Computer Science and Application 计算机科学与应用, 2021, 11(4), 1034-1041
Published Online April 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.114106

Hans汉斯

基于联盟链的信息监管平台

呼帅亮，于　淼，胡玉蝶，陈智卿

郑州大学，河南　郑州
Email: znh_ninghao@163.com

收稿日期：2021年3月23日；录用日期：2021年4月18日；发布日期：2021年4月25日

摘　要

在信息流动过程中，监管平台对信息的安全性起着重要的影响，目前绝大多数信息监管平台采用的是“区块链 + 应用”的模式运营，而随着区块链应用的发展，基于传统区块链的信息监管平台不断暴露出诸如缺失保护与监督机制、无权威的第三方专业验证机构等新的问题。因此文章对其做出了相应的探索和创新，提出了一种基于联盟链的信息流动监管平台设计方案，利用联盟链、CPK和多方计算技术，并对联盟链技术进一步创新，从而设计出一种较为新颖的、安全高效的信息监管平台。

关键词

联盟链，CPK，多方认证，数据区块嵌套

Alliance Chain-Based Information Supervision Platform

Shuailiang Hu, Miao Yu, Yudie Hu, Zhiqing Chen

Zhengzhou University, Zhengzhou Henan
Email: znh_ninghao@163.com

Received: Mar. 23rd, 2021; accepted: Apr. 18th, 2021; published: Apr. 25th, 2021

Abstract

In the process of information flow, the supervisory platform plays an important role in the security of information, and at present, most of the information supervisory platforms are operated in the mode of “blockchain + application”. With the development of blockchain applications, the traditional blockchain-based information supervision platform has been exposed to new problems such as the lack of protection and supervision mechanism and the absence of authoritative third-party professional verification institutions. Therefore, the article makes a corresponding explora-

文章引用: 呼帅亮, 于淼, 胡玉蝶, 陈智卿. 基于联盟链的信息监管平台[J]. 计算机科学与应用, 2021, 11(4): 1034-1041. DOI: 10.12677/csa.2021.114106

tion and innovation, and proposes a design scheme of information flow supervision platform based on coalition chain, using coalition chain, CPK and multi-party computing technology, and further innovates the coalition chain technology, so as to design a relatively novel, safe and efficient information supervision platform.

Keywords

Alliance Chains, CPK, Multi-Party Authentication, Data Block Nesting

1. 引言

当今社会，随着信息事业的发展，越来越多的信息企业为谋取利益，私自发布虚假信息、篡改用户信息，如公益企业伪造虚假公益信息、窃取用户信息、隐藏公益资金流向谋取利益等问题层出不穷。

虽然部分信息企业采取“区块链 + 应用”的模式，运用区块链技术构建信息监管平台，对信息进行处理，为信息的安全提供了保障[1]，但随着区块链应用的发展，基于传统区块链的信息监管平台不断暴露出新的问题，如：信息处理不及时、平台管理过于繁琐、信息处理不完善、用户响应不及时等。信息事业缺少了强制的保护与监督，其可信度就没有太强的说服力。作为区块链的一个分支，联盟链不仅应用了多中心化的多区块链结构，而且将公有链和私有链进行结合，构成一个庞大的树状区块链体系，是区块链发展推进的一个新方向。

联盟链相比于传统区块链，最大的优势是它的结构，联盟链是由多条公链私链组成的，由最高级主链监督下按照特定策略运营的多链式结构。其特点是可以根据地域不同，种类不同，处于不同位置的不同的链节点在联盟中扮演着不同的角色，从而构成一种自上而下的链式树状结构，其延展性允许其在大范围内更加方便、更加安全的提供服务。

区块链中设置的魔数是区块链赖以存在的共识基础，也是区块链中的数据真实性能够得到认可的原因。每个区块都有一个魔数，而魔数是由特定方法产生的。在公有链，特别是比特币中，魔数是由大量计算产生的，称为工作量证明(Pow)。而对联盟链来说，则不需要如此，联盟链的魔数必须由联盟成员共同生成，或由联盟成员加上监管方、公证方一起生成，安全性得以保障。

