC，该模型可以抵抗共谋攻击，但是无法抵抗 Sybil 攻击。Tian 等[9]提出了公共数据审计的体系结构，它可以有效、安全地验证云是否诚实、正确地存储外包数据。但是，这种方法无法保证审计的第三方真正可信。

为了更加安全高效地存储海量数据，可以结合区块链与云存储来解决这个问题。Zhao 等[10]设计了一个区块链双层网络 Mchain，将在云的 VMs pool 中生成的 VM Measurements 存储在 Mchain 上，通过验证 VM Measurements 和策略的完整性，来判断数据是否被篡改。Sukhodolskiy 等[11]提出了一个基于区块链事务的访问控制模型，将数据存储在不受信任的云存储中，并实现了基于属性加密的以太坊智能合约。Westerlund 等[12]通过构建分布式云，将平台货币化规则嵌入到区块链的交易结构中，与建立在集中技术上的平台相比，货币化更加透明。上面几种方案都在一定程度上提高了云数据的安全性，但对区块链交易吞吐量并没有明显的提高。因此，本文提出了一个云存储与三层架构的区块链模型相结合的存储系统 CBaaS，以更加安全高效地存储海量数据。

3　问题定义

（1）可信性（Credibility）。计算机可信性指计算机系统提

供可验证的可信服务的能力。相对于传统的计算平台而言，云计算对计算机系统的可信性提出了更高的挑战。云计算平台将超大规模的计算机系统进行整合，并且通过 Internet 的方式提供给多个不同组织的用户。相对于传统的计算平台，云计算具有超大规模、单一接口、跨组织性、以服务为中心等特性，因此云计算平台的可信性成为了云计算被广泛应用过程中必须要解决的问题。

(2)可伸缩性(Scalability)。可伸缩性是一种针对软件系统计算处理能力的设计指标，简单来说，就是以更大规模来处理事情。高可伸缩性代表一种弹性，在系统扩展成长过程中，软件能够保证旺盛的生命力，通过很少的改动甚至只是硬件设备的添置，就能实现整个系统处理能力的线性增长，实现高吞吐量和低延迟高性能。对于区块链来说，提高可伸缩性是增加事务吞吐量或区块链上执行的事务数量。

(3)储存扩展性(Storage Scalability)。区块链技术要求区块链网络中每个完全节点都保存着完整的区块链信息，占用海量节点的大量存储空间，造成极大的浪费。储存扩展性即在区块链模型具有一定安全性的前提下，同时减少了海量节点的大量存储空间，有效地增强了区块链的储存扩展性。

表 1 列出了中英文名词对照表。

表 1 中文英名词对照表

Table 1 Chinese-English index

英文	中文
SB	顶层区块链
MB	第二层区块链
UB	第三层区块链
SB-AGB	SBC 区块链的第一块
SB-DB	SBC 区块链的数据块
MB-AGB	第一个 MB 区块链的第一块
MB-RGB	非第一个 MB 区块链的第一块
MB-DB	MB 区块链的数据块
MB-TB	MB 区块链的终端块
UB-AGB	第一个 UB 区块链的第一块
UB-RGB	非第一个 UB 区块链的第一块
UB-DB	UB 区块链的数据块
UB-TB	UB 区块链的终端块

定义 1(顶层区块链(Super Blockchain, SB)) $Fs=\{$SB-AGB, SB-DB$\}$是 SB 中区块类型的集合。

定义 2(第二层区块链(Middle Blockchain, MB)) $Fm=\{$MB-AGB, MB-RGB, MB-DB, MB-TB$\}$是 MB 中区块类型的集合。$Cm_1=\{$MB-AGB, MB-DB, MB-TB$\}$是第一条 MB 区块链，$Cm_2=\{$MB-RGB, MB-DB, MB-TB$\}$为除第一条区块链之外的其他区块链。

$$S_j=[(n_0+1)+\sum_{i=1}^{j}(n_i+2)] \tag{1}$$

式(1)用于求第二层中第 j 个 MB 的终端块 MB-TB 的索引值。其中，n_0 代表 MB 中第一条区块链的第一个区块 MB-AGB 的索引，n_i 代表第 i 个 MB 的数据块 DB 的个数。

$$m_j=S_{j-1}+1 \tag{2}$$

式(2)用于求第二层中第 j 个 MB 的 MB-RGB 的索引值。其中，S_j 代表第 j 个 MB 的终端块的索引，m_j 表示 MB-RGB 的索引。

定义 3(第三层区块链(Underlying Blockchain, UB)) $Fu=\{$UB-AGB, UB-RGB, UB-DB, UB-TB$\}$是 MB 中区块类型的集合。$Cu_1=\{$UB-AGB, UB-DB, UB-TB$\}$是第一条 UB 区块链，$Cu_2=\{$UB-RGB, UB-DB, UB-TB$\}$为除第一条区块链之外的其他区块链。

$$r_k=[(p_0+1)+\sum_{l=1}^{k}(p_1+2)] \tag{3}$$

式(3)代表第二层中第 k 个 UB 的终端块 UB-TB 的索引值。其中，p_0 代表 UB 中第一条区块链的第一个区块 UB-AGB 的索引，p_i 代表第 i 个 UB 的数据块 DB 的个数。

$$q_k=r_{k-1}+1 \tag{4}$$

式(4)代表第二层中第 k 个 UB 的 UB-RGB 的索引值。其中，r_k 代表第 k 个 UB 的终端块的索引，q_k 表示 MB-RGB 的索引。

MB 与 UB 的结构和功能一样，都包含$\{$AGB, RGB, DB, TB$\}$ 4 种区块，负责存储数据并向上一层传输数据，且可以根据需要建立多条。SB 只有一条，只包含$\{$AGB, DB$\}$区块，负责存储数据并将数据推送到以太坊上。

