

# 基于区块链技术的计算机数据安全保护分析

覃 德

(中移(上海)信息通信科技有限公司,上海 201314)

**摘要:**互联网技术不断创新和发展,被广泛应用在各行各业之中,并取得较为出色效果,对计算机数据安全保护水平也提出更高的要求。因此,基于当前计算机数据安全保护实际情况,将区块链技术应用其中,从而更好针对计算机数据进行多级加密以及建模。同时依据区块链技术优势以及特点,合理构建远程验证协议,能从根本上解决计算机数据安全保护问题。文章对区块链技术在计算机数据安全保护中起到重要作用展开讨论,并提出三种密码学技术类型,旨在合理优化以及完善计算机数据安全保护机制,从而进一步提升数据安全保护质量以及水平。

**关键词:**区块链技术;计算机;数据安全保护

**中图分类号:** TP311

**文献标识码:** A

**文章编号:** 2096-9759(2023)06-0042-03

## Analysis of computer data security protection based on block chain technology

TAN De

(China Mobile (Shanghai) Information and Communication Technology Co.,Ltd.,Shanghai 201314)

**Abstract:** The continuous innovation and development of Internet technology, is widely used in all walks of life, and has achieved excellent results, the level of computer data security protection also put forward higher requirements. Therefore, based on the current actual situation of computer data security protection, blockchain technology is applied in it, so as to better conduct multi-level encryption and modeling for computer data. At the same time, according to the advantages and characteristics of blockchain technology, reasonable construction of remote verification protocol can fundamentally solve the problem of computer data security protection. This paper discusses the important role of blockchain technology in the security protection of computer data, and puts forward three types of cryptography technology, aiming at optimizing and improving the security protection mechanism of computer data, so as to further improve the quality and level of data security protection.

**Key words:** blockchain technology; Computer; Data security protection

## 0 引言

区块链技术其本质意义上,就是一种进行特殊数字加密处理数据结构。区块链技术将提取到信息和数据通过合理拆分,分解成不同节点,然后熟练应用共享机制以及共享制度,让其每个节点都具备相同权限以及地位,从而达到分享目的和效果。此外,从数据角度出发,区块链也是不可被随意更改数据分布式信息数据库。区块链技术其涉及技术较多,主要包括 P2P、链上脚本以及非对称加密技术等。计算技术不断创新和发展,已经被广泛应用在各行各业之中,在合理应用计算机技术过程中,也应将眼光着重放在提升数据安全性以及完整性上。区块链技术具有较强多样性、透明性、系统性以及安全性。将区块链技术应用在网络通信之中,能确保更加安全可靠传输数据,与传统网络安全技术项目,区块链技术有着较强防护性、安全性以及严谨性。

## 1 区块链技术概述

区块链基础框架主要由以下几部分构成:(1)网络层。主要是以合理应用 P2P 技术作为执政,主要包含数据传播、交易验证以及验证等机制。(2)数据层。数据层主要为数据链式与区块结构,其数据处理主要技术为,非对称加密、时间戳以及哈希算法等。(3)合约层。区块链技术重要延伸之一就是智能合约。因此人工必要性,会随着区块链进步和发展随之发生变化,控制、促进以及执行交易等步骤,智能合约可通过数字方式进行、验证<sup>[1]</sup>。(4)应用层。应用层实际上指在不同场景应用区块链,并在所有节点都可在带有时间戳数据区块中,合理

进行封存相关教育数据,更好维护账本。(5)激励层。激励层主要由发行机制以及分配机制两种。同时也属于分布式记账。

## 2 区块链技术在计算机数据安全保护中重要性

### 2.1 去中心化作用

区块链技术具有去除中心化作用,也能更好进行处理基础数据。因此在区块链技术运行过程中,在分布式结构支持下,有效开展数据分析、数据处理、数据更新以及数据传输,从而更好构建去中心化信息模型。在此技术环境下,系统任意节点被外界因素攻击时,系统不能干扰区块链网络整体能力<sup>[2]</sup>。

### 2.2 有效保证计算机数据安全性以及完整性

即便是出现联网服务中断或者无服务问题时,合理应用区块链技术,也能更好进行信息传输。在断开连接节点时,区块链技术也能保持较好稳定性良好运行,并且也具备较好防护能力,有效避免以及减少因恶意攻击影响数据安全性以及稳定性情况<sup>[3]</sup>。最后,合理应用区块链技术,能有效保证计算机数据具有较强安全性以及完整性。