当涉及到参与信息用户较多难以管理时，联盟链的结构特性可以按照用户规格对其进行分组，从而分开管理服务。并且，当联盟成员较多时，需要产生大量的公钥和私钥，考虑到传统的密钥管理体制如：PKI、IBE 的弱点如众多 CA 的高成本、多级链式认证造成计算量大和延时长等。因此本文采用的是更安全的 CPK 算法。CPK 采用集中式的密钥存储方式，可以以很小的资源，生成大规模的密钥，将先进的公钥管理模式 CPK 与联盟链结合在一起，基于 CPK 构造用户公私钥，将用户标识与公、私钥绑定，采用一次性的 CA 认证方式，使得密钥管理方便、高效。

2. 区块链、CPK 和多方计算

2.1. 区块链技术

区块链是计算机技术的一种新型应用模式，由数据层、网络层、共识层、激励层、合约层和应用层组成[2]。区块链是比特币的一个重要底层技术，传统因特网程序大多采用一种中心化的客户机—服务器

体系结构，而区块链作为一个去中心化的数据处理型数据库，利用块链式数据结构来安全的存储数据并提供防篡改功能、利用分布式节点的共识算法来进行数据的生成和更新、利用密码学的方式保证数据传输和访问的安全，其对数据的综合处理是当今时代信息安全离不开的一个屏障。

2.2. CPK

CPK (组合公钥)由我国密码学专家南相浩先生发明[3]，基本思想是，在 ECC 的基础上，利用多个公、私钥因子组合出海量用户公、私钥，解决了超大规模密钥管理难题。

CPK 的组合矩阵分为私钥矩阵 MSK (Matrix of SecretKey)和公钥矩阵 MPK (Matrix of Publickey)。通常，私钥矩阵 MSK 用于签名，公钥矩阵 MPK 用于验证签名。

CPK 的工作原理[4]：首先生成公私钥矩阵。由密钥管理中心选择一个基于有限域椭圆曲线上的加法群 G，设其阶为素数 n，其中 $2^{l-1} < n < 2^l$，$l \geq 192$，生成元为 P。在确保群 G 安全的前提下，通过一个安全的随机数生成函数，随机生成 $s \times t$ 私钥因子，组成私钥矩阵

$$MSK = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1t} \\ r_{21} & r_{22} & \cdots & r_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ r_{s1} & r_{s2} & \cdots & r_{st} \end{pmatrix}$$

该矩阵由密钥管理中心统一生成并秘密保管。系统的安全性基于私钥矩阵的安全性。

管理中心根据已生成的私钥矩阵生成与其对应的公钥矩阵

$$MPK = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1t} \\ g_{21} & g_{22} & \cdots & g_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ g_{s1} & g_{s2} & \cdots & g_{st} \end{pmatrix}$$

私钥矩阵和公钥矩阵中处于相同位置的私钥因子与公钥因子成为一组对应的公私钥对，$g_{ij} = r_{ij}P$。公钥矩阵公开发布，用户可将其存储于本地，在需要对某一签名进行认证时通过该用户信息索引公钥矩阵即可获取该用户公钥。管理中心选择一个适当的函数作为坐标映射算法，将用户标识符映射为公私钥矩阵中的坐标。该函数通常取单向陷门函数，以用户标识为输入，计算一个 hash 值并将其分为若干段，得到多个矩阵坐标，根据坐标取出其中的公私钥因子，诸因子之和(模 n)分别组成用户的公私钥[5]。

设用户标识映射值的行、列坐标为：$(i1, j1)\ (i2, j2)\ (i3, j3)\ \cdots\ (it, jt)$，那么得到的公钥为：$\mathrm{PK} = g_{i1,j1} + g_{i2,\ j2} + \cdots + g_{it,jt}$

