ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0111—2021

区块链密码应用技术要求

Technical requirements for blockchain cryptography application

2021-10-19 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：三未信安科技股份有限公司、国家密码管理局商用密码检测中心、北京数字认证股份有限公司、数安时代科技股份有限公司、清华大学、北京交通大学、山东大学软件学院、国家信息中心、武汉大学、齐鲁工业大学、山东师范大学、暨南大学、中国人民银行数字货币研究所、浪潮集团有限公司、格尔软件股份有限公司、公安部第一研究所、航天信息股份有限公司、阿里巴巴（北京）软件服务有限公司、山大地纬软件股份有限公司、北京智芯微电子科技有限公司、北京信安世纪科技股份有限公司、中国电力科学研究院有限公司、兴唐通信科技有限公司、深圳市金证科技股份有限公司、北京信任度科技有限公司。

本文件主要起草人：刘晓东、李国友、张永强、汪宗斌、谭武征、罗清彩、翟峰、林巍、樊海宁、孔凡玉、许涛、刘蓓、亢洋、卢伟龙、傅大鹏、张大伟、曹永峰、张庆胜、王绍刚、涂因子、甄平、胡进、刘伟、张妍、何德彪、陈国伟、孔兰菊、赵华伟、王皓、龚自洪、梅秋丽、霍云、彭晋、张海龙、顾伟平、冯云、马臣云。

引　言

区块链是分布式数据存储、点对点传输、共识机制、密码算法等技术在互联网时代的创新应用模式。随着国内外区块链技术的迅猛发展，区块链已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

为了保障我国区块链技术应用的健康发展，推动国产密码算法在区块链中的应用，制定区块链密码应用技术要求是非常必要的。

本文件对区块链技术，重点是对联盟链技术的密码安全要素以及需要遵循的相关技术要求做出规定，指导密码技术在区块链中的使用。

区块链密码应用技术要求

1 范围

本文件规定了联盟区块链的密码安全要素以及密码应用的技术要求。

本文件适用于指导联盟区块链密码应用及产品的设计、使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38635.1 信息安全技术 SM9 标识密码算法 第 1 部分：总则

GB/T 38635.2 信息安全技术 SM9 标识密码算法 第 2 部分：算法

GM/T 0033 时间戳接口规范

GM/T 0037 证书认证系统检测规范

GM/T 0038 证书认证密钥管理系统检测规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

一种采用分布式数据存储、点对点传输、共识机制、密码算法、智能合约等技术的新型应用模式和融合技术。

3.2

共识机制 consensus mechanism

区块链系统中实现不同节点之间建立信任、获取权益的算法。

3.3

智能合约 smart contract

一套以数字形式定义的约定。

注：合约参与方以及区块链系统共同遵守的条约。

3.4

分布式账本　decentralized ledger

一个可以在多个节点、不同地理位置或者多个机构组成的网络中分享的数据记录。

3.5

交易记录　transaction record

在区块链网络中广播的一条消息。

注：包含交易发起者、交易内容、交易接收者以及交易发起者的用户签名等信息。

3.6

交易　transaction

数字资产的一次转账或者对智能合约的一次调用。

3.7

公有链　public blockchain

各个节点可以自由加入或退出网络，并参与链上数据读写的区块链系统。

3.8

联盟链　consortium blockchain

各个节点与实体机构组织对应，经过授权后才能加入或退出的区块链系统。

3.9

私有链　private blockchain

各个节点的写入权限和读取权限归内部控制的区块链系统。

3.10

默克尔树　Merkle tree

一类基于哈希指针的二叉树，可以快速实现信息的完整性验证。

3.11

数字资产　digital assets

以电子数据形式存在，持有者可以出售或者交换的有价资产。

3.12

标识密码　identity-based cryptographic

基于身份标识的密码系统。

注：是一种非对称的公钥密码体系。

4　缩略语

下列缩略语适用于本文件。

CA：数字证书签发和管理机构(Certification Authority)

