

# 基于区块链的反诈骗系统框架设计与分析

张亚伟, 霍敏霞, 贾全秋, 薛富城

泰山科技学院, 山东 泰安

收稿日期: 2022年8月15日; 录用日期: 2022年9月13日; 发布日期: 2022年9月21日

## 摘要

预防电信诈骗是当下社会比较火热的一个话题。基于区块链的防诈骗(Anti-Fraud)系统能够弥补传统反诈骗系统的不足, 比如证难取、损难止以及不信任等。区块链作为颠覆性的新一代信息技术, 因其具有去中心、去信任、防篡改以及历史数据可追溯等特点, 对预防电信诈骗起到很好的辅助作用。本文通过分析分布式数据库、共识机制、密码学、激励机制以及智能合约等区块链的核心技术, 进而设计了基于区块链的反诈骗系统框架, 并从数据上链、身份认证以及合约控制等三个方面出发逐一对该系统功能进行介绍, 以期未来能够实现该系统, 从而保障用户的财产安全, 同时为相关部门提供借鉴。

## 关键词

区块链, 电信诈骗, 智能合约, 可追溯, 去信任

# Design and Analysis of Anti-Fraud System Framework Based on Blockchain

Yawei Zhang, Minxia Huo, Quanqiu Jia, Fucheng Xue

Taishan Institute of Science and Technology, Taian Shandong

Received: Aug. 15<sup>th</sup>, 2022; accepted: Sep. 13<sup>th</sup>, 2022; published: Sep. 21<sup>st</sup>, 2022

## Abstract

Telecom fraud prevention is a hot topic in today's society. The anti-fraud system based on blockchain can make up for the shortcomings of traditional anti-fraud systems, such as difficult to obtain evidence, difficult to prevent damage and distrust. As a disruptive new generation of information technology, blockchain has the characteristics of decentralization, trustlessness, anti-tampering and traceability of historical data, which plays a good auxiliary role in preventing telecommunication fraud. By analyzing the core technologies of blockchain such as distributed database, consensus mechanism, cryptography, incentive mechanism and smart contract, this paper designs an an-

ti-fraud system framework based on blockchain, and analyzes data on the chain, identity authentication and contract control. Starting from three aspects, this paper will introduce the functions of the system one by one, in order to realize the system in the future, so as to ensure the safety of users' property and provide reference for relevant departments.

## Keywords

Blockchain, Telecom Fraud, Smart Contracts, Traceability, Trustless

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

自互联网技术诞生以来,人们享受到便利的同时也面临着诸多风险,这其中就包括社会危害性极强的电信诈骗。电信诈骗会给人们的生活造成很大的影响,甚至很多家庭因此而家破人亡。如何有效预防电信诈骗已成为人们日常经常议论的话题,尽管国家采取了很多措施,比如鼓励人们在移动通信设备上安装防诈骗 APP、挂条幅宣传以及加强对实施诈骗人员的惩罚力度等,但仍然无法有效控制类似事件的发生,究其根本原因,还是因为没有形成一套行之有效的及时止损机制,将电信诈骗被扼杀在萌芽之中。

区块链作为一种分布式数据账本,俨然已成为去中心化、去信任化、集体共同参与维护、防篡改以及合约代码自动执行的象征。与传统用于传播信息的互联网不同,区块链网络中所传播的则是价值,虽然只有一词之差,却是区块链作为新一代信息技术最为明显的特征。区块链的五大核心技术之一智能合约更是使打造形式多样的去中心化应用程序(DAPP)成为可能。

将区块链技术与预防电信诈骗进行结合,打造基于区块链的预防电信诈骗系统,有利于从根本上解决取证难、止损难以及不信任等问题,从而有效改善当前电信诈骗难防的局面,最大程度减少受害者的损失。

本文设计了一种基于区块链的反诈骗系统,该系统主要实现数据上链、身份认证以及合约控制等功能,通过区块链记录用户交易数据,各参与节点对同步的交易数据进行验证,以确保交易数据的有效性。合约起到控制交易的作用,一旦交易被确认存在风险,就会触发可执行代码,使交易立即冻结。

本文剩余内容组织如下:在第 2 章会给出技术解析以及融合现状;然后第 3 章详细介绍基于区块链的反诈骗系统框架;紧接着在第 4 章对所设计的系统框架进行分析;最后是对所做工作进行总结。