私钥为：$SK = r_{i1,j1} + r_{i2,j2} + \cdots + r_{it,jt} \left(\mathrm{mod}\, n\right)$

因为：

$$\begin{aligned} \mathrm{PK} &= g_{i1,j1} + g_{i2,j2} + \cdots + g_{it,jt} \\ &= r_{i1,j1}P + r_{i2,j2}P + \cdots + r_{it,jt}P \\ &= \left(r_{i1,j1} + r_{i2,j2} + \cdots + r_{it,jt}\right)P \\ &= SK * P \end{aligned}$$

所以任意多对公、私钥，公钥之和与私钥之和构成新的公私钥对。

各用户私钥由密钥管理中心生成并秘密传递给用户，用户的公钥由验证方根据公钥矩阵和被验证方的用户标识符查询计算。

尽管 CPK 公开的是公钥矩阵，但公钥矩阵的每个元素都是基点的随机位数，相当于 SM2 算法的一个公钥，因此其安全性等同于 SM2 算法，即依赖有限域上椭圆曲线群的离散对数难解性假设。另外，CPK 的实体私钥来自于私钥矩阵的元素(称为私钥因子)，因此，私钥因子的安全是 CPK 安全的关键所在；也就是说只要保证私钥因子不泄密，CPK 算法生成的公私钥在理论上是安全的，无法破解的。

2.3. 多方认证

在每一轮区块结束后，需生成一个唯一的可验证的魔数，带入下一区块的运算中去，以确保区块中数据的真实性和不可更改性。

魔数的计算是共识机制的基础，在公有链中，魔数的计算是通过一个被称为工作量证明的过程实现的，而在本系统的联盟链中，为了实现各方成员对数据的认证和监管，采用多方计算的方式来计算魔数。

所谓多方认证，是指在区块结束之后，各方成员在对其中的数据确认并验证后，分别利用各自的签名私钥对数据进行签名，系统根据所有成员的签名计算该区块的魔数。这样，每一个区块的数据都得到了联盟成员的签名和认证，并产生了一个唯一的可验证的魔数，且在任意一方成员不参与运算的情况下，魔数无法更改，实现了基于联盟链所有联盟成员参与计算的共识机制。

要实现多方认证，需要两个公开的算法：签名算法和魔数生成算法。联盟成员需要利用自己的私钥对数据进行签名，该签名可以由成员的公钥进行验证，使得签名方无法否认。魔数生成函数以全部的必要签名为输入，计算区块的魔数，在任意一方对数据不予通过时，魔数无法生成，区块无法上链。

3. 基于联盟链的创新

3.1. 理论创新

联盟链作为一个半开放的账本，只针对某个特定的组织开放，并通过牺牲部分去中心化，解决了传统区块链效率低下的问题，并且可以加入权威的第三方专业验证机构更好的保证保护与监督的可行性。联盟链通常有一个由联盟共同维护的主链，并且允许每个成员拥有自己的私有链。私有链由成员自己负责，其中部分数据将选择上传到主链。联盟链特定的分级结构与当今时代大多数信息平台如公益信息平台、食品链数据平台等结构契合，将联盟链与之结合形成新型化的信息平台是非常可观的。

在此基础上，通过引入一些策略将第二级结构的节点服务器服务程序进行了分离，引入了一个辅助进程分担主进程的工作量，同时使主进程(区块链生成进程)与辅助进程(数据处理进程)能够独立运行，减少彼此的约束，为子链的安全、高效生成提供了保障。通过该策略，下层用户在向上层用户发送信息时，辅助进程会暂时充当主进程，对用户的数据进行处理并提供服务，直到用户的数据处理完毕服务结束，再将该用户的最终数据上传至主进程，其中用户的数据处理、存储等服务都由辅助进程进行处理，最终只将代表数据如用户标识、用户部分主要数据、用户最终象征标识值等交给主进程。通过该方案，即使用户传输非常大的数据也能够得到及时处理，主进程只负责区块的生成，大大提高了区块的生成效率和区块与数据服务之间的独立性。

