HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

Anniversary journey of TWGC GMSM TaskForce

David Liu, Senior Technology Architect, *Oracle*

我国制定密码法全面提升密码工作法治化水平

2019-10-26 18:56 来源： 新华社

新华社北京10月26日电（记者 王鹏）十三届全国人大常委会第十四次会议26日表决通过密码法，将自2020年1月1日起施行。密码法旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。

密码法共五章四十四条，重点规范了以下内容：第一章总则部分，规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施。第二章核心密码、普通密码部分，规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。第三章商用密码部分，规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。第四章法律责任部分，规定了违反本法相关规定应当承担的相应的法律后果。第五章附则部分，规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期。

密码法规定，国家对密码实行分类管理。密码分为核心密码、普通密码和商用密码。核心密码、普通密码用于保护国家秘密信息，属于国家秘密。商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

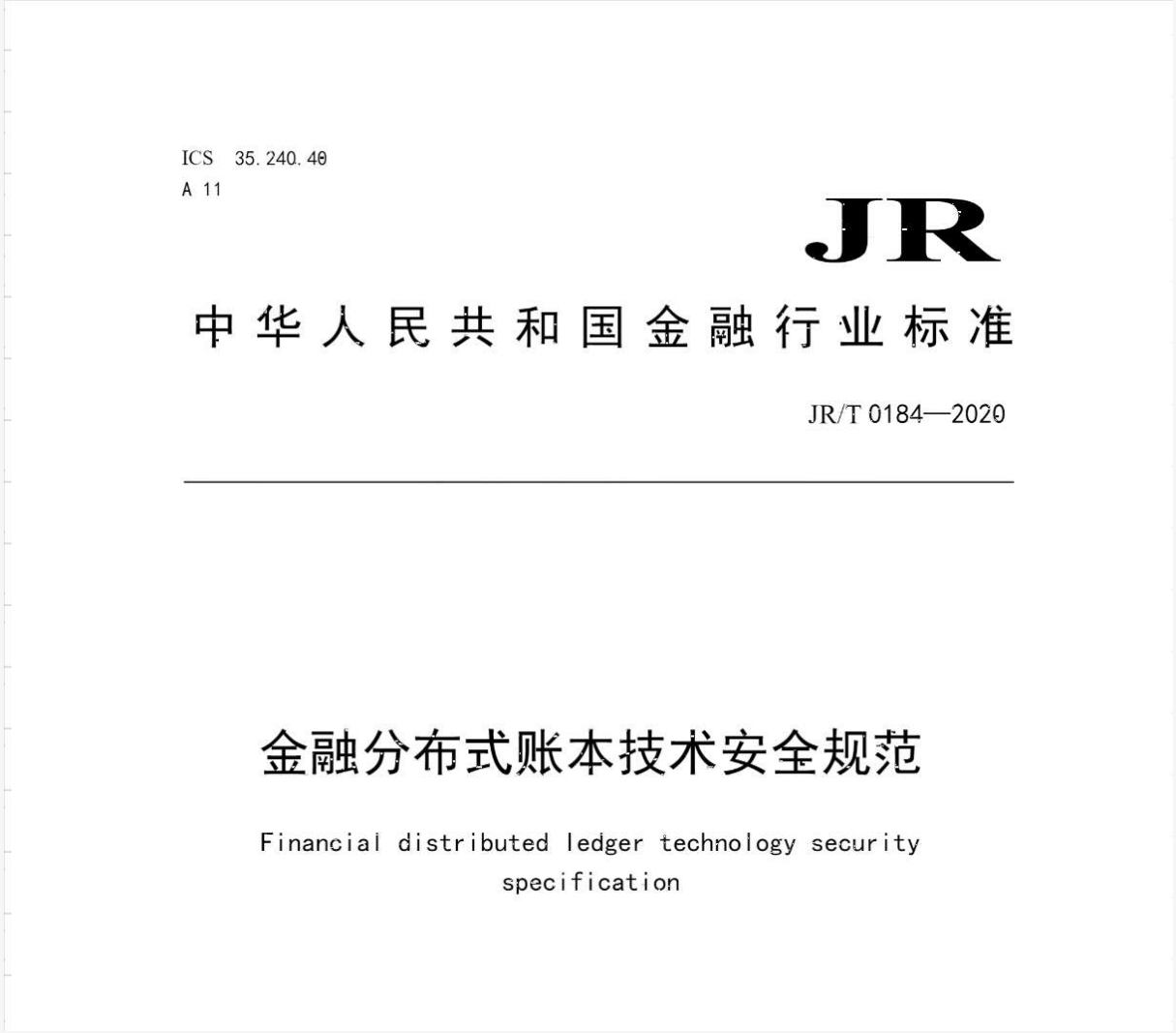
密码法规定，国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。

