ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0122—2022

区块链密码检测规范

Cryptography test specification for blockchain

2022-11-20 发布　　2023-06-01 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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：国家密码管理局商用密码检测中心、三未信安科技股份有限公司、北京信安世纪科技有限公司、兴唐通信科技有限公司、山东大学、浙江蚂蚁小微金融服务集团股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、中国金融认证中心、中国信息通信研究院、卫士通信息产业股份有限公司、中国电子科技网络信息安全有限公司、杭州趣链科技有限公司、北京众享比特科技有限公司、鼎链数字科技（深圳）有限公司。

本文件主要起草人：李国友、顾伟平、刘晓东、汪宗斌、陈妍、李冬、邓开勇、鹿淑煜、陈萧宇、陈磊、肖飞、姚长远、梁乐、童刚、王磊、刘立超、王昕、张大健、孔凡玉、廖思捷、张立廷、张珂杰、陈晓丰、吴飞鹏、刘晨、魏凯、庞伟伟、苏年乐、周辉。

区块链密码检测规范

1 范围

本文件规定了区块链密码模块中相关密码技术的检测内容、检测方法以及合格判定准则。

本文件适用于区块链密码模块的检测，可用于指导区块链密码模块的设计和使用密码技术。

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 15843.2 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 15843.5 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

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 32918(所有部分) 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 38635(所有部分) 信息安全技术 SM9标识密码算法

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GM/T 0005 随机性检测规范

GM/T 0022 IPSec VPN技术规范

GM/T 0028 密码模块安全要求

GM/T 0033 时间戳接口规范

GM/T 0111 区块链密码应用技术要求

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

一种将数据区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

3.2

共识机制　consensus mechanism

区块链系统中实现不同节点之间决策达成一致的算法。

3.3

智能合约　smart contract

存储在分布式账本中的计算机程序，由区块链用户部署，其任何执行结果都记录在分布式账本中。

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、同步的全序数据记录。

3.5

交易记录　transaction record

在区块链网络中广播和存储的一条消息。

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

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。

3.7

交易　transaction

数字资产的一次转账或者对智能合约的一次调用。

3.8

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。

3.9

节点　node

具有特定功能的区块链组件，可独立运行的单元。

3.10

共识节点　consensus node

负责产生区块，并维护区块链数据的节点。节点保存着自己的一份或者部分账本，通过投票或者算力等方式来解决共识问题，通过无信任或弱信任的方式确保全体节点遵循的账本和自己的账本是一致的。

3.11

区块　block

一种区块链的基本组成单元，通常由一系列交易和一些关于区块的元信息组成。

3.12

账户　account

区块链上能够区别数据记录归属的基本单位。

3.13

隐私保护　privacy protection

为保护隐私而采取的措施。

示例：对个人数据的收集、处理和使用加以限制。

3.14

区块链密码模块　blockchain cryptographic modules

以区块链技术为核心，用于用户安全、共识安全、账本保护、对等网络安全、计算和存储安全、隐私保

护、身份认证和管理等的软硬件密码模块。

注：一个区块链密码模块即可作为一个节点。

3.15

零知识证明　zero knowledge proof

证明者与验证者一起执行的密码协议，使验证者确信某个论断的正确性，证明者却又不向验证者泄露除论断正确性以外的其他信息。

3.16

环签名　ring signature

签名者指定了一个可能签名者的集合(或环)，并对某消息进行签名。验证者能够确信签名确实由环中的某个成员生成，但是无法指出真实签名人。

3.17

盲签名　blind signature

一种特殊的数字签名，所签的信息对签名者是不可知的。

3.18

群签名　group signature

一个群体中的任意一个成员可通过匿名的方式代表整个全体对消息进行签名。

注：与其他数字签名一样，群签名是可公开验证的，而且可用群公钥进行验证。

4　缩略语

下列缩略语适用于本文件：

CA：证书认证机构(Certification Authority)

CRL：证书撤销列表(Certificate Revocation List)

DoS：拒绝服务(Denial of Service)

DPoS：委任权益证明(Delegated Proof of Stake)

HMAC：基于杂凑的消息鉴别码(Hash-Based Message Authentication Code)

IPSec：IP 安全协议(Internet Protocol Security)

MAC：消息鉴别码(Message Authentication Code)

OCSP：在线证书状态查询协议(Online Certificate Status Protocol)

BFT：拜占庭容错算法(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)

