《基于患者E-Health诊治数据的安全存储与管理》检测报告

PaperRight™
PR（PaperRight.com）论文查重

总相似率：39.88%

基本信息

文档名称	基于患者E-Health诊治数据的安全存储与管理	报告二维码防伪
报告编号	7fb00f35-9df3-4574-9d52-7ac9b58b7c0a	
文档字数	5439	
提交人姓名	黎炜烨	
提交方式	粘贴文本检测	
检测范围	学位论文库（含硕博）、学术期刊库、会议论文库、法律法规库、互联网资源库、自建比对库	
提交时间	2019-04-11 08:45:00	

检测报告指标详情

原创率	抄袭率	引用率	字数统计	参考文献字数
60.12%	39.88%	0%	5439	-

相似片段位置图

注：红色部分为重度相似，橙色部分为中度相似，蓝色部分为引用部分

相似片段详情（仅显示前10条）

序号	篇名	来源	命中率
1	...of “Privacy-preserving attribute-keyword based data ...	互联网资源库	3.92%
2	区块链和外汇行业的有什么关联—GPP外汇_搜狐财经_搜狐网	互联网资源库	3.05%
3	智能合约开山之作:《智能合约》——尼克·萨博 - 链世界	互联网资源库	2.21%
4	区块链技术在金融领域的应用与前景研究	学术期刊库	2.17%
5	中本聪论文《比特币:一种点对点的电子现金系统》 中英文对照!	互联网资源库	1.73%
6	Blockchain can be Blocked(比特币网络通讯底层漏洞详解) - 区块...	互联网资源库	1.73%
7	区块链在金融领域的应用前景探究	学术期刊库	1.64%
8	区块链算法简介(一)	互联网资源库	1.53%
9	技术构思:通过2-of-2多重签名,构建实现类闪电支付_巴比特_服务于...	互联网资源库	1.42%
10	基于个人电脑的比特币数据统计系统	学位论文库	1.42%

文档原文标注

基于患者E-Health诊治数据的安全存储与管理

摘 要

本系统是对原有协同诊治平台的存储和分享系统进行升级，目的在于提升原有系统中对于医疗数据存储和分享的安全性。系统前端基于iOS平台，承接了原有的问诊流程，包括信息录入、病历查看等功能；后台采用了基于区块链的实现方案，其中使用以太坊平台对区块链服务进行开发，最终实现了病人医疗数据的加密存储和授权共享。经过编码实现，证明了本系统能够有效的提高诊治数据的存储、读取和管理的安全性。

关键词：协同诊治平台、医疗数据、区块链、安全性

Secure storage and management based on patient E-Health diagnosis and treatment data

Abstract

The system upgrades the storage and sharing system of the original collaborative diagnosis and treatment platform, with the aim of improving the security of medical data storage and sharing in the original system. The front end of the system is based on the iOS platform. It undertakes the original consultation process, including information entry and medical record review. The background uses a blockchain-based implementation solution, in which the Ethereum platform is used to develop the blockchain service. Encrypted storage and authorized sharing of patient medical data is achieved. Through coding, it is proved that the system can effectively improve the security of storage, reading and management of diagnosis and treatment data.

Keywords：Collaborative diagnosis and treatment platform、Medical data、Blockchain、safety

1.绪论

1.1 研究背景、目的与意义

医疗健康问题是自古以来人类的一大难题，即使目前是在科技十分先进的二十一世纪，人类也无法攻克所有的医疗难题。除此之外，医疗健康问题与每一个人都息息相关，而且随着人们生活水平的不断提高，人们已经不再只关注温饱问题，对自身的健康状况越来越重视。然而国内大部分地区在大力发展经济之余，医疗设施和设备却没能跟上。另一方面，现代人的生活压力与日俱增，亚健康人群年年增加。我国的医疗发展起步晚，医疗设施落后，医疗信息化和数字化进程缓慢，对于病人的医疗隐私数据也缺乏安全有效的管理。

医疗信息数字化是未来的发展趋势，利用现代先进的计算机技术，可以减少传统医疗系统中重复的人力操作，使得诊治过程规范化。其中医疗数据（处方、病历记录、身份信息、文档信息）的安全存储和管理更是重中之重，在传统的解决方案中，需要提高电子医疗数据的权限、隐私、安全等，以维护数据的完整性、正确性、可靠性、安全性和隐私性。