### 2.3 有效保证计算机数据可靠性

传统网络安全技术是应用边界防护程度保护数据传输,其主要是以加密和信任方式确保基础数据安全,但是这种方式存在着一定延迟性以及滞后性。信息技术不断创新以及发展,传统网络安全技术已经不能满足当前发展需求以及需要,并对传统安全技术不断升级以及完善,合理应用区块链技术,能够打破信任机制和加密技术束缚,并合理构建共识机制以及反向链接数据机制,从而更好分析以及记录区块链数据,确

保数据具有较强完整性以及安全性<sup>[5]</sup>。

## 2.4 降低篡改信息数据可能性

在区块链技术形成较大规模框架时,会相应增加数据节点,从而构建出具有全网联动性质的控制联动机制,确保能更好监督和管理全网各节点存储数据,降低信息数据出现篡改信息数据可能性。与此同时,在部分一定数量数据节点达成共识之后,区块链技术能更好完成更新以及升级。

## 3 密码学技术在计算机数据安全保护中主要类型

密码学技术在计算机数据安全保护中主要有以下几种类型:非对称加密、加密以及哈希加密等算法。因此,对以下三种加密算法进行分析,充分发挥供应链技术在计算机数据安全保护中作用以及效果。

### 3.1 非对称加密算法

非对称加密算法是密码学技术中基础部分之一,在具体实践过程中主要有两种,分别用于解密和加密。因此两种密钥分别为隐私密钥、公开式密钥。其中,非对称加密算法主要作用在于:计算机用户甲方获取一级密钥之后,甲方完成自身隐私密钥安全存储,而对外进行开放公开密钥。此外,计算机用户乙方在使用公开密钥时,应基于甲方基础上,对信息进行一些列加密措施以及方法,并将密文及时传递给甲方。甲方依据乙方基于隐私密钥,对密文进行解析。通过这种方式,能有效保障计算机用户数据信息安全。

### 3.2 对称加密算法

对称加密算法主要作用就是,能对同等密钥算法进行高效解密操作。具体操作方式为:在通信甲乙双方确定通信联系时,应实现确定密钥。同时在进行通信器件,完成传送密钥工作,并对明文数据信息采取加密措施,在进行加密数据库处理之后,即可得到相关密文信息,从而方便乙方(接收方)对密文使用密钥进行分析以及研究,从根本上提升数据传输安全性以及稳定性<sup>[6]</sup>。在实践过程中发现,对称加密算法整体计算数量不多,并且具有较为高效便捷解密以及加密能力,从而使得对称加密方法被防范应用在计算数据集安全保护工作之中。常见对称加密算法主要有 aes 以及 des 式、两种算法。此外,在甲乙双方进行交易时,使用同一组密钥从而确保在算法体系之中具有较强安全性以及严谨性。同时,密钥安全传送以及安全存储,能够极大提升甲乙双方交易双方,信息数据安全保障水平以及质量。因此,有关工作人员在设定密钥过程时,应合理应用对称加密算法,从而进一步确保加密系统具有较强安全,切实发挥对称机密算法应用价值。

### 3.3 哈希算法

密码学技术中较为关键性部分之一就是哈希算法。合理应用哈希算法,能够完美转化数据长度,从而有效提升数据传统有效性以及合理性。在大多数情况下,不同信息数据在传输过程中存在着一定差异性。同时,若是在信息输入过程中存在较大相似性是看,其大多数数据输出结构,都会表现为差异性。而哈希算法实际上是具有单一方向使用方式,并且能高效处理输入数据,有助于计算机用户获取到较为准确信息。此外,基于哈希算法优点,在通讯传输过程中,能有耿浩完成数据传输,及时将信息数据传递给计算机用户,确保哈希算法数据完整性以及可靠性,有助于接收方耿浩进行数据接收。最后,在出现二次接收以及获取相关数据信息时,合理应用哈希算法处理数据,从而通过分析结果,研究是否存在

