

ICS 35.030
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0111-2021

**Technical requirements for blockchain cryptography
application**

区块链密码应用技术要求
(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Blockchain	4
Consensus mechanism	5
Smart contract	6
Decentralized ledger	7
Transaction record	8
Transaction	9
Public blockchain	10
Consortium blockchain	11
Private blockchain	12
Merkle tree	13
Digital assets	14
Identity-based cryptographic	15
Abbreviations	16
Blockchain cryptographic application requirements	17
Digital signature requirements	18
Security requirements for cryptographic devices	19
Key management security requirements	20
Certificate management requirements	21
Data security requirements	22
Consensus protocol security requirements	23
Smart contract security requirements	24
Transaction verification	25
Ledger storage	26
Off-chain transactions	27
Identity management of nodes and users	28
Transaction supervision	29

1 Scope

This document specifies the cryptographic security elements of the consortium blockchain and the technical requirements for cryptographic applications.

This document is intended to guide the design and use of consortium blockchain cryptographic applications and products.

2 Normative references

The provisions of the following documents constitute the essential clauses of this document through normative references in this text. Among them, for referenced documents with dates, only the versions corresponding to the dates are applicable to this document; for referenced documents without dates, the latest versions (including all amendments) are applicable to this document.

GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format
GB/T 25056 Information security technology - Specifications of cryptograph and related security technology for certificate authentication system
GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm
GB/T 32907 Information security technology - SM4 block cipher algorithm
GB/T 32915 Information security technology - Randomness test methods for binary sequence
GB/T 32918 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves
GB/T 35275 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification
GB/T 35276 Information security technology - SM2 cryptographic algorithm usage specification
GB/T 37092 Information security technology - Security requirements for cryptographic modules
GB/T 38635.1 Information security technology - Identity-based cryptographic algorithms SM9 - Part 1: General
GB/T 38635.2 Information security technology - Identity-based cryptographic algorithms SM9 - Part 2: Algorithms
GM/T 0033 Interface specifications of time stamp
GM/T 0037 Certificate authority system test specification
GM/T 0038 Key management of certificate authority system test specification
GM/Z 4001 Cryptology Terminology

3 Terms and definitions

The terms and definitions defined in GM/Z 4001 and the following apply to this document.

3.1 Blockchain

A new application model and fusion technology that uses distributed data storage, peer-to-peer transmission, consensus mechanism, cryptographic algorithm, smart contract and other technologies.

3.2 Consensus mechanism

An algorithm that implements trust building and rights acquisition between different nodes in the blockchain system.

3.3 Smart contract

A set of conventions defined in numerical form.

NOTE: A treaty that is jointly observed by the contract participants and the blockchain system.

3.4 Decentralized ledger

A data record that can be shared across a network of multiple nodes, geographical locations, or organizations.

3.5 Transaction record

A message broadcasted in a blockchain network.

NOTE: It contains information such as the transaction initiator, transaction content, transaction recipient, and the user signature of the transaction initiator.

3.6 Transaction

A transfer of digital assets or a call to a smart contract.

3.7 Public blockchain

A blockchain system in which each node can freely join or exit the network and participate in the reading and writing of data on the chain.

3.8 Consortium blockchain

A blockchain system in which each node corresponds to an entity organization and can only join or exit the network after authorization.

3.9 Private blockchain

A blockchain system in which the write and read permissions of each node are internally controlled.

3.10 Merkle tree

A type of binary tree based on the hash pointer that can quickly verify the integrity of information.

3.11 Digital assets

A valuable asset that exists in the form of electronic data and can be sold or exchanged by the holder.

3.12 Identity-based cryptographic

An identity-based password system.

NOTE: It is an asymmetric public key cryptography system.

4 Abbreviations

The following abbreviations apply to this document.

CA: Certification Authority CSR: Certificate Signing Request DPoS: Delegated Proof of Stake

- a) Data layer: After the transaction passes the legality verification, it is persistently stored in the database in the form of a transaction set (such as a block) or a single transaction, and the data is time-series connected through hash values.
- b) Network layer: Each network node in the blockchain communicates through P2P technology, and TLS and other technologies can be used to establish a secure channel.
- c) Consensus layer: The consensus protocol is the core of the blockchain. In practical applications, the appropriate consensus protocol shall be selected according to needs.
- d) Incentive layer: Integrate economic factors or other incentive factors into the blockchain technology system, mainly including the issuance mechanism and distribution mechanism of economic incentives, etc. Consortium blockchains and private blockchains do not need to use incentive mechanisms.
- e) Smart contract layer: A smart contract is a set of commitments defined in digital form, including the protocols for the contract participants to execute these commitments. It can be regarded as a program deployed on the blockchain that can run automatically. It mainly encapsulates various scripts, algorithms, and instructions, and is the basis of the programmable nature of the blockchain.
- f) Application layer: Various application scenarios and environments in which blockchains are used.

Each layer in the blockchain technology architecture requires corresponding cryptographic technology support. In the blockchain technology architecture, the required cryptographic technology shall be independent of the functional architecture and provide support for the blockchain functional architecture. Therefore, it is necessary to build an independent cryptographic technology support environment (as shown on the right side of Figure 1) to