量子时代的
区块链技术白皮书

（2020 年）

中国移动研究院

前　言

近年来，量子科技发展突飞猛进，成为新一轮科技革命和产业变革的前沿领域。2020 年 10 月 16 日，中央政治局对量子科技进行了第二十四次集体学习。中共中央总书记习近平在主持学习时强调：要充分认识推动量子科技发展的重要性和紧迫性，加强量子科技发展战略谋划和系统布局，把握大趋势，下好先手棋[1]。

作为量子科技的重要领域，量子计算利用量子态叠加特性，通过量子态的受控演化实现数据的存储计算，具有巨大的信息携带和超强的并行处理能力，对信息科学等诸多领域产生颠覆性的影响。近年来，量子计算机的发展呈现加速趋势，研发更高性能量子计算机的周期显著缩短，不断有科技巨头声称实现特定领域的技术突破[2]。

区块链作为新型信息处理技术，在信任建立、价值表示和传递方面有不可取代的优势，目前已经在跨行业协作、社会经济发展中展现出其价值和生命力。为了保证其信任、价值以及传递的安全性，区块链将密码学作为其核心的底层技术。研究表明，经典密码学在量子时代将受到较大影响。本白皮书从量子计算入手，分析量子计算对密码学以及对区块链的影响，并提出相关的策略建议，为即将到来的量子时代构建安全的区块链提供技术参考。

参与本白皮书撰写的主要专家包括：中国移动通信研究院何申、阎军智、刘福文、王珂、杨波、董宁、粟栗等，北京大学信息科学技术学院区块链研究中心陈钟教授、关志副教授，中国科学技术大学张军教授，区块链技术与数据安全工业和信息化部重点实验室潘妍、李卫、李磊、余宇周等，在此表示感谢。

目 录

1. 引言

量子计算利用量子态叠加特性，通过量子态的受控演化实现数据的存储计算，具有巨大的信息携带和超强的并行处理能力，近年来量子计算机的发展呈现加速趋势，对传统密码学领域将产生颠覆性影响。区块链作为新型信息处理技术，在信任建立、价值表示和传递方面有不可取代的优势，这些优势建立在以密码学作为核心技术的基础之上，区块链将受到量子计算的较大影响[3-4]。本白皮书聚焦量子计算对区块链技术的影响，提出相应的措施和建议，为即将到来的量子时代构建安全的区块链提供技术建议。

2. 量子计算与密码学

2.1. 量子计算

量子计算是基于量子力学的全新计算模式，以微观粒子构成的量子比特为基本单元，利用量子叠加和纠缠等物理特性，通过量子态的受控演化实现数据的表示计算。相对于传统电子计算机使用比特作为基本单元，量子计算使用的量子比特具有态叠加特性：量子信息单元的状态可以处于多种可能性的叠加状态，随着量子比特数量增加，量子计算算力可呈指数级规模增长，具有经典信息处理无法比拟的巨大信息携带和超强并行处理能力。目前已有量子算法利用量子力学效应解决特定的密码学问题，其效率比经典计算机更高。

量子计算依赖于量子的物理特性，由于量子容易受到物理环境影响（如温度、磁场、压力等），导致量子计算自身容易出错。因此，量子算法的电路需要额外的量子比特进行纠错，在工程实践中实现特定功能的量子计算机比理论上更加复杂。研究机构预测，未来 10 年有可能建造一台能够破解当前强度密码算法的量子计算机[5]。

考虑到量子计算的发展趋势，有必要提前为信息安全系统做好准备，使其能

够应对这种未来必然面对的威胁[6]。例如，区块链中的存储数据可能需要多年的保护，具有较长的生命周期，因此需要足够的安全手段，以确保在数据的生命周期内对预期的安全威胁进行防范。

2.2. 量子计算对密码学的影响

2.2.1. 非对称密码算法

非对称密码算法中存在一对公私密钥，私钥一般是个人持有，不能被其他人获取；公钥一般可公开。非对称密码算法可用于数字签名、身份认证、数据加密等场景。

利用量子计算机，Shor 量子算法能够在多项式时间解决整数分解问题[7]。RSA 算法的安全性依赖于分解大整数的困难性，因此，量子计算机最终削弱了系统的安全性。Shor 算法也使得量子计算机能够在多项式时间解决有限域和椭圆曲线上的离散对数问题。该变体导致其他多种公钥密码算法不再安全，包括 ECDSA 和 Diffie-Hellman。

为了应对量子计算对非对称密码学的威胁，有必要将现有的算法替换成新的抗量子的算法。但是，对于目前备选的抗量子算法的研究比传统的公钥算法的研究要少得多。因此，需要在对抗量子威胁和确保使用稳定且经过测试的系统之间取得平衡。