TLCP：传输层密码协议(Transport Layer Cryptographic Protocol)

VPN：虚拟专用网(Virtual Private Network)

5　区块链密码应用技术架构

区块链技术是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。其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，区块链技术架构见 GM/T 0111。

6 区块链密码总体检测要求

6.1 密码算法

6.1.1 基本要求

区块链中配置和使用的密码算法符合密码国家标准、行业标准的相关要求：

a) 对称密码算法采用 SM4 密码算法，应符合 GB/T 32907；

b) 非对称密码算法采用 SM2、SM9 密码算法，应符合 GB/T 32918(所有部分)、GB/T 38635(所有部分)；

c) 密码杂凑函数采用 SM3 密码杂凑算法，应符合 GB/T 32905。

6.1.2 对称密码算法加密解密实现正确性测试

对给定密钥和明文(密文)，调用对称密码算法，测试其运算结果的正确性，包括：

a) 对给定的密钥和明文按照指定的工作模式进行加密运算，结果和给定的密文完全相同；

b) 对给定的密钥和密文按照指定的工作模式进行解密运算，结果和给定的明文完全相同。

6.1.3 杂凑密码算法实现正确性测试

对给定消息和参数，调用杂凑算法，测试其运算结果的正确性，包括：

a) 对给定消息调用杂凑算法运算接口，计算杂凑值，结果和给定的杂凑值完全相同；

b) 对给定消息和参数调用杂凑算法运算接口，计算杂凑值，结果和给定的杂凑值完全相同。

6.1.4 非对称密码算法加密解密实现正确性测试

对给定密钥和明文(密文)，调用非对称密码算法，测试其运算结果的正确性，包括：

a) 对给定明文、密钥调用非对称密码算法加密运算接口进行加密运算，检测工具对密文进行解密运算，解密结果和给定明文完全相同；

b) 对给定密文、密钥调用非对称密码算法解密运算接口进行解密运算，解密结果和给定明文完全相同。

6.1.5 非对称密码算法数字签名及签名验证实现正确性测试

调用非对称密码算法对数据进行签名/验签运算，测试其运算结果的正确性，包括：

a) 对给定待签名消息、密钥调用非对称密码算法签名运算接口进行签名运算，检测工具对签名结果进行验签运算，应验签通过；

b) 对给定签名结果、待签名消息、密钥调用非对称密码算法验签运算接口进行验签运算，应验签通过。

6.1.6 非对称密钥对配对一致性测试

对生成的公钥和私钥，调用非对称密码算法，测试其运算结果的正确性，包括：

a) 使用公钥对明文进行加密，使用私钥解密所得的密文结果，解密的结果应与原明文相同；

b) 通过数字签名的计算和验证来进行非对称密钥对一致性测试，该数字签名应验证通过。

6.2 随机数检测

随机数应采用通过密码检测认证的密码部件或模块生成，随机数质量应符合 GM/T 0005 的规定。

6.3 密码协议

使用的密码协议符合密码国家标准、行业标准的相关要求：

a) 采用 TLCP 协议时，应符合 GB/T 38636；

b) 采用 IPSec 协议时，应符合 GM/T 0022；

c) 采用经国家密码主管部门审查鉴定的零知识证明、环签名、群签名、安全多方计算等，应采集协议交互数据验证正确性和一致性。

6.4 密钥管理

密钥管理安全应符合以下要求：

a) 密钥的生成应在通过密码检测认证的密码部件或模块内部产生；私钥和对称密钥的生成及协商应使用符合 GM/T 0005 要求的随机数；

b) 对称密钥和私钥应以安全形式或密文形式存储；

c) 若涉及密钥分发过程，应具备身份鉴别等保证密钥真实性的安全措施；应采用数字签名、HMAC 等密码技术保证分发密钥的完整性，HMAC 应符合 GB/T 15852.2；应具备保证密钥的机密性的安全措施；

d) 密钥应采取加密或知识拆分等安全方式进行导入导出；

e) 密钥应具有明确用途；密钥使用过程中应有相应安全措施，防止被非授权访问、使用和篡改；

f) 对节点之间的通信数据加密的密钥应有明确的更换周期，到达一定的时间周期后进行更换；若对节点上存储数据进行本地加密，加密的密钥同样应有明确的更换周期，到达一定的时间周期后应进行更换；

