基于区块链技术的合同防伪

兴业银行股份有限公司西宁分行课题组

摘　要：近年来，由于“比特币”、“以太坊”、“超级账本”等区块链产品的火爆发展，区块链技术得到越来越多的关注。由于其去中心化、不可被篡改、信息安全可靠等特性，非常适合应用于安全需求很高的金融行业。

本文通过对区块链理论和技术进行研究，剖析兴业银行区块链防伪平台，结合兴业银行西宁分行合同管理的需要，探索建设基于区块链防伪平台的合同管理系统，从而对区块链技术的认知由理论到应用层级，为以后更多的区块链技术应用打好基础。

关键词：区块链　防伪平台　智能合约　合同管理

【中图分类号】F830.49　　【文献标识码】A　　【文章编号】1007-841X-2018(3)-0055-06

一、区块链技术概述

（一）区块链技术来源

2008年学者中本聪发表了《比特币：一种点对点的电子现金系统》白皮书，成了区块链技术的理论来源；2009年其在芬兰赫尔辛基的服务器上挖出比特币第一个区块，区块链原型诞生，到2014年比特币爆发式增长，引起了广泛的关注；2015年科技界总结比特币底层去中心化、不可篡改、无法作弊、即时交易等优点后形成了区块链概念；同年，以R3联盟、俄罗斯区块链联盟为代表的各类区块链技术研究组织相继成立。同时全球银行业也开始积极布局：加入联盟制订标准，与区块链公司合作，内部推进研究，如星展与渣打银行联手开发供应链金融业务数字化应用，全球重要经济体对区块链技术的重视程度逐步提高。

2016年，中国人民银行明确央行发行数字货币的战略目标，认可区块链技术。同时，中国相关区块链联盟组织相继成立，微众银行、蚂蚁金服相关区块链产品相继推出和上线，区块链技术在我国也逐步发展了起来。

区块链技术从原型诞生，到研究组织成立，再到商业试用行和正式应用，由于安全可靠、公开透明的特性，使其发展迅速，目前得到了广泛的共识和应用。

（二）区块链的特性

1. 分布式、去中心

所有参与方都是异地多活节点，权限对等，无中心化的特权节点，每一个全节点都维护了一个完整的数据副本，数据通过共识算法保持一致。跟传统技术相比较，区块链是无法被摧毁的。

2. 公开透明，无法作弊

所有的参与方都维护了相同的完整账本，确保账本的记录过程是公开透明的；除非控制系统网络中大多数节点，否则系统会根据多数人的结果得到真实结果，因此作弊修改自

已的账本完全没有意义。

3. 记录不可篡改

每一笔合法交易都被记录到一个区块被大家确认，后续生成的新区块都是基于前一个区块的基础之上生成的，因此，篡改任何一笔历史交易都会推翻此后的所有区块，这几乎是无法实现的，即使实现，其代价也远超收益。

4. 信息安全

所有参与者都能接到交易，但交易内容是经过密码学加密的；只有交易的参与者才能查看交易明文。

5. 发生即清算

“清算”这个概念在区块链网络中将不复存在，所有的交易都是“发生即清算”的，交易完成的瞬间所有的账本信息都完成了同步更新。

（三）区块链应用领域

1. 数字货币

当前全球数字加密货币超过 300 种，而这些大都是在区块链技术基础上的。比较出名的是比特币、以太币、瑞波币等。排名第一的比特币目前市值超过 100 亿美元，可见区块链技术的潜在市场价值非常大。

2. 公正审计

区块链数据带有时间戳、由共识节点共同验证和记录、不可篡改和伪造，这些特点使得区块链可广泛应用于各类数据公证和审计场景。例如区块链可以永久地安全存储由政府机构核发的各类许可证、登记表、执照、证明、认证和记录等，并可在任意时间点方便地证明某项数据的存在性和一定程度上的真实性。本文研究的合同管理系统就是基于区块链的此特性来建设和实施的。

3. 数据存储

区块链的高冗余存储（每个节点存储一份数据）、去中心化、高安全性和隐私保护等特点使其特别适合存储和保护重要隐私数据，以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露。目前，利用区块链来存储个人健康数据（如电子病历、基因数据等）是极具前景的应用领域。