2.2.2. 对称密码算法

对称密码算法中加密密钥和解密密钥相同，一般用于数据加密。

Grover 搜索算法对非结构化的搜索问题提供二次方的加速[8]。将其应用于对称密码算法，可通过 $O(2^{N/2})$次量子运算恢复 N 位密钥。在实际应用中，Grover 算法提供的加速取决于多种因素，例如量子位数量、量子纠错能力等。有研究指出，随着量子计算机的发展，128 位 AES 算法的安全性会有所降低，但不会降低至相当于 64 位的安全性。

业内研究表明，将密钥长度延长一倍，就足够应对量子计算对对称密码算法的威胁。

2.2.3. 哈希算法

哈希算法（Hash 算法，也叫散列算法）可将一串任意长度二进制值输入映射为一串较短的固定长度的二进制值，输出值称为哈希值，也叫摘要或者指纹。

Grover 算法对也能影响散列算法的安全。有研究认为，对 SHA-256 算法的单一原像攻击需要大约 2^{166} 次操作，而不是理论上的 2^{128} 次[9]。碰撞是散列算法安全性的另一度量，对于寻找碰撞，目前尚没有公开比经典算法更加有效的量子算法。

2.2.4. 量子随机数

由于量子状态具有随机性，利用该特点提取出的随机数称为量子随机数，与从经典物理噪声（如热噪声，电噪声等）中提取的随机数相比随机性更高。

3. 区块链与密码学

区块链是基于块链式数据结构、密码学、分布式节点共识等技术组成的一种全新的分布式基础架构与计算范式。密码学作为区块链的核心技术之一，是确保区块链安全运作的基石。

3.1. 非对称密码算法在区块链中的应用

在区块链技术中，非对称密码算法被广泛用于确保保密性、真实性、完整性、不可否认性和隐私性。具体可用于以下用途：

1) **参与方身份认证：**在许可区块链中，节点首先经过身份认证加入区块链网络中，基于身份进行节点及参与者权限管理及监管等，身份认证可基于公私钥体系。以 Hyperledger Fabric 为例，其提供了一个成员身份服务

MSP（Membership Service Provider），使用基于 ECDSA 算法的数字证书管理用户身份。成员提交交易、访问通道账本及修改网络配置等操作基于身份及策略进行授权，并会被适当记录和披露以用于监管审计。

2) **所有权认证：**在一些使用 UTXO（Unspent Transaction Outputs）机制的区块链系统中，账户资产的所有权是通过密钥和签名来确立的，公钥或经转换后用于接收资产，私钥用于支付这笔资产时的交易签名。公私钥间的数学关系，使得节点可通过验证签名和公钥之间的关系来确定资产是否由签名者所拥有进而验证交易是否有效。例如，比特币使用基于 secp256k1 椭圆曲线签名算法进行支付账户所有权的验证，进而完成资产转移和交易。

3) **背书签名：**一些区块链系统使用背书机制，即存在承担背书任务的节点为区块链交易进行交易信息验证，对验证通过的交易声明此交易合法，当收到足够多的背书节点的结果后，表示这个交易已经正确背书。背书节点必须通过有效签名来证明本节点对这笔交易的认可。比如 Hyperledger Fabric 中，背书节点（Endorser）模拟执行链码后生成提议结果，并对结果进行背书，即利用基于 ECDSA 算法的私钥对结果进行签名。

4) **消息完整性保护：**对消息进行签名可用于消息的完整性验证，如传输和存储中的交易。具体算法与上述签名算法一致。

5) **通信保护：**一些数据隐私要求比较高的应用中，需要对数据在区块链网络中的传输通道进行安全保护，一般会使用 TLS 机制，应用非对称密码算法及证书体系进行身份认证和密钥分发，从而在节点间建立安全通道。通常采用 RSA、ECDSA 等非对称密码算法。

6) **隐私保护：**一些对账户隐私要求比较高的应用中，需要确保交易双方的身份匿名化。目前有环签名、群签名等签名机制用于身份认证或交易验证中混淆或隐藏身份。

3.2. 对称密码算法在区块链中的应用

对称密码算法中只存在一个密钥，用于发送和接收双方对明文进行加解密。

在区块链中可用于模糊数据及隐私保护，比如 Hyperledger Fabric 中，使用常见的加密算法（如 AES）对链码中的部分或全部值进行加密，然后再将交易发送给排序服务并将区块添加到账本中，一旦加密数据被写入账本，就只能由拥有用于生成密码文本的相应密钥的用户解密。

