基于区块链的计算机信息安全技术研究

王利波，么子燕
国网山东省电力公司临清市供电公司，山东 临清 252600

摘　　要： 随着计算机终端的不断发展和越来越强大，它给人们带来了方便，但也给计算机终端的信息安全提出了更高的要求。计算机终端资料是一种可增值的、可共享的、可加工的资源，如果出现这种情况，势必会给使用者带来极大的冲击。计算机终端的信息安全认证，其实质就是利用一种安全的认证方式，使其不会受到任何形式的损害和干扰。现有的研究手段主要有大数据技术和可信的 SoC 启动框架等。但是，以上两种方式在智能卡中的处理能力都受到限制，在不断增加的计算机终端中，难以高效地进行安全认证。由于区块链技术所具备的诸多优点，使得它在信息安全方面有着天然的优势，因而受到了世界各国的重视。

关 键 词： 区块链技术；计算机信息终端；安全认证

Research on Computer Information Security Technology Based on Blockchain

Wang Libo, Yao Ziyan
State Grid Shandong Electric Power Company Linqing Power Supply Company, Linqing, Shandong 252600

Abstract: With the continuous development and increasing power of computer terminals, they have brought convenience to people, but also put forward higher requirements for information security of computer terminals. Computer terminal data is a valuable, shareable, and processable resource. If this situation occurs, it will inevitably bring great impact to users. The essence of information security authentication for computer terminals is to use a secure authentication method to prevent any form of damage or interference. The existing research methods mainly include big data technology and trustworthy SoC startup frameworks. However, the processing power of both methods in smart cards is limited, making it difficult to efficiently perform security authentication in the increasing number of computer terminals. Due to the many advantages of blockchain technology, it has natural advantages in information security and has therefore received attention from countries around the world.

Keywords: blockchain technology; computer information terminal; security certification

一、区块链技术特征

从根本上说，区块链就是由多个区块按照发生的先后次序排列而成，最后组成一条链，也被储存在这个系统中的所有伺服器之中。只要所有的服务器都能正常运行，那么区块链就是安全的。在区块链技术中，每一台服务器都是一个节点，它能够为网络的计算与存储提供支持。若要对储存于区块链中的资料进行修改，则需得到半数以上节点的一致认可，且对各节点进行一致的修改。一般来说，每个节点都是独立的，所以很难窜改区块链的信息。

相对于传统的 Web 技术，区块链技术具有以下两大特征：

①安全。如果没有“51% Attack”，那么很难被篡改，所以区块链上的信息更加可信，避免了用户之间的不信任。

②中心化。区块链技术不需要集中管制，也不需要对硬件设备的过分依赖，也不需要对第三方的管制。该系统采用了分布式的存储与运算方式，使各节点能够有效地进行信息的自主管理与自检。用“去中心化”来形容区块链技术的最根本的核心特性一点也不为过。

③匿名性。从区块链的角度来看，不需要对每个节点的身份进行认证，也不需要暴露自己的身份，可以进行匿名的信息传输。

④开放的。以开放源代码为基础的区块链技术，除交易双方的私密资料以外，其它一切资料均可公开。任何人都可以通过共同的界面来发展应用层，或者是对区块链的数据进行直接的询问。在整个区块链系统中，信息具有很高的透明度。

⑤独立的。在区块链中，各主体通过谈判达成共识，使整个区块链都能遵守一个统一的协议与标准，因而不会受到第三方的干扰。各节点之间能够进行数据传递和相互校验，保证了充分的独立性。

二、基于区块链技术的信息网络安全

在当今因特网的飞速发展下，信息的传播日益透明化，它巧妙渗透到人们的日常生活之中。目前，我国正处于一个非常重要的时期。目前，我国计算机网络安全领域的犯罪活动频繁发生，且呈多发态势，对我国的公共秩序构成了很大的压力。由于因特网具有很强的隐蔽性，所以在对信息网络中存在的安全隐患进行及时检测是非常困难的。由于区块链技术的“去中心化”特性，

使得所保存的数据更加可信，并能有效地避免用户之间的相互不信任。由于因特网具有独一无二的可追踪性“标签”，因此，它非常适于保障数据信息的安全传送，并能有效地防止被骇客所侵害。本文从以下几个方面阐述了区块链技术在信息网络安全领域的应用。

（一）信息数据分析中区块链技术的应用

信息数据分析是一项非常关键、却极易发生泄漏的工作。基于区块链的数字能够很好地解决这一问题。

（二）用于信息安全的区块链技术

为了保证信息安全，采用了哈希算法，并采用了不对称公私钥加密算法，使得整个系统中的节点都可以参与到其中。这样可以有效地避免出现诸如数据遗失和账目窜改之类的不良状况。

