doi :10.3969/j.issn.1671-1122.2023.03.009

支持国密算法的区块链交易数据隐私保护方案

王晶宇[1]，马兆丰[1]，徐单恒[2]，段鹏飞[1]
（1. 北京邮电大学网络空间安全学院，北京 100876；2. 杭州安存网络科技有限公司，杭州 310000）

摘　要：随着区块链技术的发展，链上数据共享越来越重要。当前区块链交易数据在链上公开透明，存在隐私数据共享受限问题，而且 Hyperledger Fabric 平台缺乏国密算法的支持，在国内应用中受限。文章首先采用国密算法改造 Hyperledger Fabric 平台；然后提出交易数据隐私保护方案，以国密算法完成对交易数据的安全和限时共享；最后对改造的 Hyperledger Fabric 平台和提出的方案做系统实现和性能测试。实验结果表明，文章方法实现了对 Hyperledger Fabric 平台的国密改造，该方案的执行效率和系统性能均满足实际需求。

关键词：区块链；隐私保护；国密算法；Hyperledger Fabric

中图分类号：TP309　**文献标志码：**A　**文章编号：**1671-1122（2023）03-0084-12

中文引用格式：王晶宇，马兆丰，徐单恒，等 . 支持国密算法的区块链交易数据隐私保护方案 [J]. 信息网络安全，2023，23（3）：84-95.

英文引用格式：WANG Jingyu, MA Zhaofeng, XU Danheng, et al. Blockchain Transaction Data Privacy-Preserving Scheme Supporting National Cryptographic Algorithm[J]. Netinfo Security, 2023, 23(3): 84-95.

Blockchain Transaction Data Privacy-Preserving Scheme Supporting National Cryptographic Algorithm

WANG Jingyu[1], MA Zhaofeng[1], XU Danheng[2], DUAN Pengfei[1]
(1. *School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*; 2. *Hangzhou Ancun Network Technology Co., Ltd., Hangzhou* 310000, *China*)

Abstract: With the development of blockchain technology, the realization of data sharing on the chain has become an important application to promote the implementation of the blockchain industry. The transaction data of the current blockchain is open and transparent on the chain, with problems of restricted sharing. At the same time, considering that the Hyperledger Fabric platform is limited in domestic applications due to the lack of support of the national cryptographic algorithm, this paper transformed the Fabric platform by adopting the national cryptographic algorithm firstly. Secondly, a transaction data privacy-preserving scheme was proposed to complete the security and limited sharing of transaction

收稿日期：2022-10-19
基金项目：国家重点研发计划 [2020YFB1005500]；北京市自然科学基金 [M21034]
作者简介：王晶宇（1999—），女，内蒙古，硕士研究生，主要研究方向为区块链与隐私保护技术；马兆丰（1974—），男，甘肃，副教授，博士，主要研究方向为区块链理论与技术、区块链核心创新及应用；徐单恒（1994—），男，杭州，硕士，主要研究方向为区块链技术与应用；段鹏飞（1995—），男，山东，博士研究生，主要研究方向为区块链及安全技术。
通信作者：马兆丰 mzf@bupt.edu.cn

data with national cryptographic algorithm. Finally, the modified Fabric platform and the proposed solution were tested for system implementation and performance. The experimental results show that this paper completes the national cryptographic algorithm transformation of the Fabric platform, which ensures the correctness of various operations. The implementation efficiency and system performance of the privacy protection scheme also meet the practical requirements.

Key words: blockchain; privacy-preserving; national cryptographic algorithm; Hyperledger Fabric

0 引言

区块链技术起源于2008年[1]，是比特币的技术支撑。近年来，随着区块链技术的发展，各行业逐渐与其深度融合发展。“区块链+”的发展模式受到广泛关注，如区块链+教育[2]、区块链+医疗[3]等。区块链被广泛应用于数据共享[4]、信息溯源[5]、版权保护[6,7]、数据可信管理[8,9]等领域。在区块链应用的众多领域中，用户的隐私数据安全成为关注的重点。然而，区块链的公开性、透明性等特点会导致交易隐私数据的安全遭到威胁[10]。因此，保证链上用户隐私数据的安全性是区块链真正落地应用的关键。目前，国内外学者针对区块链交易数据的隐私保护做了大量的工作。文献[11]提出了一种基于差分隐私算法和账户映射技术的隐私保护方案 BLDP-AM 来解决交易数据的泄露问题，该方案通过重新设计数据扰动机制来构造BLDP算法，从而保护交易数据的隐私。文献[12]提出了一种基于群签名与属性加密的区块链可监管隐私保护方案，该方案利用群签名实现交易的可监管，对数据进行属性加密来保证链上数据的隐私保护。文献[13]提出了一种基于联盟链的个人数据隐私保护方案，该方案利用改进后的 Paillier 同态加密算法来加密存储原始数据，利用分布式私有集群来存储加密数据，通过链下存储和链上传输协同，提高数据传输效率。文献[14]结合区块链、群签名、非对称加密设计了一种医疗数据隐私保护方案，可以实现医疗机构间可靠的医疗数据共享，保证数据的隐私性。

针对区块链中用户交易隐私数据安全共享的问题，本文采用国密算法来解决。国密算法作为国内自主研发的一套数据加密算法，具有高安全性、高效性、稳定性等特点，目前在隐私保护、身份认证、数据加密等方面具有重要作用。文献[15]提出了一种基于无证书联合签名的电子发票真伪公开验证方案，该方案利用SM2加密算法对电子发票中的用户隐私数据进行保护，并利用SM2签名算法实现了电子发票数据的公开核验。文献[16]基于国密算法和区块链提出了一种移动端的安全电子身份证及身份认证协议，该协议采用SM2签名算法和SM3哈希算法实现用户身份的安全认证。文献[17]将SM4对称加密算法应用于车载PEPS和EMS的动态加密安全认证来提高效率。利用国密算法高效性和高安全性的特点，本文将其应用到区块链中，提出一个基于国密算法的区块链交易数据隐私保护方案。该方案将采用SM4对称加密算法作为加密手段，对链上必要的交易数据进行加密，同时规定数据的有效时间，利用SM2公钥加密算法来实现时间校验。

另外，区块链目前的底层密码学算法采用的是国际通用标准。以Hyperledger Fabric为例，其涉及的加密算法主要是ECDSA 签名算法、ECDH加密算法、AES对称加密算法和SHA-256哈希算法。一方面，由于区块链的安全性依赖于底层密码学算法的强度，因此安全高效的加密算法是区块链持续安全发展的关键。根据目前的研究，SM2、SM3算法的安全性略高于ECC-256和SHA-256算法，SM4算法的加解密速度略高于AES算法[18-20]。另一方面，Hyperledger Fabric作为联盟链的代表平台，其应用十分广泛。但是目前Hyperledger Fabric平台并没有正式地提供国密算法的支持，导致Hyperledger Fabric平台无法进一步在国内商用。因此，采用国密算法来改造Hyperledger Fabric平台底