数据信息篡改几率。

## 4 基于区块链技术的计算机数据安全保护策略

### 4.1 基于区块链技术合理构建计算机数据隐私保护计划

针对计算机隐私数据进行保护时,合理应用区块链技术,对其展开全方位保护,并合理构建针对性较强计算机保护系统模型。其主要包含以下几种功能板块。(1)数据层。将计算机用户进行集中,从而共同进行数据维护。同时为保护数据隐私,要想更好进行数据加密,可合理应用 ntru 密码系统进行,并将机密后数据上传到云端,从而实现信息共享目的,此外因为在此期间应用阈值同态密码程序,所以在集中用户时,应通过数据执行进行解密。(2)云端。此功能板块主要作用是,针对部分用户加密信息存储,并为其提供与之相匹配数据下载以及上载服务,同时还支持与快链之间读写交互。(3)区块链。区块链板块能够读取云端传输过来具体内容。但是当区块链被集体用户接收以及采纳时,不能将整体信息进行随意移除以及更改操作,同时用户可以与进行与之相对应交易。(4)用户层。用户层板块主要是通过数据共享方式,合理进行数据交换,并且也可进行相应计算,从而实现其目的。最后,在应用区块链技术过程中,能有效避免信息共享时,出现被随意篡改情况,也能基于实际情况,进行相应跟踪和处理。

### 4.2 合理构建计算机用户数据隐私保护计划

为能更好保存以及保护计算机用户数据,可在恰当时合理使用 NTRU 算法加密需要保护信息,并在区块链中保存 HASH 值,以防止随意篡改密码。同时用户要想访问相关数据,只有通过密钥才能进行。通过这种方式能起到较好隐私保护作用。HASH 值其本身具有较好的防篡改特性。所以,合理应用区块链技术能充分发挥区块链防篡改效果。此外,若是针对多个用户需要访问加密数据时,应分发密钥。要想进行解密,多个用户获取密文才能共同解密。

### 4.3 合理构建计算机数据共享保护机制

计算机数据共享保护机制主要分为两部分构成,主要有保护原理以及保护机制。(1)保护原理。应用区块链技术,能更好保护计算机数据共享,并在安全云服务、区块链、第三方数据请求人员、传感器所有者之间都有着较为紧密联系。在实践运行过程中,传感器拥有者激活传感器,并在智能合约下注册。传感器进行精密测量数据,并且将相关数据输送到云储存服务器之中。同时,第三方数据请求人员通过对传感器进行请求数据类型操作。传感器签订相关协议之后,再深度挖掘智能合约实际内涵。再由安全云板块进行过滤处理数据。并且按照不同计算机用户实际需求,相应变动重新签署密钥。加密相关数据之后,存储在云服务器临时位置上。安全云板块在解签密同时进行数据恢复,并将数据发送给第三方请求人员。(2)数据共享保护机制。有关工作人员在设计以及构建区块链数据模型过程中,应明确数据主体。计算机用户发送内容与数据使用目的以及范围,都会被告知将要采集数据信息和用途,并经过授权之后,才会在其系统中反映授权信息,并在全网发布共享请求。同时,为能确保全网不同节点都能收到相关共享请求,应基于区块链技术,合理构建分布式网络结构。此外,信息提供人员应按照共享请求实际情况,在区块链网络上传相应内容是,应符合清切数据格式,或者根据实际需求,在云服务上进行上传以及加密程序。通过这种方式能有效避免相关数据内容不被篡改。另外,在数据共享过程中,

# 基于自适应蚁群的无线传感网络节点覆盖优化方法

袁平亮<sup>1</sup>, 张红蕾<sup>2</sup>

(1. 国网甘肃省电力公司信息通信公司, 甘肃 兰州 730070;

2. 兰州城市学院 实验室与设备管理中心, 甘肃 兰州 730070)

**摘要:**针对常规网络覆盖优化方法效果不佳的问题,提出了一种基于自适应蚁群的无线传感网络节点覆盖优化方法。先构建无线传感网络节点覆盖优化模型,确定网络节点覆盖消耗的能量。然后基于自适应蚁群算法修订优化模型的隶属度函数,为中继节点覆盖提供适应性。最后优化无线传感网络节点覆盖的时间复杂度,找出隶属度函数矩阵中的最佳中继节点,进而实现无线传感网络节点的有效覆盖。结果表明,该方法的覆盖优化效果更佳,能够应用于实际生活中。