## 2. 相关技术解析与融合现状

### 2.1. 区块链

区块链诞生于 2009 年,是比特币、以太坊、柚子币等数字加密货币的底层核心技术,该技术突破了传统互联网技术的桎梏,旨在打造去中心化应用程序,终极目标是实现去中心化社会。广义上讲,区块链是指利用分布式数据库进行存储,利用共识算法进行有效性验证,利用密码学进行加密、解密、Hash 化处理以及身份校验,利用激励机制维护网络运行,利用智能合约自动执行预先定义好的程序的分布式记账技术。广义上讲,区块链实则是一种特殊的数据库。

图 1 展示了区块链最为经典的数据结构，区块链中的每一个块与块之间通过 Hash 链接在一起，共同构成链式结构，每个区块都有自己的编号。区块头(head)包含当前区块链 Hash、前一区块 Hash、Timestamp (时间戳)、Nonce (随机数)等关键信息；区块体(body)用于存储交易数据，这些交易数据会通过 Hash 计算得到默克尔树根(Merkle Root)，即当前区块链的 Hash，因而即使数据发生细微的变化，也会导致得到的 Hash 不同，起到很好的防篡改作用。

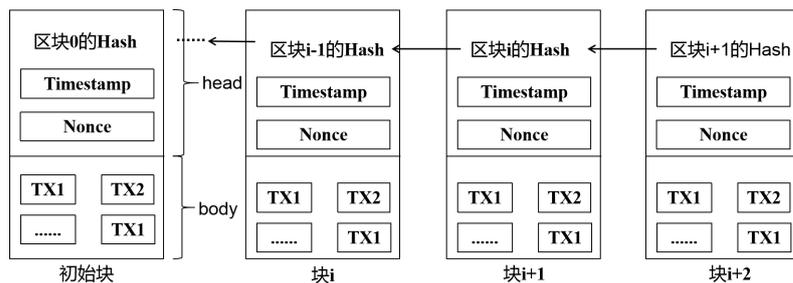


Figure 1. Blockchain data structure

图 1. 区块链的数据结构

## 2.2. 智能合约

智能合约(Smart Contract)这一概念由美国著名密码学家尼克·萨博 Nick Szabo 于 1993 年首次提出，以太坊创始人 Vitalik Buterin 将其应用到区块链，开启了可编程区块链的新纪元。我们可以将智能合约理解为运行在区块链账本上的一段程序，该程序一旦满足预先设定好的触发条件，就会不受人为控制地自动执行，这和区块链去中心化的理念十分契合。图 2 展示了智能合约模型，所有节点都可以在区块链账本上部署并执行不同用途的智能合约，并将执行结果作用于区块链数据。此外，不同区块链开发平台智能合约的运行环境不同，以太坊智能合约的运行环境为 EVM (以太坊虚拟机)，而 Fabric 链码(智能合约在 Fabric 中的另外一种叫法)的运行环境为 docker (容器)。总之，智能合约在区块链的大面积应用和推广过程中扮演着十分重要的角色，弥补了比特币等加密数字货币只能用于转账交易的缺陷，开启了区块链 2.0 新时代。

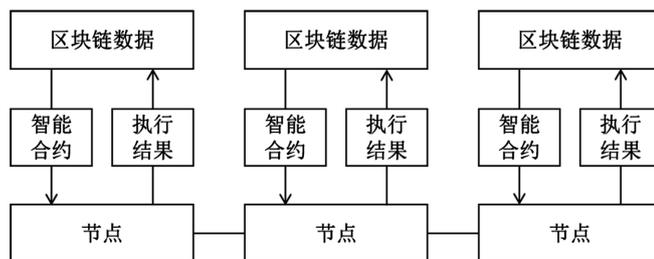


Figure 2. Smart contract model

图 2. 智能合约模型

## 2.3. 电信诈骗

所谓电信诈骗，一般情况下是指利用通讯工具远程对受害人实施的非接触式的、制造虚假信息的、以骗取钱财为目的的非法行为。随着国家加大对实施电信诈骗人员的处罚力度，并通过下载反诈骗 APP 等多种方式进行预防，但仍然会有很多人上当受骗，甚至导致家破人亡的严重后果。究其原因，首先归

鉴于受害者的联系方式、家庭住址等私密信息已被泄露，从而被不法分子利用；此外传统防诈骗系统并未发挥应有的作用，不能在第一时间进行干预止损，再加上诈骗人员往往都以虚构的身份、地址进行伪装，因而警方很难破案。