层的密码学算法是持续发展区块链技术十分关键的一步，也是必要的一步。

综上所述，本文利用SM2、SM3、SM4等国密算法来替换联盟链代表平台Hyperledger Fabric 1.4版本的底层密码学算法，改造任务分为3个部分，包括对Hyperledger Fabric区块链网络、Fabric-CA和Fabric-SDK的改造。同时基于国密算法，提出一种区块链交易数据隐私保护方案，用于对隐私数据进行保护。本文采用SM4对称加密算法对隐私数据加密，保证只有交易接收者能够获取隐私数据。同时利用SM2公钥加密算法来实现对数据有效期的验证，适用于投标、文件下载等场景。最后，本文系统实现国密算法改造后的Hyperledger Fabric平台，仿真实现基于国密算法的区块链交易数据隐私保护方案，并对其进行功能测试与性能分析。

1 背景知识

1.1 区块链技术

区块链本质上是一种分布式账本技术，以去中心化的方式对交易进行存储与验证，由大量的对等节点来共同维护其一致性[21]，从而使得链上交易数据公开透明。区块链中的交易数据以区块形式打包存储，各区块之间通过哈希值相连，保证了链上数据的不可篡改性和可追溯性[22]。由于区块链消除了对第三方参与验证和记录交易的依赖性[23]，因此可以作为现有应用系统的信任基础，在金融、教育、医疗等领域发挥重要作用。

密码学技术作为区块链的核心，用于确保交易信息的完整性、不可抵赖性和不可篡改性。区块链技术底层的密码学算法主要包括哈希算法和非对称加密算法。利用哈希算法对前一个区块进行哈希计算，将得到的固定长度摘要保存在当前区块中，从而实现区块链的完整性和不可篡改性。在非对称加密算法中，交易发起者会利用自己的私钥对交易进行数字签名，来确保交易传输的完整性和交易发送者的不可抵赖性[24]。

1.2 国产密码算法

国产密码算法是由我国公开发布的一系列商用密码算法，其中使用最为广泛的包括SM2椭圆曲线公钥密码算法、SM3密码杂凑算法和SM4分组密码算法。这3种国密算法可以满足较多应用的安全性需求[25]。

SM2椭圆曲线公钥密码算法[26]主要与国际通用的ECC算法和RSA算法相对应。SM2算法包括公钥加密算法、密钥交换协议和数字签名算法三个部分[27]。本文主要采用SM2数字签名算法来替换区块链底层数字签名算法。相对于ECDSA算法来说，SM2数字签名算法安全性更高[18]。

SM3密码杂凑算法是一种哈希算法，通过单向散列函数将任意长度的消息压缩成长度为256 bit的摘要，其中消息分组长度为512 bit，其安全性高于MD5算法和SHA-1算法。另外，相较于国际通用的SHA-256算法，SM3算法的结构更为复杂，可以更有效地抵抗具有强碰撞性的差分分析、弱碰撞性的线性分析和比特追踪法等，其安全性较高，实现效率略高于或等同于SHA-256算法[18]。

SM4分组密码算法是一种对称加密算法，采用对称密钥对消息进行加解密。SM4算法由加解密算法和密钥扩展算法组成，二者均采用32轮非线性迭代结构[28]。相比于高级加密标准AES算法，SM4算法可以有效抵抗差分攻击、线性攻击、积分攻击等多种密码分析，具有较强的安全冗余度[29]。

根据文献[29]给出SM4算法的密钥扩展算法和加解密算法。密钥扩展算法用于根据初始密钥生成轮密钥。$MK=(MK_0,MK_1,MK_2,MK_3)\in(Z_2^{32})^4$为初始密钥，则轮密钥生成过程如下：

已知系统参数$FK=(FK_0,FK_1,FK_2,FK_3)$，固定参数$CK=(CK_0,CK_2,\cdots,CK_{31})$，$T(\cdot)=L'(\tau(\cdot))$是一个可逆变换，其中$\tau$是非线性变换，$L'$是线性变换。则轮密钥生成方法为$rk_i=K_i+4=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus CK_i),(i=0,1,2,\cdots,31)$，其中，$K_i=MK_i\oplus FK_i,(i=0,1,2,3)$。将轮密钥生成算法记作$rk=Gen_rk(MK,FK,CK)$。

SM4算法的加密运算过程如下：已知明文输入是$M=(X_0,X_1,X_2,X_3)\in(Z_2^{32})^4$，轮密钥是$rk=(rk_1,rk_2,\cdots,rk_{31})(Z_2^{32})^{31}$，

可逆变换是$T(\cdot)=L(\tau(\cdot))$，其中τ是非线性变换，L是线性变换。则加密算法的运算过程：$X_{i+4}=X\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)$,$(i=0,1,\cdots,31)$，密文输出$C=(Y_0,Y_1,Y_2,Y_3)=(X_{35},X_{34},X_{33},X_{32})$。

将加密算法的运算过程记为$C=SM4_Enc(M,rk)$。

SM4算法的加解密算法的变换结构相同，只是轮密钥的使用顺序不同。解密算法的轮密钥顺序为$(rk_{31},rk_{30},\cdots,rk_1)$。将解密算法的运算过程记为$M=SM4_Dec(C,rk)$。

1.3 Hyperledger Fabric

Hyperledger Fabric是一个由Linux 基金会托管的企业级开源许可区块链平台，目前在区块链领域内是联盟链的代表性平台[30]。Hyperledger Fabric平台的体系架构高度模块化，因此各模块之间可以独立升级，以提高可扩展性。Hyperledger Fabric平台由Fabric网络、Fabric-CA和Fabric-SDK三部分组成，各部分之间通过交互连接得到完整的Fabric平台交易流程[31]。

首先，Fabric-SDK应用程序客户端会向证书颁发机构Fabric-CA申请登记注册，获取身份证书。然后，客户端可以向Fabric区块链网络中的背书节点提交交易提案。当客户端收集到足够的背书结果后，会将其打包并向排序节点发起交易。排序节点使用PBFT共识算法[32]对所有的交易打包并生成区块。最后，排序节点使用Gossip协议将区块广播给所有的对等节点，每个对等节点验证块内交易无误后会更新分布式账本。

Fabric平台提供了客户端SDK、链码API等调用接口，向Fabric应用提供身份管理、账户管理等服务。值得注意的是，在Fabric区块链网络交易流程涉及的每一个交易环节中，都存在数字签名和签名验证操作，以确保客户端私钥的所有权和交易的不可抵赖性。而交易的签名与验证的功能是由底层安全与密码服务所提供。该服务包含BCCSP组件，为Fabric提供了密钥生成、消息的签名与验证、哈希算法和加解密等服务。因此，利用国密算法替换Fabric底层的密码学算法最核心的研究内容是BCCSP底层实现基于国密算法的接口[33]。

