Computer Science and Application 计算机科学与应用, 2021, 11(12), 3148-3155
Published Online December 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.1112318

Hans汉斯

基于区块链的属性加密细粒度访问方案

邹　健

天津工业大学，天津

收稿日期：2021年11月27日；录用日期：2021年12月23日；发布日期：2021年12月30日

摘　要

个人数据隐私安全一直是近年来研究的热点，然而现有的数据访问模型，多数是基于第三方中心化结构，虽然在一定程度上可以解决数据隐私保护和细粒度访问问题，但是同样会造成数据的泄露和经济成本的增加。在本文中，一种基于区块链的去中心化的结构被提出，通过结合新兴技术属性加密、区块链BC、智能合约SC和IPFS分布式存储，解决了数据安全和细粒度访问问题，保证用户之间数据交易的隐私性，使个人用户对数据拥有绝对的控制权。最后，通过仿真实验，证明论文提议的框架是可行并且有效的。

关键词

数据安全，隐私保护：细粒度访问，属性加密

Blockchain-Based Attribute Encryption Fine-Grained Access Scheme

Jian Zou

Tianjin Polytechnic University, Tianjin

Received: Nov. 27th, 2021; accepted: Dec. 23rd, 2021; published: Dec. 30th, 2021

Abstract

Personal data privacy security has always been a hot research topic in recent years. However, most of the existing data access models are based on a third-party centralized structure. Although data privacy protection and fine-grained access problems can be solved to a certain extent, they will also cause data leakage and increase economic costs. In this article, a decentralized structure based on blockchain is proposed, which solves the problem of data security and fine-grained access by combining emerging technology attribute encryption, blockchain BC, smart contract SC, and IPFS distributed storage and ensures the privacy of data transactions between users, so that individual users have absolute control over the data. Finally, through simulation experiments, it is

文章引用: 邹健. 基于区块链的属性加密细粒度访问方案[J]. 计算机科学与应用, 2021, 11(12): 3148-3155.
DOI: 10.12677/csa.2021.1112318

proved that the framework proposed in the thesis is feasible and effective.

Keywords

Data Security, Privacy Protection: Fine-Grained Access, Attribute Encryption

1. 引言

传统的数据交易模式是建立在第三方基础上的，用户将个人数据交由第三方机构管理，或者第三方机构通过采集个人数据并经过分析，给数据需求方提供服务，这种模式已经工作了很长一段时间，虽然在某种程度上可以保证个人数据访问的便捷性和隐私性，但是很难想象近年来科技的快速发展和数据的大体量式增加，这种数据交易模型在某种程度上存在巨大的隐患，数据的集中存储不仅很容易通过中心化的机构泄露，导致信息安全，而且数据的集中管理会耗费大量的财力。同时隐私泄露案例频繁发生，导致用户安全意识提升，所以用户不得不重视个人隐私保护，并且对个人数据控制的要求越来越高。综上所述，迫切需要一种解决方案将数据的访问控制权交给用户，让用户可以控制自己的数据，而不是交由传统的第三方机构。另一方面，用户可以对自己的数据分门别类，指定访问者访问数据时的权限和粒度性。

针对上述的问题和需求，Zyskind 等[1]在现有技术的基础上设计了数据安全访问模型，结合了区块链，IPFS [2]等先进技术，对数据的隐私进行保护，但是由于系统缺乏细节上的实现以及框架设计比较简单，所以存在很多没有解决的问题，需要更细致化的方案。2018 年 Wang [3]等通过同态加密技术[4]实现数据的交互，虽然在某种程度上实现了数据的细粒度访问，但是同态加密算法的复杂性会导致系统的效率降低，并不利于系统的设计与拓展。Li 等[5]以零知识证明方法保护用户的隐私，但是在频繁的交易模式下，数据共享难以满足需要。从上述研究可知，数据细粒度访问主要通过同态加密和零知识证明方案解决，但是系统缺乏扩展性，无法满足用户的需求和体验。