定义 4 TBchain(Three-tier architecture Blockchain)是一个三层架构的区块链模型，以一个安全的基础层区块链(以太坊)为基础，并在基础层区块链上构建协议。$L=\{$SB, MB, UB$\}$是构成 TBchain 的区块链的集合。

定义 5 CBaaS(Cloud and Blockchain as a Service)是云存储和三层架构的区块链模型 CBaaS 结合生成的安全高效地存储海量数据的模型。

4 提高区块链可伸缩性的三层架构模型

区块链的协商一致性要求区块链网络中的每一个节点处理区块链中的每一个块，使得整个系统中的所有节点能够在去信任的环境中自由安全地交换数据。但这也给区块链带来了可伸缩性限制，导致区块链的交易吞吐量低。本文的三层架构模型以一个安全的基础层区块链(以太坊)为基础，并在基础层区块链上构建协议，以提高区块链的可伸缩性。对于区块链来说，提高可伸缩性是增加事务吞吐量或区块链上执行的事务数量。

4.1 传统的区块链体系结构

在传统的区块链(如图 1 所示)中，所有节点共同维护一条不断增长的单一的全球链(比如比特币区块链或者以太坊区块链)，只能添加记录，不可删除、篡改记录。同时，在传统的区块链中，通常将一段时间内的多个事务打包在一个区块中以增加事务吞吐量。区块之间通过 hash 值以防篡改的方式连接在一起，其中每个块都指向前面的块。

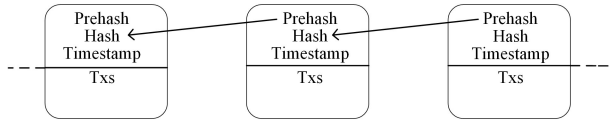

图 1 传统的区块链体系结构

Fig. 1 Traditional blockchain architecture

4.2 三层架构的区块链的模型

本文实现了一个不可变的按时间顺序排列的交互链 TBchain，第一层的区块链称为 SB，第二层的区块链称为 MB，第三层的区块链称为 UB。区块链网络中的每一个节点都可以在第二层和第三层创建自己的 genesis 块，并构建可伸缩的区块链，它在本质上是并行的。提高区块链的三层架构模型 TBchain 如图 2 所示。

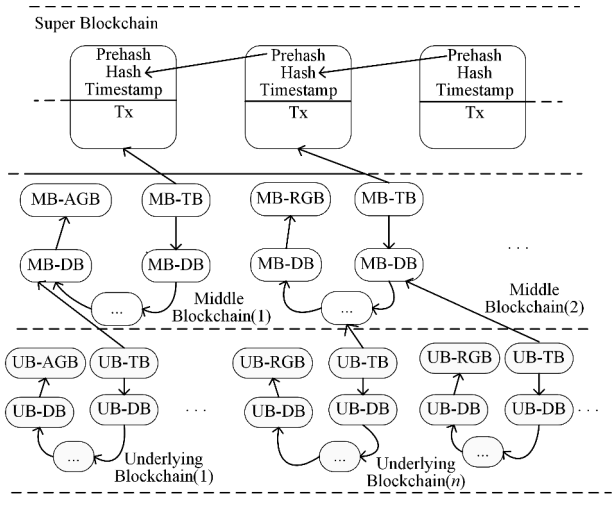

图 2　区块链的三层架构模型

Fig. 2　Three-tier architecture model of blockchain

由式(1)和式(2)可知，第二层前一个 $MB_{(i)}$ 中 MB-TB 的索引加 1 等于下一个 $MB_{(i+1)}$ 中 MB-RGB 的索引。同理，由式(3)和式(4)可知，第三层前一个 $UB_{(j)}$ 中 UB-TB 的索引加 1 等于下一块 $UB_{(j+1)}$ 中 UB-RGB 的索引。第二层、第三层的小区块链通过索引连接成一条长区块链。

传统区块链直接将交易数据存储在区块链上，虽然保证了数据安全可靠，但区块链上所有节点都必须存储所有的交易，这极大地浪费了存储空间，也极大地限制了以区块链技术为基础的数据库系统的发展与应用[4]。同时，由于区块上所有节点都必须对每个交易进行验证，导致了区块链上交易的吞吐量较低。与传统的区块链不同，TBchain 将传统区块链作为基础层或“第一层”，在安全的基础层区块链之上构建了一个三层的区块链模型，扩展了公共区块链的有用性，让交互发生在需要的时候，但仍然可以追溯到可靠的基础层。每个用户将自己的交易存储在本地，将多个交易的 hash 值合成一个 hash 值向上传递至基础区块链，提高了基础层区块链存储容量的可扩展性和区块链上交易的吞吐量。同时，为了提高区块链对篡改的抵抗力，每个数据块还引用了下一层中对应区块链的终端块，这确保了每个存储交易的区块有两个传入指针和一个传出指针。每个参与者都增长并维护自己的事务链，而不是所有节点共同维护一条不断增长的单一的全球链。另一个区别是，传统的区块链中通常将多个事务打包在一个区块中以增加事务吞吐量，而在 TBchain 中，我们假设每个区块最多描述一个事务。