3.2. 技术创新

联盟链分为多分支结构，主链上的数据对全体用户公开，对任何一个用户可见，且其信息不可更改，每个区块都与上一个区块有着紧密不可分割的联系。本文所提联盟链的内部区块标准 hash 函数用的是国家标准哈希算法 SM3，并在此基础上引入局部哈希函数，对哈希函数的结构进行了部分更改，使得上层服务器在进行用户服务时可以使用特定的局部哈希函数可以为每个用户提供相互独立的服务。

为了确保联盟链数据的不可篡改性，每一个联盟成员需要对自己产生的区块数据负责，因此需要产

生大量的公钥和私钥进行数字签名。考虑到传统 PKI 模式的弱点，如众多 CA 的高成本、多级链式认证造成计算量大和延时长等，越来越明显，因此本文采用的是更安全的 CPK 算法。CPK 采用集中式的密钥存储管理方式，以很小的资源，生成大规模的密钥，并且采用一次性的 CA 认证方式[6]，使得密钥管理方便、高效。CPK 密钥管理系统采用集中生产分发，分散存储使用的管理模式。所有身份验证活动都是端到端的，不需要第三方身份验证，因此理论上也不需要中心的支持。

本文将先进的公钥管理模式 CPK 与联盟链结合在一起，基于 CPK 构造用户公私钥，将用户标识与公、私钥绑定，实现了基于标识的认证方式；可以脱离第三方在线运行；私钥安全存储在个人的安全芯片中，无需通过网络传输；公钥通过计算直接获得，无需第三方确认其合法性；颁发证书，直接存储在安全芯片中，不直接存储证书，减少了数据库的维护量。

3.3. 结构创新

联盟链通常有一个由联盟共同维护的主链，并且允许每个成员拥有自己的私有链。私有链由成员自己负责，其中部分数据将上传到主链。这是联盟链的特色所在，它将私有链和公有链按照特定的规律进行结合，组织一个链式结构而构建一个新颖的、高效的链式结构，但这种链式结构，将一个公有链作为主链，子链作为公有链的用户分担了公有链的压力，但是结构层次却并不太清晰，下层结构相对来说比较杂乱，同时服务器的处理能力相对来说还是要求的比较大。

本文结构方面的创新点在于通过改变传统的三层结构引入新型的三级链式结构，传统的三层结构只是通过简单的主链－子链－用户[7]单一的层次结构进行联盟链的展开与管理，虽然安全方面程度较高，但在层次展开时带来了诸多不便，如分支较多，不便于管理等等。而引进的链式三级结构在原有的三层结构基础上扩展了第二层结构子链的功能，使得子链的直接下层可以是用户也可以是其他子链，从而形成一个大型以链为节点的树状结构，使其可以根据区域、环境等因素而适当的构建其节点，因此链式二级结构的上层可以是一级结构主链，也可以是其他高等级的二级结构，下层不单单是联盟用户，也可以是其他低等级的二级子链，级与级之间进行展开，最终形成主链－可扩展二级子链－用户三级树状结构，大大缩小了联盟链结构的分支，更加方便于管理，使得联盟链的实现变得更加层次化，将联盟链之间的上下层关系表现得更为突出，并加强了每个链式节点组成的独立性。

4. 基于联盟链的信息监管平台设计

4.1. 设计思路

联盟链体系中，节点通过对某段时间 T 内的交易数据进行大量的 hash 函数运算，得到该区块的 hash 值，存放到区块头中。同时，一个区块的 hash 值自动带入下一个区块，不仅存放在下一区块头中，还参与下一个区块的 hash 计算。通过这种方式，将区块链接起来，形成一条条链，构成了联盟链的基本公私链结构[8]。