此外，为突显人才培养对于密码事业的重要性，密码法规定国家加强密码人才培养和队伍建设，对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

New Specification released

Noise from competitor

How we react



ICS 35.240.40

A 11

JR

中华人民共和国金融行业标准

JR/T 0184—2020

金融分布式账本技术安全规范

Financial distributed ledger technology security specification

HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

解析《金融分布式账本技术安全规范》Beta

A new initiative proposed by Jay Guo

Official release at github.com

Hyperledger-TWGC/fabric-evaluation-JRT0184

How we react on “Not satisfied”

本文档旨在从Hyperledger Fabric的角度，对中国人民银行发布的《金融分布式账本技术安全规范》文件进行梳理和解读，由Hyperledger中国工作组志愿者共同编写和审阅。

会议信息：

分工：（请在下方表格中填写个人信息，认领任务，每项一至多有多人认领，请自行沟通协调，进一步分工或协作时间完成）

章节	姓名+公司(可多人)
6 基础组件	吴旭(众享金联)，刘宇翔(Medtioncen),
7 基础软件	吴旭(众享金融)，王海龙（京东数科）
8 密码算法	朱建伟(小米金融)，张保佳(小米金融)，
9 节点通讯	朱建伟(小米金融)，张保佳(小米金融)，
10 账本数据	朱建伟(小米金融)，张保佳(小米金融)，
11 共识协议	郭剑鹏(树根互联)，
12 智能合约	刘宇翔(Medtioncen)，金志鹏(京东数科)
13 身份管理	曹龙(海尔数科)，刘宇翔(Medtioncen)
14 隐私保护	刘宇翔(Medtioncen)
15 监管支撑	吴旭(众享金联)，
16 运维要求	姚志超(众享金联)，吴旭(众享金联)
17 审计规则	郭剑鹏(树根互联)，李正涛(北理瑞渤)

- 原文：《金融分布式账本技术安全规范》规则原文
- 评估：结合Fabric对于规则实例的支持，可分为三种情况
  - 不满足：Fabric当前的版本或实现根据满足该条例的要求，应予以注意
  - 可满足：服务提供商需要通过额外的增值服务、业务逻辑，软/硬件设施、或/和基础改Fabric源码，满足条例要求
  - 满足：Fabric已经满足该条例要求
  - 不适用：与Fabric无直接关系，或Fabric不需满足条例的前提要求
  - 不清晰：条例中所描要求不够清晰，不足以做出判断
  - 定义：概念性条例，未做具体要求
- 相关措施：为了满足该条例要求，Fabric开发者，应用开发者，以及Fabric提供商应当采取的措施，以及需要注意的事项