3.3. 哈希算法在区块链中的应用

哈希算法具有正向快速、逆向困难的特点，即给定输入和 Hash 算法，在有限时间和资源内能计算出哈希值，但反过来，给定哈希值，在有限时间内很难逆推出明文。另外，哈希算法对输入敏感和输入信息修改会极大影响输出值，而优秀的 Hash 算法应该具备抗碰撞能力，即，很难找到两个不同的输入，产生相同的哈希值。

基于上述特征，在区块链技术中，Hash 算法被用于以下用途：

1) **生成账户地址：**在一些分布式账本系统中，账户地址基于账户所有者的公钥的哈希值生成，以比特币为例，以公钥 K 为输入，计算其 SHA256 哈希值，并以此结果计算 RIPEMD160 哈希值，得到一个长度为 20 字节的字符串，编码后即为地址，即，Address = Base58check (RIPEMD160 (SHA256(K)))。在公开的交易记录中使用公钥的哈希值，可以在标识交易相关方的同时减少公钥的暴露，降低使用公钥推导出私钥的风险，尤其是对于金融类应用的收款方，作为密钥被公开的唯一代表，哈希后的地址更便于广泛分发使用。
2) **构建 Merkle 树：**Merkle 树的叶节点包含存储数据或其哈希值，中间节点以及根节点是它子节点内容的哈希值。底层数据的任何变动，都会传递到父节点直到根节点。区块链中可对区块内的所有交易构建 Merkle 树，把 Merkle 根记在区块头里，区块内任意一笔交易的改变都会影响 Merkle 根及叶节点到根节点之间中间节点的值，因此可以快速发现及定位区块内的交易篡改；另外，Merkle 树也可以用于快速交易验证，即判断一笔交易是否已经写入一个区块中：只需要提供 Merkle 树从叶子节点到根的路径，并进行对数级的哈希运算和验证，就可以判断交易是否属于该

区块。

3) **链接区块：**区块链是由包含交易信息的区块从后向前有序链接起来的数据结构，每个区块头中都包含它的父区块头的哈希值，通过把每个区块链接到各自父区块的哈希值序列就创建了一条可以追溯到创世区块的链条。任何一个区块的篡改都可以通过检查后一个区块的记录来发现，除非篡改后面所有的区块。

4) **竞争记账权：**在使用 PoW（Proof of Work，工作量证明）竞争记账权来达成共识的区块链系统中，节点通过验证区块的工作量证明来决定是否接收该区块，验证要求区块头中的哈希值满足特定特征，基于区块寻找满足要求的哈希值需要大量的运算，因此这个哈希值可以被视作工作量证明。

5) **处理大文件或隐私数据：**为了处理大文件或隐私数据保护，可将原始事务数据哈希处理后存于链上。比如，在一些存证类区块链应用中，通过对链上哈希值与链下原始数据的对比，可验证原始数据是否可信，同时可减少区块链存储空间需求或降低原始数据公开程度。

3.4. 随机数产生算法在区块链中的应用

随机数产生算法在区块链中有广泛应用，最为典型的用于产生公私钥对的种子。传统随机数发生器有使用软件产生的伪随机数，以及使用硬件物理噪声产生的随机数。

4. 量子计算对区块链的影响

非许可区块链和许可区块链都具有链上数据不可篡改、链上数据可信的特性，但两者在链的接入控制、用户的账户管理方面有显著差异，这导致两者在非对称密码算法的使用范围和程度上有显著不同。

4.1. 量子计算对非许可区块链的影响

以比特币为代表的非许可区块链没有接入控制，任何人都可以加入链中进行区块链上的操作。大多数非许可区块链使用基于工作量证明的共识机制确定记账节点，将交易数据上链。量子计算技术对非许可区块链各种功能的影响如下：