4.2.1　区块的构成

SB，MB，UB 区块链中的区块都包含 Index，TS，Data，PH，CH，Nonce 几个部分。

(1)Index 表示该区块链中该区块的索引。

(2)TS 表示区块生成时刻的时间戳。

(3)PH 表示前一个区块的 hash 值。

(4)CH 表示当前区块的 hash 值，区块之间通过 hash 值以防篡改的方式连接在一起，其中每个块都指向前面的块。

(5)Nonce 是一个无意义的随机数，用于工作量证明，与挖矿的难度有关。

Index，TS，PH，CH，Nonce 与普通区块链中区块的对应域基本一致。但 SB，MB，UB 区块链中区块的 Data 域与普通区块链中区块的 Data 域有所不同。

Data 域在 AGB 与 RGB 中存放的是固定写好的数据，在 DB 中存放的是写入区块链的数据，在 TB 中存放的是该区块链中 TB 之前所有区块的当前的 hash 值连接之后的 hash 结果；UB-DB 中存放的是交易的数据，MB-DB 中存放的是 UB-TB 的内容，SB-DB 中存放的是 MB-TB 的内容。

4.2.2　在三层架构的区块链模型中将交易存储在区块链上

在本文中，UB 和 MB 区块链都包含 GB(AGB 或者 RGB)，DB，TB 3 种类型的区块，因此要求每条区块链的长度至少为 3。交易存储在区块链上共分为 4 种情况：UB 与 MB 的长度 m_1，m_2 均设为 3；UB 的长度 m_1 为 3，MB 的长度 m_2 大于 3；MB 的长度 m_2 为 3，UB 的长度 m_1 大于 3；UB 与 MB 的长度 m_1，m_2 均大于 3。

在算法 1 中，当有交易传来时，需要先通过函数 create_new_UnderlyingBlockchain()创建一条第三层 UB 区块链，根据具体条件生成对应的区块，然后将交易存储到区块的数据域中。通过函数 create_new_MiddleBlockchain()创建一条 MB 区块链，每当生成一条完整的 UB 区块链后，创建 MB 的区块，将 UB-TB 中的数据传到 MB 的数据域中。生成一条完整的 MB 区块链后，通过 create_new_block(SB)创建 SB 的区块将 MB-TB 中的数据传到 SB-DB 的数据域中，最后将 SB-DB 中的数据推送到以太坊上。通过算法 1 可以将交易的数据推送到区块链上进行存储。

算法 1　将交易推送到区块链的过程

```
Input:transaction data
Output:push transaction to Ethereum
Var dataset=read input data;
tra=dataset
1. for tra is not empty do
2.    create_new_UnderlyingBlockchain()
3.       Generate UB-AGB,UB-RGB,UB-DB,UB-TB
4.    create_new_MiddleBlockchain()
5.       Generate MB-AGB,MB-RGB,MB-DB,MB-TB
6.    create_new_block(SB)
7.       GenerateSB-AGB,SB-DB
8.    Push_to_ethereum(SB)
9. end for
```

本文创建了三层的区块链模型，验证了高级区块的完整性，确定了所有低级区块的完整性，减少了验证链所需的操作数量。每一个运行了该框架的用户均可以在自己的节点上创建 UB，MB 和 SB，通过 API 接收交易数据，将交易存储在本地并完成验证；然后将包含这些交易的所有 hash 值的 hash 最终存储在 SB-DB 中，通过在不同层的区块之间建立哈希绑定关系，将 SB-DB 中与交易相关的 hash 值推送到区块链上并完成验证。这个过程是并行的，在一定程度上降低了区块链协商一致性的要求，提高了区块链的可伸缩性和交易的吞吐量。

5　基于区块链提高云存储的可信性

为了处理海量数据，越来越多的应用借助云平台来扩大用户终端的存储容量。虽然区块链具有不可篡改、去中心化、可追溯等优点，但在区块链中存储海量数据是不现实的。此外，存储在区块链中的数据是开放和透明的，因此不建议在链

上存储敏感数据。本文模型利用云存储来提高存储效率，利用区块链的自身特性来存储数据的元数据，以提高块的构建效率和云存储的可信性。

5.1 CBaaS 存储模型

基于三层架构的区块链存储模型 TBchain，本文将云存储和 TBchain 区块链存储模型结合，以实现高可信存储模型 CBaaS。如图 3 所示，CBaaS 存储模型共由 4 层模块组成：用户层、验证层、存储层和数据层。

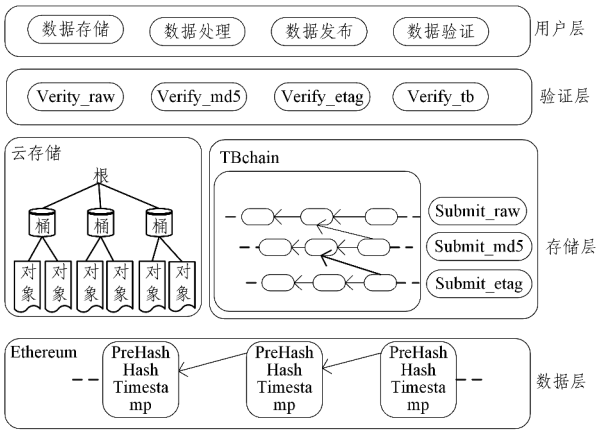

图 3 三层架构模型中各区块链数据块之间的关系

Fig. 3 Relationship between each blockchain data block in three-tier architecture model

5.2 CBaaS 系统的运行

元数据中包含对象存储中的 Object 生成时创建的相应 ETag，ETag 用于标示一个 Object 的内容。对于 PutObject 请求创建的 Object，ETag 值是其内容的 MD5 值；对于其他方式创建的 Object，ETag 值是其内容的 UUID。MD5 是一种 Hash 运算，输入数据的稍微改变都会引起 Hash 运算结果面目全非，而 UUID 是一种通用的唯一识别码。当 Object 内容发生变化时，ETag 中对应的 MD5 或 UUID 都会相应发生变化，因此 ETag 值可以用于检查 Object 内容是否发生变化。