CSR：证书请求文件(Certificate Signing Request)

DPoS：委任权益证明(Delegated Proof of Stake)

PBFT：实用拜占庭容错算法(Practical Byzantine Fault Tolerance)

PKI：公钥基础设施(Public Key Infrastructure)

PoS：权益证明(Proof of Stake)

PoW：工作量证明(Proof of Work)

P2P：点对点(Peer to Peer)

SM2：SM2 算法(SM2 Algorithm)

SM3：SM3 算法(SM3 Algorithm)
SM4：SM4 算法(SM4 Algorithm)
SSL：安全套接字层(Secure Socket Layer)
TLS：传输层安全(Transport Layer Security)
VPN：虚拟专用网(Virtual Private Network)

5 区块链密码应用技术架构

区块链的技术架构可分为数据层、网络层、共识层、激励层、智能合约层和应用层，如图 1 左侧所示。

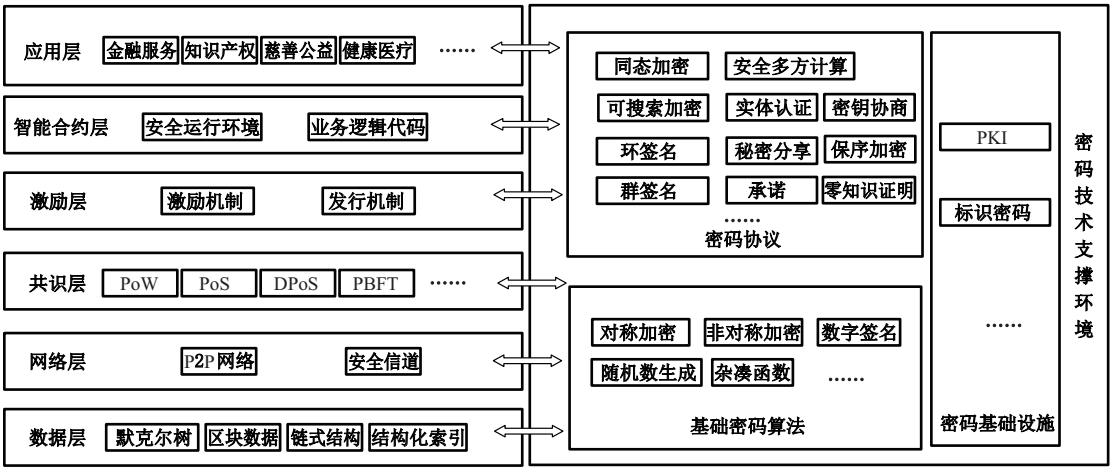

图 1 区块链技术架构

a) 数据层：交易通过合法性验证后以交易集合(如区块等形式)或者单条交易的形式持久化存储到数据库中，并通过杂凑值将数据时序化串联。
b) 网络层：区块链中各个网络节点通过 P2P 技术进行通信，同时可采用 TLS 等技术建立安全信道。
c) 共识层：共识协议是区块链的核心，在实际应用中应根据需要选择合适的共识协议。
d) 激励层：将经济因素或其他激励因素集成到区块链技术体系中，主要包括经济激励的发行机制和分配机制等。联盟链和私有链可以不使用激励机制。
e) 智能合约层：智能合约是一套以数字形式定义的承诺，包括合约参与方执行这些承诺的协议，可视为一段部署在区块链上可自动运行的程序，主要封装各类脚本、算法、指令，是区块链可编程特性的基础。
f) 应用层：使用区块链的各种应用场景和环境。

区块链技术架构中的每个层均需要用到相应的密码技术支持。在区块链技术架构中，所需的密码技术应独立于功能架构之外，为区块链功能架构提供支持。因此，需要构建独立的密码技术支撑环境(如图 1 右侧所示)，为区块链功能架构中的各层服务，以保护其应用安全及运行安全。