属性加密算法近年来在数据安全尤其是细粒度访问方面尤为突出，该算法最早是由 Sahai [6]等在 2005 年提出，该算法提出如果用户属性满足访问结构，就可以解密。根据加密策略的所处不同，可以分为基于密钥策略的属性加密 KP-ABE [7]和基于密文策略的属性加密方案 CP-ABE [8]，在访问数据过程中 CP-ABE 的效率和安全性要比 KP-ABE 更好。2011 年，Water [9]证明了 CP-ABE 的安全性，并且提供了 CP-ABE 应用的简单方案。Yang [10]等在 2018 年通过现有框架和属性加密的有效结合，在保护数据安全的同时也实现了数据的细粒度访问，但是框架中角色与角色之间并没有进行有效的身份验证，所以容易导致攻击者使用虚假身份获取数据交易过程中的重要数据。基于现有框架的不足和设计细节，Truong 等[11]提出了合适的解决方案，区块链的去中心化结构，公私钥加密技术和数据流动的过程中各个角色之间的认证保障了数据安全和用户隐私，让用户可以真正地访问和控制自己的数据，通过区块链的匿名性、可靠性以及不可篡改性来保证数据的安全传输，但是并没有通过技术解决数据细粒度访问问题，针对这一问题，我们可以加以改进。

基于以上分析，迫切需要一种有效的解决方案去解决这些问题，因此本文通过结合现有框架和属性

加密，来保证数据的细粒度访问。主要的贡献有：

1) 实现数据细粒度访问。结合现有的安全访问模型，改进 Truong 等提出的框架，确保系统安全有效，用户通过系统可以对数据细粒度访问。

2) 实现数据交易过程中隐私保护。通过区块链、智能合约、IPFS 和身份验证确保数据交易过程中的安全。

论文剩余部分将通过以下几点进行阐述，第二节介绍相关工作；第三节关于提出方案模型的概述；性能和安全评估将在第四部分讲解；最后给出文章的结论。

2. 相关工作

2.1. 区块链

区块链[12]的技术理念来源于 2008 年盛行的加密货币比特币，其流行的原因不仅仅是加密货币本身，更重要的是其底层技术区块链，区块链的诸多特性有非常大的应用价值。区块链是一种节点连接而成的数据结构，结合非对称加密技术，分布式网络和共识机制形成的一条长链。这种数据结构可以记录用户产生的信息，保证信息一旦记录便无法篡改，区块之间通过哈希算法联系在一起，篡改信息就会改变节点的哈希值，导致前后区块不一致。同时区块链的匿名特性可以隐蔽用户的身份信息，避免个人身份泄露。区块链的另一特性是去中心化，通过 p2p 网络技术[13]，使分布式节点中不存在中心化节点，实现所有区块节点的对等。由于所有节点都可以加入这个巨大的网络系统，那么为了保证所有节点的公平性和系统的安全性，就需要一种有效的解决方案－工作量证明机制，工作量证明机制通过共识算法实现系统节点的平等。

迄今为止，区块链已经得到了广泛的应用，不仅在信息安全，金融、物联网等领域发挥了重要的价值，同时在医疗，溯源等方面造诣不菲。区块链在本文中是一种十分有效的解决方案，来解决去中心化和数据记录、传输等问题。

2.2. CP-ABE

CP-ABE 是基于策略的属性加密方案，通过公钥加密技术，将秘密策略嵌入到密文中，属性集合嵌入到用户的密钥当中的一种加密方案，解密时，通过对比密钥中的属性是否满足公共策略确定能否解密成功，与传统的公私钥相比，这种加密方案不仅可以减少公钥的产生，而且用户可以将自己的文件加密成不同的部分，控制其他用户只能访问特定的数据。

CP-ABE 算法主要由初始化，密钥的产生，加密，解密四个部分组成，具体步骤如下：

1) 初始化：初始化算法需要提供一个生成元为 g 的双线性群 G_1， G_1 的素数阶位 p，然后随机选择两个指数 $\alpha, \beta \notin Zp$，产生安全参数 PK 和主密钥 MK；

2) 生成密钥：输入属性集合 S 和对应的主密钥 MK，通过密钥产生关于属性的密钥 SK；

其中 r 是属于 Zp 的随机值，对于每一个属性 $j \in S$ 的都对应一个 $r_j \in Zp$；

3) 加密：加密算法要求输入初始化阶段产生的公共密钥 PK 和加密时所用的访问结构 P，访问结构是一个树形结构，如图 1 所示树的每个节点是关于 x 的多项式，多项式中包含秘密值 S，对于多项式的最高次幂是 $d_x = k_x - 1$，其中 k_x 表示门限值，即子节点满足条件个数，k 表示子节点个数。只有满足条件的子节点大于等于门限值才能解密该节点的秘密值。加密的过程中从树的根节点到叶子节点，依次产生各个节点的秘密值，最终得到叶子节点的秘密值 $att(y)$，使用对应的属性加密 $att(y)$。简单来说，即输入明文 M，通过使用访问结构 P 加密，产生所需的密文 CT；