4. 金融交易

区块链技术与金融市场应用有非常高的契合度。区块链可以在去中心化系统中自发地产生信用，能够建立无中心机构信用背书的金融市场，从而在很大程度上实现了金融脱媒，这对第三方支付、资金托管等存在中介机构的商业模式来说是颠覆性的变革；在互联网金融领域，区块链特别适合或者已经应用于股权众筹、P2P 网络借贷和互联网保险等商业模式；证券和银行业务也是区块链的重要应用领域，传统证券交易需要经过中央结算机构、银行、证券公司和交易所等中心机构的多重协调，而利用区块链自动化智能合约和可编程的特点，能够极大地降低成本和提高效率，避免繁琐的中心化清算交割过程，实现方便快捷的金融产品交易。

二、区块链防伪平台

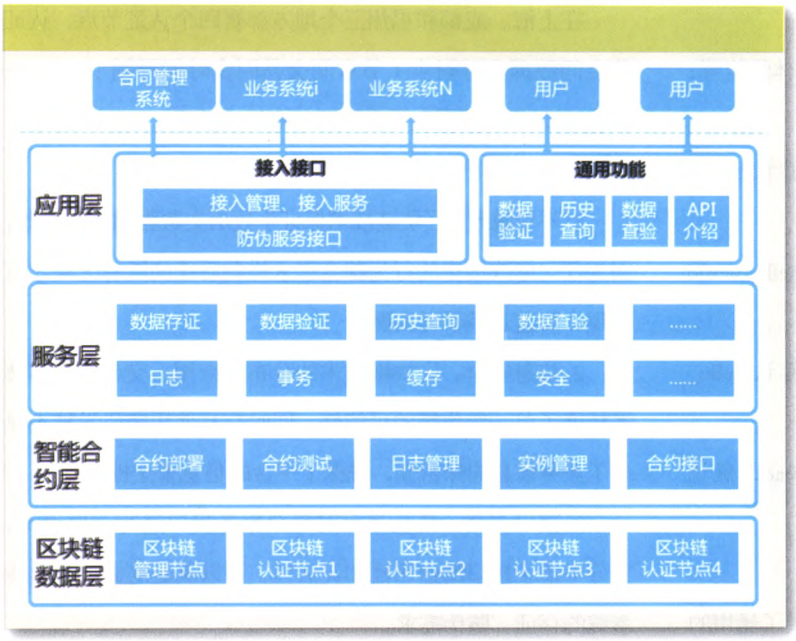
区块链技术发展迅速，获得了国内外金融同业的积极关注和尝试。该技术也受到兴业银行总行高度重视，兴业银行信息科技部区块链技术研究小组于 2016 年初成立，研究小组积极探索比特币原理、共识算法等核心技术理论，深入研究 Hyper Ledger Fabric、以太坊、Sawtooth-lake、Openchain 等主流开源产品，挖掘银行承兑汇票、汽车金融、积分抽奖平台、银行存证防伪等 8 个银行应用场景。

综合考虑外部应用案例和本行实际需求，研究小组提出建设区块链防伪平台满足行内快速、安全、便捷的存证与防伪需求。

（一）平台架构和功能

兴业银行区块链防伪平台基于 Hyperledger Fabric 开源区块链框架自主研发，实现一个高级别的通用防伪、存证平台，服务于行内所有具有防伪、存证需求的业务系统，快速提升防伪能力，节省防伪需求的研发成本。

根据功能，平台分为应用层、服务层、智能合约层和区块链数据层等四个逻辑层，应用层主要实现外部系统和用户的接入；服务层为接入系统提供数据存证、历史查询、数据查验等服务；智能合约层包括合约管理、测试和部署等，为各认证节点提供相关合约服务；区块链数据层实现了数据的管理和存储。



1. 智能合约的解释

“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”

承诺指的是合约参与方同意的（经常是相互的）权利和义务。这些承诺定义了合约的本质和目的。以一个销售合约为典型例子。卖家承诺发送货物，买家承诺支付合理的货款。

数字形式意味着合约必须写入计算机可读的代码中。因为只要参与方达成协定，智能合约建立的权利和义务，是由一台计算机或者计算机网络执行的。

通俗的理解，智能合约为一段代码，被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。可以这样简单的概括：它是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值。