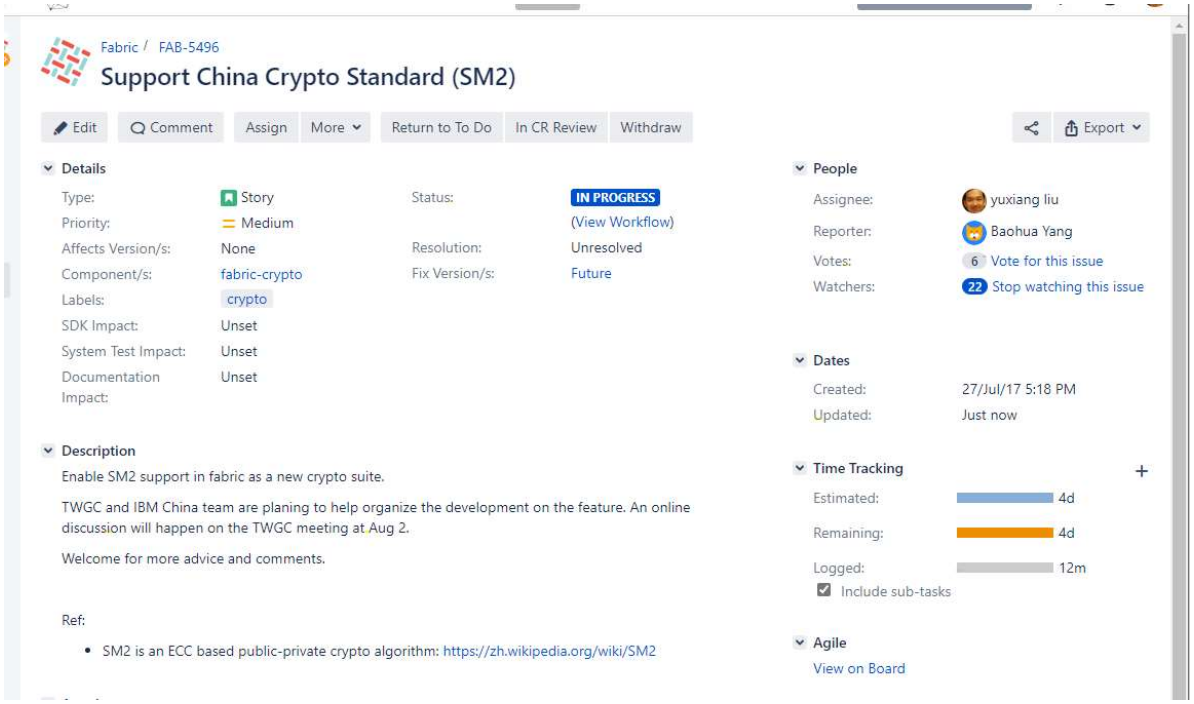
原文	评估	相关措施，备注

HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

TWGC 不曾放弃



Fabric / FAB-5496

Support China Crypto Standard (SM2)

Edit | Comment | Assign | More | Return to To Do | In CR Review | Withdraw | Export

Details

Type:	Story	Status:	IN PROGRESS (View Workflow)
Priority:	Medium		
Affects Version/s:	None	Resolution:	Unresolved
Component/s:	fabric-crypto	Fix Version/s:	Future
Labels:	crypto		
SDK Impact:	Unset		
System Test Impact:	Unset		
Documentation Impact:	Unset		

Description

Enable SM2 support in fabric as a new crypto suite.

TWGC and IBM China team are planing to help organize the development on the feature. An online discussion will happen on the TWGC meeting at Aug 2.

Welcome for more advice and comments.

Ref:

- SM2 is an ECC based public-private crypto algorithm: https://zh.wikipedia.org/wiki/SM2

People

Assignee:	yuxiang liu
Reporter:	Baohua Yang
Votes:	6 Vote for this issue
Watchers:	22 Stop watching this issue

Dates

Created:	27/Jul/17 5:18 PM
Updated:	Just now

Time Tracking

Estimated:	4d
Remaining:	4d
Logged:	12m

Include sub-tasks

Agile

View on Board

[FAB-5496] Support China Crypto Standard (SM2) - Hyperledger JIRA

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

Let us start the Formation

- Group Meetings
  - 2019-Q1
  - 2019-Q2
  - 2019-Q3
  - 2019-Q4
  - 2020-Q1
  - 2020-Q2
    - 2020-04-08
    - 2020-04-22
    - **2020-05-06**
    - 2020-05-20
  - 2020-Q3
  - 2020-Q4
  - 2021-Q1
  - 2021-Q2
- Chair Board