CBaaS 系统运行的过程如下：

(1)当数据需要进行安全存储时，首先将平安城市的视频、语音、文件存储在腾讯云上，云上会生成对应的元数据；

(2)信息宿主使用 HeadObject 命令获取对象的元数据；

(3)信息宿主通过相应的提交函数(Submit 类函数)的 API 接口将元数据存储在区块链 TBchain 上；

(4)当从云上下载需要的数据时，验证者向云存储平台申请对应对象的元数据；

(5)云对验证者的请求作出响应；

(6)验证者通过相应的验证函数(Verity 类函数)的 API 验证区块链上是否存在与此时的元数据相匹配的数据，如果存在匹配数据，说明云上对应存储的数据安全可信，可以作为法律依据，否则说明数据已被篡改。

6 CBaaS 存储模型四层模块的设计

6.1 数据层

本文的基础区块链是以太坊，每一个区块都包含区块头和区块体。如图 4 所示，在以太坊区块链中，数据在区块中以 Merkle 树[22]的形式存储。交易数据存储在交易体中，并通过不断地两两哈希运算得到只有一个哈希值的 Merkle 树根，Merkle 树根被存储在交易头中。当用户需要访问或者验证一笔交易时，系统会向存储了所有交易的节点发出请求，该节点就会将该笔交易的叶子组合和子节点组合发送过来。最后将算出的 Merkle 树根哈希值与区块头保存的哈希值进行对比，其相互一致，就证明交易验证通过。

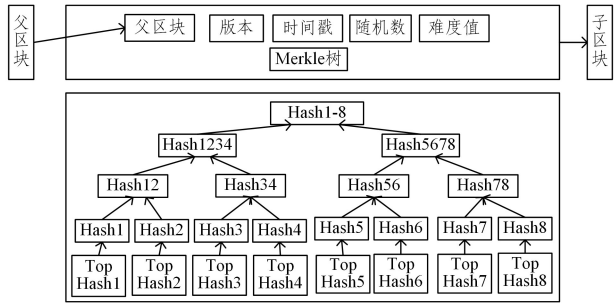

图 4 区块的内部结构

Fig. 4 Internal structure of the block

随着区块链上保存的数据越来越多，普通节点难以维持一个区块链全节点，本文的 TBchain 区块链模型在一定程度上缓解了这个问题。TBchain 将用户的数据放在自己的本地节点上，基础层区块链上存储的交易数据实际是 Super Blockchain 的 Data 域中存储的 Top Hash。一个 Top Hash 可以追溯到多个交易数据，从而进一步提高区块链容量的可扩展性。每一个区块的 Merkle 树根都放进下一个区块的区块头里成为父区块哈希值，相当于下一个区块保存了上一个区块的所有交易，这样环环相扣的链接，让任何虚假交易或伪造区块都难以混进系统的区块链接中，除非从创世区块开始就修改交易内容，但这个代价太大，几乎不可能完成，从而保证了 TBchain 中交易数据的安全性。

6.2 存储层

CBaaS 的存储层由云存储和区块链两部分构成。将用户提供的视频、图片等海量数据存储在云上，需要使用对象存储。数据存储在云上后会生成对象元数据，将对象的元数据信息存储在区块链上能减轻区块链的存储负担。在存储层设计了 3 种存储元数据的方式：用 Submit_raw 存储元数据自身信息，用 SBmit_md5 存储元数据的 MD5 值，用 Submit_etag 存储元数据中的 ETag。后两种方式可以进一步地减少区块链的存储空间，增加了区块链的存储容量可扩展性。云上元数据并没有存储在公共区块链上，而是存储在自己本地的区块链 TBchain 上。存储层中，UB，MB，SB 的区块中存储数据的框架如图 5 所示。

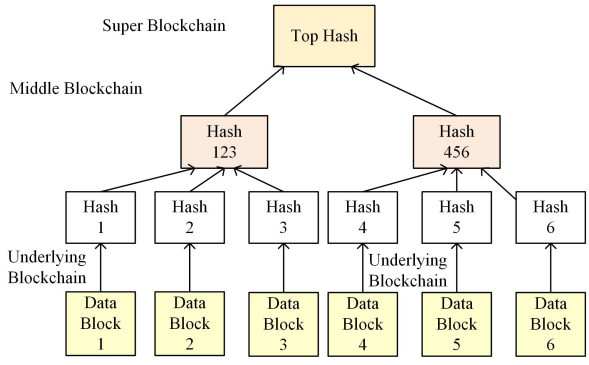

图 5 三层架构的可扩展存储框架

Fig. 5 Extensible storage framework with three-tier architecture

UB 的数据块中存放的是来自云存储的元数据信息，每一个区块都会根据交易数据生成一个 hash 值。区块链 UB 的终端块 UB-TB 中存放的是该区块链上 UB-TB 之前所有区块的当前 hash 值连接之后的 hash 结果。MB-DB 中存放的是 UB-TB 的内容，即一个 MB 的数据块中存放的是一条 UB 区块链所有交易数据 hash 值的 hash 结果。同理，区块链 MB 的终端块 MB-TB 中存放的是该区块链上 MB-TB 之前所有区块的当前 hash 值连接之后的 hash 结果。SB-DB 中存放的是 MB-TB 的内容，即一个 SB 的数据块中存放的是一条 MB 区块链所有交易数据 hash 值的 hash 结果。最后，将 SB 层区块链中的 hash 数据推送到以太坊上，以便在需要的时候能够根据以太坊上的 hash 值追溯到交易所在区块链，得到交易所在区块的索引号、时间戳和原始交易数据，从而提高区块链的容量可扩展性。