## 2.4. 融合现状

区块链的出现为反诈骗带来了曙光，一些学者开始对这两者的结合进行了理论研究[1]。赵东明等人通过联盟链构建了一套完整的、服务于的电信运营商、公安以及银行的反诈骗识别系统，该系统致力于打造多方合作的可信网络，解决单点欺诈和过度依赖中心的问题[2]。金鑫以区块链的应用为视角，研究了当前预防电信诈骗所面临的困难和突破，认为在实际打击电信诈骗的时候，由于存在信息不对称等问题，会使取证、抓捕、追赃遇到阻碍，而区块链作为一种分布式共享账本，可通过自身技术优势弥补以上缺陷[3]。刘宗妹研究了利用区块链技术实现电信诈骗的协同治理，从而保障电信数据的安全，不给不法分子可乘之机[4]。郭燕飞等人研究了基于区块链的电信诈骗号码标记库共享的方法，认为传统电信诈骗号码标记库会出现数据孤岛、标记不全、被修改以及错标等问题，利用区块链去中心化、多点参与、不可篡改等特点可以很好地解决这一问题。

通过对上述区块链与预防电信诈骗的融合现状进行分析，会发现相关研究还很少，而已发表见刊的文献大都偏向于基础的理论研究，并未深入从技术本身出发对涉及到的相关技术进行解析，也未对两者融合的底层逻辑和系统架构进行设计。鉴于此，本文设计了基于区块链的防诈骗系统框架，在弥补上述文献缺陷的同时，更进一步为实现相关应用的落地提供借鉴。

## 3. 基于区块链的反诈骗系统框架设计

### 3.1. 系统底层架构设计

本系统底层架构设计如图3所示，共包含有5层，舍弃了激励层，这是因为所选区块链框架为联盟链，参与者都是利益相关方，因而不需要对打包交易的节点进行奖励。首先第一层为数据层，该层主要由电信数据、Merkle根、随机数等组成，是以上其他层次正常运转的基础。第二层为网络层，包括P2P(Point To Point)网络通信、数据传输以及数据验证，该层主要用于维持节点与节点之间的通信。第三层为共识层，该层主要用于使区块链网络上的节点在高度分散的情况下能够快速对区块数据的有效性达成共识，本系统设计选择使用PBFT(实用拜占庭容错算法)这一共识机制，其工作原理如下：由链上节点进行投票，一旦反对票数低于 $(N - 1)/3$ ，那么这个被投票的节点就可公示信息[5]。第4层为合约层，该层封装了智能合约，为系统数据提供逻辑上的控制。最后一层是应用层，包含一些实际的应用，比如数据上链、身份认证以及合约控制等。

### 3.2. 系统总体架构设计

本系统总体架构如图4所示，用户登录系统前端，如果收到疑似诈骗信息，电信公司会将其与诈骗信息标记库中的诈骗信息进行比对，如果比如成功，便可证实为诈骗信息，然后将其进行上链处理。共识联盟节点中的主节点负责打包数据上链，这一过程需要通过智能合约来完成，调用Write方法将诈骗信息写进区块链中。备份节点(公安机关、银行)负责同步诈骗信息，以便于公安机关快速取证、破案，而银行也会将与诈骗信息相关的银行账户进行冻结，从而及时挽救受害人的损失，整个过程都由部署到区块链的智能合约自动执行，可确保关键证据在无人为因素干预的情况下自动获取，一旦银行账户面临被欺诈的风险，智能合约会立即被触发，快速将该账户进行锁定[6]。



