

商用密码在金融安全中的 应用和测评

中国密码学会密码测评专业委员会主任委员

李大为博士

目 录



.....



.....



.....



密码简介

密码在金融领
域的应用要求

密码产品检测
和应用测评

区块链与密码

A decorative graphic consisting of several concentric circles. The innermost circle is white and contains the number '01'. Surrounding it are several rings of varying shades of blue and white, some of which are partially broken or segmented, creating a dynamic, circular pattern.

01

密码简介

密码的 **含义**

- ◆ 《辞海》：按特定法则编成，用以对通信双方的信息进行**明密变换**的符号
- ◆ 《密码法》：使用特定变换对数据等信息进行**加密保护**或者**安全认证**的物项和技术。

密码的 性质

1 真实性：防假冒

- ◆ 已授权用户可正常访问使用
- ◆ 未授权用户禁止访问

2 机密性：防泄密

- ◆ 已授权的用户可正常查看
- ◆ 未授权的用户看不到

3 完整性：防篡改

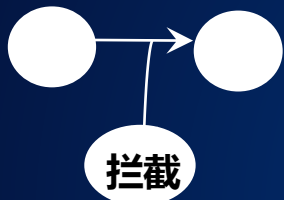
- ◆ 保证信息被未经授权的改动

4 非否认性：抗抵赖

- ◆ 用户不可否认之前针对资源的任何操作，包括访问、修改、删除、增加等

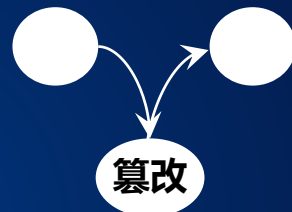
密码是核心技术

Privacy (保密)



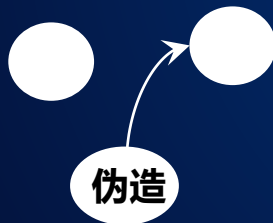
确认信息的保密，
不被窃取

Integrity (完整)



确保你收到信息
没有被篡改

Authentication (认证)



确认对方的身份
并确保其不越权

Non-Repudiation (抗抵赖)



有证据
保证交易不被否认

未发出 ← Claims → 未收到

P+A+I+N=PAIN 密码可以解决网络安全的痛点：
保密/完整/授权/抗抵赖

密码的 应用

密码是解决网络安全**最有效、最可靠、最经济**的方式

是维护网络安全的**核心技术和基础支撑**

随着互联网的广泛应用，**密码将无处不在**

我国已纳入ISO国际标准的密码算法

- ◆ SM2椭圆曲线公钥密码算法
- ◆ SM3杂凑密码算法
- ◆ SM4分组密码算法
- ◆ SM9标识密码算法
- ◆ ZUC序列密码算法(3GPP标准)

我国密码技术水平总体处于世界前列，要增强使用国产密码的信心

构建自主密码体系难度是非常大的。以金融IC卡为例，我国用自主密码替换国外密码，涉及到PBOC标准替换EMV标准，更新或改造**十亿量级**的IC卡、**千万量级**的POS机、**百万量级**的ATM机，以及巨量的后台加密设备。



A decorative graphic consisting of several concentric circles. The innermost circle is white and contains the number '02' in white. The next circle out is a light blue color. The outermost circle is a darker blue color. The circles are slightly offset from each other, creating a sense of depth and movement.

02

密码在金融领域的应用要求

- ◆ 2014年，国办印发《金融领域密码应用指导意见》（国办发[2014]6号文件）
- ◆ 2015年国家对重要领域密码应用提出要求
- ◆ 2018年国家对金融和重要领域密码应用与创新发展工作进行规划

相关法规举例

国家密码管理局

《密码法（草稿征求意见稿）》

《商用密码管理条例》

《信息安全等级保护商用密码管理办法》

《电子认证服务密码管理办法》

公安部

《网络安全法》

《公安机关商用密码应用安全性评估管理办法（试行）》

《网络安全等级保护条例（征求意见稿）》

《公安机关商用密码应用指南（试行）》

其他

《关键信息基础设施安全保护条例（征求意见稿）》

《政务信息系统政府采购管理暂行办法》

金融领域密码应用政策要求-- 银行业

央行制订总体规划

对银行机构使用的密码基础设施、金融IC卡、网上银行、移动支付、关键信息系统提出了**密码应用要求**，要求采用**符合国家密码法律法规和标准要求的密码算法和密码产品**，构建**安全可控的密码保障体系**。