2. 区块链层

具体数据存放于区块链，区块由区块头和区块体组成，区块头包含了上一区块和本区块的 hash 签名值，区块体包含了交易的具体信息，区块链则是由无数区块形成的链。我们可以将区块链形象地理解为一本书，区块链的区块对应于书本的一页纸。页眉的标题对应于区块的区块头，描述了区块的整体信息；纸的具体内容对应于区块的区块体，描述了区块的具体交易信息；而页码对应于区块的数字签名，说明了区块在区块链中的相对位置。

（1）区块链的形式

书本通过页码将描述具体内容的页面串联起来，达到有意义的描述事物的意图。区块链使用了相同的思想：不同的区块内包含了不同的交易信息，将这些区块通过数字签名连接起来，完整描述了随着时间以来的交易记录。区块链的本质是一串有序的、有具体意义的、可追溯的交易数据的集合。

（2）区块链数据交换方式

传统的应用大部分是基于客户端 / 服务器（Client/Server）的模式进行设计的。服务器存储所有必要的数据，客户端通过网络从服务器上存取所需数据。但是区块链技术不采用这样的模式，区块链是基于对等网络来实现数据交换的。

在对等网络中，没有中心节点，每个节点都可以充当服务器和客户端，区块链中所需要的数据部分或者全部存储到对等网络的各个节点，整个网络包含完整区块链的多个副本，达到了高度的数据冗余性，那么相对于传统的中心化 C/S 模式，就不太需要考虑数据损坏或者丢失带来的潜在风险。

（二）实现原理

以下实例通过一个简单的数据修改程序，能直观地体现区块链的编程流程，实现了一个区块链防伪平台的开发实例。

实例主要实现的功能：初始化，以键值形式存放信息，允许读取和修改键值；代码中，首先初始化了 hello_world 的值，并根据请求中的参数创建修改查询链上 key 中的值，本质上实现了一个简单的可修改的键值数据库。

主要函数：

deploy：该方法实现链码的部署；

read：读取 key args[0] 的 value；

write：创建或修改 key args[0] 的 value；

init：初始化 key hello_world 的 value；

invoke：根据传递参数类型调用执行相应的 init 和 write 函数；

query：调用 read 函数查询 args[0] 的 value。

1. 用 jim 用户登录模拟环境中的一个节点；

2. 用户 jim 调用方法 deploy，将链码部署到具体的位置；初始化 hello_world 的值为“8989898989”

3. 用户 jim 调用方法 query 的函数 read，确认 hello_world 的值为“8989898989”；

4. 用户 jim 调用方法 invoke 的函数 write，将 hello_world 的值修改为“9999999999”；

5. 用户 jim 调用方法 query 的函数 read，确认 hello_world 的值为“9999999999”；

6. 用户 diego 登录，调用方法 query 的函数 read，确认 hello_world 的值已经修改为“9999999999”。

（三）平台功能

作为通用防伪平台，区块链防伪平台目前提供了通用的数据防伪存证、数据验证、数据查询、数据查验、文件查验等功能模块以及平台防伪服务相关 API。

1. 数据存证是指接入系统通过调用数据存证 API 将业务系统需求防伪、防篡改的关键数据保存到区块链防伪平台作为以后核对查验的证据。数据存证 API 是数据提交接口，只有经过认证合法的接入 ID 才可以调用此接口。

2. 业务人员可以通过上传数据文件的方式快速验证数据真伪，便于业务人员审核业务数据。支持主流的数据文件，包括：Word/Excel/PPT/TXT/PDF 等格式。

3. 数据历史查询功能支持业务人员以数据的业务唯一编号为查询条件，查询对应数据当前在区块链防伪平台记录的处理流程结果，而不直接验证数据。适用于跟踪业务实际处理进度、审核业务流程合规性等场景。