Minutes

1. Team development and Innovation @Jay Guo @Zhangjiong Xuan , @David Liu)
   a. Community Project开发者社区项目列表 @David Liu
   b. Fabric-sdk-node 2.1 status update @David Liu
      i. sdk-node-notes.pdf
2. Team i18n and Education (@Zhenhua Zhao @lidong guo @Yang Cheng)
   a. 文档翻译指引增加英文版 Getting Started
   b. 本周将增加FabricCA文档的翻译
   c. Document WG: Proposal about merge FabricCA doc to Fabric main doc
3. Team Collaboration and Scenarios (@Dorothy Cheng @Scott Long)
   a. <金融分布式账本技术安全规范>fabric解析
4. Team Event Organization (@Jay Guo , @Zhenhua Zhao @Scott Long)
   a. online meetup by zoom
   b.
      i. Hyperledger Tencent video channel QRCode
   c. 5月10日 腾讯跨链技术分享
   d. BaaS系列 （时间待定）
      i. 5月17日 联想
      ii. 5月23日 点融
      iii. 5月30日 华为
5. Fabric 2.x adoption status discussion @Baohua Yang
6. fabric-gm open governance proposal @David Liu @Scott Long

[2020-05-06 - Technical Working Group China - Hyperledger Confluence]

信息收集（完成）

这个阶段的主要工作是联络一批愿意为这个项目做出贡献的志愿者们，并收集已经在社区中进行的、或者完成了的国密化改造项目，进行公示。

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

*Not Full List

愿意参与到该项目未来贡献的朋友，请将您的联系信息增加到以下表格中：

姓名或者昵称	邮箱	微信	所属机构（可选）
郝利鹏	55643774@qq.com	17791285157	华为西安研究所
龙文选	hncslwx@qq.com	hncslwx	树根互联
伊文龙	wlong.yi@gmail.com	wlong_yi	
谢振元	xiezhenyuan@hotmail.com	xiezy16	
冯翔	411321681@qq.com	j2ee110	
严志伟	1957855254@qq. com	yzw-dream-sky	
刘地军	flyinox@163.com	flyinox	
陈桂军	877020907@qq.com	cgjmi47	
段焱明	itlabers@gmail.com	spirit_demon	
苏云龙	su881120@126.com	349297019	中国网安
王珂	ke@bll.io	569689535	北京大学
朱振博	zhenbo.zhu@easy-visible.com	magog-	易见天树
何弘宇	hongyu.he@easy-visible.com	hy883835	易见天树
王连诚	15484450@qq. com		民生银行
关志	guan@pku.edu.cn	13810631266	北京大学区块链研究中心
陈序	chenxu@wutongchain.com	czdyxs	苏州同济区块链研究院
朱芸生	545305939@qq.com	18190723501	
郑运荣	24733573@qq.com	z__y__r	人民银行
David Zhang	luckforzhang@foxmail.com	luckforzhang	
谢佳洋	cdfr1@163.com	13408644731	
邹云峰	zouyunfeng@peersafe.cn	zouyunfeng001	众享比特
刘子豪	19621362@qq.com	19621362	
刘鑫	97417168@qq.com	liusd20	
kEN	renyinew@gmail.com	wxid_7w8nwletqccc32	

已知开源国密改造 & beyond

项目实施

经过一个多月的讨论和工作细化，TWGC下属的Fabrci国密改造小组现在将志愿工作进行划分，即将进入代码编写阶段。
实际的工作内容由组长与组员协商沟通决定，由初始成员分配任务，issue认领的方式进行开发

1. 3个基础库小组 TWGC国密基础库分别贡献自北京大学，苏州同济区块链研究院，中国网安，每个基础库有独立的维护者和贡献者

2. Fabric本体小组 为了让国密基础库能够适配到Fabric当中，Fabric本身需要在可配置/可插拔设计上进行改进和完善

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

How to host our Source Code?