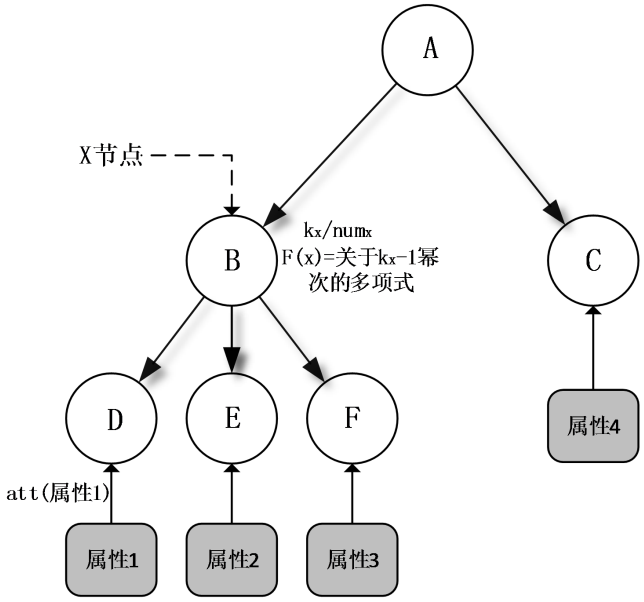

Figure 1. Property encryption access tree
图 1. 属性加密访问树

4) 解密：解密的过程需要对应的密文 CT 和访问结构 P 之外，还需要用户提供的属性值 x，找出对应的属性集，算出访问叶子节点对应的秘密值 $att(y)$，然后再解密父亲节点的秘密值，最终解密出根节点的秘密值，通过更根节点的秘密值可以算出明文 M 。

CP-ABE 属性加密在本文的方案中对于用户访问控制起到关键的作用，数据通过指定加密数据的属性，对数据进行加密，对于一份完整的数据，完全可以分割成不同的部分，指定不同的属性；通过加密好的密文传递给用户，如果用户拥有密钥和属性值，那么就可以解密出对应的文件。

3. 系统模型概述

3.1. 模型架构

在提议的系统模型中，主要包含以下角色：数据请求者 DP，数据控制着 DC，数据提供者 DS，区块链 BC，分布式存储 IPFS，智能合约 SC [14]，并且提议的框架是如图 2 所示。

数据访问者 DP：DP 主要请求用户的数据，通常被假设为不可信的节点，属于数据交易通信三方中请求数据的一方。数据在交给 DP 之前需要通过 DS 确认之后才能拿到属于自己的一部分数据，同时将交易过程数据记录在区块链上。

数据主体 DS：DS 作为整个系统核心，是提供数据的一方，应该拥有绝对的控制权，对于个人用户数据，不论对数据做了任何处理，都可以被系统告知并且在数据泄露之前做出回应，这就需要 DS 对不同数据做细致的划分，拥有特性属性的 DP 才能访问到资源。

数据控制者 DC：DC 在整个系统中起着重要的作用，不仅需要验证 DP 和 DS 的身份，确保获取数据的过程实体是安全可靠的，而且负责处理用户的数据并授权，访问数据库信息，取出用户所必要的信息。