基于 CPK 的公钥管理体系使得每个联盟成员都有自己独特的私钥，该私钥与用户自己的信息进行绑定。在一个区块内，所有参与成员加上监管方共同使用自己的私钥参与区块的计算，可以确保一个区块结束时，能产生独特的魔数，加入到下一个区块中使得该链的每个区块一经生成，数据将无法更改，除非参与计算的每个参与方(包括联盟成员和所有监管方)都同意更改。此外该平台设计引用服务器分离技术和三级结构，使得该链式结构更加清晰、简单明了。

将上述三种技术结合在一起，相互联系、相互作用，运用区块链基层技术和联盟链技术，通过公链、私链共同组成多层分级链式结构，通过 CPK 公钥管理体系合理安全的控制联盟成员公私钥，从而为联盟链的信息追溯提供保障，构建起我们的信息流动监管平台。

4.2. 平台架构设计

实现该监管平台引入新型的三级结构，即主链、子链和大众用户。在该结构中，主链由一个所有子链共同维护的服务器运行，是所有链式结构的顶层，子链之间的交叉数据必须传输至主链存储，每个子链必须对自己的客户端进行直接服务，客户端可以根据自己意愿选择数据的存储对象并通过子链来确定是否上传主链。

第一级结构也就是根结构(图 1 中的一级服务器)，它作为联盟链的核心维护着一个全局主链，与其他链节点不同的是，它是所有构成联盟链成员的最上级所在，因为在三级结构中每个联盟成员都可以直接或者间接通过上级参与到这个结构中进行计算，而且任何人都可以下载获得该结构的完整区块数据(全部账本)，同时他们作为一级结构链的下层也需为上层提供维护与保障，同时监督联盟链的运行。

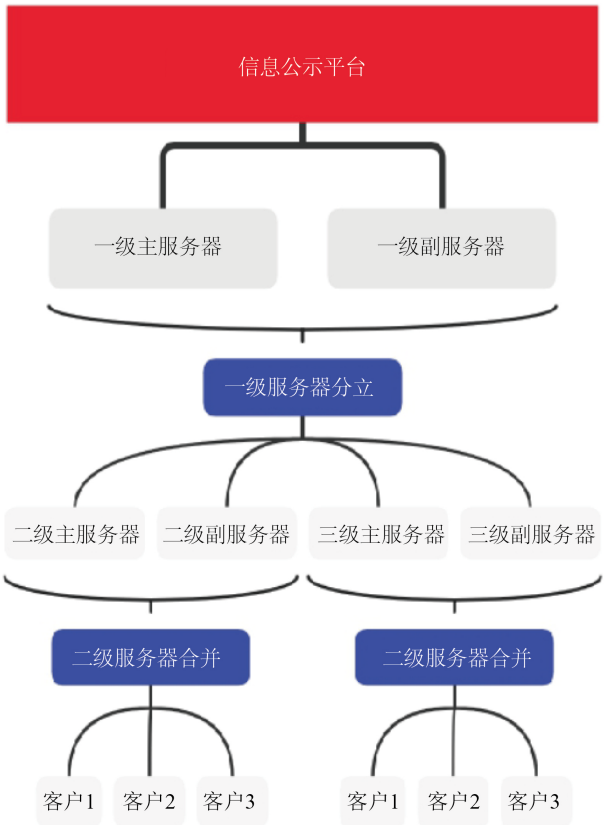

Figure 1. Oversee the basic architecture of the platform
图 1. 监管平台基本架构

第二级结构也就是子链(图中二级服务器)，通常由一些信息企业、政府部门或者一些拥有可以维护一条链式节点能力的成员组成，他们是联盟链得以展开的关键所在。它在为上层提供维护与服务的同时也要为自己的下层提供服务。它的直接上层组成可以是根结构也可以是其它链式节点，下层由它的直接子链或者公益参与用户组成，由此新型联盟链才可以通过三级架构做到多层的链式结构。