4. 数据查验功能同时实现了数据防伪的验证和处理流程结果查询的功能，第一步先验证上传数据是否存在于区块链平台中，验证通过后再查询对应业务的处理流程结果。

5. 为了便于各类具有防伪需求的业务系统可以快速便捷地投入区块链防伪平台，平台提供了防伪服务 API。包括数据的上传、保持、验证、查询、修改等一系列 API，通用防伪服务 API 具有简单、灵活、适用性广、防伪与篡改能力强等优点，业务系统调用 API 可以快速提升系统防伪能力。

（四）平台部署及特点

在上海、成都和福州三个地方部署四个认证节点，认证节点间数据实时同步（节点间交易同步时间开销：0.08ms-0.17ms），任何数据变更需要四节点达成共识。

平台有以下几个特点：

1. 不可篡改，区块链技术保证生效历史数据的无法篡改，因为任何篡改历史的行为都会需求推翻后续的所有区块才可实现，而这几乎不可实现。

2. 信息安全，区块链技术的分布式应用、交易透明等技术杜绝了单一统作弊的可能性，同时交易使用密码学技术保证了业务信息的保密性，确保了平台的信息安全性。

3. 接口灵活，防伪平台对每个服务接口进行全面设计，充分考虑了接口的通用性和灵活性，可以满足绝大部分业务系统的存证、防伪需求。

4. 快速接入，为了便于各类具有防伪需求的业务系统可以快速便捷地投入区块链防伪平台，平台对接口进行了优化，业务系统只需简单几步就可以快速接入。

三、基于区块链防伪技术的合同管理系统

（一）分行合同管理系统介绍

为掌握合同管理的全部技术，方便系统升级和运维管理，合同管理系统使用兴业银行自主知识产权的 cap4j 开发平台自主开发，系统建成后满足分行日常的制式合同和非制式合同的管理需要。合同管理系统复用 cap4j 平台的用户和权限管理，采用类似在线 word 编辑功能，根据上传的合同模板，用户根据需要可以随意填写留空处，从而生成带有水印的合同文件；合同文件生产的验证码保存至区块链中，在之后的所有合同审批流程中，都将打开的合同文件的验证码与区块链中的数据进行验证，确保每一步审核的合同文件都未被篡改；同时增加电子印章功能，在合同最终审核通过后，用印人员加盖电子印章，合同即可打印生效。

（二）系统功能介绍

合同管理系统主要包括：合同模板维护、合同新建录入、合同预览、合同审核、电子印章管理和合同打印等功能模块。

合同模板维护功能：应用类似在线 word 编辑功能的技

术，将合同模板 word 文档导入到系统中，该 word 文档中将用户可编辑部分的内容使用下划线进行留空。用户根据需要导入不同的各种种类的合同模板文档。

合同的新建和录入功能：用户选择当次合同需要的模板，新建相应的合同，再根据当次合同的实际内容，填写新建合同中的下划线留空处，保存新建的合同文档。

合同预览功能：用户可以根据不同的权限，查看和预览自己权限的相关合同。

合同审核：根据合同审核流程，合同审核人员查看合同内容，填写审核内容，提交下一处理人。

电子印章管理：将分行所有用于合同签章的印章都纳入到电子印章管理范畴中，用户可进行电子印章的添加、删除等操作。

合同打印功能：合同审核的所有流程处理完成后，有权限用户给合同加盖电子印章，选择打印按钮进行合同打印，合同打印支持在线打印。

（三）系统特点

1. 规范合同版本，对制式合同进行统一版本管理，规范业务人员使用的制式合同版本。

2. 提高合同管理效率，经办人员可以在线填写、审批、打印合同，同一合同无需多次往返至分行审核机构进行审批；审核人员可以直接在线进行合同查看、审批。

（四）合同管理系统与区块链防伪平台对接

针对系统数据库保存防伪码关键信息存在可能被恶意删除、修改、覆盖等问题，项目组将合同管理系统接入了区块链防伪平台，将合同管理系统的合同防伪关键信息保存至防伪平台，大幅提升系统防伪安全级别。