1) **接入控制**：量子计算技术对非许可区块链的接入控制没有影响，因为非许可区块链没有采用密码学技术对链的接入进行控制。
2) **共识机制**：工作量证明是对哈希函数的输入进行求解，要求其哈希值需满足特定特征，为此每个节点需要不断改变哈希函数输入值进行运算，首先得到答案的节点获得记账权。目前普遍认为常用的哈希函数（如 SHA-256、SM3）[10]能够抗量子计算攻击，因为目前所知的 Grover 量子算法及其变体还没有传统的算法对哈希函数求碰撞解的速度快。因此，量子计算技术对共识机制基本上没有影响。
3) **链上数据**：区块上的交易数据的完整性由哈希值保证。每个区块通过使用哈希函数对上一个区块的区块头进行运算所得哈希值与上一个区块进行链接，从而形成链式数据结构。攻击者要篡改区块链上的交易数据，需要能够破解使用的哈希函数，而目前常用的哈希函数（如 SHA-256、SM3）是能够抗量子计算攻击的。目前的研究表明，量子计算技术对链上交易数据的完整性基本没有威胁。如果链上数据使用对称算法进行加密，其安全强度相当于经典计算中密钥长度减半的效果。
4) **账户管理**：非许可区块链一般采用用户客户端（以下简称客户端）的方式管理用户账户。客户端里可以包含多个公私钥对用于转账交易，即客户端与公私钥对不是一对一的关系。客户端的访问控制一般采用口令短语的方式。只要口令短语的有效信息长度为 256 位，量子计算技术也不能在有效时间内破解用户私钥。与传统的软件和硬件随机数发生器相比，采用量子随机数发生器可以提升密钥的随机性，增加密钥安全强度。
5) **交易**：非许可区块链上交易时，发送方使用自己的私钥对交易信息进行签名，并把交易信息、签名以及与私钥对应的公钥在区块链上公布。接受方使用收到的公钥对签名进行验证以确定交易信息的真实性。由于交

易使用了非对称密码算法，量子计算技术将对交易产生重大影响。攻击者使用 Shor 算法有可能从链上的公钥推导出私钥，从而能篡改交易信息并伪造签名。一些非许可区块链建议用户每次交易使用不同的公私钥对，这在一定程度上可以减轻这种影响。

6) **隐私保护：**有些非许可区块链采用零知识证明的方法来隐藏交易信息。隐藏信息的方法是基于椭圆曲线密码技术的同态加密来实现。量子计算技术能够在有效时间内破解椭圆曲线密钥，从而使隐私保护的方法失效。

4.2. 量子计算对许可区块链的影响

以 Hyperledger Fabric 为代表的许可区块链依赖 PKI 技术对用户接入区块链以及用户在链上的角色进行控制。许可区块链一般基于签名背书的机制的共识机制以使分布节点达成共识，并通过排序节点把数据上链。量子计算技术对许可区块链的各种功能的影响如下：

1) **接入控制：**针对依赖 PKI 技术进行接入控制的许可区块链，量子计算技术对接入控制有非常大的影响。PKI 基本上使用非对称密码算法构建而成。攻击者使用 Shor 算法可以从 CA 的公钥推演出 CA 的私钥，从而可以伪造任何用户身份接入许可区块链。
2) **共识机制：**基于签名背书作为实现共识机制基础的区块链中，签名一般使用非对称密码算法，因此量子计算技术对共识机制有很大影响，例如伪造背书结果。
3) **链上数据：**与非许可区块链相似，区块上的数据的完整性由哈希函数保证。区块之间基于哈希值进行相互链接。攻击者要篡改链上数据，需要能够破解使用的哈希函数，而目前的普遍认知是安全标准化的哈希函数是能够抗量子攻击的。因此，量子计算技术对链上交易数据的完整性基本没有威胁。如果链上数据使用对称算法进行加密，其安全强度相当于经典计算中密钥长度减半的效果。
4) **账户管理：**用户的身份由 CA 通过证书的方式确定和发布。一般一个用户在一个许可区块链上只有一个证书。证书对应私钥的访问控制一般采用短语口令的方式。只要短语口令的有效长度为 256 位,量子计算技术也

不能在有效时间内获得破解对私钥的访问控制。但是由于证书是公开信息，攻击者使用 Shor 算法能从证书中的公钥推导出相应的私钥，从而使账户管理失效。

5) **交易：**许可区块链上交易时，发送方使用自己的私钥对交易信息进行签名，并把交易信息，签名，以及与私钥对应的证书在区块链上公布。接受方使用收到的公钥对签名进行验证确定交易信息的真实性。由于交易使用了非对称算法，量子计算技术将对交易产生重大影响。攻击者使用 Shor 算法破解 CA 的私钥后，可以伪造任何证书并发起交易，从而使许可链上的交易失去真实性。

6) **隐私保护：**许可区块链存在两种方法来实现隐私保护：零知识证明、交易通道。比较成熟的零知识证明方法一般都基于非对称密码算法构建，因此不能抵抗量子计算的攻击。交易通道用于保证链上的信息只能由本链的参与者访问，通道内的通信使用基于使用证书的 TLS 保护。使用证书的 TLS 要使用非对称算法对通道双方进行验证并建立加密密钥，攻击者使用 Shor 算法破解证书后，可以实现中间人攻击获得加密密钥，从而获得交易信息。