6.3　验证层

由 5.2 节可知，ETag 值可以用于检查云存储中 Object 内容是否发生变化。本文使用对象存储完成云存储，当在对象存储上上传平安城市的视频、语音、文件后，会生成对应元数据。元数据中包含内容类型、内容长度、连接状态、ETag、最后修改时间等。在云上存储文件后，将相应的元数据通过 API 提交到区块链上。区块链的去中心化、不可篡改、可追溯的特性，可以保证存储在区块链上的数据不被篡改。当需要下载云上数据作为公认有效的法律依据时，在区块链上检索此时云上的元数据。由于 ETag 具有唯一性，如果可以在区块链上找到相匹配的数据，说明云上数据未被修改，可以下载作为法律依据；否则，说明此时云上的数据已被篡改，不满足数据的完整性，不可以作为法律依据。

CBaaS 的验证层提供了 4 种不同的验证方法：verify_tb 保证了 UB 和 MB 区块链的块序列没有被篡改；与 submit_raw 对应，verify_raw 可以用来验证区块链上是否存在与此时云中数据的元数据匹配的数据；与 submit_md5 对应，verify_md5 可以用来验证区块链上是否存在与此时云中数据的元数据的 MD5 值匹配的数据；与 submit_etag 对应，verify_etag 可以用来验证区块链上是否存在与此时云中数据的元数据的 ETag 匹配的数据。

6.4　用户层

CBaaS 用户层主要设计了数据存储、数据处理、数据发布、数据验证 4 个功能，每一个可信数据的验证过程都需要经过这 4 个步骤。

数据存储指用户负责将需要存储的数据存放在云上。数据处理指针对不同的用户要求，将元数据处理成满足要求的数据，包括存储元数据本身、元数据的 MD5 值，或者只存储元数据中的 ETag。根据存储数据的容量大小或敏感程度，决定对数据做哪些处理。数据发布指将处理好的元数据发布在 TBchain 上，最终将其推送到全球区块链以太坊上。区块链具有去中心化、不可篡改、集体维护等特性，因此可以保证这些存储在以太坊上的数据不会被篡改，可以作为验证云上数据是否可信的依据。数据验证是指当需要验证云上数据的安全性时，调用对应的方法验证区块链上是否存在与云上元数据匹配的数据来判断数据是否安全可信。如果可信，会从区块链上返回存储数据的具体信息；如果不可信，会返回没有找到匹配数据的信息。

7　性能测试与评价

7.1　数据集及实验环境

本实验使用 YouTube-8M 视频数据集进行测试。YouTube-8M 视频数据集包含 800 万个视频地址、50 万小时的视频、19 亿的帧画面、4 800 个类目，平均每个视频有 1.8 个标签。每个视频的长度在 120 s 到 500 s 之间，每个视频至少与一个知识图谱实体相联系，4 717 个视觉实体被分为 24 个垂直领域，本实验主要使用了 People&Society 和 Travel 垂直领域的数据集，如表 2 所列。本实验是在 Inter Core i5-4590 CPU @ 3.3 GHz 和 8 GB RAM 的惠普台式机上进行的。作为区块链基础层的是区块链的测试链 Ropsten，Ropsten 利用 Infura 提供的 API 访问以太坊并与以太坊进行交互。为了使用户可以和区块链交互，利用 Postman 的 API 实现 submit 类函数和 verify 类函数来向区块链提交或验证数据。

表 2　数据统计

Table 2　Statistics of data sets

	实体数量	视频数量
People&Society	62	26 678
Travel	207	96 038

7.2　CBaaS 系统提高云存储可信性

在云上存储原始数据，然后在区块链上仅存储原始数据存储在云上后产生的元数据。由于 ETag 具有唯一性，当需要使用云上数据时，通过检索区块链上是否存在与此时云上元数据相匹配的数据来验证该数据的完整性。提交函数和验证函数都包括多个，本文以 submit_raw() 和 verify_raw() 为例进行说明。

(1)通过 submit_raw() 在区块链上存储数据的元数据，verify_raw() 验证区块链上是否存在匹配的元数据。

图 6 展示了可以找到与此时云上元数据匹配的存储在区块链上的交易记录，返回“An exact match for submitted raw data has been found”，以及区块号、交易发生的时间戳、交易的具体内容、父哈希和当前哈希等内容，说明此时云上数据安全可信。

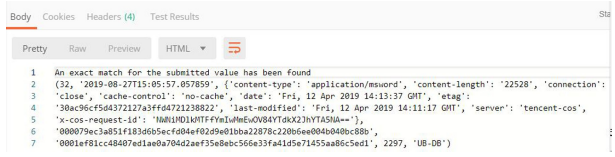

图 6　与存储在区块链上元数据匹配的交易记录

Fig. 6　Transaction record that matches metadata stored on blockchain

图 7 展示了未找到区块链上与此时云上元数据匹配的交易记录，返回“No match was found for the received data”，说明云上数据已被篡改。

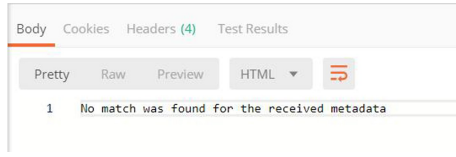

图 7　未找到与存储在区块链上元数据匹配的交易记录

Fig. 7　No transaction record is found that matches metadata stored on the blockchain