g) 若支持密钥备份与恢复，应以安全形式或密文形式备份到安全存储介质中，应支持以安全形式恢复备份的密钥；密钥备份或恢复应进行记录并生成审计信息；

h) 若涉及密钥归档过程，应使用有效的安全措施，保证归档密钥的安全性和正确性；归档密钥应只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录并生成审计信息；归档密钥应进行数据备份，并使用有效的安全保护措施；

i) 在密钥生命周期结束、发生泄露或有泄露风险时应支持密钥销毁。

6.5 证书管理

证书管理和验证功能检测时，数字证书应符合 GB/T 20518、GB/T 35276、GB/T 35275 的规定。

a) 应检查数字证书以及 CRL 格式，包括证书有效期、证书链验证；

b) 应检查数字证书和 CRL 格式是否符合 GB/T 20518 要求；

c) 应检查证书有效期、证书链、证书是否通过 OCSP 协议验证或在 CRL 列表中。

d) 证书使用前应具有证书验证机制，先进行证书正确性、有效性验证。

6.6 密码设备

区块链应使用通过密码检测认证的密码部件或密码模块，如密码卡、服务器密码机、VPN、智能密码钥匙、时间戳服务器、签名验签服务器等。

7 区块链密码模块密码检测要求

7.1 身份管理

7.1.1 账户创建

检测要求：

在账户创建阶段，应生成可以标识用户的交易地址，并使用通过密码检测认证的密码部件或模块生成SM2算法的公私钥对。用户私钥应在密码模块内部安全地产生并存储，密码模块应满足GM/T 0028的相关要求。

检测步骤：

a) 模拟账户创建流程；

b) 核查账户创建过程中生成SM2算法的公私钥对机制，核查是否采用通过密码检测认证的密码部件或模块生成；

c) 核查分析用户私钥产生及存储是否在通过密码检测认证的密码部件或模块中。

结果判定：

若a)～c)结果为肯定，则该检测项为通过。

7.1.2 实名认证

检测要求：

在需要进行实名交易时，应使用数字证书技术鉴别用户身份的合法性及有效性。

检测步骤：

a) 模拟实名认证流程，核查是否能记录实名信息；

b) 核查是否使用数字证书技术鉴别用户身份。

结果判定：

若a)、b)结果为肯定，则该检测项为通过。

7.1.3 鉴别与授权

检测要求：

在区块链中，应确保所有节点和用户身份在区块链密码模块间的可识别性与合法性。节点的准入或退出宜采用数字证书技术验证节点身份、授权节点权限，并生成审计日志。节点和用户身份的鉴别机制应符合GB/T 15843.2、GB/T 15843.3、GB/T 15843.4、GB/T 15843.5中的一种要求。

检测步骤：

a) 核查分析用户的身份鉴别机制是否采用基于密码技术的认证机制；

b) 模拟用户链上交易过程，对合法用户身份应成功鉴别，对非法用户身份应鉴别失败，无法通过安全通信接入区块链网络，或交易验证失败；

c) 模拟节点准入过程，对合法节点身份应成功鉴别并准入，对非法用户身份应鉴别失败，不允许节点进入；

d) 模拟节点准入、链上交易的过程，使用合法节点进行授权权限操作，应允许节点操作；使用合法节点进行非授权权限操作，不允许节点操作；

e) 核查是否生成审计日志，并验证审计日志的完整性；

f) 若用户的身份鉴别机制使用数字证书技术，应通过6.5章节检测。

结果判定：

若 a)～e)结果为肯定，则该检测项为通过。若涉及 f)项，且结果为肯定，则该检测项为通过。

7.2 链上交易

7.2.1 交易创建

检测要求：

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) 对交易中的敏感信息使用加密方式进行保护，保证交易传输、存储的安全；

c) 交易被打包进区块中，通过共识机制在节点间达成共识，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 SM3 算法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 算法；