4.3. 小结

密码算法是区块链健康发展的基础。未来量子计算技术的普及后，将对现有密码算法体系产生冲击，因此会对现有区块链系统和应用产生潜在安全挑战。对于非许可区块链，其账户管理、链上数据等功能不受影响，但交易过程受到影响；对于许可区块链，其账户管理、交易过程、共识机制等功能可能存在安全风险。

我们也应认识到，量子计算机仍面临量子比特相干态维持时间短、需要大量冗余量子比特维持精度等众多基础工程问题，近期尚不会对密码算法产生实质影响。我们应以此为契机，提前布局，加大国产密码算法和量子安全的密码算法攻关，构建量子安全的区块链体系，保障区块链生态的安全发展。

5. 总结与工作展望

目前业界普遍认为大规模量子计算机将在 2030 年左右出现，提前规划和研究引入量子安全算法已势在必行。中国移动于 2019 年开展了与量子计算有关的区块链技术研究，并已于 2020 年初在 ITU-T 主导“Guidelines for quantum-safe DLT systems”课题立项[11]，联合学术和产业力量，以开放的形态从全球视角开展协作和技术攻关，分析量子计算对区块链的威胁，探索量子时代安全区块链的发展之路。

未来，随着量子计算时代的到来，为了区块链保持安全可用，保证其数据和价值的稳定，基于现有研究提出以下建议：

1) **引入量子安全算法，构建量子安全的区块链体系：**无论是非许可区块链或者是许可区块链，将传统非对称密码算法替换为量子安全算法。如今已有大量公开的量子安全算法，它们在安全性、公私钥长度、签名长度以及性能上有较大的差异。公钥长度和签名长度将对区块链的存储空间产生较大影响，需要选择公钥长度和签名长度较小的量子安全算法。算法的性能也是需要考虑的一个重要方面，因为它会影响到交易的执行速度。
2) **推动量子安全算法及安全协议的标准化：**目前国际上已经开展对量子安全算法的征集，已有多种算法成为候选算法[12-13]。应积极参与量子安全算法及安全协议的征集和安全性评估。
3) **评估区块链系统适配及影响：**量子安全算法的公钥和签名长度远大于传统的非对称密码算法，量子安全算法在区块链系统上的引入需要做必要的适配，并需要进一步评估对系统可能造成的影响。
4) **开展区块链系统演进机制研究：**现有区块链上已经积累了大量数字化的资产，在量子时代将受到新的安全挑战。为了确保这些资产的安全，需要提前研究如何做好现有区块链系统向量子安全区块链的演进，以及现有数据的安全迁移机制。

量子时代的区块链是一个包含理论、算法、标准、应用、产业、生态在内的重要工程问题。我们期望全球技术和工程领域开展更加密切的合作，为信息技术和区块链发展的未来奠定基础。

缩略语列表

缩略语	英文全名	中文解释
AES	Advanced Encryption Standard	高级加密标准
CA	Certificate Authority	证书颁发机构
DLT	Distributed Ledger Technology	分布式账本技术
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
MSP	Membership Service Providers	成员服务提供者
PKI	Public Key Infrastructure	公钥基础设施
PoW	Proof of Work	工作量证明
SHA	Secure Hash Algorithm	安全散列算法
TLS	Transport Layer Security	传输层安全
UTXO	Unspent Transaction Outputs	未花费的交易输出

参考文献

[1] 习近平在中央政治局第二十四次集体学习时强调 深刻认识推进量子科技发展重大意义 加强量子科技发展战略谋划和系统布局. 新华网. 2020-10-17.

[2] Frank Arute, et al., Quantum supremacy using a programmable superconducting processor, Nature volume 574, pages. 505–510 (2019).

[3] MITRE Technical Report. Blockchain and Quantum Computing, June, 2017.

[4] Recommendation ITU-T X.1401, Security Threats to Distributed Ledger Technology.

[5] Practical Quantum Computers. Available at: https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/

[6] Rachid EI B andsarkhani, et al., PQChain: Strategic Design Decisions for Distributed Ledger Techonlogies against Future Threats. IEEE Computer and Reliability Societies, July/August 2018.

[7] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5):1484–1509.

[8] Grover L K. A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212.

[9] Matthew A, Olivia D M, Vlad G, et at. (2016): "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3". https://arxiv.org/pdf/1603.09383.pdf

[10] 陈钟, 关志. 国产密码体系在区块链中的应用与挑战. 中国信息安全. 2019(11): 71-73.

[11] ITU-T, Guidelines for quantum-safe DLT systems, 2020.

[12] NIST Interagency Report 8105, Report on Post-Quantum Cryptography, 2016.

[13] NIST Interagency Report 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.