

基于区块链技术的疫情健康码方案

檀钟盛, 陈春晖

(福建工程学院 互联网经贸学院, 福建 福州 350118)

摘要:随着 Covid-19 爆发,健康码成为生活中不可或缺的一部分。尽管被广泛关注和运用,但是目前健康码存在着信息不安全和个人隐私泄露等问题。为了解决这些问题,通过区块链技术,提出一种基于以太坊智能合约的健康码方案。首先,分析了健康码防疫工作中的不足之处,介绍了区块链技术去中心化、不可篡改、可追溯等特点,研究了区块链技术与健康码相结合的可行性;然后,介绍了智能合约属性和机制,详细描述了业务逻辑和系统架构。通过将非对称加密和区块链相结合,满足了健康码信息安全和隐私保护的需求。仿真实验证明了健康码方案的可行性。通过基于以太坊智能合约的健康码平台与传统健康码进行对比,证明了该方案能够有效解决健康码信息安全、数据孤岛和用户隐私泄露的问题。

关键词:疫情防控;健康码;区块链;智能合约;隐私保护;以太坊

中图分类号:TP391

文献标识码:A

文章编号:1673-629X(2023)07-0215-06

doi:10.3969/j.issn.1673-629X.2023.07.032

Epidemic Health Code Scheme Based on Blockchain Technology

TAN Zhong-sheng, CHEN Chun-hui

(School of Internet Economics and Business, Fujian University of Technology, Fuzhou 350118, China)

Abstract: With the outbreak of Covid-19, health codes have become an integral part of life. Although it has been widely concerned and used, the current health code has problems such as information insecurity and personal privacy leakage. In order to solve these problems, we propose a health code scheme based on Ethereum smart contracts with blockchain technology. Firstly, we analyze the shortcomings of the health code epidemic prevention work, introduce the characteristics of blockchain technology such as decentralization, non-tampering, and traceability, and study the feasibility of blockchain technology application with health code. Then, the smart contract properties and mechanisms are introduced, and the business logic and system architecture are described in detail. By combining asymmetric encryption and blockchain, it meets the needs of health code information security and privacy protection. The feasibility of the health code scheme is verified by simulation experiments. By comparing the health code platform based on the Ethereum smart contract with the traditional health code, it is proved that the proposed solution can effectively solve the problems of health code information security, data silos and user privacy leakage.

Key words: epidemic prevention and control; health code; blockchain; smart contract; privacy protection; Ethereum

0 引言

2019年发生 Covid-19 疫情,中国政府反应迅速,采取果断措施,其中健康码就是措施之一。健康码是一项可以安装在智能手机上的软件,个人可以实名认证并填报健康状况^[1]。“健康码”诞生于数字政府建设发达的杭州。杭州健康码是依据《浙江省疫情防控责任令》,为解决疫情期间返工返岗及公共空间管控而采取的应急性技术治理措施^[2]。随着疫情常态化,健康码也出现长期存在的趋势,但目前健康码存在着以下问题:(1)信息不安全。主流健康码平台目前仍

是中心化系统,中心化平台容易遭受外部攻击。例如,北京健康宝就曾在疫情的高峰期,遭到境外网络的攻击。而且这样的攻击并不只有一次,早在北京冬奥会、残奥会期间,健康宝就曾多次遭受境外攻击,一旦这些外部攻击成功,将会导致不可估量的损失;(2)各地健康码相互不流通。在疫情防控中,健康码几乎等于身份通行证,然而目前由于数据不共享、地方政策不同等原因导致各地健康码各不相同,互不相认,甚至出现同一省份出现省市两级不同的健康码,造成了码上加码,给交通枢纽的人群造成不便;(3)健康码中个人隐私

收稿日期:2022-08-03

修回日期:2022-12-07

基金项目:福建省科技创新战略研究项目资助(2019R0086)

作者简介:檀钟盛(1997-),男,硕士生,CCF 会员(K6850G),通讯作者,研究方向为区块链技术与应用;陈春晖(1974-),男,副教授,硕导,博士,研究方向为数据、模型与决策。