Figure 3. System underlying architecture  
图 3. 系统底层架构

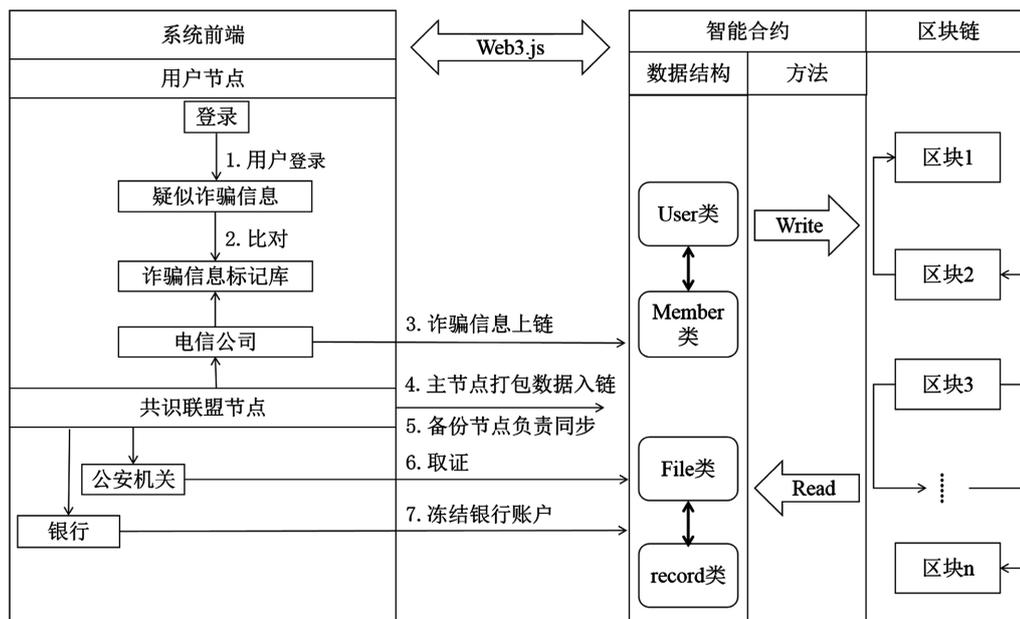


Figure 4. Overall system architecture  
图 4. 系统总体架构

### 3.3. 诈骗信息上链

诈骗信息上链是本系统设计的主要功能，旨在利用区块链的不可篡改、历史数据可追溯等特性保障数据的有效性和完整性。用户在使用通信设备的过程中只要接收到不明电话、短信以及链接等，系统都会在第一时间进行响应、跟踪以及防范。这些陌生信息一旦被确认为诈骗信息，联盟共识节点就会加以应对，最后做上链处理，以供相关节点读(Read)出数据进行比对，或用作证据保全，提高公安机关办案效率[7]。图 5 展示了诈骗信息上链的整个过程：首先，系统会通过调用已编译、部署好的智能合约将诈骗信息存储在区块链中；然后，新生成的区块会同步到联盟节点中，以便于后续对历史数据进行追溯[8]。

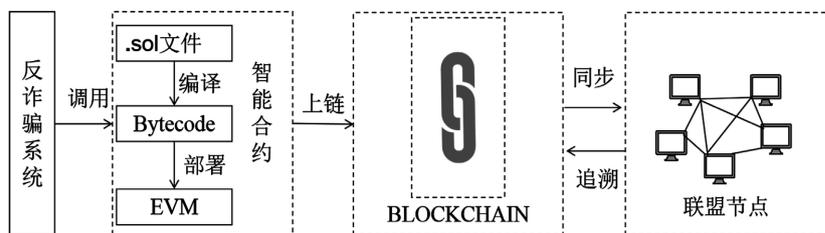


Figure 5. Fraud information on the chain  
图 5. 诈骗信息上链

### 3.4. 合约控制

本系统所选用的区块链为联盟链，各节点都是利益共同体[9]。为了达到各自的目的，各联盟节点通常会在区块链上部署具有专门功能的智能合约，满足一定条件即可触发，并返回执行结果[10]。图 6 展示了系统合约控制逻辑公安机关通过智能合约自动生成证据，从而弥补现实中诈骗案难破的局面；电信公司负责把经过确认的诈骗信息存储到区块链中，以供其他节点查询使用；银行作为金融机构，有责任对异常账户进行冻结，防止受害者在无任何干预的情况下贸然把欠款汇入从事非法活动的账户，从而造成无法挽回的损失，在这种情况下，区块链上的智能合约会自动冻结风险账户，从而保障该账户的资金安全[11]。