（三）数据流通中区块链技术的应用

正如前面提到的，区块链技术是一种很好的可追踪性，它可以帮助我们对各种类型的数据进行完全的掌控，比如：数据的回溯历史分析，多主体的利益保护等等。

（四）区块链技术在防止信息记录篡改中的应用

提出基于区块链的认证和一致性的方法，该方法能够对特定的区块链数据进行精确的判断，从而有效地防止了数据的篡改。同时，利用区块链技术构建的分布式域名存储体系，可以有效地抵抗 DDos 攻击，使其安全性能得到最大程度的提高。

（五）区块链技术的应用

随着 5G 技术的迅猛发展，信息共享与开放已经成为 T 产业发展的新潮流。每一天，都会产生海量的信息，其中大部分都是隐私的核心。一旦泄露，毫无疑问将造成极大的危害。区块链技术能较好的解决以上问题，同时又不影响数据共享。基于公开的数据，可以有效地保护数据的完整性，并对其进行安全管理。

（六）用于用户身份验证的区块链技术的应用

可以使用不对称的公开密钥和私有密钥的加密方法来对用户的识别信息进行加密。该方案采用两个独立的密钥体系，保证了各系统之间的信息安全。由于网络犯罪的特殊性，使得网络使用者的身份信息难以被识别、伪造，从而有效地避免了个人信息的泄漏。

三、利用区块链技术进行计算机终端信息安全验证的方法

（一）整体体系结构的设计

①安全验证过程

在进行信息安全验证的过程中，计算机终端管理模块一般起着使用者和管理员两种作用。系统管理员一般使用区块链技术，能够高效地对终端服务节点及相关的链码进行管理与维护。一旦通过了安全验证，那么就可以对云存储模块进行读取和写入，同时也可以对其进行某种程度的访问控制。同时，该系统还采用了区块链的结构，将该系统的所有信息安全验证过程都记录在了区块链结构中，也就是说，indexDB 中存储了索引信息，historyDB 中存储了状态参数的改变信息，stateDB 中存储了设备的最新状态信息。首先，使用者需要在系统中登记自己的身份，其次，当使用者成功登陆后，系统会对使用者进行认证，验证使用者的权限，如果认证通过，使用者就会获得相应的权限，可以进行使用。

②链式代码技术的应用

Fabric 超记账系统中，其智能合同功能的实现以链式代码为主，包括用户链和身份验链式代码 2 个方面。验证模式链式代码主要实现验证和配置等功能，并能在终端的 peer 进程中有序稳定地运行；而用户链式代码是一种信息数据，该信息数据有助于最终用户对操作进行动态地执行，比如，Invoke 方式下的 deleteData 能够消除不合法的信息，Invoke 方式下的 modify Permission 能够更改计算机终端的权利，Invoke 方式下的登录能够让用户登陆计算机终端，Invoke 手段中的 QueryPermission 能够对应用程序的权利策略进行查询，init 方法能够起到对计算机终端进行初始化的作用。

在进行安全性验证时，链式代码将所需的信息数据动态地传送给计算机终端，并对其进行实时的响应。Fabric 超记账系统中的信道可以看作是两个结点的连线，也可以看作是由多台计算机间的数据交互构成的一个独立的网。在 Fabric 的超级账本中建立信道，本质上就相当于建立了一条信息安全的链接，不管是哪一种安全的验证，都必须通过信道进行。一般情况下，Fabric 的超级账本会同时产生多条信道，每一条信道都可以独立地存在于不同的信道中，并可以通过信道之间的通讯来完成。

（二）设置密码服务

当前，大部分的计算机终端都是以集中式的方式进行信息安全验证。然而，由于存在着较强的脆弱性和单点失效等问题，这类问题往往对网络中的核心节点具有很强的依赖性。若基站中的核心节点受到诸多拒绝服务等的恶意攻击，则会导致整个系统的信息安全认证失效。针对以上问题，利用区块链技术，建立一套基于区块链的身份验证模型。该方案使用带授权的 Fabric 超级账本，实现分布式的安全性验证，并对计算机终端生成的数据进行存取与控制。