由引言部分的介绍可知，当文件通过对象存储的方式存储后会产生该 Object 的元数据，元数据中包含用于标识一个 Object 内容的 ETag，ETag 值可以用于检查 Object 内容是否发生变化。将文件存储后生成的元数据信息通过 submit() 函数存储在区块链上，借助区块链的不可篡改的特性可以保证元数据信息安全可靠。当需要使用对象存储上存储的文件时，取出此时 Object 的元数据，通过 verify() 函数来验证区块链上是否存在相匹配的信息，如果可以找到相匹配的信息，说明 Object 内容没有发生变化且是安全可信的，否则说明 Object 内容已被篡改，从而提高了云存储的可信性。

7.3 三层架构区块链提高了区块链的可伸缩性

TBchain 是一个三层的区块链模型，它将一部分交易放在本地的区块链上进行存储并验证存储低级区块的完整性，再在公共区块链上验证高级区块的完整性，减少了验证链所需的操作数量，既提升了事务吞吐量，又增加了区块链上执行的事务数量，从而提高了区块链的可伸缩性。

7.3.1 三层架构区块链与以太坊测试链的交易吞吐量对比

图 8 和图 9 中为将 TBchain 中的第三层区块链 UB 中的数据块分别设为 1，5，10 时，Tbchain 与 Ethereum 处理交易的时间对比。实验中假设每次提交一个交易至以太坊的区块中。

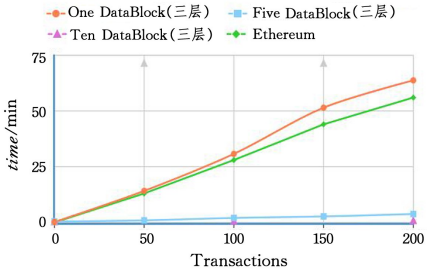

图 8 TBchain 与以太坊处理 200 个交易的时间对比

Fig. 8 TBchain and Ethereum deal with 200 transactions in time

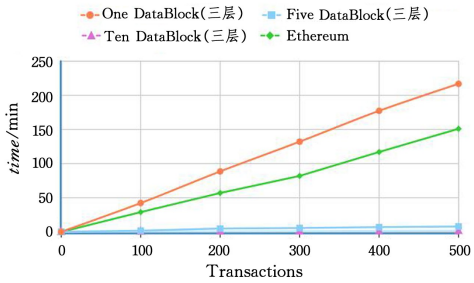

图 9 TBchain 与以太坊处理 500 个交易的时间对比

Fig. 9 TBchain and Ethereum deal with 500 transactions in time

由图 8 和图 9 实验结果可知，当 TBchain 的数据块数量设为 5，10 时，其交易的处理速度远远高于以太坊的交易处理速度。当 TBchain 的数据块设为 1 时，其交易的处理速度略低于以太坊的交易处理速度，但两者随着交易数量的增加，交易吞吐量对比应该始终接近于 1，这主要是因为在三层架构的区块链上存储交易会有传输延时。当处理一定数量的交易时，以太坊、UB 和 MB 不同数量的数据块对应的处理时间如表 3 所列。

表 3 三层架构下不同数量数据块和以太坊对应的交易时间对比

Table 3 Comparison of trading time of different data blocks under the three-tier architecture and Ethereum

	DataBlock/DB	200 Transaction/min	500 Transaction/min
TBchain	1	63.72	216.80
	5	3.78	7.97
	10	0.74	1.84
Ethereum		56.00	151.0

当 MB 和 UB 区块中的数据块为 1 时，交易的处理速度相当于以太坊测试链 Ropsten 本身的处理速度。由表 3 可知，当交易量为 200，UB 和 MB 的数据块为 5 时，TBchain 的交易吞吐量为基础层以太坊的 16.86 倍；UB 和 MB 的数据块为 10 时，TBchain 的交易吞吐量为基础层以太坊的 86.12 倍。当交易量为 500，UB 和 MB 的数据块为 5 时，TBchain 的交易吞吐量为基础层以太坊的 27.2 倍；UB 和 MB 的数据块为 10 时，TBchain 的交易吞吐量为基础层以太坊的 117.8 倍。

表 4 为当交易数量分别为 200 和 500 时，三层架构区块链在不同数量的数据块下与基础层以太坊的交易吞吐量对比。忽略传输延迟，可以近似认为三层架构区块链在数据块为 1 的情况下的交易吞吐量与以太坊相等。同时，随着交易数量的增加，三层架构的区块链的交易吞吐量将越来越接近真实速度。

表 4 三层架构区块链与基础层以太坊交易吞吐量的对比

Table 4 Comparison of trading throughput between three-layer architecture blockchain and foundation layer ethereum

	DataBlock/DB	200(三层)/倍	500(三层)/倍	Average/倍
TBchain	1	1	1	1
	5	16.84	27.2	22
	10	86.12	117.8	102