区块链 BC: 区块链主要通过账本信息用于记录用户之间的行为，并且存储数据的索引。通过区块链和智能合约的相互配合，完成系统的自治。

分布式系统 IPFS：是一个分布式系统，存储 DS 产生的各种数据，假设是可信并且安全的，DS 会生

成的用户数据存储到 IPFS 中，IPFS 将存储的数据生成索引记录到区块链中。

智能合约 SC：实体双方交易时的运行程序，保证系统的自治和交易有序进行。

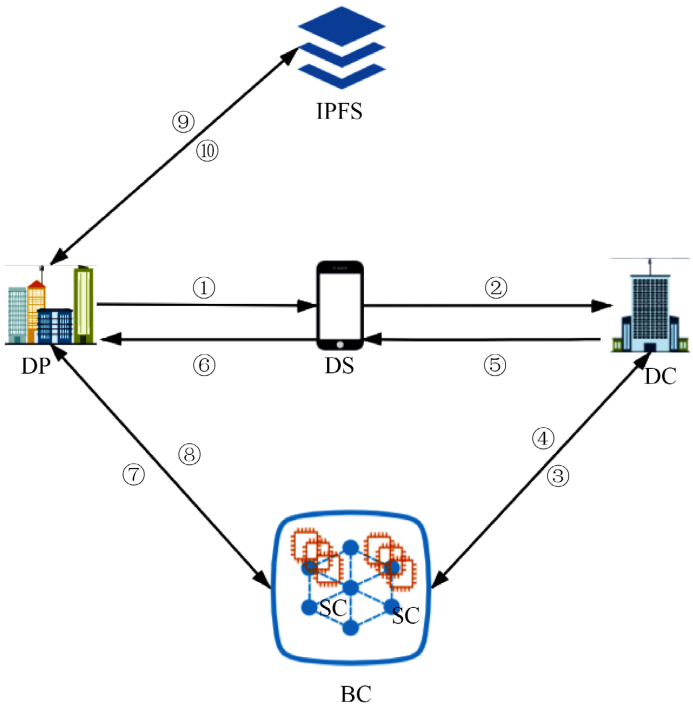

Figure 2. Model design framework
图 2. 模型设计框架

图 2 中各个实体间数字代表的含义分别如下所示：

① DP 将自己的签名和属性值交给交由 DS 验证，并且指明需要进行的操作；

② DS 确认 DP 所要做的操作，并且验证 DP 的签名，成功便放行，将自己的签名交给 DC 进行身份验证；

③ DC 不做任何操作，传递 DC 和 DS 的签名到区块链上认证身份，并且将操作记录在区块链中；

④ 身份认证成功，返回结果；

① ⑤ DC 将返回结果传递给 DS，DS 验证步骤①传递过来的 DP 的属性，验证成功并进行解密操作；

⑥ DP 获得 DS 产生的私钥；

⑦ DP 访问区块链，记录访问历史；

⑧ 返回 token 信息，token 用于访问数据库时验证；

⑨ 访问数据库 IPFS，验证 token；

⑩ 返回访问的数据集。

3.2. 算法设计

本节利用属性加密方案对系统的实施细节和算法进行合理的改进，完成数据安全条件下的细粒度访问。图 2 显示的是整个框架中 DP 访问数据结构的流程，具体的细节主要分为授权和数据访问两个阶段，具体过程如下。

1) 授权。授权是让网络中的节点拥有处理数据权利。授权之前需要经过身份的验证保证节点是安全

可信的。正如图 2 中步骤①②③，身份验证通过，确保数据交易的双方都是可信之后，才能验证 DP 提供的属性是否满足访问结构。身份验证和密钥验证的整个过程都是通过智能合约运行，具体见表 1 所示。

Table 1. Authorization
表 1. 授权认证

算法 1：DP 授权、认证
输入: Sp,Ss,Sc,操作 OP. 1　　Sp,Ss,Sc 分别是 DP,DS 和 DC 的签名. 2　　OP 是进行的操作,包含具体的 CRUD 操作. 输出：R 3　　R 表示授权返回的结果。 4　　S = Valid(Sp) && Valid(Ss) && Valid(Sc) 5　　S 表示签名验证的结果 6　If(S) 7　　更新区块链中的账本，记录现有的 OP 操作记录. 8　　将处理的结果返回给 DC. 9　　R = true 10　else 11　　R = false 12　end

2) 数据访问。当授权过程验证成功，DC 会获取到验证成功的结果，并且将验证结果返回给用户 DS，DS 告知 DP 将访问的属性信息发送给自己，经过属性验证，如果满足访问结构，那么将满足属性的数据索引的加密密钥返回给 DP，如图 2 中的步骤④⑤⑥。DP 收到信息之后需要请求区块链验证是否满足可以访问数据库所有要求，如果满足，将密钥信息发送给 DP，并且给与 DP 访问所需的 token 信息，DP 携带 token 信息和数据库 hash 的解密密钥去访问 IPFS，通过调用智能合同中的函数 Get (token)和& isValidToken (token)验证，验证成功，DP 访问数据库并取出数据，具体的算法如表 2 所示。