区块链密码技术支撑环境涉及 3 个方面的内容。

a) 基础密码算法：为保障区块链系统中信息的机密性、完整性、真实性、抗抵赖性所使用的最底层密码算法，主要包括对称密钥算法、非对称密钥算法、杂凑算法等。
b) 密码协议：密码协议需要多方交互完成，用以满足区块链系统中的各类安全需求。密码协议主要包括同态加密、可搜索加密、环签名、群签名、安全多方计算、实体认证、密钥协商、秘密分享、保序加密、承诺、零知识证明等。

c) 密码基础设施：区块链系统的密码基础设施主要包括 PKI 密码体制和标识密码体制等。

6 区块链密码应用需求

区块链系统根据节点准入控制机制与应用场景的不同，可分为公有链、联盟链和私有链，其交易通常包括用户注册、实名认证、创建交易、验证交易与区块共识、区块确认与同步、区块查询等环节。用户之间的交易行为等数据，以分布式账本的形式存储在多个参与节点上。为保证区块链交易的安全性，存在以下密码应用安全需求。

a) 区块链交易的实体鉴别与权限控制需求。实体鉴别是实体(用户、设备、系统等)在区块链网络中进行交易时，确认实体的身份是否真实、合法。权限控制需要确保区块链用户具有权限执行交易等操作。

b) 交易的机密性需求。防止用户交易信息中的秘密信息在存储、传输过程中被非法窃取。

c) 区块链交易记录与区块链账本的完整性需求：

——需要确保区块链网络中的交易各方所看到的信息完全一致，因此要求在交易生成、存储、传输过程中，能确保交易信息的完整性，不被非法篡改；

——需要确保保存在各个节点上的区块链账本信息的一致性，因此在结合共识协议的基础上，确保区块链账本的完整性，不被非法篡改。

d) 交易的抗抵赖性需求。需要保证区块链用户交易的双方或者多方都不能够抵赖已经执行的交易。

e) 区块链用户匿名与隐私性保护需求。某些区块链需要保证用户的匿名性和交易的隐私性，为了确保用户和交易信息的隐私保护，需要环签名、零知识证明等多种密码技术的支持。

f) 交易的可监管需求。在实现用户匿名与隐私保护的同时，区块链中的交易还需要满足可监管的需求，主要包括：用户匿名身份与实体身份的映射关系授权可查看、交易金额或交易信息授权可解密、交易授权可撤销等，以保证区块链交易的合法合规和可审计。

7 区块链密码应用总体要求

7.1 密码算法要求

区块链中配置和使用的密码算法(如分组密码算法、公钥密码算法、杂凑算法及随机性检测规范)应符合密码国家标准、行业标准的相关要求：

a) 分组密码算法应采用 SM4 密码算法，符合 GB/T 32907；

b) 公钥密码算法应采用 SM2 椭圆曲线公钥密码算法，符合 GB/T 32918；

c) 密码杂凑函数应采用 SM3 密码杂凑算法，符合 GB/T 32905；

d) 随机数生成算法所产生的随机数，符合 GB/T 32915。

7.2 数字签名要求

数字签名格式和使用要求应符合 GB/T 35276、GB/T 35275、GB/T 38635.1 和 GB/T 38635.2。

7.3 密码设备安全要求

应通过商用密码检测认证。

7.4 密钥管理安全要求

区块链应用中的身份鉴别密钥、数据加密密钥等应使用通过商用密码检测认证的密码设备或模块

对密钥的生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节实现安全管理。

对区块链节点之间的通信数据加密，以及对区块链节点上存储数据加密的密钥，应通过商用密码检测认证的密码设备或模块将私钥妥善保存。密钥还应进行严格的生命周期管理，不应为永久有效，到达一定的时间周期后需进行更换。