1. 每步操作合同文件都使用加密算法生成与文件对应的防伪码。

2. 合同的防伪码保存到区块链当中，根据部署的链码，区块链的各个节点执行数据保存步骤。

3. 所有的操作过程（新建、审批）都被记录到区块链当中，各个节点的相关记录都有链码来完成。

4. 审批合同之前会自动与区块链平台进去验证，确保每一步审批的内容都是未被篡改的。

（五）合同防伪主要处理步骤

1. 新建合同。包括合同信息填写、附件上传、合同编辑、合同保存、提交审核和保存区块链等步骤，用户可以重复合同内容编辑和保存操作，保证合同填写的准确性，在合同提交审核步骤过程中，系统自动计算得到的防伪码，通过调用区块链防伪平台接口，创建合同对应的区块链，并将防伪码保存至区块链的第一个数据区块中，区块链防伪平台的其他各认证节点，按照部署的协议执行链码（chaincode 链上代码）完成数据的同步。

2. 合同审核。审核人员打开合同，系统计算相应的文档防伪码并与存在于区块链中的防伪码进行验证。验证通过后，审核人员对合同进行审核、填写审核意见，进而提交下一审核人进行处理。如果验证不通过，系统将提示不通过。此过程中系统自动计算文档的防伪码，调用区块链防伪平台接口将防伪码保存至上一步合同创建时建立的区块链中，并与上一区块的数据进行验证，区块链防伪平台的各认证节点，按照部署的协议执行链码完成数据的同步，在合同审核完成后，系统自动计算一个新的文档防伪码，再次调用区块链防伪平台接口，将新防伪码保存至该文档对于区块链中的后续数据区块中，同时其他认证节点根据链码进行数据同步，从而保证在合同审核过程中的每一步都进行数据的验证和保存，防止了合同信息和审核信息被篡改的可能。

（六）基于区块链防伪平台的合同管理系统特性

本项目实施的合同管理系统具有以下几个特性：

1. 安全技术可控

合同管理系统将关键信息保存在区块链防伪平台中，区块链防伪平台由四个独立的认证节点组成，每个节点相互备份，修改数据时要将每个节点都进行修改，正常的数据修改和更新是根据部署的链码来实施，这样就保证了数据信息不被篡改；同时使用了国密算法，保证了按照技术的可控性；对合同模板和合同内容都进行相关验证码计算和验证，保证了模板和合同内容的安全性；系统还引入兴业银行文档加密系统（dsm），可以根据用户的不同，分配不同的修改、查看、复制和打印权限。

2. 审批流程自定义

目前很多流程管理系统只支持系统预定义固定审批流程，流程相对简单，已经不能很好的满足大多数据审批需求；本项目实施的合同管理系增加了灵活性更大的自定义流程功能，可以满足实际业务中各类特殊场景的需求。

3. 支持非制式合同

原有的合同管理系统只支持格式固定的制式模版合同的管理功能，新系统在此基础上针对实际业务场景中部分特殊非制式合同需求，增加了支持由客户经理自拟定的自由格式的非制式合同的功能。

五、结束语

本文通过对区块链技术的深入分析，应用超级账本(Hyperledger Fabric)的开源技术，讲述了构建兴业银行区块链防伪平台的框架和步骤，并应用兴业银行区块链防伪平台，结合行内的合同管理需要，探索建立基于区块链防伪技术的合同管理系统。经过近一年的研究和探索，兴业银行区块链防伪平台成功上线运行。平台目前虽然只有四个认证节点，随着以后越来越多的需要数据认证的系统上线，平台的认证节点或副本会逐步增多。根据推广计划，未来至少在兴业银行的每个分支机构都建设相关的认证节点，或者根据需要认证的系统数量来创建副本节点，促使该平台有更深更广的应用。基于兴业银行区块链防伪平台实现区块连防伪技术的合同管理系统也成功在兴业银行西宁分行上线运行，目前分行的合同管理系统能够充分利用区块链防伪平台的去中心化、不可被篡改、信息安全可靠等特性，完成合同防伪功能，满足分行关于制式合同和非制式合同的管理需要。通过本研究和项目的实施，使兴业银行在区块链技术的应用上有了更深层次的认知，为以后更多、更深入的区块链技术研究及推广打下了坚实的基础。

课题组组长：高海明

课题组成员：吴大炜　林　筱　魏学江　杨树磊

责任编辑：刘永合

校　　对：LYH