7.3.2 三层架构和二层架构下区块链交易吞吐量的对比

图 10 和图 11 给出了两层架构区块链与三层架构区块链的交易吞吐量对比。分别设置 MB 和 UB 区块中的数据块为 1，5，10。

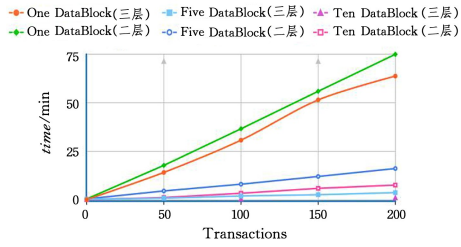

图 10 不同数量的数据块处理 200 个交易的时间

Fig. 10 Processing time for 200 transactions in different amounts of data blocks

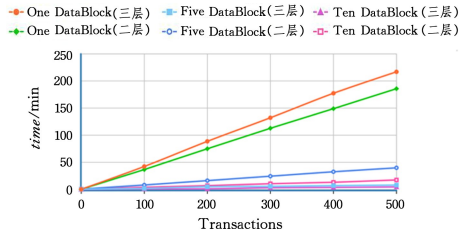

图 11 不同数量的数据块处理 500 个交易的时间

Fig. 11 Processing time for 500 transactions in different amounts of data blocks

由 7.3.1 节可知，当 MB 与 UB 的数据块设为 1 时，区块链的交易吞吐量可以近似认为是基础层以太坊的交易吞吐量。如表 5 所列，当交易量为 200，二层架构的 MB 的数据块为 5 时，其交易吞吐量为基础层以太坊的 4.63 倍；MB 的数据块为 10 时，其交易吞吐量为基础层以太坊的 9.79 倍。当交易量为 500，二层架构的 MB 的数据块为 5 时，其交易吞吐量为基础层以太坊的 4.67 倍；MB 的数据块为 10 时，其交易吞吐量为基础层以太坊的 10.69 倍。

表 5　二层架构和三层架构下区块链交易吞吐量的对比

Table 5　Comparison of trading throughput of blockchain under two-tier architecture and three-tier architecture

DataBlock /DB	200(二层) /倍	200(三层) /倍	500(二层) /倍	500(三层) /倍
1	1	1	1	1
5	4.63	16.86	4.67	27.2
10	9.79	86.12	10.69	117.8

当交易量为 200，三层架构的 MB 的数据块为 5 时，区块链的交易吞吐量为基础层以太坊的 16.86 倍；MB 的数据块为 10 时，其交易吞吐量为基础层以太坊的 86.12 倍。当交易量为 500，二层架构的 MB 的数据块为 5 时，其交易吞吐量为基础层以太坊的 27.2 倍；MB 的数据块为 10 时，其交易吞吐量为基础层以太坊的 117.8 倍。

由表 5 可知，当数据块为 5 时，二层架构的区块链的平均交易吞吐量为基础层区块链的 4.65 倍；当数据块为 10 时，二层架构的区块链的平均交易吞吐量为基础层区块链的 10.24 倍。当数据块为 5 时，三层架构的区块链的平均交易吞吐量为基础层区块链的 22 倍；当数据块为 10 时，三层架构的区块链的平均交易吞吐量为基础层区块链的 102 倍。

结果表明，二层架构的区块链中 MB 的数据块的数量为二层架构的区块链的平均速度相比基础层区块链的提升倍数，三层架构的区块链中 UB 和 MB 的数据块的数量的乘积为三层架构的区块链的平均速度相比基础层区块链的提升倍数。因此，三层架构的区块链的交易吞吐量相比基础层以太坊和二层架构的区块链都有很大的提高。当区块链中这样的节点增加时，交易吞吐量也会成倍增加。除此之外，区块链的交易吞吐量还与区块链的层数和每层区块链中数据块的个数有关。

TBchain 将传统区块链作为基础层或“第一层”，在安全的基础层区块链之上构建了一个三层的区块链模型。在 TBchain 中的 MB 层和 UB 层区块链上的每个区块最多描述一个事务，同时不改变“第一层”区块链将多个事务打包在一个区块中的特性。因此，TBchain 模型每向以太坊推送一个交易，就相当于在以太坊上存储了所有与生成该交易 hash 值相关的 UB 的数据块上的交易，从而提高了区块链的可伸缩性。三层架构的区块链交易吞吐量提高倍数的计算公式如下所示：

$$TBchain_{(\text{Throughput})}=Number(MB-DB)*Number(UB-DB) \tag{5}$$

三层架构的区块链虽然提高了区块链的可伸缩性和可扩展性，但也为在区块链上存储数据带来了一定的负面影响。TBchain 是将传统区块链作为基础层或“第一层”，在安全的基础层区块链之上构建的一个三层的区块链模型。因此，TBchain 区块链模型具有一定的稳定性、容错性和安全性，但是由于一部分交易存储在本地节点，克服了区块链协商一致协议带来的弊端，同时由于 TBchain 中一部分交易存储在本地节点，也为区块链上存储的交易数据带来了一定的安全隐患。

7.4　区块链容量的可扩展性

假设 UB 层区块链的数据块数量为 m，MB 层区块链的数据块数量为 n，对象存储后生成的元数据信息平均为 s 个字节。本文通过实现三层的区块链 TBchain 来实现区块链存储容量的可扩展性，TBchain 上不同高度的区块中不同数量数据块对应存储的交易数量如图 12 所示。

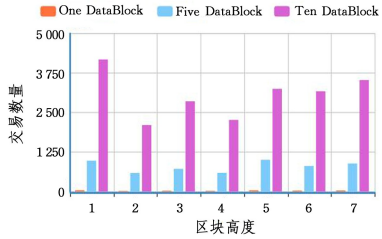

图 12　TBchain 上不同数量数据块对应存储的交易数量

Fig. 12　Number of transactions stored corresponding to different number of data blocks on TBchain

图 12 中的区块高度从以太坊测试链中随机开始，本文为了表示方便，从 1 开始。TBchain 模型中数据块为 1 时的交易数量为区块链测试链 Ropsten 中区块中的交易数量，且当 TBchain 模型中数据块数量为 5 和 10 时，以太坊区块链中实际存储的交易数量远大于原来的交易数，而这些交易存储在本地节点的区块链上，因此增加了区块链的储存容量可扩展性。