区块链是目前新兴的一种分布式存储技术，它具有去中心化、不可篡改、匿名性等优点。区块链技术与传统的医疗信息系统相结合，可以有效的实现医疗记录的安全存储和分享。

综上所述，设计出一套基于区块链的电子医疗数据存储系统有极大的研究和社会意义。

1.2 国内外研究现状

21世纪是信息化时代，个人数据被大量收集和利用，医疗数据也不例外。对医疗数据的挖掘和分析，有利于医疗机构进行对于疾病的研究和防控，但同时也会带来隐私问题。隐私保护是针对公开发布的数据采取的一系列措施，防止第三方通过数据挖掘等不法手段获取病人的敏感信息。在数据发布领域，学者提出了多种隐私保护模型，主要包括：t-closeness、I-多样性、k-匿名模型等。这些模型的原理都是通过隐藏公开的隐私数据和具体个人之间的关系，但是保证发布数据的信息公开可用。

2.本论文相关理论

2.1 区块链技术

2.1.1 定义

2008年，中本聪在《Bitcoin：A peer-to-peer Electronic Cash System》一文中首次提出了“区块链”的概念。但是该文着重描写比特币系统，对于区块链技术并没有给出具体的定义。在中本聪的论文中，区块和链被描述为一种用于记录比特币交易过程中交易历史的数据结构。维基百科对于区块链的定义是：区块链是一种分布式数据库技术，通过维护链式的数据结构，来保证不可篡改的数据记录的可持续增长。

本文从狭义和广义两方面对区块链下定义：

狭义上，区块链是一种链式的数据结构，以区块作为基本单位。区块中通过数字摘要对过往的交易信息进行校验，具有可持续增长、去中心化、不可篡改等特点。

广义上，区块链代指一系列分布式记账技术，包括智能合约、加密技术、分布式共识等。

区块链的共享价值被众多的加密货币，如比特币、莱特币、以太币等所效仿，并在工作量证明和加密算法上做了许多改进，如采用Proof-of-stake、Scrypt算法等。截止至今，区块链生态在全球逐步扩大，出现了智能合约区块链以太坊、区块链众筹ICO、资产代币化共享经济等新兴产业。

2.1.2 应用

区块链的共享价值被众多的加密货币，如比特币、莱特币、以太币等所效仿，并在工作量证明和加密算法上做了许多改进，如采用Proof-of-stake、Scrypt算法等。截止至今，区块链生态在全球逐步扩大，出现了智能合约区块链以太坊、区块链众筹ICO、资产代币化共享经济等新兴产业。

2.1.3 工作原理

传统的交易系统，都需要可信赖的第三方机构作为担保，实践证明这种机制一直运转良好，但是这类系统仍然天生受制于“基于信任的模式”的弱点。传统的交易系统无法实现完全不可逆的交易，因为第三方机构不可避免的会产生分歧。另一方面，金融机构的存在，一定程度上增加了交易的复杂性，并且限制了小额支付交易。所以，人们需要一种电子支付系统，基于密码学原理而不基于信用。达成共识的买方和卖方可以直接进行交易，交易过程不需要第三方金融机构的参与，并且产生的交易是不可逆的。区块链或者说比特币的出现解决了上述难题，中本聪的论文中提出了一种完全通过点对点技术实现的电子现金交易系统。买家可以通过系统在线将货币支付给卖家，中间不需要经过任何的金融机构。数字签名(Digital signatures)一定程度上可以解决第三方依赖的问题，但是仍然需要第三方的支持才能防止双重支付(double-spending)，这无疑不符合去中心化的特点。因此中本聪提出了一种解决方案，该系统通过随机散列对全部交易记录加上时间戳，将他们合并进一个持续增长的基于随机散列的工作量证明(proof-of-work)的链条作为交易记录，除非重新完成所有的工作量证明，否则这条链条被认为是不可更改的。只要互联网中大多数的计算能力没有合起来对系统发起攻击，那么可以认为这条链条是安全的。

1）交易

从技术上看，电子货币是一串数字签名：所有者对前一次交易记录和下一位所有者的公钥合起来进行签署生成的一个随机散列。将生成的签名附加在电子货币的尾部，电子货币就被认为发送给了下一位所有者。收款人通过对签名进行校验，确认自己收到了货币。

图 1 基于数字签名的电子货币

上述过程的问题在于难以检验双花问题，所谓双花问题就是付款者是否将同一枚货币支付了两次。通常的解决方案是引入权威的第三方机构进行公证，对每一笔交易进行检验。每一次交易结束后，第三方机构都要回收这枚货币，然后发行一枚新的货币，只有第三方机构发行的货币才可以在市面上流通，这样就可以解决双花问题。这种方案的痛点在于交易依赖于对第三方机构的信任，无法做到去第三方化。通过分析，为了避免发生双花问题，我们只需要了解之前的交易记录，而对于以后的交易记录其实是不关心的，如果要在电子现金交易系统中排除第三方机构的影响，那么就应该向全网公开所有的交易信息，整个系统内所有的交易者都有唯一公认的历史交易序列，收款人需要大多数交易者都承认该交易是第一次进行（之前没有使用过该货币）。