7.5 证书管理要求

区块链中的数字证书主要分为两类：一是最终用户用以完成身份鉴别、安全通信和交易签名的数字证书；二是区块链节点用来完成身份鉴别、交易背书、安全通信的数字证书。

a) 证书认证系统和相关的密钥管理系统建设应符合 GB/T 25056 、GM/T 0037 和 GM/T 0038；

b) 数字证书以及 CRL 格式应符合 GB/T 20518。

7.6 数据安全要求

区块链的节点和节点之间的数据交换，原则上不应明文传输，宜采用非对称密码技术协商密钥，用对称加密算法进行数据的加密和解密。数据提供方也应严格评估数据的敏感程度、安全级别，决定数据是否发送到区块链，是否进行数据脱敏，并采用严格的访问控制措施。

区块链各个节点之间、应用端与节点之间可配置安全通道，以保证数据通信的安全。安全通道应使用符合密码国家标准、行业标准相关要求的密码算法和密码协议，保证传输数据的机密性和完整性。

7.7 共识协议安全要求

共识协议应提供明确的密码学机制，确保共识协议在运行环境中具有以下性质：

a) 参与共识协商各方应采用密码技术实现身份鉴别；

b) 共识协议执行过程中发送的敏感信息应采用密码技术保证机密性、完整性、抗抵赖性；

c) 应提出明确的保证共识协议执行的容错性、一致性和可用性的安全边界；

d) 所有诚实共识协商节点在约定时间内完成共识；

e) 所有诚实共识协商节点记录内容相同；

f) 所有诚实共识协商节点的共识请求都应有处理回应；

g) 所有诚实共识协商节点处理共识请求的顺序相同；

h) 共识协议还应具备抗 DoS、双花等攻击能力；

i) 在遭受恶意攻击的情况下，各节点自身的数据安全需得到保障；或通过适当的干预，各节点可自动恢复正常状态。

7.8 智能合约安全要求

在部署智能合约时，应检查用户是否获得相应的权限，同时应采用密码技术来防止智能合约被篡改。在调用智能合约之前，应检查链上代码的完整性，并拒绝执行被篡改的智能合约。

8 区块链的各业务环节的密码应用技术要求

8.1 用户注册

在用户注册阶段，应生成可以标识用户的交易地址，并使用符合 GB/T 32915 的随机数发生器来生成 SM2 的公私钥对。用户私钥宜在密码模块内部安全地产生并存储，密码模块应满足 GB/T 37092 的相关要求。

8.2 实名认证

在需要进行实名交易的区块链系统中，由用户向可信的第三方 CA 提交包含用户身份信息的证书签发请求(CSR)，证书颁发机构在对用户身份执行鉴别，并为用户签发数字证书。证书签发系统应满足7.5 相关要求，签发的数字证书格式应满足 GB/T 20518。

8.3 交易创建

新交易创建过程中应满足以下密码要求：

a) 交易发起者使用自己的私钥对本次交易进行数字签名；
b) 对交易中的秘密信息使用加密方式进行保护，保证交易在传输、存储和使用过程中的安全；
c) 有效交易被打包进区块中，通过共识协议在节点间达成共识，区块的有效性验证应确保区块中记录的上一个区块杂凑值的有效性；
d) 在创建区块时，应使用 GB/T 32905 规定的 SM3 来计算上一个区块杂凑值，并且在基于交易信息生成默克尔树的各层次的杂凑值时也应采用 SM3；
e) 如果有数据隐私需求，宜对交易信息或者区块信息采用密码技术进行处理，如采用对称加密算法应符合 GB/T 32907；
f) 如果在区块中包含第三方可信时间戳，则时间戳服务规范应符合 GM/T 0033。

8.4 交易验证

交易生成后需要广播给区块链网络中的节点，然后由节点对交易进行验证，并打包成区块，运行共识协议，保证网络中的节点对所有合法交易达成共识。区块链对交易达成共识过程中的密码要求应满足：

a) 如果采用数字证书方式，应先进行数字证书的有效性验证，包括证书信任链验证、证书有效期验证、证书是否被吊销、使用策略是否正确等；
b) 验证交易记录中的数字签名，确保交易发起者身份的真实性和交易记录的完整性；
c) 验证交易签名时间的有效性等；
d) 区块的有效性验证应确保区块中记录的上一个区块杂凑值的有效性，其他方面的验证与交易的验证类似；
e) 如果在区块中包含第三方可信时间戳，则按照 GM/T 0033 检查时间戳数字签名的有效性，并检查时间戳签名证书是否连接到被信任根 CA。