保护不足。健康码数据中涉及姓名、身份证、联系方式等大量敏感数据,然而目前健康码平台五花八门,个人信息需要多次提交,泄露风险高。尤其在疫情期间,确诊患者信息泄露,极有可能导致社会歧视、网络暴力等严重后果;(4)健康码稳定性。由于主流健康码是中心化系统,一旦系统发生故障,可能导致系统数小时不能正常使用,给市民造成极大不便;(5)健康码职权滥用。健康码作为政府防疫工作中的重要工具,已经成为社会的普遍共识。在特殊的疫情时期,红码已经成为禁止令,滥用红码是对国家公信力的损害。区块链去中心化、可追溯、公开透明等特点为解决上述问题提供了技术支持,该文将区块链技术与非对称加密相结合,提出了一种基于区块链技术的健康码方案,并基于此方案构建一个系统来验证上述方案的可行性。

1 相关工作

1.1 区块链与智能合约

比特币属于区块链(blockchain)的 1.0 版本,比特币可以在没有第三方的情况下进行交易^[3]。区块链能够将数据分布式存储在不同的节点,任何节点都必须按照共识协议进行更新,从而实现了多方信息共享和监督^[4]。Buterin 在 2013 年提出了以太坊,它作为区块链 2.0 版本在区块链 1.0 的基础上,新增了图灵完备的编程语言,首次将区块链和智能合约相融合^[5]。Nick Szabo^[6]提出智能合约的概念,智能合约是一种可执行或验证的计算机协议,智能合约一旦生效就会坚定不移地按照合约内容进行自我验证和自我执行^[7]。总的来说,区块链由数据层、网络层、共识层、应用层、激励层和合约层组成,具体架构如图 1 所示。



图 1 区块链结构模型

区块链主要有以下两大特点:(1)去中心化:区块

链是由各参与节点组成的 P2P(Peer to Peer)网络构造的,没有中心服务器,所有参与节点都是服务器,数据分布在各个参与的节点上,所有节点在区块链中都是平等的。(2)不可篡改性:数据经过节点验证通过后会被永久存储在区块链上,除创世区块外,每个区块都有上一个区块的 Hash 值,如果修改某个区块的数据,则之前所有区块的 Hash 值都要重新计算,除非能掌握区块链中 51% 算力,否则某些恶意的节点修改是无效的。

1.2 非对称加密

1976 年,非对称加密这一概念首次由 W. Diffie 和 M. Hellman 提出。非对称加密需要两个密钥,即公钥和私钥。非对称加密的公钥和私钥是成对产生,如果使用公钥对一个明文进行加密,那么只有对应的私钥可以对密文进行解密。反之,如果用私钥对一个明文进行签名,那么同样也只有对应的公钥可以对其进行验证,具体非对称加密原理见图 2。目前,RSA 加密算法是用途最为广泛的非对称加密算法之一。

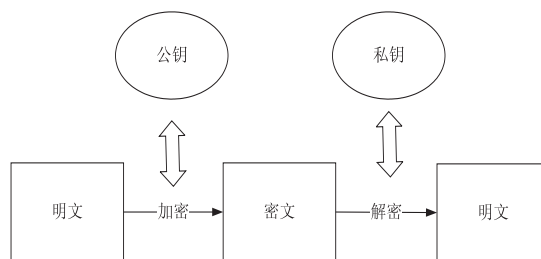


图 2 非对称加密流程

RSA 加密算法目前是最有影响力的公私加密算法之一。RSA 密码体制中包含一组密钥对,公钥和私钥,私钥归个人保管,公钥可公布给所有人。使用 RSA 加密首先需要知道接收方的公钥,使用接收方的公钥对明文进行加密,发送方将密文发送给接收方,此时即便遭遇外部攻击信息被拦截下来,拦截方没有对应私钥也无法破解加密文件,接收方收到密文使用私钥解密获取明文。RSA 加密算法安全性依赖于大数的因式分解,将两个大质数相乘是十分容易的,但是对两个大质数进行因式分解是十分困难的,所以用乘法作为加密密钥,安全性极高^[8]。

RSA 生成算法如下:

- (1) 随机产生两个不同的大质数 p 、 q ;
- (2) 计算 $n = p * q$, 同时计算欧拉函数 $\varphi(n) = (p-1) * (q-1)$;
- (3) 随机产生一个整数 e , e 与 $\varphi(n)$ 互质, 令 $\gcd(e, \varphi(n)) = 1$, 且满足 $1 < e < \varphi(n)$;
- (4) 计算 $d \equiv e^{-1}(\text{mod } \varphi(n))$;
- (5) 公钥 $\text{PublicKey} = \{e, n\}$, 私钥 $\text{PrivateKey} = \{d, n\}$ 。