e) 若有数据隐私需求，宜对交易信息或者区块信息采用密码技术进行处理；

f) 若在区块中包含第三方可信时间戳，则时间戳应符合 GM/T 0033；

g) 交易应具有唯一性，应添加 nonce 值计数等防重放攻击的措施；

h) 若采用经国家密码主管部门审查鉴定的盲签名、环签名、群签名等，应验证正确性和一致性。

检测步骤：

a) 模拟交易创建流程；

b) 使用发起者的公钥对交易数据中包含的数字签名进行验证，是否能验证成功；

c) 核查分析交易过程中敏感信息的密码技术保护机制，是否正确、有效；

d) 检测有效交易是否能被打包进区块中，通过共识机制在节点间达成共识；

e) 验证在创建区块、基于交易信息生成默克尔树时是否采用 SM3 算法；

f) 若有数据隐私需求，核查交易信息或者区块信息是否采用密码技术进行处理；

g) 若在区块中包含第三方可信时间戳，核查分析交易创建过程中使用的时间戳是否符合 GM/T 0033；

h) 核查验证交易是否添加 nonce 值计数等防重放攻击的措施；

i) 若采用经国家密码主管部门审查鉴定的盲签名、环签名、群签名等，核查验证相关技术的实现正确性和一致性。

结果判定：

若检测步骤中 a)～e)、h)结果为肯定，则该检测项为通过。若涉及检测步骤中 f)、g)、i)项，且结果为肯定，则该检测项为通过。

7.2.2 交易验证

检测要求：

交易创建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，保证网路中的节点对所有合法交易达成共识。

区块链密码模块对交易达成共识过程中的密码要求应满足如下条件。

a) 若采用数字证书方式，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) 验证交易记录时间的有效性等。

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) 若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。

检测步骤：

a) 模拟交易验证流程；

b) 若采用数字证书方式，是否能通过 6.5 章节检测；

c) 核查交易记录是否有数字签名，数字签名是否能验证通过；

d) 核查交易记录是否具有防重放攻击措施，修改交易签名时间或 nonce 值计数等信息，是否能够及时进行错误处理；

e) 若在区块中包含第三方可信时间戳，核查是否符合 GM/T 0033，检查时间戳签名证书是否连接到被信任根 CA。

结果判定：

若检测步骤 a)、c)、d)结果为肯定，则该检测项为通过。若涉及检测步骤 b)、e)项，且结果为肯定，则该检测项为通过。

7.3 链下交易

检测要求：

区块链中链下交易宜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、链外数据的完整性。

在链下交易系统执行周期性的上链操作时，区块链密码模块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。

检测步骤：

a) 模拟链下交易流程；

b) 核查分析链下交易流程中交易各方的身份认证机制，验证身份认证机制是否正确有效；

c) 核查分析链下交易流程中审计记录，验证是否采用 MAC、数字签名等密码技术保证审计记录的完整性；

d) 核查分析是否采用 MAC、数字签名等密码技术保证链外数据的完整性；

e) 模拟上链操作，核查分析区块链密码模块是否具有检查所有未登记交易的有效性机制；

f) 核查分析区块链密码模块是否具有检查交易清算机制；

g) 若采用数字签名来确认交易各方的真实身份，核查数字签名是否验证通过。

结果判定：

若支持链下交易，a)～f)结果为肯定，则该检测项为通过，若涉及 g)项，且结果为肯定，则该检测项为通过。

7.4 账本存储

检测要求：

a) 应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) 应采用身份鉴别和访问控制措施保证账本数据的授权访问。

检测步骤：

a) 模拟账本存储过程；

b) 核查验证区块头杂凑算法是否采用 SM3 算法；

c) 核查分析账本重要内容存储是否采用密码技术加密保护；

d) 核查分析是否采用身份鉴别和访问控制措施保证账本数据的授权访问，使用授权身份访问，是否能正确访问；使用非授权身份访问，是否能拒绝访问。

结果判定：

若检测步骤中 a)～d)结果为肯定，则该检测项为通过。

7.5 通信安全

检测要求：

区块链各个节点之间、应用端与节点之间通信可配置安全通道，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。

检测步骤：

a) 模拟应用端与节点、节点与节点之间的通信过程，核查分析通信数据中的密码算法和密码协议是否符合密码国家标准、行业标准相关要求；

b) 核查验证通信数据的完整性和机密性保护机制是否正确、有效。

结果判定：

若 a)～b)结果为肯定，则该检测项为通过。

7.6 共识机制

检测要求：

使用的共识机制应满足一致性、活性等基本安全需求，提供明确的密码学机制，参与共识机制协商各方应采用密码技术实现身份鉴别，共识机制执行过程中发送的敏感信息应采用密码技术保障机密性、完整性、不可否认性。