2015年，中国人民银行印发《关于推动移动金融技术创新健康发展的指导意见》，求增强移动金融技术创新的安全可控能力，采取有效的加密措施，保证敏感信息的生产、传输、存储、使用等环节的安全，防止信息泄露，并提出优先**应用安全可控的技术产品和密码算法**

2016年，中国人民银行与中国银行业监督管理委员会共同发布了《银行卡清算机构管理办法》，要求银行卡清算业务基础设施应满足国家信息安全等级保护要求，使用经国家密码管理部门认可的**商用密码产品**。

《关于开展支付安全风险专项排查工作的通知》（银办发〔2018〕146号文件）支付交易涉及的软硬件应使用经国家密码管理机构认可的**商用密码产品**。银行账户系统密码算法应满足的要求：**①应采用国家密码管理部门认可的密码算法②密码算法的应用过程实现应正确有效**

金融领域密码应用政策要求-- 保险业

2015年，中国保险监督管理委员会制定了实施方案，要求逐步在**电子保单、电子认证、办公系统**，以及**各类保险业务系统**中完成密码应用升级改造，使用符合国家密码法律法规和标准要求的**密码算法和密码产品**，加强**密码应用的检测评估**，确保**密码应用的规范性和安全性**。

金融领域密码应用政策要求-- 证券业

2015年，中国证监会制订了工作规划，明确要求逐步在**网上证券、网上期货、网上基金**等业务中完成**密码应用建设和升级改造**，使用符合国家密码法律法规和标准要求的**密码算法和密码产品**，并将密码应用工作纳入机构部门及其派出机构日常工作范围，纳入证券期货行业信息安全检查内容。

2018年2月8日，国家密码管理局发布公告GM/T 0054-2018
《信息系统密码应用基本要求》，对信息系统提出了总体要求。



A decorative graphic consisting of several concentric circles. The innermost circle is white and contains the number '03'. Surrounding it are several rings of varying shades of blue and cyan, some of which are partially broken or segmented. The entire graphic is set against a dark blue background with faint, larger circular outlines.

03

密码产品检测和应用测评

密码检测

依据《商用密码管理条例》（1999年10月7日国务院令第273号发布）

第九条 商用密码产品，必须经国家密码管理机构指定的产品质量检测机构检测合格。

密码检测是执行密码标准和维护密码市场的核心环节。

商用密码应用安全性评估



网络安全等级保护条例（征求意见稿）

第四十七条【非涉密网络密码保护】

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，**委托密码应用安全性测评机构开展密码应用安全性评估**。网络通过评估后，方可上线运行，并在投入运行后，**每年至少组织一次评估**。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

商用密码应用安全性评估

对象

- ◆ 重要信息系统
- ◆ 关键信息基础设施

方法

- ◆ 专项测试
- ◆ 综合评估

内容

- ◆ 密码算法、协议、产品
- ◆ 技术体系、密码管理
- ◆ 密码与应用结合等

以评促建

目的

以评促管

以评促改

测评案例-- 金融IC卡系统

- ◆ 金融IC卡系统密码应用主要解决卡片与发卡行之间的身份鉴别、持卡人的身份鉴别、交易数据的传输安全与存储安全等方面的问题。
- ◆ 信息系统密码应用安全性方案设计和测评的重点是下列方面**合规、正确、有效使用。**：

基于金融IC卡系统推进密码在身份标识与鉴别

关键参数数据/关键数据的机密性和完整性保护

测评案例-- 网上银行系统

- ◆ 网上银行系统是商业银行等金融机构通过互联网、移动通信网络、其他开放性公正网络或专业网络基础设施向其他用户提供各种金融服务的信息系统。
- ◆ 在用户身份标识与鉴别、关键数据的机密性和完整性保护、关键操作的不可否认性等方面，都需要利用密码技术进行保护。



服务器



密码产品



设备



人员



文档

A decorative graphic consisting of several concentric circles. The innermost circle is white and contains the number '04' in white. The next ring is a light blue arc. The outermost ring is a darker blue arc. The background is a dark blue gradient with faint, larger concentric circles.