1.3 相关研究

为了保证健康码隐私不被泄露和信息非法篡改的

问题,去中心化和非对称加密是健康码方案中不可忽视的重要环节。区块链作为一项新型技术,其去中心化、不可篡改等特点可用于多个领域,比如医疗^[9]、筹款^[10]、能源^[11]、人工智能^[12]、金融^[13]、疫情预警^[14]等。文献[15]提出了一种基于 Django 架构的校园健康码系统,系统高效整合了校园健康码信息,但系统并未对校园师生的信息进行加密存储。文献[16]使用 TDC 搭建了健康码系统,但同样未能对用户信息进行加密保护。文献[17]讨论了由于数字技术抗疫成为主流抗疫手段,导致了个人私密信息的泄露,应该加强对信息匿名化和脱敏化的处理。文献[18]认为目前 App (Application) 的隐私泄露严重,应该加强对 App 用户的法律保护。然而,中心化平台对信息有着绝对的控制权,故其容易遭受外部攻击导致信息被篡改或泄露。为了解决中心化带来的种种问题,相关工作则研究基于区块链技术的 Dapp (Decentralized Application) 应用。例如文献[19]提出了一种基于区块链技术的个人信息管理系统,使用区块链来管理信息。文献[20]提出利用区块链技术做一个隐私性投票,在不透露投票人的隐私的前提下通过投票决定是否进行以太坊资助。文献[9]提出了基于区块链的电子病历,通过部署在区块链上的智能合约来对病历进行增加、删除、修改、查询等功能。文献[21]提出将区块链技术与云存储技术相结合,实现基于区块链技术的医疗数据存储方案。上述研究虽然利用区块链技术防止了信息被篡改,但是并没有考虑到用户隐私泄露的问题。综合上述情况,该文提出将区块链技术与健康码相结合。利用区块链去中心化、信息公开透明、可追溯等特点保证了健康码信息公开透明,打破数据壁垒,为全国统一健康码的使用奠定了基础,同时满足了系统安全、用户隐私保护和红码追责的需求。

2 系统架构模型

将区块链技术引入健康码平台设计,基于以太坊平台进行去中心化的健康码方案设计。功能包括申请健康码、健康码信息展示、健康报备、高风险区域黄码等功能。为了保证用户隐私不被泄露,系统会用非对称加密对用户重要信息加密,然后上传区块链,以此保护用户隐私可靠,避免了用户的隐私泄露被不法分子利用,同时利用区块链不可篡改、去中心化的特点有效解决了信息安全的问题。

相较于传统的健康码平台,所提出的方案以区块链技术为核心,通过利用区块链不可篡改、去中心化、公开透明等特点实现了基于以太坊智能合约的健康码系统,有效解决了健康码信息安全、个人隐私泄露、红码追责等问题。

2.1 业务模型

图3展示了基于以太坊智能合约的健康码系统中用户提交数据进行链上存储以及平台操作流程。

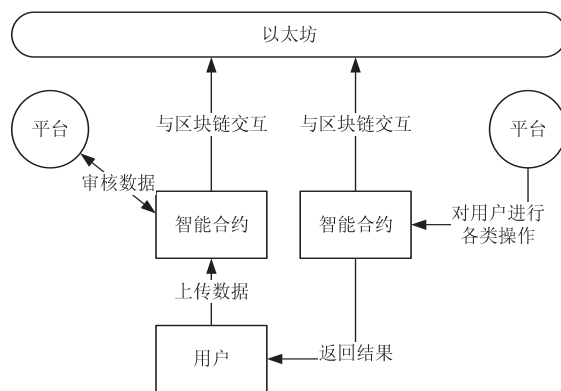


图3 业务模型

首先,用户提交信息到系统,系统收到用户的信息后使用平台公开的公钥对用户的隐私信息,如身份证、电话等进行加密;然后,将加密信息上传到以太坊。平台收到用户上传的加密信息使用平台的私钥解密得到原始信息,确认用户信息无误则审核通过。

健康码平台会对用户信息进行各类分析,用户过去14天行程中去过高风险地区,健康码则会从绿码变为黄码,变回绿码需要两次核酸检测,若两次核酸均没有问题,则自动变回绿码,红码人员在完成居家隔离和医学观察后,自动转为绿码,后台会自动把用户的健康信息更新到区块链上,方便工作人员查询。