2）时间戳服务器

第一个改进方案就是给每个区块进行随机散列时加上一个当前时间的时间戳，并将得到的随机散列进行全网公告。显然，可以证明某个区块针对于特定时间是肯定存在的，因为只有在该时间存在才可以获得该散列值。此外，每个时间戳应当将前一个时间戳纳入其随机散列中，每一个后面的时间戳都对前一个时间戳进行增强，从而形成一个链条。

图 2时间戳服务器

3）工作量证明

工作量证明（Proof-of-work）是比特币和以太坊等货币中最常用的算法，其核心依赖于密码学。在分析工作量证明算法前先介绍散列函数（哈希函数）的概念。一个散列函数是可以将任意大小的数据映射到固定大小的数据的函数。以MD5算法举例如下：

MD5（“Hello World”）= B10A8DB164E0754105B7A99BE72E3FE5

MD5（“Hello World!”）= ED076287532E86365E841E92BFC50D8C

由上述结果可见，原文细小的改变都会导致随机散列值巨大的变化。

回到工作量证明算法，区块链通过共识算法来选举一位领导者来决定下一个区块的内容。领导者还要负责把该区块广播到网络，便于其他节点检验该内容的有效性。一个成员要想成为领导者并选择下一个添加到区块链的区块，必须要找到解决一个特定数学问题的方法。对该问题简单叙述如下：给定数据X，找到一个数n，使得X+n得到的哈希值是一个小于Y的数。举例如下：

Y = 10，X = “Hello World!”

hash(X) = hash（“Hello World”）= 0x0f = 15 > 10

hash(x+1) = hash（“Hello World1”）= 0xff = 255 > 10

hash(x+2) = hash（“Hello World2”）= 0x09 = 9 < 10

因此，找到n为2满足要求。由于MD5函数式加密安全的，所以我们通过暴力求解来尝试所有的

组合。我们把最快计算出上述结果的成员称为矿工，每一个区块被开发的时候，矿工会获得一部分奖励。在工作量证明中，其他节点通过检查区块的散列是否小于给定的数字来检验区块的有效性。

另一方面，工作量证明解决了如果确定最长的链条的问题。最长的链条被认为是安全的，因为最长的链条包含了最大的工作量。如果大多数的CPU被安全的节点控制，那么诚实的链条将会以最快的速度延伸，并超过其他的竞争链条。如果要对现在的区块进行篡改，那么攻击者需要完成当前区块之前的所有工作量，并最终超越现有的区块的工作量。经过证明，攻击者想要追赶上现有的区块，其成功概率呈指数化递减。但是，这不意味着区块链系统是绝对安全的。根据摩尔定律，硬件的运算速度在高速增加，而且诚实节点参与的网络状况也会有所变化。为了解决这种不安全的因素，工作量证明将难度与区块的生成速度的平均值相关联，如果区块生成的速度过快，那么难度将会提高。

图 3 区块链数据结构

2.1.4 智能合约

智能合约(smart contract)是一种特殊协议，在区块链内制定合约时使用，当中内含了函数(Function)，也能与其他合约进行互动、做决策、存储资料以及传送以太币等功能。智能合约主要提供验证及执行合约内所订立的条件。智能合约允许在没有第三方的情况下进行可信交易，这些交易可被追踪且不可逆转。智能合约的概念于1994年由从事智能合约和数字货币研究的尼克萨博(Nick Szabo)博士提出，尼克1996年在《Extopy》期刊上发表了对智能合约的描述，他认为智能合约是一个由数字表单指定的承诺，这个承诺包含关系到多方执行的一组协议。不同于法律意义上的合约概念，区块链领域的合约表达的是可以“自治自理”的计算机协议，这套协议具有自我执行、自我验证的属性。从技术上看，智能合约等价于一段被事先规定好逻辑和条款的计算机代码运行时的状态，同时，智能合约也提供了通用的用户接口，用户可以通过接口与用户交互。比特币是第一个实现了智能合约的产品，比特币的五种标准交易脚本提供了多方共同签名支付的脚本，又称多重签名支付，多重签名支付可以看做是智能合约的一种表现形式。

2.1.5 以太坊

以太坊是一个运行着智能合约的分布式平台：应用程序完全按照程序运行，不存在故障、审查、欺诈或第三方干预的可能性。换句话说，以太坊给予了人们使用区块链技术来验证运行代码的执行情况的能力。

2.1.3 应用类型

参考文献：