第三级结构，也就是该监管平台的最终用户(图中联盟客户)，是整个联盟链的直接使用者。他们是联盟链的最下层，可以直接或者间接接受一级、二级结构所提供的服务，并监督上层链节点的运行

结合部分区块链技术用传统区块链架构作为联盟链的一条子链，将子链安排在两个独立的服务器如下面图所示的分立服务器，其中主进程由主服务器运行，辅助进程由副服务器运行，从而使区块的生成、

链式结构的链接和为下层提供的服务隔开，相互独立。利用子链提供的接口设计主链，主链也同样采用服务器主进程分离的技术。采用分离技术引入辅助进程分担主进程的工作量，为子链的安全、高效生成提供保障。

参与该信息平台的用户，作为该平台的第三级结构，会拥有一对独有的用户公私钥：由 CPK 注册机构根据用户信息生成。用户可以根据该公私钥对涉及的信息进行加密处理，之后将加密的信息上传至平台的二级服务器合并筛选机构，经筛选后的信息将上传至对应的上层服务器(二级服务器)。此外，在二级副服务器处将会生成一个对应该用户的小数据块——小区块：该小区块会根据特定规则暂时接收并处理来自对应用户的数据；一旦该用户的数据传输完毕，该小区块隶属的副服务器便会采集该小区块的特征值和对应用户的标识以及完成时间结束判断标志(可以是时间戳，也可以是其他判断条件)，进一步将上述数据上传至该服务器对应的区块子链生成机构——主服务器。

根据某种策略，在判定一个区块结束时，二级子服务器在采集完毕用户小区块数据后便会启动区块结束操作，将一个个小区块数据集进行 hash 处理，得到最终区块 hash 值。同时，该区块的一些必要特征数据根据也将上传至上层结构——可以是上层二级结构子服务器，也可以是顶层一级服务器(取决于该链对应的筛选器)，接受上层服务器的监督——形成一个由顶向下依次提供服务，由下往上依次接受监督的树状结构，最终服务于公益参与的用户，共同监督联盟链的正常运行。同时，出于安全性和透明性考虑，在整个公益平台运行期间，存在一个公益信息流动公示平台，能定期公示该联盟链的运行情况和必要的公益信息流动和运算处理数据，使得联盟链接受大众监督。

4.3. 监管平台性能分析

4.3.1. 安全性分析

首先，联盟链上每条链的每个区块 hash 值的计算必然是正确的、可验证的，从而能够保证信息流动数据的真实性。同时因为核账子系统的核算，保证了 hash 值的计算不会发生错误；而平台的其他联盟成员有权复制和保存数据，并可对 hash 值重新计算核对，进一步验证其正确性。

其次，魔数是不可伪造的。因为魔数是由每个联盟成员与监管方、公证方在确认区块正常运行后分别使用私钥对已完成的区块hash值和新时戳进行签名后，再经hash计算而得，如果这个魔数是可伪造的，则意味着 hash 函数是不安全的(随意修改输入而产生意定的输出)，或者参与方的签名是可伪造的，基于目前的技术想要做到这一点是不存在可能性的。

一旦数据被记入区块，则该数据不能被篡改，不论是单方篡改，还是联盟的部分成员乃至所有成员合谋篡改。如果某一方或联盟的部分成员乃至全部成员合谋篡改了区块体的数据，则将导致该区 hash 值的改变，从而导致所有参与方签名值的改变，使得生成的下一个区块的魔数发生改变，进而导致此后所有区块的 hash 值和魔数都发生改变。由于存在监管方和公证方，他们的签名是不可伪造的，因此这种篡改不能得到监管方和公证方的认可。

由于任一数据纳入联盟链后将不可篡改，因此数据的生成者在哪一个区块中提交了数据是可以追溯、不可否认的。特别是在每个数据提交时必须由生成者签名的要求下，如果他想改变该数据并重新签名，将导致与该区块 hash 值不符，因而不被认可。