由式(5)可知，每在以太坊上存储一个交易(32 Byte hash 值)，相当于在本地存储了 $m\times n$ 个交易。本文假设每个区块存储的数据容量固定为 s，则 TBchain 实际上存储的容量如式(6)所示：

$$Capacity=m\times n\times s \tag{6}$$

由式(6)可知，在以太坊上存储一个 32 Byte 的交易，相当于存储了 $Capacity\ Byte$ 的数据。当 m 和 n 一定时，在 UB 层区块链上存储的数据容量越大，区块链的存储容量的扩展性就越好。对象存储后生成的元数据信息平均为 340 Byte，这里 s 相当于 340。由于 TBchain 将传统区块链作为基础层或“第一层”，在安全的基础层区块链之上构建了一个三层的区块链模型，因此 TBchain 区块链模型具有一定的稳定性、容错性和安全性，同时减少了海量节点的存储空间，有效地提高了区块链的容量可扩展性。

结束语　本研究利用云存储来提高存储效率，同时利用区块链存储元数据，以提高块的构建效率并最小化分布式存储浪费。本系统还实现了一个三层的区块链模型 TBChain，通过分割区块链的一部分并将其锁定在更高级别区块链的块中，让交互发生在需要的时候，仍然可以追溯到基础区块链，从而提高区块链的可伸缩性。TBChain 模型可以将交易数据存储在本地区块链上，在基础区块链上提交这些交易的联合 hash 值来提高区块链的容量可扩展性。本研究建立在一个安全的基础层区块链之上，因此可以在不影响安全性的前提下提高吞吐量，但三层架构的区块链 TBChain 的安全性不及

传统区块链的安全性。本文将云上的元数据信息存储到区块链上是手工操作，数据量大时，代价太高，不易实现，未来可以尝试将云上元数据自动传输到区块链上。

参 考 文 献

[1] NAKAMOTO S, BITCOIN A. A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf.

[2] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: Architecture, consensus, and future trends[C]// 2017 IEEE International Congress on Big Data (BigData congress). IEEE, 2017: 557-564.

[3] OTTE P, DE VOS M, POUWELSE J. TrustChain: A Sybil-resistant scalable blockchain[J]. Future Generation Computer Systems, 2020, 107: 770-780.

[4] JIA D Y, XIN J C, WANG Z Q. Storage Capacity Scalable Model of Blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2018, 12(4): 525-535.

[5] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-ng: A scalable blockchain protocol[C]// 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16). 2016: 45-59.

[6] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 507-527.

[7] ZHOU L, VARADHARAJAN V, HITCHENS M. Trust enhanced cryptographic role-based access control for secure cloud data storage[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(11): 2381-2395.

[8] UIKEY C, BHILARE D S. TrustRBAC: Trust role based access control model in multi-domain cloud environments[C]// 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC). IEEE, 2017: 1-7.

[9] TIAN H, CHEN Y, JIANG H, et al. Public auditing for trusted cloud storage services[J]. IEEE Security & Privacy, 2019, 17(1): 10-22.

[10] ZHAO B, FAN P, NI M. Mchain: a blockchain-based VM measurements securestorage approach in IaaS cloud with enhanced integrity and controllability[J]. IEEE Access, 2018, 6: 43758-43769.

[11] SUKHODOLSKIY I, ZAPECHNIKOV S. A blockchain-based access control system for cloud storage[C]// 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2018: 1575-1578.

[12] WESTERLUND M, KRATZKE N. Towards distributed clouds: A review about the evolution of centralized cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications[C]// 2018 International Conference on High Performance Computing & Simulation (HPCS). IEEE, 2018: 655-663.

[13] POURMAJIDI W, MIRANSKYY A. Logchain: blockchain-assisted log storage[C]// 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018: 978-982.

[14] ZHU L, WU Y, GAI K, et al. Controllable and trustworthy blockchain-based cloud data management[J]. Future Generation Computer Systems, 2019, 91: 527-535.

[15] ESPOSITO C, DE SANTIS A, TORTORA G, et al. Blockchain: A panacea for healthcare cloud-based data security and privacy? [J]. IEEE Cloud Computing, 2018, 5(1): 31-37.

[16] SHEN M, MA B, ZHU L, et al. Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 940-953.

[17] XIA Q I, SIFAH E B, ASAMOAH K O, et al. MeDShare: Trustless medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5: 14757-14767.

[18] GUO R, SHI H, ZHAO Q, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems[J]. IEEE access, 2018, 6: 11676-11686.

[19] LIANG G, WELLER S R, LUO F, et al. Distributed blockchain-based data protection framework for modern power systems against cyber attacks[J]. IEEE Transactions on Smart Grid, 2018, 10(3): 3162-3173.

[20] ZYSKIND G, NATHAN O. Decentralizing privacy: Using blockchain to protect personal data[C]// 2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

[21] LIANG X, SHETTY S, TOSH D, et al. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]// 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE, 2017: 468-477.

[22] JIA D, XIN J, WANG Z, et al. ElasticChain: support very large blockchain by reducing data redundancy[C]// Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data. Cham: Springer, 2018: 440-454.

[23] GAETANI E, ANIELLO L, BALDONI R, et al. Blockchain-based database to ensure data integrity in cloud computing environments[C]// Italian Conference on Cybersecurity. 2017.

[24] YANG C, CHEN X, XIANG Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage[J]. Journal of Network and Computer Applications, 2018, 103: 185-193.

LI Ying, born in 1994, postgraduate. Her main research interests include blockchain and cloud computing.

YU Ya-xin, born in 1971, Ph. D, associated professor, MS supervisor, is a member of China Computer Federation. Her main research interests include data mining and social network.