2 国密算法改造 Fabric 平台

本章将研究利用基于Go标准的国密算法来替换Fabric平台的底层密码学算法，包括基于SM2的数字签名与验证算法、基于SM3的哈希算法和基于SM4的加解密算法。国密算法的实现将采用同济区块链研究院的开源代码[34]。Fabric平台的改造将从Fabric区块链网络、Fabric-CA和Fabric-SDK三方面展开，下面将详细给出改造方案。

2.1 Fabric 区块链网络改造

改造Fabric区块链网络的密码学算法主要的工作是实现 BCCSP模块下的国密算法接口以及利用Factory生成国密BCCSP实例并修改相关应用的调用接口，使其调用国密算法接口。

BCCSP模块下需要实现的国密算法接口包括SM4加解密算法、SM3哈希算法、SM2数字签名和验证算法、SM2证书和标准X.509证书转换算法。Factory包的作用是生成BCCSP实例，需要将Factory的默认选项改为国密，并添加gmfactory.go文件来实现BCCSPFactory接口，实现国密BCCSP的创建，如图1所示。

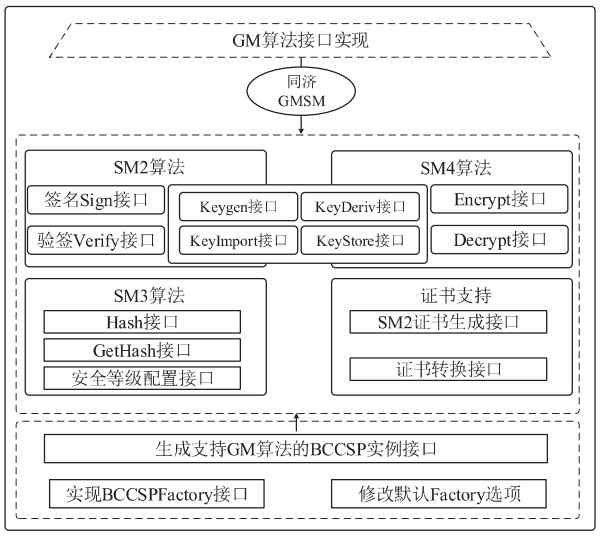


图 1 BCCSP 模块下国密算法接口实现

接下来需要实现Fabric上层应用支持国密的相关调用接口。首先，在网络启动之前需要利用工具cryptogen为网络中的节点生成静态的国密证书和密钥。因此需要

对common包下的工具cryptogen进行修改，包括CA结构体、证书的生成、MSP证书等，具体要修改的文件夹是ca、msp和csp。然后，将core、peer、orderer、gossip等包下调用的密码算法接口修改为国密BCCSP提供的相关接口，保证交易过程中的交易验证、区块生成、区块分发和链码调用等应用支持国密算法。

2.2 Fabric–CA 改造

Fabric-CA是Fabric平台的数字证书颁发机构，主要功能包括用户注册、数字证书颁发和数字证书管理等。与Fabric区块链网络中的cryptogen工具不同，Fabric-CA可以为网络节点动态生成证书。改造Fabric-CA使得生成支持国密类型的证书。Fabric-CA分为Client端和Server端，Client端负责向Server端发出签发证书的请求并存储证书，Server端负责签发并管理国密证书。证书动态生成过程如图2所示。

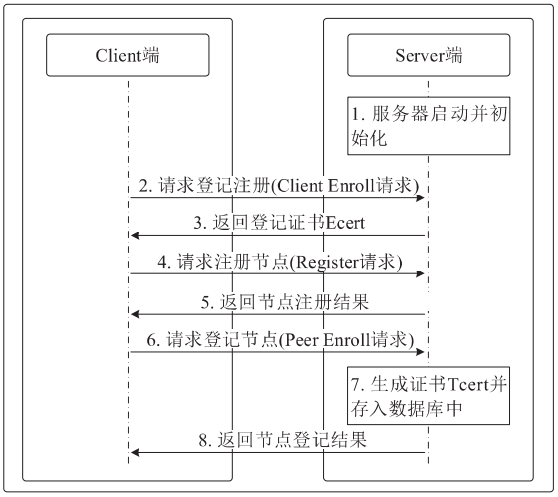


图 2 Fabric–CA 证书动态生成过程

根据证书生成过程，从底层算法实现和上层应用的初始化、注册、登记等方面修改调用接口以实现支持国密算法的调用。首先需要修改Fabric-CA-Server和Fabric-CA-Client中的config.go文件，将BCCSP的默认实例改为GM，并将CSR中的算法指向为国密。然后在lib包下申请证书请求与签发证书流程的调用接口更改为国密算法，并添加gmca.go文件实现生成证书、对证书签名等支持国密算法的接口。接着，修改util包下相关调用接口为国密算法，并添加token获取和证书管理等方法。最后，替换对Fabric包的引用以修改依赖包vendor，实现对国密算法的支持。

2.3 Fabric–SDK 改造

Fabric-SDK是与Fabric网络和Fabric-CA进行交互的客户端应用程序。本文主要针对Fabric-SDK-GO版本的语言开发包进行国密改造。Fabric-SDK-GO的改造需要国密TLS的支持，本文将采用同济区块链研究院开源的gmtls代码[35]。Fabric-SDK-GO下包含了internal、third-party、pkg等包。internal包中主要是Fabric和Fabric-CA的源码，按照前两节的内容将其均修改为国密算法接口。pkg是Fabric-SDK的主要功能包，包括交易管理、链码管理、身份管理等。因此，改造Fabric-SDK最核心的部分就是对pkg的修改。

pkg包下对相关接口调用的部分修改如图3所示，主要包括对client、common、core和fab等相关密码算法接口的修改。其他需要修改的部分就是将相关证书管理接口更改为国密接口。最后，将相关依赖添加到vendor包下。

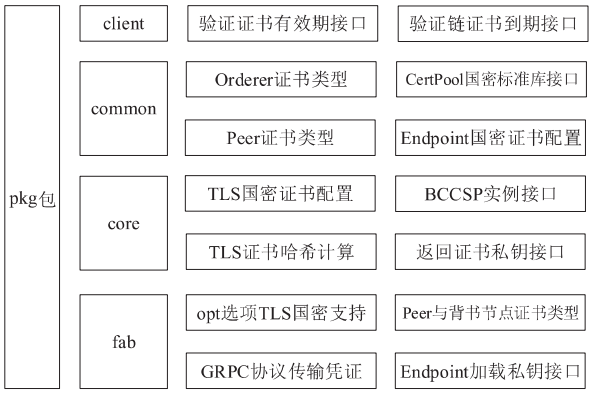


图 3 pkg 包下部分接口的修改

3 基于国密算法的交易数据隐私保护方案

基于第2章提出的国密区块链架构，本章将提出一种基于国密算法的交易数据隐私保护方案。在该方案中，用户数据被划分为普通数据与隐私数据，数据提供者自行决定数据的类型。普通数据可以直接上链，不会对用户隐私造成威胁。隐私数据由用户利用SM4