04

区块链与密码

区块链与密码

区块链的定义：“区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的链式数据结构，并以**密码学**方式保证的**不可篡改**和**不可伪造**的**分布式账本**。”

从**密码工程师**的视角来看，**区块链是解决不可篡改和不可伪造的分布式账本的密码应用**。

密码在区块链中的运用

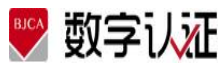


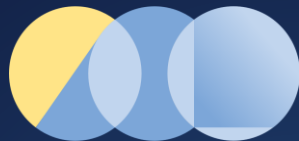
区块链密码创新联盟



2017年11月，发起成立
区块链密码创新联盟，采
用Java语言自主开发区
块链底层技术平台。

区块链密码创新联盟





聚龙链
JULONGCHAIN



自主代码



自主密码



联盟链

聚力研发



12家



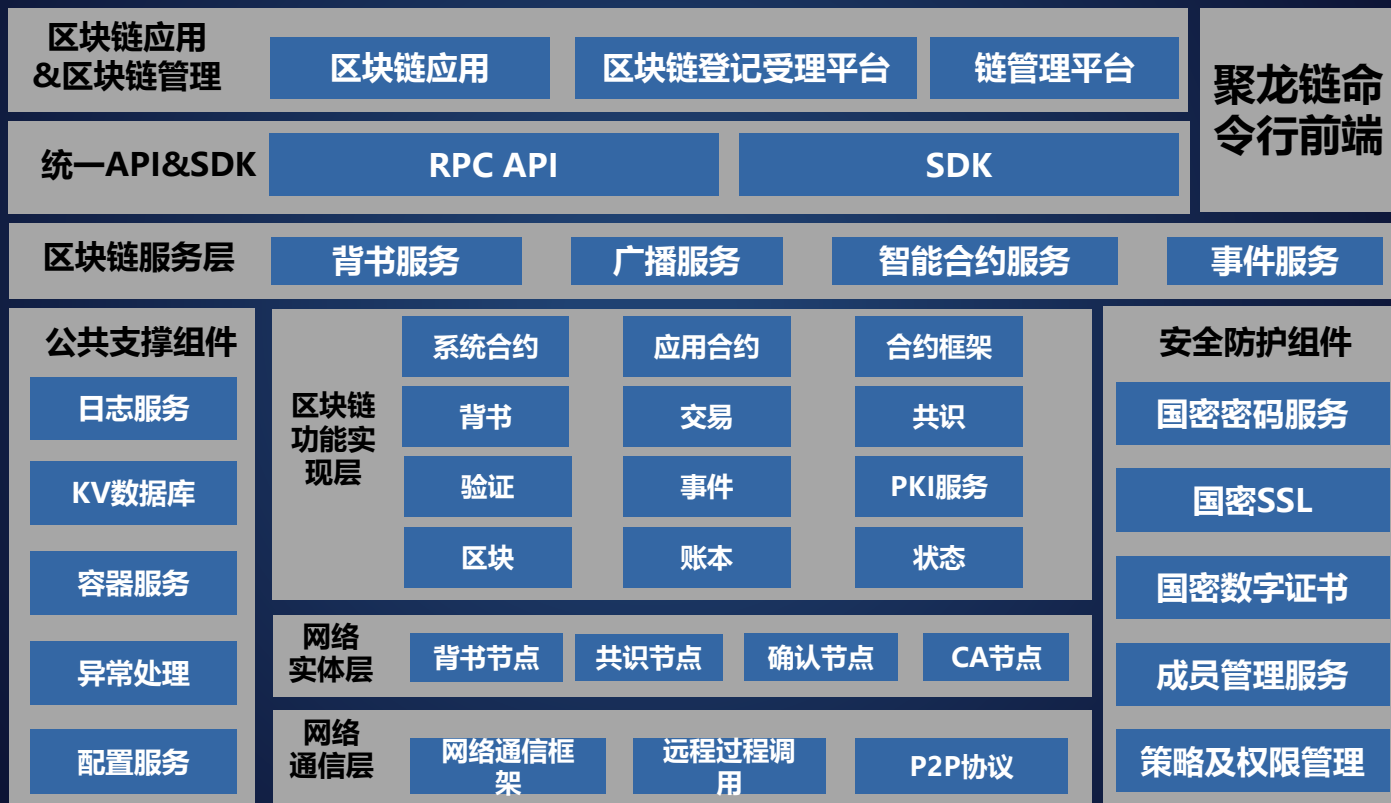
10个月



20万+行代码

对比项	超级账本	以太坊	聚龙链
对称加密算法	AES	AES	SM4
哈希算法	SHA256	SHA256	SM3
非对称密码算法	ECDSA、RSA	ECDSA	SM2
SSL协议	OpenSSL	OpenSSL	国密SSL
数字证书	OpenSSL	-	国密数字证书