因此，无论是联盟链的最上层主链还是下层子链的数据，其真实性都将得到保证，在该流动监管平台上所公开的公益资金去向必然是安全的。

4.3.2. 效率分析

从该平台所用的联盟结构的主链和子链的构造过程中可以看出，整个链中只涉及到hash函数的计算、时间戳的获取和基于数字签名的多方认证。在一个区块体的形成过程中，时间戳的获取极快，hash 函数

的计算也极快。基于数字签名的和 hash 运算的魔数生成过程虽然要稍慢一些，但一个区块开始后，立即进行下一个区块的魔数的计算，中间有一个区块时长的间隔，足以用来收集签名从而生成魔数。等该区块结束时，只要取到时间戳，即可立即开始下一个区块，这就保证了区块间可以无缝地进行衔接、极为高效地运行。

需要说明的是，对于一个区块的哈希值、哈希值签名等数据都会在本区块的区块头中进行记载，便于后期数据的可追溯性。另外对于时间间隔内接收到的数据还有中间所产生所有的哈希值，都会有一个公告对其进行记录。保证了数据的完整性、防篡改性和可追溯性。从而在对于公益项目的具体记录中，项目记录的安全性和数据的处理效率都可以得到保障。基于联盟链的记录体制使得每个联盟成员都有自己独特的私钥，所有成员加上监管方共同用私钥参与的计算，可以确保一个区块结束时，能够产生独特的魔数，之后将其加入到每个区块中，从而使得联盟链中每个区块一旦生成，数据将无法再更改，除非参与计算的每个成员(包括联盟成员和所有监管方)都同意更改，并且必须其监督之下进行更改，从而保证其公开性、透明性和安全性。

5. 结束语

本文提出了一种较为新颖的基于联盟链的信息监管平台设计方案，利用联盟链，CPK 和多方计算技术解决了信息流动过程中的监管问题。采用 CPK 模式的区块链因为标识与公、私钥绑定，不需要链式认证，也不需要像 PKI 模式下 CA 等认证机构，成本低、效率高，同时使用联盟链技术也大大提高了监管平台的安全性，在诸多信息领域存在较大的发展方向。

致　谢

本项目为郑州大学大学生创新创业训练计划资助项目，感谢指导老师的倾力指导，感谢团队成员的团结合作。

参考文献

[1] 王莉, 段婷, 董珺. 区块链与企业网络融合: 机遇、挑战与对策[J]. 经济问题, 2021(4): 23-30.

[2] 郭上铜, 王瑞锦, 张凤荔. 区块链技术原理与应用综述[J]. 计算机科学, 2021, 48(2): 271-281.

[3] 南相浩. CPK 算法与标识认证[J]. 信息安全与通信保密, 2006(9): 12-16.

[4] 马宇驰, 赵远, 李益发. 浅谈基于 CPK 的可信认证[J]. 信息工程大学学报, 2009, 10(3): 309-312.

[5] 南相浩, 陈化平, 陈钟, 李益发. 组合公钥(CPK)体制标准(V3.0) [J]. 计算机安全, 2009(11): 1-2.

[6] 马宇驰, 赵远, 邓依群, 李益发. 基于 CPK 的可信平台用户登录认证方案[J]. 计算机工程与应用, 2010, 46(1): 90-94.

[7] 谭朋柳, 万里旭冉. 一种具有主从区块的区块链架构[J/OL]. 物联网学报: 1-9. https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CAPJ&dbname=CAPJLAST&filename=WLWX20210319001&v=iS4f2xeIvIUkBYoleHe%25mmd2F7XgifzW8ylE%25mmd2FUC7%25mmd2BoVIzVtS25TvCFmgGj117DB8%25mmd2BXXTK, 2021-04-04.

[8] 王新庆. 区块链的技术创新原理与金融应用[J]. 征信, 2019, 37(2): 8-13.