对称加密算法进行加密，保证其在链上的安全性。本文采用区块链隐蔽信道对交易双方的SM4对称密钥进行传输，可以保证对称密钥的隐蔽性、不可篡改性和抗干扰性[36]。另外，本文利用SM2加密算法来验证隐私数据的有效性。即只有在规定的时间之内才能解密数据，一旦超出时间该数据就无法被解密，保证数据的时效性。该功能的实现可以满足知识产权保护、招标投标等应用场景。本章首先给出系统模型，再给出方案的详细设计。

3.1 系统模型

根据业务场景需求，首先给出基于国密算法的交易数据隐私保护方案的系统模型，如图4所示。该系统模型由数据提供者、国密区块链网络和数据接收者3部分组成。

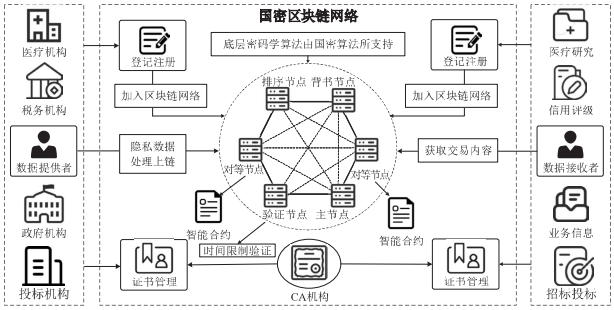


图 4 系统模型

1）数据提供者是指向需求方提供数据的医疗、税务、政府和投标等机构；数据提供者将数据分为普通数据和隐私数据，在上传到区块链网络前对隐私数据进行加密处理。

2）国密区块链网络是指利用国密算法替换Fabric平台底层密码学算法的Fabric区块链平台；数据提供者通过登记注册后，作为对等节点添加到网络的不同组织中；区块链网络中存在验证节点，该节点的主要功能为验证签名的有效性和验证交易的正确性；对等节点可以发起交易调用智能合约实现相关密文数据的上传和数据的加密共享，保证交易数据的安全性、完整性和时效性。

3）数据接收者是指实现各种业务应用而需要数据的一方，包括利用用户数据进行医疗研究、对用户信用评级、获取用户个人信息完成各种业务、项目的招标投标等；数据接收者通过发起数据请求交易来获取密文数据，在客户端可以解密所获取数据。

3.2 方案设计

根据系统模型，本文设计了详细的基于国密算法的交易数据隐私保护方案。方案中涉及的参数由表1给出说明。

表 1 参数说明

符号	符号定义
FK	SM4 中 4 个 8 字节的系统参数
CK	SM4 中 32 个 8 字节的固定参数
M_p	待加密的用户隐私数据
C_p	SM4 加密后的密文
MK	SM4 初始密钥
MK''	经过编码调制后的对称密钥
$Cert$	CA 机构向用户颁发的数字证书
sk_v	区块链中验证节点的 SM2 私钥
pk_v	区块链中验证节点的 SM2 公钥
sk_i	数据提供者客户端的 SM2 私钥
pk_i	数据提供者客户端的 SM2 公钥
$SM2\_Enc(m,pk)$	SM2 的加密算法
$SM2\_Dec(c,sk)$	SM2 的解密算法
ID	区块链交易 ID
$payload$	区块链交易数据内容
$Timestamp$	区块链交易时间戳

基于国密算法的区块链交易隐私数据方案的具体流程如图5所示。

1）隐蔽传输规则初始化：数据提供者和数据接收者事先初始化生成隐蔽传输时对消息的处理规则，包括编码表 $R(R_1,R_2,\cdots,R_n)$ 和调制符号表 $S(S_1,S_2,\cdots,S_n)$。

2）密钥生成：数据提供者生成SM4对称加密算法所需要的初始密钥，即 $MK=(MK_0,MK_1,MK_2,MK_3)\in(Z_2^{32})^4$。

3）加密：数据提供者根据初始密钥生成轮密钥 $Gen\_rk(MK,FK,CK)\rightarrow rk$；利用轮密钥 rk 加密用户隐私数据 M_p，得到密文 C_p，即 $SM4\_Enc(M_p,rk)\rightarrow C_p$。

4）生成隐蔽信息：数据提供者根据与数据接收者

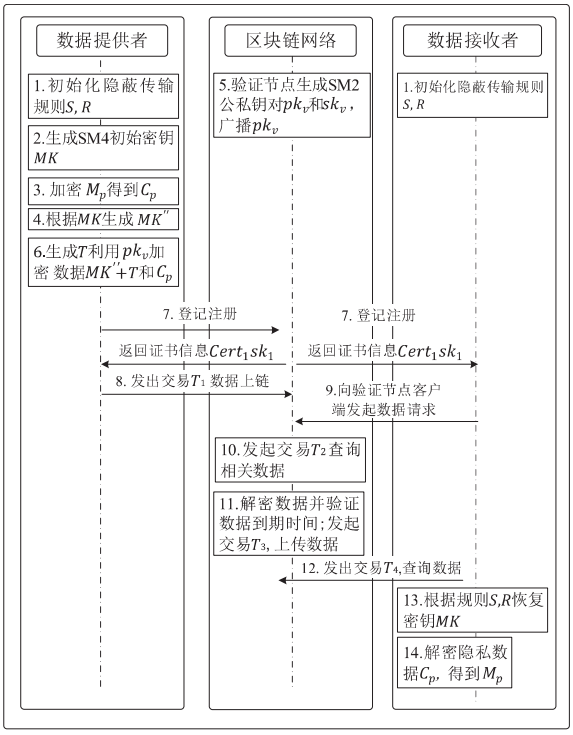


图 5 方案设计流程

约定的消息处理规则对初始密钥 MK 进行编码与调制，得到隐蔽信息 MK''，即 $S(R(MK)) \rightarrow MK''$。

5）公私钥对生成：区块链网络中的验证节点根据系统参数获取到SM2算法的公私钥对 (pk_v, sk_v)，并对 pk_v 进行广播公开，sk_v 本地存储。

6）加密数据：数据提供者生成限制解密隐私数据的时间 T。然后利用验证节点的公钥 pk_v 分别对数据 $MK''+T$ 和 C_p 进行加密，得到密文 C_1 和 C_2。即 $SM2\_Enc(MK''+T, pk_v) \rightarrow C_1$，$SM2\_Enc(C_p, pk_v) \rightarrow C_2$。