聚龙链系统架构



链

聚龙链 V0.8 版本

发布仪式

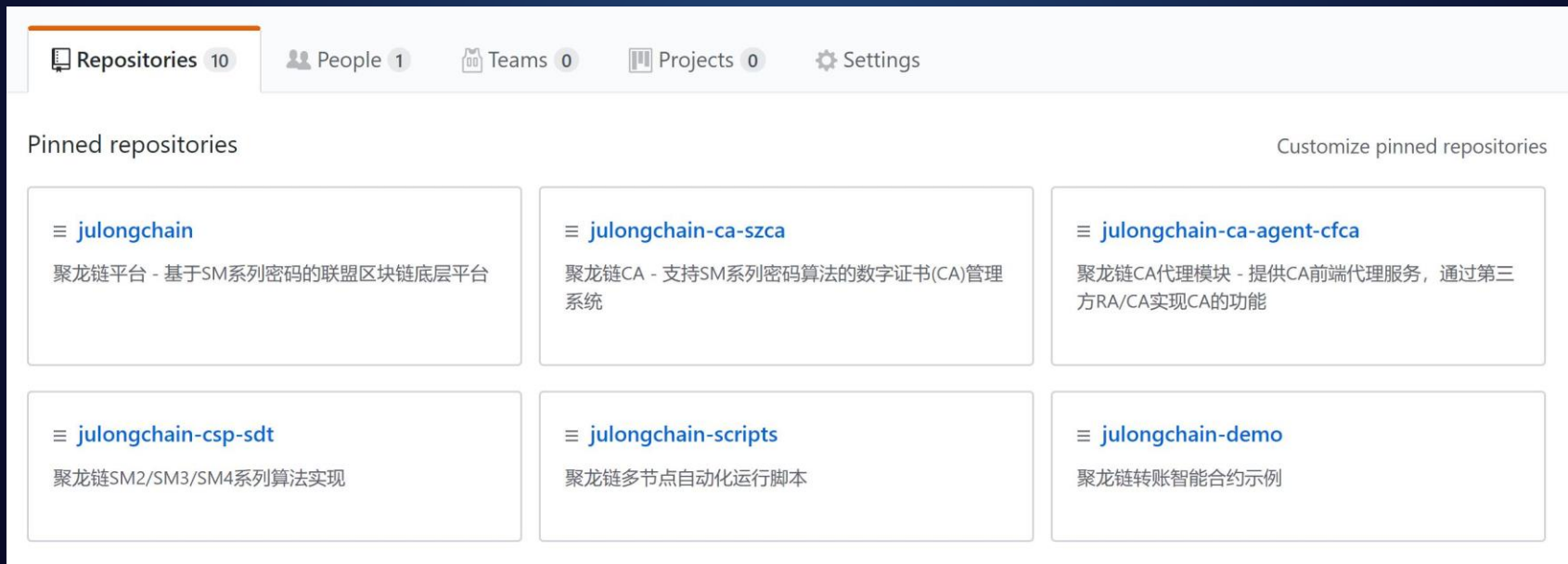
聚龙链



聚龙链

聚龙链开源，由深圳商密协会运维

<https://github.com/JulongChain>



The screenshot displays the GitHub profile page for the organization JulongChain. The top navigation bar includes links for Repositories (10), People (1), Teams (0), Projects (0), and Settings. The main section is titled 'Pinned repositories' and contains six repository cards arranged in a 2x3 grid. Each card shows the repository name, a menu icon, and a brief description. A link to 'Customize pinned repositories' is located in the top right corner of the pinned section.

Repository Name	Description
julongchain	聚龙链平台 - 基于SM系列密码的联盟区块链底层平台
julongchain-ca-szca	聚龙链CA - 支持SM系列密码算法的数字证书(CA)管理系统
julongchain-ca-agent-cfca	聚龙链CA代理模块 - 提供CA前端代理服务, 通过第三方RA/CA实现CA的功能
julongchain-csp-sdt	聚龙链SM2/SM3/SM4系列算法实现
julongchain-scripts	聚龙链多节点自动化运行脚本
julongchain-demo	聚龙链转账智能合约示例

谢谢观看