Table 2. DP accesses data in the database
表 2. DP 访问数据库中的数据

算法 2：DP 访问数据库中的数据
输入: R 1　If(R) 2　　DP 将自己的属性集 TDP 交给 DS 进行验证，返回结果为 RA 3　　If(RA) 4　　skenc → DP 5　　DP 请求区块链，并获取 token 6　　If(Get(token)&&isValidToken(token)) 7　　获取 DP 所要访问的数据 8　else 9　　访问被拒绝 10 end

4. 实验分析

4.1. 性能分析

本系统对区块链的性能进行了测试，基于 Windows10 系统，处理器为 AMD Reyzen5，内存为 16 G 的基础上，从读取数据和存储数据的角度出发，分别对系统的读取和存储性能进行了分析，并且对数据

中交易的公私钥增长情况也做出了分析，得出了主要的分析结论。

对于读取和存储数据，抽取数据交易过程的 1500 条数据，按交易递增的方式对系统的吞吐量进行分析，如图 3 对读取和存储数据吞吐量进行分析，对于读取数据，当交易量在 120 之前，系统吞吐量是递增的方式，当系统交易量达到了 120 之后，系统的吞吐量会迅速下降，直到数据达到 150 之后，系统的的吞吐量达到瓶颈，逐渐趋于平稳，基本维持在 150 的吞吐量之间，可以看出系统读取数据的性能比较稳定。对于存储数据，交易量在 90 之前都是趋于稳定的，在系统达到 90，系统中存储的吞吐量有所下降，并且区域稳定，所以系统的大致吞吐量在 60 左右。

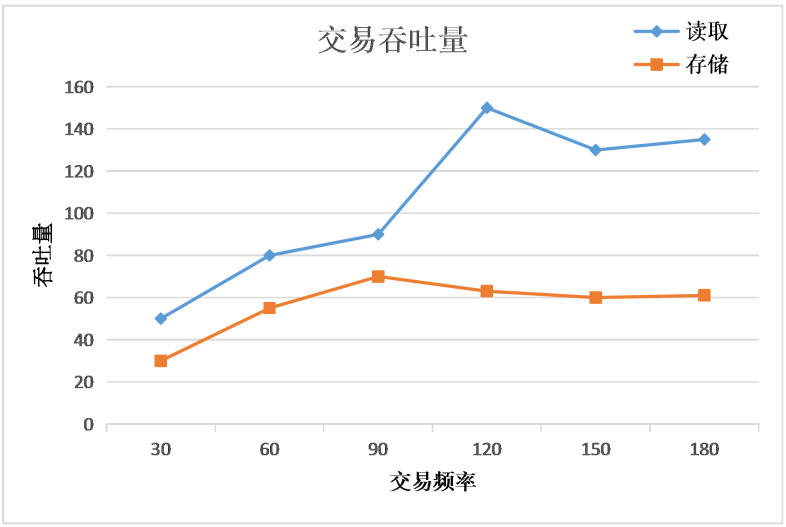

Figure 3. Transaction throughput
图 3. 交易吞吐量

4.2. 安全性分析

本节主要讨论论文中所提方案的授权，数据访问，以及系统完整性和可行性等问题，并且验证是可行的，安全性验证主要考虑以下两点：

授权：假设不诚实的节点通过伪装身份来冒充以太坊网络中的 DP、DS 或者 DC 中的任何一个节点，在身份认证的过程中就无法通过，因为网络中 DS 需要验证 DP 身份的真实性，区块链 BC 需要验证 DS 和 DC 的身份，所以无论哪一方伪造身份，都无法获得相应的授权，访问到对应的数据。

数据存储安全：数据存储在 IPFS 分布式系统中，存储之后将数据 hash 存储在区块链上，由于区块链的不可篡改性，所以一旦存储不可修改，只有授权之后的用户通过添加区块来改变 hash 值，所以即使有攻击者刻意去攻击，也不会导致数据库数据的篡改和丢失。