7）用户登记注册：数据提供者和数据接收者对应的SDK客户端分别向证书颁发机构申请登记注册，获取数字证书 $Cert_1$、$Cert_2$ 和签名私钥 sk_1、sk_2。

8）数据上链：数据提供者客户端发起交易 T_1，将加密后的密文 C_1 和 C_2 上传到区块链中。具体的交易形式为 $T_1 = \{ID_1, payload(C_1, C_2), Timestamp_1\}$。

在上传区块链之前，各个记账节点利用数据提供者客户端的公钥 pk_1 对交易 T_1 的签名进行验证，验证通过则将交易加入区块；验证失败则拒绝将交易上传到区块链中。

9）数据请求：数据接收者需要数据提供者上传的隐私数据 M_p 时，其客户端向验证节点客户端发起数据请求。

10）验证节点数据查询：验证节点客户端接收请求后，发起交易 T_3，查询区块链中的数据 C_1 和 C_2，即 $T_2 \rightarrow (C_1, C_2)$。具体的交易形式为 $=\{ID_2, payload(Null), T_2, Timestamp_2\}$。

11）时间验证：验证节点利用私钥分别解密 C_1 和 C_2，即 $SM2\_Dec(C_1, sk_v) \rightarrow MK''+T$，$SM2\_Dec(C_2, sk_v) \rightarrow C_p$。

解密后，验证节点判断是否超过当前时间。若超出当前时间，验证节点客户端则给数据需求者返回 $Invalid$。否则发起交易 T_3，上传 MK'' 和 C_p，具体的交易形式为 $T_3 = \{ID_3, payload(MK'', C_p), Timestamp_3\}$。

12）数据接收者数据查询：验证节点客户端向数据接收者发起数据可查询的信息，然后数据接收者发起交易，查询区块链中的数据 MK'' 和 C_p，即 $T_4 \rightarrow (MK'', C_p)$。具体的交易形式为 $T_4=\{ID_4, payload(Null), Timestamp_4\}$。

13）密钥恢复：数据接收者根据与数据提供者约定的消息处理规则对隐蔽信息进行解调与解码，得到初始对称密钥 MK，即 $R(S(MK'')) \rightarrow MK$。

14）解密：数据接收者根据恢复出的初始对称密钥 MK 生成轮密钥 $Gen\_rk(MK, FK, CK) \rightarrow rk$；利用轮密钥 rk 解密用户密文隐私数据 C_p 得到解密文 M_p，即 $SM4\_Dec(C_p, rk) \rightarrow M_p$。至此，数据提供者与数据接收者的隐私数据共享过程完成。

通过上述方案，用户隐私数据在上传到区块链之前进行SM4对称加密处理，可实现隐私数据的链上安全性。SM4对称密钥采用隐蔽信道传输，可实现密钥的不可篡改性、安全性和完整性。同时，由于对用户数据进行分类，只有隐私数据进行加密，普通数据可以直接上链，提高了数据共享的效率。数据需求者在获取数据时由验证节点来验证时间的有效性，保证了隐私数据的时效性。底层区块链网络采用国密算法改造后的Fabric平台，进一步加强了区块链交易的安

全性。

4 系统实现

本文实验的主要工作是搭建国密算法改造后的Hyperledger Fabric1.4区块链平台并基于该平台仿真实现基于国密算法的交易数据隐私保护方案。本章首先给出实验环境，然后分别实现两项工作，最后对实验结果进行分析。

4.1 实验环境

本文的实验均在虚拟机环境中执行，采用的虚拟机是VMware Workstation Pro 16。虚拟机的环境配置为Ubuntu20.04操作系统，处理器内核8个，内存8GB。主机配置为Intel(R)Core(TM)i7-8550U CPU@1.80 GHz 2.00GHz。Ubuntu操作系统中Fabric所需的环境配置包括go1.15.6、docker20.10和docker-compose2.3等服务。对于Hypeledger Fabric联盟链的国密算法改造采用的是1.4版本。本文隐私保护方案中的智能合约采用go语言进行开发。

4.2 实验实现

本次实验首先对Hyperledger Fabric1.4进行国密改造，然后在此基础上实现提出的隐私保护方案。利用SM2签名算法、SM3哈希算法和SM4对称加密算法替换了Fabric中使用的通用算法，从而保证了生成证书、签名、验签、哈希等操作都通过调用国密算法接口来实现。本文主要测试验证国密证书是否有效生成和Fabric网络的启动是否正常。然后在该Fabric平台的基础上，模拟实现了提出的交易数据隐私保护方案。本文主要测试验证该方案的可行性。

4.2.1 国密算法证书生成

国密算法证书可以通过cryptogen工具静态生成和Fabric-CA动态生成。因此，此处的测试验证国密证书的有效生成包含两部分。第一部分是利用cryptogen在终端执行生成静态证书的命令，为Fabric网络中的节点生成静态证书。证书的签名算法指向1.2.156.10197.1.501，该标识是由国家商用密码标准规定，指向SM2证书中的签名算法。

第二部分是利用Fabric-CA容器为节点生成动态证书。启动容器后，fabric-ca-server会执行服务器初始化，生成根证书和私钥。然后各节点通过fabric-ca-client命令来生成证书。证书内容中签名算法同样指向SM2签名算法。

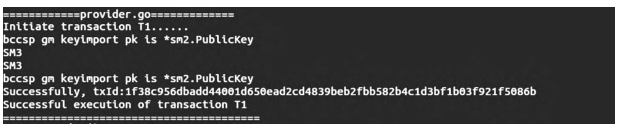
综上所述，Fabric网络和Fabric-CA成功替换为国密算法来生成证书。

4.2.2 国密改造后的 Fabric 网络启动

通过编写脚本network.sh分别执行Fabric国密区块链网络的节点创建、网络启动、加入通道、安装链码和发起一次交易等操作，来测试验证Fabric网络是否正常启动。执行结果显示，测试完成了fabric网络创建、容器启动、组织加入通道和链码的安装，发起交易也查询到了对应的记录。可以证明Fabric网络的启动正常。