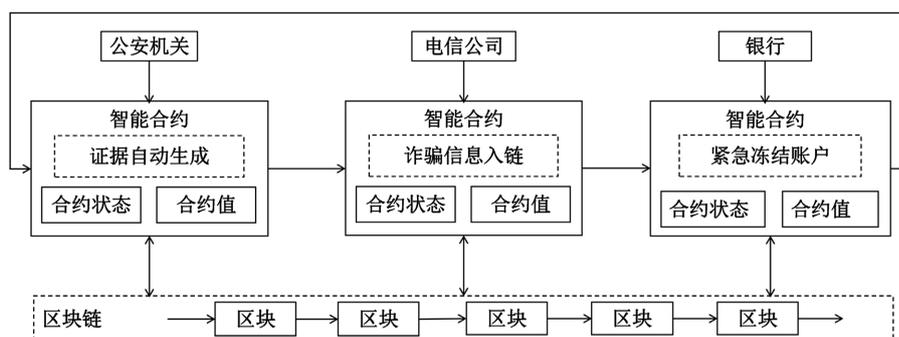


Figure 6. Contract control logic  
图 6. 合约控制逻辑

## 4. 基于区块链的反诈骗系统分析

传统反诈骗系统存在效率低下、证据难以获取、信息不对称等问题，如果在系统中融入区块链这一技术可谓是一种创新，基于区块链的反诈骗系统充分利用区块链去中心化、防篡改、代码自动执行以及历史数据可追溯等特征，及时有效地记录诈骗信息，并通过共识机制验证数据的有效性，进而同步新生成的区块数据到每个节点。此外，区块链网络中的每个节点都可以往区块链中部署专属智能合约，从而使其自动执行并反馈相应的结果。此外，选择使用 Fabric 这一联盟链进行开发，相较于公链和私链这两种框架，它并不需要使用 Token，这就省却了为了挖矿而浪费的大量资源，同时也有利于系统的维护与扩展[12]。

## 5. 总结

鉴于电信诈骗在当下非常普遍，且社会影响极大，本文设计了基于区块链的反诈骗系统框架，该框架底层选用五层架构，由联盟节点共同维护。用户一旦收到电信诈骗信息，系统会快速做出反应，并通

过链上已部署的合约自动将电信诈骗信息上链，并同步至其他节点，完成账户冻结、证据生成等操作，从而最大程度降低电信诈骗所带来的风险。

## 基金项目

“大思政”育人格局下计算机专业教育与思政教育融合教学研究——以《计算机科学导论》嵌入思政教育为例一般项目(NO. YTJG202048)。

## 参考文献

- [1] 赵东明, 刘静, 张淑英, 张建涛. 基于区块链的电信运营商跨行业数据融合反诈识别系统[J]. 通信世界, 2022(14): 40-43.
- [2] 金鑫. 打击电信诈骗犯罪的困局和突破[D]: [硕士学位论文]. 北京: 中国人民公安大学, 2021.
- [3] 刘宗妹. 区块链助力电信网络反欺诈协同治理[J]. 信息通信技术与政策, 2021, 47(3): 61-65.
- [4] 周艳娥, 何林娜, 陈军. 基于区块链技术的事业单位内部控制建设研究[J]. 会计之友, 2022(14): 154-158.
- [5] 金义富. 区块链 + 教育的需求分析与技术框架[J]. 中国电化教育, 2017(9): 62-68.
- [6] 何泾沙, 张琨, 薛瑞昕, 等. 基于贡献值和难度值的高可靠性区块链共识机制[J]. 计算机学报, 2021, 44(1): 162-176.
- [7] 王蓓蓓, 王骐鑫, 李雅超, 等. 区块链环境下考虑信用的需求响应资源交易机制[J]. 电力系统自动化, 2021, 45(5): 30-38.
- [8] 徐晨阳, 陈艳娇, 王会金. 区块链赋能下多元化发展对企业风险承担水平的影响——基于数字经济时代视角[J]. 中国软科学, 2022(1): 121-31.
- [9] Floersch, C.A. (2022) System and Method for Providing an Automated Trade Transaction Using Blockchain Technology. *Energies*.
- [10] Alrebdi, N., Alabdulatif, A., Iwendi, C., et al. (2022) SVBE: Searchable and Verifiable Blockchain-Based Electronic Medical Records System. *Scientific Reports*, **12**, Article No. 266. <https://doi.org/10.1038/s41598-021-04124-8>
- [11] 郑荣, 张薇, 高志豪. 基于区块链技术的政府数据开放共享平台构建与运行机制研究[J]. 情报科学, 2022, 40(5): 137-143.
- [12] Mark, G., Rhonda, B.L., Tuttle-Newhall, J.E., et al. (2022) Blockchain and Population Health. *Journal of Public Health*, **17**, 2-12.