2.2 系统技术架构

系统分为三个部分,Web前端模块、中间模块、区块链模块,系统具体架构如图4所示。

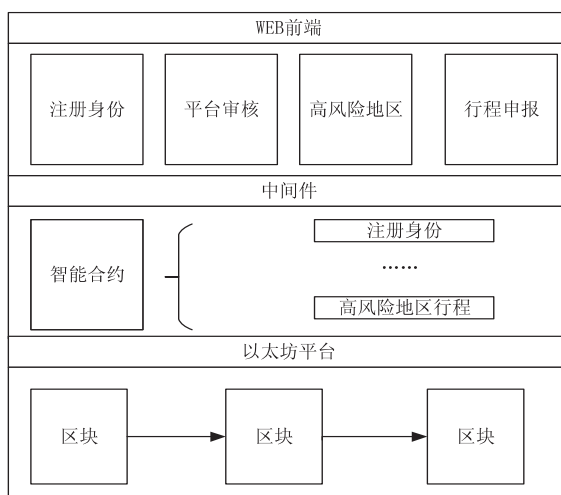


图4 系统架构

应用层 Web 模块使用 react 为前端框架。Web 模块为用户提供良好可视化的交互界面,提交多方请求,通过智能合约提供的接口将数据提交到区块链上。

中间模块由智能合约与 Web3 组成,用户与健康码平台的需求与业务逻辑均以智能合约的形式写入以

太坊节点中。智能合约规定了各方的执行操作和操作规范,所有的操作只能按照智能合约的内容执行。该文使用 Solidity 语言编写智能合约,实现健康码平台的各项功能。Web3 是实现智能合约具体操作的接口 API(application programming interface),通过 Web3 获取节点的状态、监听事件、调用合约等,实现智能合约和上层应用与以太坊的交互。

以太坊分布式交易账本为底层提供数据存储环境,支持并存储智能合约操作所产生的各个区块,使用 PoW(Proof of Work)共识协议来实现记账功能,每个节点会得到一个防篡改、真实的账本。

3 模块功能与合约设计

3.1 前端设计

Web 前端页面主要分为用户注册、用户信息查询、高风险地区判断、行程申报共四部分。Web 交互界面采用 Html、Css 和 Javascript 进行界面设计,使用 react 开发交互界面。通过 web3.js(与以太坊兼容的 JavaScript API)与以太坊节点连接,从而调用智能合约方法。通过 remix(以太坊官方推荐的网页编译器)来进行智能合约的编写与测试,利用 MetaMask 插件(以太坊钱包)与以太坊进行交互,生成的交易数据通过 MetaMask 钱包发送到以太坊网络,并通过 MetaMask 钱包支付 gas(以太坊中每步操作都会消耗一个固定的消耗值)手续费等支付操作。

3.2 合约属性设计

在业务层进行应用开发,首先需要对智能合约进行编写,健康码智能合约属性信息见表 1。用户结构体包含了身份证、姓名、联系方式、核酸检测等信息详情,见表 2。

表 1 健康码合约属性

字段	类型	属性信息
manage	address	平台地址
operator	address[]	工作人员
person	perinfo[]	存储用户信息的集合
high_risk	string	高风险地区

表 2 用户结构体属性

字段	类型	属性信息
uid	uint	健康码编号
identity	string	身份证号码
status	string	健康码状态
passed	bool	身份审核
name	string	姓名
phone	string	联系方式
trip	string[]	14 天行程
nucleic_acid	uint	核酸次数

3.3 合约功能实现

3.3.1 用户注册

用户注册是本系统主要功能之一,用户需要提交信息到系统,系统会对用户的隐私信息进行加密,加密算法使用 RSA 算法。系统收到用户提交的信息后,使用平台发布的公钥对用户隐私信息加密,之后将加密后的信息上传区块链,平台工作人员通过区块链获得用户加密信息,用平台私钥对加密部分进行解密,审核用户信息,确认没有问题则审核通过。用户注册的合约代码如下:

Algorithm 1: addper

```
(1) //生成公密钥
(2) key = NodeRsa( {b: 指定密钥长度} );
(3) //导出公钥
(4) pub = key.exportKey( 'public' );
(5) //导出私钥
(6) pri = key.exportKey( 'private' );
(7) myEncrypt = NodeRsa( platform_pubKey );
(8) //加密隐私信息
(9) Encrypt = myEncrypt( person_message, 'base64' );
(10) function ( person message ) {
(11)   perinfo memory pe = perinfo( {
(12)     identify : 经过公钥加密过的身份证,
(13)     status : 健康码状态,
(14)     .....
(15)     phone : 经过公钥加密的联系方式
(16)   } );
(17) person.push( pe );
```