4.2.3 隐私保护方案的实现

本文方案的实现将采用go项目来完成。首先编写数据提供者客户端代码provider.go来实现隐私数据的相关处理，并分别编写上传数据、数据请求和数据查询的链码操作；然后编写验证节点客户端代码verify.go来实现对密文的处理和时间的校验；最后编写数据接收者客户端代码receiver.go来发起数据请求并对接收的数据进行处理。另外利用改造后的SDK-Go来实现创建通道，安装、实例化和调用链码等，从而进行相关业务逻辑操作。本文方案需要编写的链码操作包括：init()、create()、update()和query()。Init()实现链码的实例化，create()和update()实现数据的上传与更新，query()实现数据的查询。该项目在go后端直接命令行调用，根据终端日志输出可以得出各端执行流程成功，如图6所示。



a）数据提供者运行结果

b）验证节点运行结果

c）数据接收者运行结果

图 6 隐私保护方案各阶段执行结果

4.3 结果分析

本文采用go提供的时间包对国密算法进行改造生成Fabric平台，利用JMeter测试工具来对提出的隐私保护方案进行性能测试，并根据测试结果进行分析。

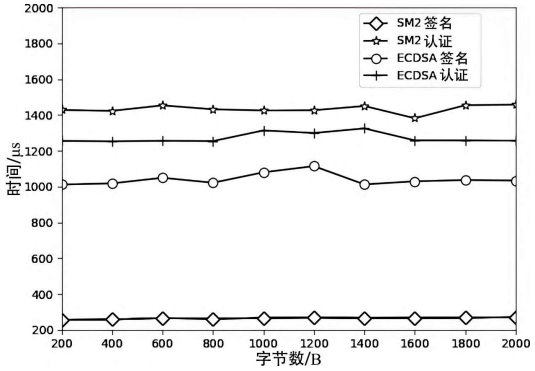
为了体现国密算法改造的Fabric平台的性能，本文测试了国密Fabric与原生Fabric的网络启动时间和利用SDK客户端发起交易的时间。网络启动时间包括静态证书生成、docker容器创建、加入通道、安装实例化链码和调用链码的操作。测试网络启动时间的方式为编写执行脚本fabric_gm.sh和fabric.sh并测试其运行5次的平均时间。编写测试代码fanric-main.go来实现利用Fabric-SDK-Go执行创建并加入通道、安装实例化和调用链码的操作。

运行时间如表2所示，国密Fabric网络平均执行时间为13.302 s，原生Fabric网络平均执行时间为12.337 s。相较于原生Fabric网络，国密Fabric网络的启动时间增加了7%。SDK发起交易时间只包含调用链码的执行时间，根据表2可得，经过国密改造后的Fabric-SDK调用链码时间相比于原生的SDK发起交易时间增加了13.28 ms。二者的网络启动与SDK发起交易时间差异均在可接受的范围内。

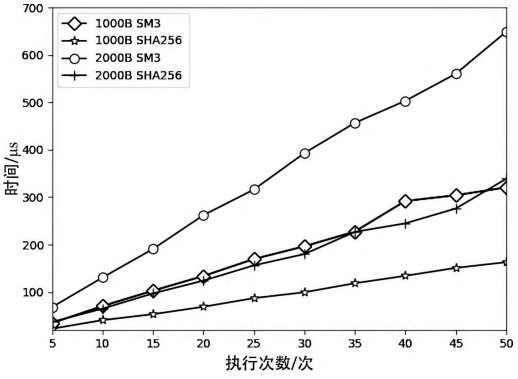
表 2 运行时间对比

	国密 Fabric 平台	原生 Fabric 平台
网络启动执行时间 /s	13.302	12.337
SDK 发起交易时间 /ms	33.86	20.58

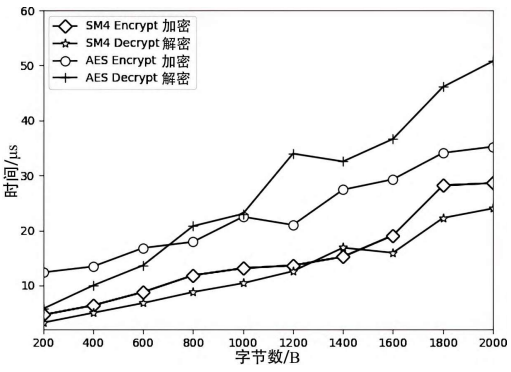
根据测试结果可以得出，国密改造后的Fabric平台会比原生Fabric平台的性能开销大。其可能的原因是国密算法和国际标准算法的性能存在差异。本文对两种算法的性能进行了测试，结果如图7所示。



a）SM2 与 ECDSA 的签名与验证时间测试



b）不同次数下 SM3 和 SHA256 哈希时间测试



c）SM4 与 AES 加解密时间测试

图 7 国密算法时间测试

根据图7a）得出，SM2和ECDSA的签名与验证算法执行时间不会随着字节的增多而增加，始终处于一个平均状态。SM2签名算法效率优于ECDSA，而验签算法效率略次于ECDSA。

根据图7b）得出，SHA256和SM3哈希算法在不

同字节数下会有不同的效率，其中SHA256算法的效率略优于SM3算法。随着调用次数的增加，SM3和SHA256的运行时间也呈线性增长。但SM3增长的速度比SHA256快。在执行25次2000B的数据时，SM3的执行时间大约是SHA256的2倍左右。

根据图7c）所示，SM4和AES算法随着字节的增长而增加，SM4加密与解密算法的效率都优于AES。

根据国密算法与国际标准算法的时间测试结果，可以分析得出国密Fabric平台性能略次于原生Fabric平台的主要原因是SM3算法的性能低于SHA256算法。

本文采用JMeter工具来测试方案的执行时间和区块链的吞吐量。通过设置不同的线程并发量来测试方案的性能。

各阶段的执行时间如图8所示。根据图像可以看出，随着并发量的增加，各阶段执行时间会随之增加。数据提供者执行的工作包括链下数据加密和链上数据更新；验证节点执行的工作包括链上数据查询、链下数据解密和数据验证及链上数据更新；数据接收者执行的工作包括链上数据查询和链下数据解密。因此，验证节点的执行时间最长，数据提供者的执行时间次之，数据接收者的执行时间最短。在并发量为500的情况下，3个阶段的执行时间分别为1.877 s，4.221 s和1.269 s。

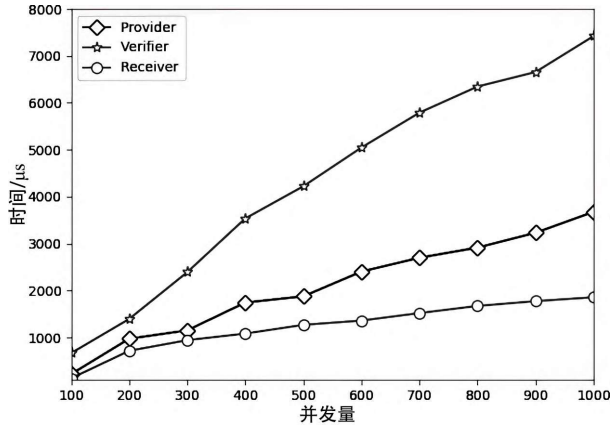
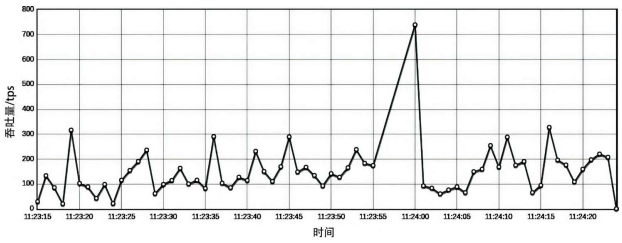