8.5 账本存储

在区块链中，用户的交易记录会通过区块的方式进行组织，然后通过一种块链结构将区块串联在一块，形成区块链账本。每个区块会包含区块头和区块体，区块体用来记录具体的交易记录，区块头主要用来链接前一个区块并保证账本完整性。区块链账本的存储安全管理应满足以下要求：

a) 通过区块头的杂凑值标识区块，用于链接相邻区块，保障区块数据的完整性；
b) 应采用加密措施保证账本重要内容的机密性；
c) 需要采用身份鉴别和访问控制措施保证账本数据的授权访问。

8.6 链外交易

区块链中还可支持链外交易的模式，该模式应采用数字签名来确认交易各方的真实身份，保存所有交易的审计记录，并采用密码技术保证审计记录的完整性。

在链外交易系统执行周期性的上链操作时，区块链系统应检查所有未登记交易的有效性，并根据预

先定义的业务规则检查交易清算的正确性。

8.7 节点和用户的身份管理

在区块链中，需确保所有节点和用户的身份在系统中的可识别性与合法性。在联盟链中，节点的准入或退出宜采用数字证书技术验证节点身份，并生成审计日志。

8.8 交易监管

通过密码技术保证监管节点对于用户实体身份、交易信息等内容可查看；保证监管节点权限受控；在某些特定场景下，保证交易的合法可撤销，同时不影响随后产生的交易区块，不改变整条链的可验证性。