5. 结论

在本文中，根据现有框架对数据细粒度访问结构进行了改进，提出了一种改进的方案，利用属性加密方案对用户数据加密，访问者只有满足数据加密访问结构才能访问指定的数据，解密过程中数据用户可以确定访问者访问的具体数据和访问者所要访问数据的类型，解决了现有框架数据细粒度访问的问题。并且巧妙了利用了 BC 区块链，分布式数据库 IPFS 和以太坊等比较新颖的技术，消除中心化机构，通过系统自治，保证数据传输过程中的安全。本文所提出的框架拥有广阔的应用场景，不仅为数据细粒度访问解决方案提供良好的思路，而且还可以通过改进本文的方案提供不错的可见性。

6. 总结与展望

针对数据隐私保护和访问控制，本文提出了一种比较合理的方案，结合区块链、智能合约、分布式存储系统 IPFS 以及属性加密，对数据的访问合理控制，完成了数据流向的安全，保障数据主体对数据拥有绝对的控制权，让用户可以对数据进行细粒度访问。针对大数据的发展步伐，数据的访问控制仍然面临着很大的挑战，GDPR 虽然给出了具体的法律方案，但是仍然需要去研究如何将数据通过技术的方案去解决，本文虽然给出了合理的设计方案，但是仍然存在不足之处，具体如下：

1) 本文的方案并没有给出信息溯源的解决方案。溯源作为追踪恶意行为，记录数据在系统中的流向都有十分重要的作用，对用户来说有更好的体验，区块链作为溯源这方面有很多的应用，但是时间的原因，并没有进一步研究，以后的工作可以在这方面进一步展开。

2) 模型中废弃的属性缺乏管理。尽管框架对加解密模块进行了合理的设计，但是并没有将属性撤销的方案融入到本文提出模型的框架中，因此对于系统的属性管理不是很方便，一旦随着时间的发展，属性的数量就会随着时间不断增加，将会给系统带来一定的负担。

参考文献

[1] Zyskind, G., Nathan, O. and Pentland, A.S. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 *IEEE Security and Privacy Workshops* (*SPW*), San Jose, CA, 21-22 May 2015, 180-184. https://doi.org/10.1109/SPW.2015.27

[2] Benet, J. (2014) IPFS-Content Addressed, Versioned, P2P File System. Eprint Arxiv.

[3] Wang, R., Tsai, W.T., He, J., *et al*. (2018) A Medical Data Sharing Platform Based on Permissioned Blockchains. *International Conference on Blockchain Technology and Application*, Xi'an, 10-12 December 2018, 12-16. https://doi.org/10.1145/3301403.3301406

[4] Lei, X., Shah, N., Lin, C., *et al*. (2017) Enabling the Sharing Economy: Privacy Respecting Contract Based on Public Blockchain. *ACM Workshop on Blockchain*, Texas, April 2017, 15-21.

[5] Xu, L., Shah, N., Chen, L., *et al*. (2017) Enabling the Sharing Economy: Privacy Respecting Contract Based on Public Blockchain. *ACM Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates, 2 April 2017, 15-21. https://doi.org/10.1145/3055518.3055527

[6] Sahai, A. and Waters, B. (2005) Fuzzy Identity-Based Encryption. *International Conference on Theory & Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 457-473. https://doi.org/10.1007/11426639_27

[7] Goyal, V., Pandey, O., Sahai, A., *et al.* (2006) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of the* 13*th ACM Conference on Computer and Communications Security* (*CCS* 2006), Alexandria, VA, 30 October-3 November 2006, 89-98. https://doi.org/10.1145/1180405.1180418

[8] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. *IEEE Symposium on Security & Privacy*, Berkeley, CA, 20-23 May 2007, 321-334. https://doi.org/10.1109/SP.2007.11

[9] Waters, B. (2008) Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. *International Workshop on Public Key Cryptography*, Springer, Berlin Heidelberg, 53-70.

[10] Yang, S. (2020) A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems.

[11] Truong, N.B., Sun, K., Lee, G.M., *et al*. (2020) GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, **15**, 1746-1761. https://doi.org/10.1109/TIFS.2019.2948287

[12] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

[13] 赵宝艳. P2P 技术[J]. 电信工程技术与标准化, 2007(4): 77-79.

[14] Ouyang, L.W., Wang, S., Yong, Y., *et al*. (2019) Smart Contracts: Structure and Progress. *Acta Automatica Sinica*, **45**, 445-457.