检测步骤：

a) 模拟共识过程，核查分析共识机制的密码机制是否一致；

b) 模拟共识机制执行的过程，对合法共识用户身份是否能成功鉴别，对非法用户身份是否能鉴别失败，无法参与共识执行；

c) 模拟共识机制执行的过程，执行过程中发送的敏感信息是否被加密保护，是否具有完整性校验，是否具有不可否认性机制；

d) 审查厂商提供的设计文档和安全性自测试文档，审查文档是否包含保证共识协议执行的容错性、一致性和可用性的安全边界的说明；

e) 审查厂商提供的设计文档和安全性自测试文档，审查文档是否包含所有诚实共识协商节点在约定时间内完成共识、记录内容相同、共识请求都应有处理回应、处理共识请求的顺序相同的说明；

f) 审查厂商提供的设计文档和安全性自测试文档，审查文档是否包含对节点作恶的防范能力，对女巫攻击、抗 DoS、双花攻击的防御能力等说明。

结果判定：

若 a)～f)结果为肯定，则该检测项为通过。

7.7 智能合约

检测要求：

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。

检测步骤：

a) 模拟智能合约部署、更新等过程；

b) 核查分析用户权限鉴别机制，具有权限的用户是否能正确部署智能合约，非授权用户部署智能合约，是否能拒绝部署；

c) 在部署和更新过程中代码被篡改后，验证是否能够及时发现并做出合理响应；

d) 核查分析智能合约代码保护机制，是否使用数字签名、HMAC 等密码技术防止非法篡改；未被篡改的代码，智能合约是否能部署成功；被篡改的代码，智能合约是否能部署失败。

结果判定：

若 a)～d)结果为肯定，则该检测项为通过。

7.8 隐私保护

检测要求：

宜采用密码技术实现用户的匿名性和交易的隐私性，确保隐私信息的机密性和完整性，不被非授权的第三方获取，并保护交易双方的身份不被识别和冒用。

检测步骤：

a) 核查分析隐私信息是否使用密码技术进行保护；

b) 核查分析隐私信息访问时是否使用密码技术进行有效的身份鉴别；

c) 若采用经国家密码主管部门审查鉴定的环签名、盲签名、群签名、零知识证明、安全多方计算等技术，核查分析相关技术的实现正确性和一致性。

结果判定：

若 a)～b)结果为肯定，则该检测项为通过。若涉及 c)项，且结果为肯定，则该检测项为通过。

7.9 交易监管

检测要求：

宜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，监管节点权限受控。

检测步骤：

a) 若支持交易监管，核查分析是否采用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，核查密码技术有效性；

b) 若支持交易监管，核查监管节点权限控制，核查权限设置是否合理有效。

结果判定：

若支持交易监管，a)～b)结果为肯定，则该检测项为通过。

7.10 性能测试

7.10.1 测试场景

测试场景设置要求如下：

a) 网络规模：宜设定 N 个（N 可选择 4、8、16 及以上）共识节点；

b) 交易类型：转账类交易、存证类交易、查询类交易以及其他类型；

c) 系统资源消耗情况：记录 CPU、内存、网络、磁盘等资源消耗情况。

7.10.2 系统性能

系统性能设置要求如下：

a) 交易延迟，在正常交易负载下，从应用端发起交易连续发送交易 T 秒（T 可选择 600、1 200、

1 800)，记录接收交易数 N，确认交易数 M，交易延迟时间 D，计算每笔交易延迟 TD(秒/笔)。

b) 吞吐量，从应用端发起交易连续发送交易 T 秒(T 可选择 600、1 200、1 800)，记录接收交易数 N，确认交易数 M，计算每秒接收交易数 TPS(笔/秒)，每秒确认交易数 CTPS(笔/秒)。

c) 多节点账本同步延时，统计区块链网络节点的账本同步延时。将其中一个节点暂停，每秒发送 N 笔交易，10 min 后停止发送新的交易事务，重启暂停节点，记录暂停期间发送的交易量、交易大小和同步时间，检查节点是否能在合理时间范围(交易同步时间不能超过交易暂停时间)内同步上；暂停 20 min，重复以上步骤。计算账本同步延时。

d) 账本同步时间，设定账本数据大小为 1 GB、5 GB、10 GB，记录账本同步时间。

8 送检技术文档要求

研制单位按照检测认证机构要求提交相关文档资料，作为送检产品的检测依据。

9 合格判定准则

本文件中 7.3、7.7、7.8、7.9 章节为可选检测项，如果未实现该项密码功能，则为不适用。

本文件中必选检测项和适用的可选检测项，任何一项检测结果不符合相应检测指标，即判定为产品不合格。