Fabric 超级记账可以在不同的计算机终端应用环境中使用，包括 Cello，FabricSawtotheIroha 等。由于应用场合和用途的不同，Fabric “超级记录簿”的构成也会有所不同。另外，Fabric 的超记账也能被用于开放的公有链模式。Fabric 超记账采用了数字凭证的方法，其主要目的在于通过数字签名来验证其真伪。每一位区块链信息使用者都会有一张不会复制的数位凭证（FabricCA），以保证计算机终端机资讯的安全性。另外，Fabric 超记账还使用了 SCCSP 加密算法，能够在不改动核心代码的前提下实现多种加密算法，并通过特殊的传输通道将其传送到接收者。接收方可利用解密密钥及相应的算法将其加密，以达到最大的安全保障。

四、试验设计及结论分析

（一）试验预备

利用区块链技术对计算机终端进行信息安全验证，将三

个 Zookeeper，4个 Kafka 终端信息结点，4个 Peer 结点，3个 Orderer 序列验证节点，并对其进行验证。这样既可以在区块链技术中作为计算机终端装置的一个轻结点，又可以对计算机终端装置的使用者进行识别和鉴别。在 Ubuntu 桌面14.04 LTS 中。在以区块链为基础的 Fabric “超级账本”中，加入了机构（Org1）和机构（Org2）两个机构，各机构由2个终端信息结点和 CA 结点组成，并配置在 Peer0结点上。以区块链为基础，在初始化时，由序列结点、认证点对结点组成六个结点。该方案由两个 Peer 节点构成一个机构，共用同一个 Fabric 超账本的鉴权信道，而各节点之间则可以通过链代码进行交互。

（二）试验程序

以区块链分布式计算为基础，构建了一种以分布式计算为基础的加密算法。以区块链为基础的计算机终端信息安全验证，其实质并不只是涉及到多方的参与与维护，而是要构建一个日益壮大的分布式数据库。以区块链为基础的 Fabric 超级账本，通过 Golang，Java，JavaScript 等多种程序设计，实现与终端设备之间的数据交互。

以区块链为基础，在计算机终端启动时，必须先登记并确认各节点的身份。一旦取得了法律上的识别，就变成了计算机终端上的一个合法节点。在区块链的基础上，各节点之间并不要求彼此间的信任，并且不会对已计算机进行数据交换。相对于传统的计算机终端信息安全验证方式，采用区块链技术，能够在不需要中央控制的情况下，达到一致同意的目的。

（三）试验结果

利用区块链技术对计算机终端进行了一系列的验证试验。针对目前存在大量数据存贮的问题，对传统的计算机终端信息安全鉴别方法和所采用的方法进行了并对各种方式的结果作了对比。通过试验比较，证明了采用传统的身份验证技术能够实现对计算机终端的信息安全的基础验证。但是，当一个计算机终端上存有大量的数据时，采用传统的身份验证方式，会因其容量的限制而耗时过长；而以区块链为基础的计算机终端进行信息安全验证，可以在2秒内完成正常的安全性验证和安全证书的更新，大大节省了时间，提升了认证的效率。

结束语：

综上所述，将区块链技术运用于计算机终端的信息安全认证，能够快速、精确地完成使用者的授权及节点的更新查询。针对这一问题，文章中运用区块链技术，利用 Fabric 超级账本，来实现分布式认证。该方法能够在系统的存取与控制中生成对应的数据资料，便于对用户进行身份管理，并对其进行授权与使用。经过试验证明，提出的算法是一种快速、高效的安全认证算法。

参考文献：

[1] 王良敏．基于区块链技术的计算机终端信息安全认证模式设计［J］．电脑知识与技术，2023,19(20):109-111.

[2] 任刚．基于区块链技术的计算机终端信息安全认证［J］．电子技术与软件工程，2022,(16):14-17.

[3] 刘亚男．基于区块链技术的计算机终端信息安全认证研究［J］．吉林工程技术师范学院学报，2021,37(05):81-84.

[4] 郑帅．基于区块链与大数据分析的信息处理方法研究［J］．科技创新与应用，2023,13(12):122-125.

[5] 吴小迪．基于区块链的计算机通信网络安全加密控制系统设计［J］．信息记录材料，2022,23(11):163-165.

[6] 茹兴旺．基于区块链技术的物联网节点信息安全研究［J］．九江学院学报（自然科学版），2022,37(3):28-31.

[7] 金丽双．区块链技术在电子档案安全管理中的应用［J］．黑龙江档案，2022(4):55-57.

[8] 杨茜．关于区块链在信息安全领域的研究［J］．信息记录材料，2022,23(8):23-25.

[9] 周丽．区块链技术在信息安全中的应用研究［J］．电子元器件与信息技术，2020，4（4）：30-32.

[10] 石超．区块链技术的信任制造及其应用的治理逻辑［J］．东方法学，2020（1）：108-122.