附 录 A
（资料性）
基于区块链的电子存证应用方案

A.1 方案概述

基于区块链的电子证据存证应用方案是分布式数据存储、点对点传输、共识机制、密码算法等技术在电子存证应用领域的创新应用模式，其应用网络如图 A.1 所示。

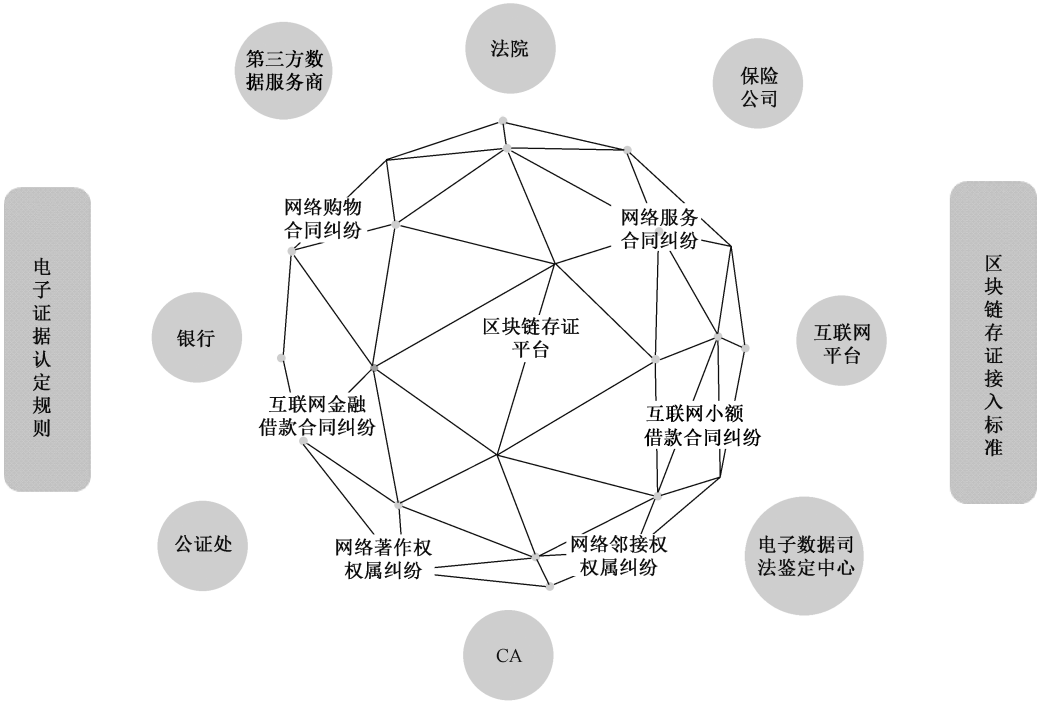

图 A.1 基于区块链的电子证据存证平台应用网络

银行、保险公司、互联网平台、电子数据司法鉴定中心、CA、公证处、第三方数据服务商作为联盟链的节点，法院作为监管方加入区块链，统一制定区块链存证平台的运行标准和合约条件。区块链上的各节点和加入者都应按照事先制定的交易规则参与和运行，共同维护联盟链，解决各种互联网纠纷电子证据认定问题，通过区块链对互联网合同、知识产权等全流程的状态进行记录和存取，有效解决互联网纠纷中存证不可信、法律效力不足等问题。银行、保险公司、互联网平台和第三方数据服务商通过将相关的合同数据、权属证据进行区块链电子证据存证，当发生相关的合同和权属等纠纷时，法院作为监管方查看相关的电子数据存证信息，实现利用区块链电子存证信息进行司法采信和下一步的审判。

方案采用 SM2、SM3、SM4，以及基于这些算法的数字证书和安全通信 TLS 协议。作为监管方，法院负责为加入区块链的使用方进行身份审核，通过审核后为其颁发数字证书，持有合法证书的用户方可作为区块链的服务平台节点参与共识记账，共同维护区块链电子存证账本。区块的杂凑值通过 SM3 运算得到，同时也支持本区块链与外部区块链之间通过跨链操作，外部区块链的区块头通过 SM3 运算得到杂凑值存到本区块链中，实现区块链不可篡改的特性。各区块链节点之间通过 TLS 协议保障通信安全，实现区块链账本的一致存储。

A.2 密码应用设计

A.2.1 密码应用总体设计要求

a) 使用 SM4 完成敏感数据的保护；
b) 使用 SM2、SM3 完成签名、验签运算，使用该算法生成数字证书；
c) 使用 SM3 完成数据杂凑运算；
d) 建立 TLS 安全通道使用 SM2、SM3、SM4。

A.2.2 隐私保护模块密码应用设计

a) 使用 SM4 对区块链敏感数据加密处理；
b) 使用 SM4、SM2 实现授权查看功能；
c) 对链外数据采用 SM3 杂凑上链存储。

A.2.3 节点管理模块密码应用设计

a) 各节点身份鉴别操作均需使用 SM2、SM3 签名算法；
b) 各节点之间通信需通过 TLS 安全通道；
c) 各节点需使用 SM2 生成密钥对及证书请求文件。

A.2.4 创建交易密码应用设计

a) 交易发起者对本次交易使用 SM2、SM3 进行数字签名，签名满足 7.2 的要求；
b) 对交易中的秘密信息使用 SM4 进行保护，保证交易在传输、存储和使用过程中的安全；
c) 对链外存储数据使用 SM3 杂凑上链存储。

A.2.5 交易验证与区块共识密码应用设计

a) 验证用户的证书是否合法；
b) 验证交易 SM2、SM3 数字签名，确保交易发起者身份的真实性和交易记录的完整性；
c) 验证节点使用 SM3 有效性验证应确保区块中记录的上一个区块杂凑值的有效性。

A.2.6 账本记录密码应用设计

a) 通过区块头的 SM3 杂凑值标识区块，用于链接相邻区块，保障区块数据的完整性；
b) 采用 SM2、SM4 保证数据的机密性；
c) 需要采用数字证书鉴别和访问控制措施来保证账本数据的合法授权访问。