**关键词:**自适应蚁群;无线传感网络;网络节点;中继节点

中图分类号:TP393.4

文献标识码:A

文章编号:2096-9759(2023)06-0044-04

## Adaptive ant colony based node coverage optimization method for wireless sensor networks

YUAN Pingliang<sup>1</sup>, ZHANG Honglei<sup>2</sup>

(1.State Grid Gansu Electric Power Company Information Communication Company, gansu lanzhou 730070,China

2.Laboratory and equipment management center, Lanzhou City University, gansu lanzhou 730070,China)

**Abstract:**Aiming at the problem of poor performance of conventional network coverage optimization methods, a node coverage optimization method for wireless sensor networks based on adaptive ant colony is proposed. Firstly, the wireless sensor network node coverage optimization model is constructed to determine the energy consumed by the network node coverage. Then the membership function of the optimization model is revised based on adaptive ant colony algorithm to provide adaptability for relay node coverage. Finally, optimize the time complexity of wireless sensor network node coverage, find the best relay node in the membership function matrix, and then realize the effective coverage of wireless sensor network nodes. The results show that the coverage optimization effect of this method is better and can be applied in real life.

**Key words:** adaptive ant colony; Wireless sensor network; Network node; Relay node

## 0 引言

网络节点的覆盖范围是判断该网络使用性能的关键指标,研究人员针对网络节点覆盖优化问题,设计了多种优化方法。如基于改进人工鱼群算法的覆盖优化方法<sup>[1]</sup>和基于改进

狮群算法的覆盖优化方法<sup>[2]</sup>,以上两种方法均能够对网络节点的覆盖问题进行优化,但是,无论是对 Map/Reduce 的覆盖机制还是 Logistic 函数的优化,均存在一定的局限性,受到网络时延、吞吐量等问题的限制,节点覆盖效果始终不佳。因此,

收稿日期:2023-02-16

作者简介:袁平亮(1990-),男,汉族,河南商丘人,硕士,中级工程师,研究方向:无线传感器定位技术。

为确保其数据共享工程具有较强安全性以及隐私性,信息提供人员应事先将需要数据信息进行加密,然后再将相关数据上到云服务器之中,区块链接收到相关数据信息及时,计算机用户即可使用与之相对应密钥进行下载数据操作。因此,在设计数据共享模型时,应构建具有代理重加密区块链共享机制,以便更好分享相关数据,有效控制访问。但是若是计算机用户数量较多、需求量较大时,应合理控制信息提供人员同时上传信息数量。通过这种加密方式,能够更好实现授权人和被授权人之间信息共享,不仅能在一定程度上降低节点通信量,也能极大提高共识效率。最后,为能准确在 EAA 节点上传数据,可通过区块链方式,将其中信息传递给节点,信息共享人员也能够通过相应密钥,访问相关共享数据,从根本上提升计算机数据共享合理性、安全性以及及时性。

## 5 结语

综上所述,在计算机数据安全保护中,应用区块链技术已经充分发挥出其特点如,较好公开透明性、去中心化、持续性、安全性、稳定性等。同时以区块链技术为基础,融合多种数据安全技术,从而有效提升各行业计算机数据安全性、透明性,

并根据不同行业实际需求,合理优化以及完善计算机网络安全技术,充分发挥区块链技术应用价值以及作用。此外对其有效利用能从根本上改变传统安全保护缺点和不足,有效降低企业成本,防止篡改各种信息行为,帮助企业提升经济效益,获取长足稳定发展。

## 参考文献:

- [1] 符安文.区块链角度下计算机数据安全的保护方法[J].电脑知识与技术,2022,18(12):24-25.
- [2] 张丽.基于区块链技术的计算机数据安全保护分析[J].无线互联科技,2021,18(12):101-102.
- [3] 祝烈煌,董慧,沈蒙.区块链交易数据隐私保护机制[J].大数据,2018,4(01):46-56.
- [4] 孙志勇.基于区块链的计算机数据安全保护策略研究[J].电子设计工程,2020,28(24):29-32.
- [5] 刘格昌,李强.基于可搜索加密的区块链数据隐私保护机制[J].计算机应用,2019,39(S2):140-146.
- [6] 陈杰妹.基于区块链的物联网数据信息共享安全机制研究[J].数字通信世界,2019,000(11):136.