图 8 方案各阶段执行时间

国密改造后的Fabric平台发起更新数据交易的测试结果如图9所示，设置并发线程为1000，全部启动时间为20 s，循环次数为6次。根据聚合报告可以得出，吞吐量达到141.77 tps，错误率为0。

Requests	Executions			Response Times (ms)							Throughput	Network (KB/sec)	
Label	#Samples	FAIL	Error %	Average	Min	Max	Median	90th pct	95th pct	99th pct	Transactions/s	Received	Sent
Total	10000	0	0.00%	5649.75	40	17229	5475.00	9105.30	10244.00	12763.99	141.77	10.38	16.48
HTTP请求	10000	0	0.00%	5649.75	40	17229	5475.00	9105.30	10244.00	12763.99	141.77	10.38	16.48

a）更新数据的交易接口聚合报告



b）更新数据的交易接口吞吐量

图 9 方案测试结果

根据实验结果可以得出，随着并发量的增多，执行时间在不断增大。并且并发线程为1000时，吞吐量相对较低。根据图9的结果，分析平台性能较低的主要原因可能是随着并发线程的增多，SM3算法的时间在不断增大，从而影响了方案的整体性能。但是，本方案的执行效率也在可接受的范围之内，满足了可用性的同时也增强了平台的安全性。

5 结束语

为了满足Hypperledger Fabric平台在国内的商业化，本文利用国密算法分别从Fabric网络、Fabric-CA和Fabric-SDK三方面进行了底层密码学算法的改造。同时，为了解决隐私数据在区块链上的公开透明而分享受限的问题，本文在国密Fabric平台的基础上提出了一种基于国密算法的交易数据隐私保护方案。该方案采用SM4算法对隐私数据进行加密保护，并通过隐蔽通道进行对称密钥的链上传输；在方案中引入SM2公钥加密算法，对密文数据在有效时间内进行加密，满足了多种实际场景的应用。通过对实验结果分析可以得出，本文成功基于国密算法改造了Fabric平台，其平台的系统性能开销在可接受的范围内。本文提出的基于国密算法的交易数据隐私保护方案具有可行性，其整体执行效率和系统性能都具有良好的表现。该方案的提出对相关场景的实际应用都有一定的参考价值。

未来，将针对Fabric平台的国密算法改造性能做出进一步优化，提高其效率。同时将继续研究基于区块链的隐私保护方案，来完善目前未涉及的监管功能。

参考文献：

[1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. [2022-09-06]. https://bitcoin.org/bitcoin.pdf.

[2] XIA Yadong, CHE Lu, WANG Guanxiang, et al. Design of Passwordless Authentication System Using Decentralized Identity in Universities[EB/OL]. (2022-07-13)[2022-09-06]. http://kns.cnki.net/kcms/detail/61.1224.TN.20220712.1526.002. html.

夏亚东，车路，王关祥，等 . 高校去中心化身份无密码认证系统设计 [EB/OL]. (2022-07-13) [2022-09-06]. http://kns.cnki.net/kcms/detail/61.1224. TN.20220712.1526.002. html.

[3] LIN Chao, HE Debiao, HUANG Xinyi. Blockchain-Based Electronic Medical Record Secure Sharing[EB/OL]. (2022-01-17)[2022-09-06]. http://kns.cnki.net/kcms/detail/51.1307. TP.20220115.1014.002. html.

林超，何德彪，黄欣沂 . 基于区块链的电子医疗记录安全共享 [EB/OL]. (2022-01-17) [2022-09-06]. http://kns.cnki.net/kcms/detail/51.1307.TP.20220115.1014.002. html.

[4] ZHAI Sheping, TONG Tong, BAI Xifang. Blockchain-Based Attribute Proxy Re-encryption Data Sharing Scheme[EB/OL]. (2022-07-20)[2022-09-21]. http://kns.cnki.net/kcms/detail/11.2127. TP.20220719.1534.004. html.

翟社平，童彤，白喜芳 . 基于区块链的属性代理重加密数据共享方案 [EB/OL]. (2022-07-20) [2022-09-21]. http://kns.cnki.net/kcms/detail/11.2127. TP.20220719.1534.004. html.

[5] AZZI R, CHAMOUN R K, SOKHN M. The Power of a Blockchain-Based Supply Chain[J]. Computers & Industrial Engineering, 2019, 135: 582-592.

[6] JING Nan, LIU Qi, SUGUMARAN V. A Blockchain-Based Code Copyright Management System[EB/OL]. [2022-09-21]. https://xueshu.baidu.com/usercenter/paper/show?paperid=1u630e30dh420p90xj430270st462748&site=xueshu_se.

[7] MA Zhaofeng, JIANG Ming, GAO Hongmin, et al. Blockchain for Digital Rights Management[J]. Future Generation Computer Systems, 2018, 89: 746-764.

[8] MA Zhaofeng, WANG Xiaochang, JAIN D K, et al. A Blockchain-Based Trusted Data Management Scheme in Edge Computing[J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 2013-2021.

[9] MA Zhaofeng, WANG Lingyun, WANG Xiaochang, et al. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data[J]. IEEE Internet of Things Journal, 2019, 7(5): 4000-4015.

[10] ZHONG Sheng, HUANG Xinyi. Introduction to Security and Privacy in Blockchain Applications[J]. Chinese Science: Information Science, 2020, 50(3): 461-462.

仲盛，黄欣沂 . 区块链应用中的安全隐私专题简介 [J]. 中国科学：信息科学，2020，50 (3): 461-462.

[11] SHI Kun, ZHOU Yong, ZHANG Qiliang, et al. Privacy-Preserving Scheme of Energy Trading Data Based on Consortium Blockchain[EB/OL]. (2022-08-12)[2022-09-13]. http://kns.cnki.net/kcms/detail/50.1075.tp.20220810.0952.024. html.

时坤，周勇，张启亮，等 . 基于联盟链的能源交易数据隐私保护方案 [EB/OL].(2022-08-12) [2022-09-13]. http://kns.cnki.net/kcms/detail/50.1075.tp.20220810.0952.024. html.

[12] LI Li, DU Huina, LI Tao. Blockchain Supervisable Privacy Protection Scheme Based on Group Signature and Attribute Encryption[J]. Computer Engineering, 2022, 48(6): 132-138.

李莉，杜慧娜，李涛 . 基于群签名与属性加密的区块链可监管隐私保护方案 [J]. 计算机工程，2022，48 (6): 132-138.

[13] LIANG Wei, YANG Yang, YANG Ce, et al. PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data[J]. IEEE Transactions on Reliability, 2022: 1-13.

[14] WANG Baocheng, LI Zetao. Healthchain: A Privacy Protection System for Medical Data Based on Blockchain[J]. Future Internet, 2021, 13(10): 247.