3.3.2 判断是否为黄码

健康码分为绿码、黄码、红码,其中黄码的判定规则为过去 14 天去过高风险地区,并且没有做过核酸检测的人员。判断为黄码的人员变回绿码需要做两次核酸,若两次核酸都为阴性则转回绿码。高风险地区判断合约代码如下:

Algorithm 2: isYellow

```
(1) function ( ) onlymanage {
(2)   for( i=0; i<person.length; i++ ) {
(3)     for( j=0; j< 2 weeks; j++ ) {
(4)       //过去 14 天去过风险区则为 True, 反之为 Fales
(5)       flag = isEqual( 14 天行程, 高风险地区 );
(6)       //如果为真则修改健康码状态
(7)       if( flag ) {
(8)         status = 黄码;
(9)       }
(10)    }
(11)  }
(12) }
```


4 实验分析

4.1 方案可行性

实验在 window10 操作系统下设计实现,在构建的基于以太坊智能合约的健康码系统下构建以太坊开发环境,同时实现健康码功能,需要安装 Node.js, Truffle 框架, MeantMask 钱包, Ganache-cii 测试框架, web3.js, remix。使用 remix 来测试智能合约的功能,通过 Ganache 模拟以太坊的真实环境,最后部署到以太坊 rinkeby 网络上。

针对系统的用户注册、平台审核、黄码判断、信息展示等一系列重要功能做了测试。用户注册、平台审核等一系列会改变区块链数据的操作都会通过 MetaMask 钱包打包到以太坊节点中。信息展示操作不会对区块链数据产生修改的操作,只产生调用信息,无交易。

部分重要模块功能实验如图 5 所示,图 5 展示了用户注册时的操作。可以看到,用户上传的部分隐私信息将会以密文的形式显示。

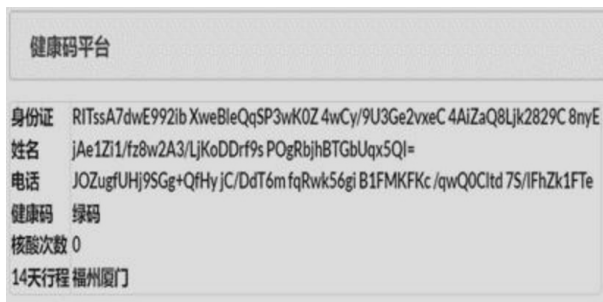


图 5 信息展示

以太坊中需要改变状况的操作都需要消耗 gas。gas price 是单个 gas 的价格,实际交易花费成本为 gas * gas price。在该系统中,智能合约部署在以太坊 rinkeby 网络中,部署合约的账户地址为 0xC2FC51c9eD99905bCBDBcB1d5fe296E6E5977510,智能合约的部署地址为 0x1eda70be3a1fd92dfa783c698c00fb5114fcd97d92890223e6da6dbd855ef。利用智能合约分析各函数消耗的花费。合约发起者发起 constructor 需要花费 0.004 383 7 ETH(以太币)。用户注册 addper 需要花费 0.000 806 78 ETH。工作人员对与确诊病例轨迹重合人员变更为黄码需要花费 0.000 120 57 ETH。工作人员对确诊病患或高风险人员设置红码需要花费 0.000 078 892 ETH。工作人员对病愈人员或核酸检测超过 2 次为阴性的人员变更为绿码需要 0.000 097 492 ETH。智能合约具体花费见表 3。表 3 证明了方案所消耗的成本是可接受的。

4.2 其他方案分析

与文献[15-18]所提出的方案进行对比,具体对比见表 4。文献[15-16]提出了一种健康码方案,但方

案仅实现了健康码的监控功能,并未保障健康码用户的隐私安全。文献[17-18]提出应对用户信息进行脱敏处理,但方案没有考虑中心化系统带来的危险,且未解决信息孤岛问题。文中方案利用区块链解决了中心化和数据孤岛问题且保证了数据可溯源,同时利用非对称加密保障了用户的隐私安全。通过与现有文献的比较,不难看出提出的基于区块链和非对称加密的健康码方案能够有效地保障在疫情下的人身安全,且能够有效保护用户隐私安全。

表 3 智能合约花费测试

函数	消耗的 gas	实际花费/ether
Constructor	1,753,498	0.004 383 7
addper	322,713	0.000 806 78
Sethighlevel	46,932	0.000 117 33
setpass	46,191	0.000 115 47
isyellow	48,231	0.000 120 57
isgreen	38,997	0.000 097 492
sethealth	36,357	0.000 078 892