"Hi Ry,
Are we allowed to create a source code space for TWGC developers and potential brainstorm projects? We consider if we could have a code collaborate space only within the WG"

"OK, how about https://github.com/hyperledger/TWGC"

"Not exactly, TWGC have visions much more than that…"

*Designed Dialog

Hyperledger - Technical Working Group China

https://wiki.hyperledger.org/display/T... @hyperledger Verified

Repositories 25 Packages People 52 Teams 5 Settings

Pinned repositories

Customize pinned repositories

Hyperledger-TWGC
超级账本中国技术工作组
☆ 33 1

fabric-gm-wiki
Fabric国密项目 wiki
☆ 87 22

fabric-performance-wiki
TWGC Fabric 性能优化小组 wiki
☆ 20 5

tape
A Simple Traffic Generator for Hyperledger Fabric
Go ☆ 136 54

Learning-Material
☆ 5 1

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

And it is not an end…

国密基础库

- Hyperledger-TWGC/pku-gm: GMSSL (https://github.com/guanzhi/GmSSL) go 语言接口
- Hyperledger-TWGC/ccs-gm: 中国网安go语言国密库 (github.com)
- Hyperledger-TWGC/tjfoc-gm: GM SM2/3/4 library based on Golang (基于Go语言的国密SM2/SM3/SM4算法库) (github.com)

更多语言的国密基础库

Hyperledger-TWGC/java-gm: Java语言国密基础库 (github.com)

Hyperledger-TWGC/node-gm: GM crypto nodeJS library (github.com)

Hyperledger-TWGC/libsm: A Rust Library of China's Standards of Encryption Algorithms (SM2/3/4) (github.com)

Data security in-rest and in-transit

Https go package: Hyperledger-TWGC/net-go-gm (github.com)

Grpcs: Hyperledger-TWGC/grpc: 国密版Go language implementation of gRPC. HTTP/2 based RPC (github.com)

GM HSM： SDF interface compliance: Hyperledger-TWGC/sdf-go (github.com)

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

GM-interoperability

- How can we know all libraries are implemented in a right way?
- How do you know our code change in library break compliance?
- Hyperledger-TWGC/GM-interoperability: Home of interoperation tests among pku-gm, tjfoc-gm and ccs-gm, java-gm

“Sorry but wait…
How are these related to Hyperledger?”

Review after 信息收集

- Poor open source GMSM library options in market
- Fabric fork: out of maintain, hardcode, version locked
- Are these codes verifiable or trustable?