[15] LUO Yurong, CAO Jin, LI Hui, et al. Electronic Invoice Public Verification Scheme based on SM2 Coalition Signature Algorithm[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 122-131.

罗玛榕，曹进，李晖，等 . 基于 SM2 联合签名的电子发票公开验证方案 [J]. 网络与信息安全学报，2022，8 (2): 122-131.

[16] HU Wei, WU Qiuhan, LIU Shengli, et al. Design of Secure eID and Identity Authentication Agreement in Mobile Terminal Based on Guomi Algorithm and Blockchain[J]. Netinfo Security, 2018, 18 (7): 7-15.

胡卫，吴邱涵，刘胜利，等 . 基于国密算法和区块链的移动端安全 eID 及认证协议设计 [J]. 信息网络安全，2018，18 (7): 7-15.

[17] LI Min, CHEN Fulong, PANG Hui. Vehicle PEPS and EMS Security Certification Based on Encryption Algorithm SM4[J]. Journal of Nanjing University of Information Science & Technology(Natural Science Edition), 2022, 14(5): 543-550.

李敏，陈付龙，庞辉 . 基于国密算法 SM4 的车载 PEPS 和 EMS 安全认证方法研究 [J]. 南京信息工程大学学报 (自然科学版)，2022，14 (5): 543-550.

[18] WANG Xiaoyun, YU Hongbo. SM3 Cryptographic Hash Algorithm[J]. Journal of Information Security Research, 2016, 2(11): 983-994.

王小云，于红波 . SM3 密码杂凑算法 [J]. 信息安全研究，2016，2(11): 983-994.

[19] SUN Rongyan, CAI Changshu, ZHOU Zhou, et al. The Comparision between Digital Signature Based on SM2 and ECDSA[J]. Network Security Technology & Application, 2013(2): 60-62.

孙荣燕，蔡昌曙，周洲，等 . 国密 SM2 数字签名算法与 ECDSA 算法对比分析研究 [J]. 网络安全技术与应用，2013 (2): 60-62.

[20] WU Zhihong, ZHAO Jianning, ZHU Yuan, et al. Comparative Study on Application of Chinese Cryptographic Algorithms and International Cryptographic Algorithms in Vehicle Microcotrollers[J]. Netinfo Security, 2019, 19(8): 68-75.

吴志红，赵建宁，朱元，等 . 国密算法和国际密码算法在车载单片机上应用的对比研究 [J]. 信息网络安全，2019，19 (8): 68-75.

[21] ALI O, JARADAT A, KULAKLI A, et al. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities[J].

IEEE Access, 2021, 9: 12730−12749.
[22] MA Zhaofeng. Blockchain Technology Development Guide[M]. Beijing: Tsinghua University Press, 2020.
马兆丰 . 区块链技术开发指南 [M]. 北京：清华大学出版社，2020.
[23] BHUTTA M N M, KHWAJA A A, NADEEM A, et al. A Survey on Blockchain Technology: Evolution, Architecture and Security[J]. IEEE Access, 2021, 9: 61048−61073.
[24] WANG Huaqun, WU Tao. Cryptography on the Blockchain[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition), 2017, 37(6): 61−67.
王化群，吴涛 . 区块链中的密码学技术 [J]. 南京邮电大学学报（自然科学版），2017，37（6）：61−67.
[25] YANG Long, HAN Dan, OUYANG Weile. Application of Commercial Cipher Algorithm in Blockchain Technology[J]. Computer Engineering and Applications, 2020(s): 29−35.
杨龙，韩丹，欧阳维乐 . 商用密码算法在区块链技术中的应用 [J]. 计算机工程与应用，2020（s）：29−35.
[26] GM/T 0003−2012 SM2 Elliptic Curve Public Key Cryptography[S]. China: State Cryptography Administration, 2012.
GM/T 0003−2012 SM2 椭圆曲线公钥密码算法 [S]. 中国：国家密码管理局，2012.
[27] WANG Zhaohui, ZHANG Zhenfeng. Overview on Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves. [J]. Journal of Information Security Research, 2016, 2(11): 972−982.
汪朝晖，张振峰 . SM2 椭圆曲线公钥密码算法综述 [J]. 信息安全研究，2016，2（11）：972−982.
[28] YANG Kai. IP Core Design Compatible with DES, AES and SM4 Algorithms[D]. Xi'an: Xidian University, 2017.
杨凯 . 兼容 DES、AES 和 SM4 算法的 IP 核设计 [D]. 西安：西安电子科技大学，2017.
[29] LYU Shuwang, SU Bozhan, WANG Peng, et al. Overview on SM4 Algorithm[J]. Journal of Information Security Research, 2016, 2(11): 995−1007.
吕述望，苏波展，王鹏，等 . SM4 分组密码算法综述 [J]. 信息安全研究，2016，2（11）：995−1007.
[30] Hyperledger Fabric Official Documentation[EB/OL]. [2022−08−21]. https://hyperledgerfabric.readthedocs.io/en/release−1.4.
[31] XU Xiaoqiong, SUN Gang, LUO Long, et al. Latency Performance Modeling and Analysis for Hyperledger Fabric Blockchain Network[EB/OL]. (2021−01−12)[2022−07−21]. https://xueshu.baidu.com/usercenter/paper/show?paperid=1x5v0gc04w1q0aj0xy3y0cg00v032442&site=xueshu_se.
[32] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance and Proactive Recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398−461.
[33] CAO Qi, RUAN Shuhua, CHEN Xingshu, et al. Embedding of National Cryptographic Algorithm in Hyperledger Fabric[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 65−75.
曹琪，阮树骅，陈兴蜀，等 . Hyperledger Fabric 平台的国密算法嵌入研究 [J]. 网络与信息安全学报，2021，7（1）：65−75.
[34] Tongji Blockchain Research Institute. Implementation of State Secret SM2, SM3 and SM4 algorithms[EB/OL]. [2022−08−21]. https://github.com/tjfoc/gmsm.
同济区块链研究院 . 国密 SM2、SM3 和 SM4 算法实现 [EB/OL]. [2022−08−21]. https://github.com/tjfoc/gmsm.
[35] Tongji Blockchain Research Institute. TLS/SSL Code Based on National Secret Algorithm[EB/OL]. [2022−08−26]. https://github.com/tjfoc/gmtls.
同济区块链研究院 . 基于国密算法的 TLS/SSL 代码库 [EB/OL]. [2022−08−26]. https://github.com/tjfoc/gmtls.
[36] LI Yanfeng, DING Liping, WU Jingzheng, et al. Research on a New Network Covert Channel Model in Blockchain Environment[J]. Journal on Communications, 2019, 40(5): 67−78.
李彦峰，丁丽萍，吴敬征，等 . 区块链环境下的新型网络隐蔽信道模型研究 [J]. 通信学报，2019，40（5）：67−78.