表 4 相关方案功能比较

方案	数据溯源	去中心化	健康码	隐私保护
文献[15]	×	×	√	×
文献[16]	×	×	√	×
文献[17]	×	×	√	√
文献[18]	×	×	√	√
文中方案	√	√	√	√

5 结束语

区块链技术本质上就是分布式数据库,区块链上各个节点通过共识协议记账,它与传统数据库最大的区别就在于中心化和非中心化。方案根据区块链技术去中心化、不可篡改、信息可追溯等特点,研究设计了基于以太坊智能合约的健康码方案,该方案采用非对称加密,保证了用户隐私信息的安全性,同时利用区块链公开透明、不可篡改等特点,确保了信息的真实性。但该方案在具体实现过程中仍存在一定问题和挑战需要解决。如让电信、联通等运营商共享海量数据、共同维护方案的运行。解决上述问题,对方案进一步落地具有重要意义。对区块链技术在疫情健康码方面的应用提出了设计方案,希望能对当前健康码存在的痛点提出新的解决思路,也希望对接下来区块链的应用研究做一些启发和建议。

在后续工作中,还将继续完成健康码智能合约的逻辑需求,并将区块链和移动端开发相结合,进一步实现健康码方案的可靠性与多适用性。

参考文献:

- [1] 史晨,马亮. 协同治理、技术创新与智慧防疫——基于“健康码”的案例研究[J]. 党政研究, 2020(4): 107-116.
- [2] 单勇. 健康码应用的正当性及其完善[J]. 中国行政管理, 2021(5): 53-60.
- [3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008) [2022-11-23]. <http://www.bitcoin.org/bitcoin.pdf>.
- [4] 邵奇峰,张召,金澈清,等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
- [5] BUTERIN V. A next-generation smart contract and decentralized application platform[EB/OL]. (2014) [2022-11-23]. <https://ethereum.org/en/>.
- [6] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9): 548.
- [7] 贺海武,延安,陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.
- [8] 王煜,朱明,夏演. 非对称加密算法在身份认证中的应用研究[J]. 计算机技术与发展, 2020, 30(1): 94-98.
- [9] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management[C]//Proceedings of the 2nd international conference on open and big data. Vienna: IEEE, 2016: 25-30.
- [10] 谭文安,王慧. 基于智能合约的可信筹款捐助方案与平台[J]. 计算机应用, 2020, 40(5): 1483-1487.
- [11] PIERONI A, SCARPATO N, DI NUNZIO L, et al. Smarter city: smart energy grid based on blockchain technology[J]. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8(1): 298-306.
- [12] 朱建明,张沁楠,高胜,等. 基于区块链的隐私保护可信联邦学习模型[J]. 计算机学报, 2021, 44(12): 2464-2484.
- [13] PORRU S, PINNA A, MARCHESI M, et al. Blockchain oriented software engineering: challenges and new directions[C]//Proceedings of the IEEE/ACM 39th international conference on software engineering companion. Buenos Aires: IEEE, 2017: 169-171.
- [14] 胡剑,朱鹏,戚湧. 基于区块链的重大公共卫生事件下应急情报体系构建[J]. 情报理论与实践, 2022, 45(5): 156-164.
- [15] 徐秀芳,许森,夏旻,等. 基于 Django 的校园疫情防控系统设计与实现[J]. 软件导刊, 2021, 20(2): 24-30.
- [16] 李佳莹,刘汪根. 健康码系统架构设计与实现[J]. 信息技术与标准化, 2020(11): 71-75.
- [17] 唐林焱. 常态化数字抗疫时代的个人信息保护[J]. 中国政法大学学报, 2021(4): 240-250.
- [18] 付少雄,赵安琪. 健康 APP 用户隐私保护政策调查分析——以《信息安全技术 个人信息安全规范》为框架[J]. 图书馆论坛, 2019, 39(12): 109-118.
- [19] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]//Proceedings of the 2015 IEEE symposium on security and privacy workshops. San Jose: IEEE, 2015: 180-184.
- [20] 付利青,田海博. 基于智能合约的以太坊投票协议[J]. 软件学报, 2021, 30(11): 3486-3502.
- [21] CHEN Y, DING S, XU Z, et al. Blockchain-based medical records secure storage and medical service framework[J]. Journal of Medical Systems, 2019, 43(1): 1-9.