From Bottom-Up

HYPERLEDGER GLOBAL FORUM JUNE 8–10, 2021 | VIRTUAL EXPERIENCE

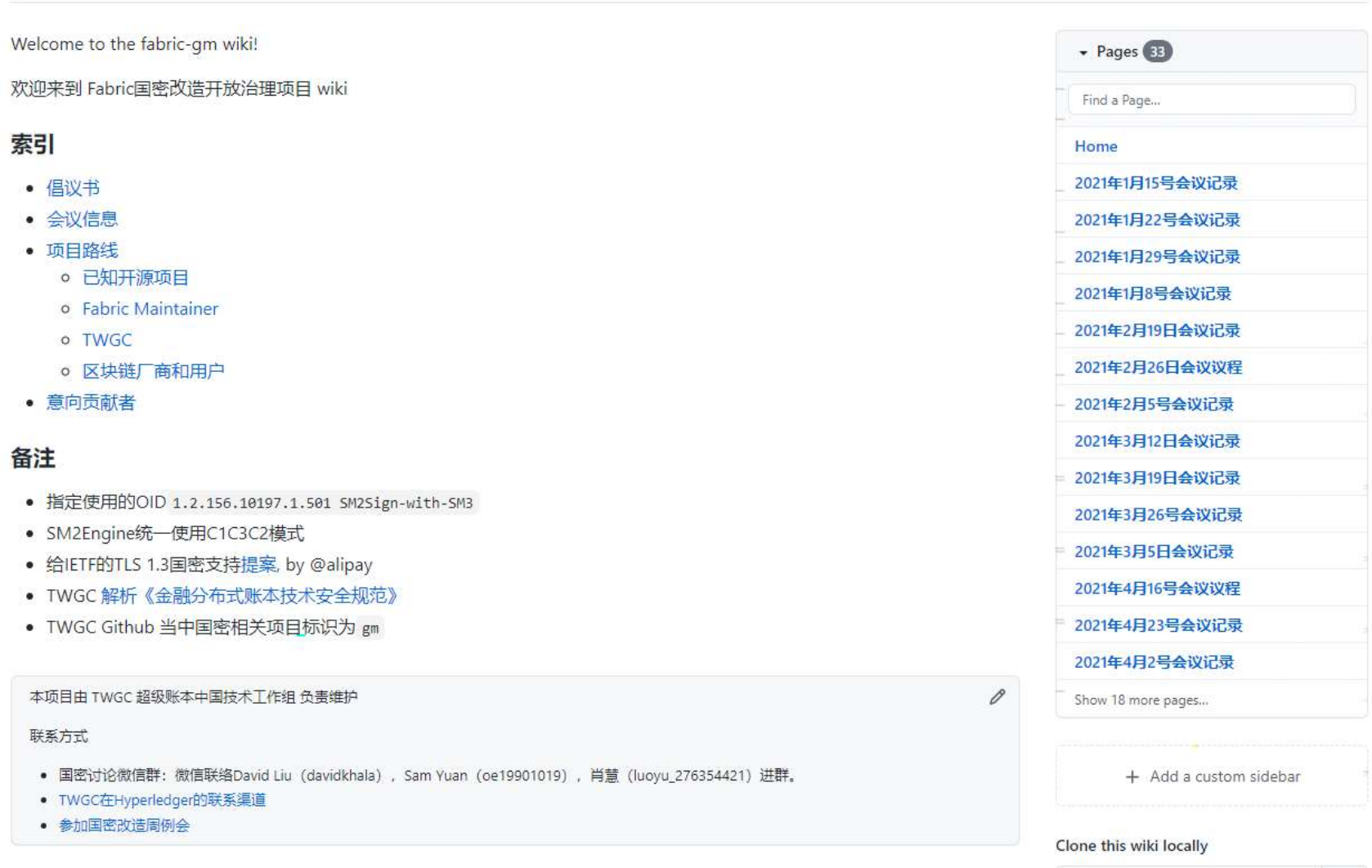
Roadmap May 2021

- Fabric-RFC
  - Fabric block-hash options
  - BCCSP
- Data in transit
  - TLS on https and grpcs
- Extend on language support
- SDF-go Continue Test

All Are Welcome

&

Come Join Us!



Welcome to the fabric-gm wiki!

欢迎来到 Fabric国密改造开放治理项目 wiki

索引

- 倡议书
- 会议信息
- 项目路线
  - 已知开源项目
  - Fabric Maintainer
  - TWGC
  - 区块链厂商和用户
- 意向贡献者

备注

- 指定使用的OID `1.2.156.10197.1.501 SM2Sign-with-SM3`
- SM2Engine统一使用C1C3C2模式
- 给IETF的TLS 1.3国密支持提案, by @alipay
- TWGC 解析《金融分布式账本技术安全规范》
- TWGC Github 当中国密相关项目标识为 `gm`

本项目由 TWGC 超级账本中国技术工作组 负责维护

联系方式

- 国密讨论微信群：微信联络David Liu（davidkhala），Sam Yuan（oe19901019），肖慧（luoyu_276354421）进群。
- TWGC在Hyperledger的联系渠道
- 参加国密改造周例会

Pages 33

Find a Page...

Home

2021年1月15号会议记录

2021年1月22号会议记录

2021年1月29号会议记录

2021年1月8号会议记录

2021年2月19日会议记录

2021年2月26日会议议程

2021年2月5号会议记录

2021年3月12日会议记录

2021年3月19日会议记录

2021年3月26号会议记录

2021年3月5日会议记录

2021年4月16号会议议程

2021年4月23号会议记录

2021年4月2号会议记录

Show 18 more pages...

+ Add a custom sidebar

Clone this wiki locally

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS


HYPERLEDGER
GLOBAL FORUM
June 8–10, 2021 | Virtual Experience
#hyperledgerforum