量子时代的区块链

CSA GCR cloud security alliance GREATER CHINA REGION

CSA cloud security alliance®

云安全联盟量子安全工作组地址：
https://cloudsecurityalliance.org/working-groups/quantum-safe-security/
云安全联盟大中华区区块链安全工作组地址：
https://c-csa.cn/research/union-detail/i-22.html

致 谢

本文档《量子时代的区块链》(Blockchains in the Quantum Era)由 CSA 量子安全工作组专家编写，CSA 大中华区区块链工作组专家翻译并审校。

中文版翻译专家：

组织者：刘洁

贡献者：姚凯、余晓光、吴潇、杨喜龙、王贵宗、邓辉、于乐、张威、赵刚

主要审核者：黄连金、刘洁

贡献单位：华为、天融信、吉大正元、宇链科技

英文版原创作者：

主要作者：Bruno Huttner

贡献者：John Hooks 、Aaron Kent 、John Young

审核者：Boulevard Aladetoyinbo、Andrew Brick、Nadia Diakun-Thibault 、Ken Huang（黄连金）、Ashish Mehta 、Urmila Nagvekar

CSA 员工：Hillary Baron、AnnMarie Ulskey (GraphicDesign)

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

序　言

首先祝贺《量子时代的区块链》(Blockchains in the Quantum Era)的中文版本的发布，这本白皮书由 CSA 量子安全工作组专家编写，CSA 大中华区区块链工作组专家翻译并审校。

量子计算技术的飞速发展，使得采用量子计算机攻击区块链的现实威胁越来越近。量子计算机可以执行传统计算机无法执行的计算，威胁到区块链中使用的几种密码学原语。一些公司和世界各国政府已经建造了具有有限输入规模和有限计算量的小型量子计算机，有些量子计算机甚至可以通过互联网访问，并可用于测试量子算法。

量子技术的发展对于区块链的安全有什么影响？这本文档总结了区块链的技术和可能受到量子计算破解的区块链密码学算法，分析了一些主流区块链网路的密码学算法和量子计算的关系，包括比特币、以太坊、超级账本框架 (HLF)和 Zcash，同时分析了抵抗量子破解的密码学算法和在区块链中的应用。文章深入浅出，值得大家参考。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

1. 简介

区块链等分布式账本技术（DLT）正作为跨越多个细分市场的众多应用程序的一部分进行部署。开发人员利用区块链去中心化、不可篡改、加密安全和透明的特点，发挥其在数据冗余、不可篡改和增强审计/合规方面的优势。区块链基础设施广泛使用数字签名算法、哈希算法和公钥加密技术。量子计算技术的飞速发展，使得量子计算机网络攻击的前景变得非常现实。例如，可见于最近 CSA 发表的关于量子威胁的文章。

因此，目前正在采取措施来设计用于抵抗量子计算机攻击的加密算法，用来增强当今的 DLT/区块链基础设施。这些后量子算法是基于量子计算机很难用 Shor 算法或 Grover 算法来解决的计算问题。本文介绍了 DLT/区块链技术及其一些代表性应用，并总览了目前正在积极研究的领先的后量子算法中有代表性的部分。

2. 区块链概述

我们假设读者对区块链有一定的了解。如果没有，我们推荐以下相关资料：CoinDesk 的区块链介绍或 NIST 的区块链技术介绍。这里我们简要回顾一下区块链主要的思想和工具。

2.1 区块链是什么？

区块链是一个去中心化的分布式帐本，在一个多节点网络上，具有特定的更新机制，确保所有节点之间的同步。帐本由包含交易的区块互相链接组成。用户创建一笔交易，这些交易必须通过网络中的节点验证后才能追加到账本。为了保证数据不可篡改，整个数据结构被加密过程保护：通过网络验证的交易不能被篡改。

区块链主要基于两个密码学原语，密码哈希函数和公钥签名。签名有两个目的，它们允许用户使用其私钥对他们的交易进行身份验证， 并使区块链能够使用公钥验证其有效性。哈希函数提供了不可变性: 一旦交易块的哈希在区块链上发布，该交易就无法被修改。然后这个哈希值将包含在下一个交易块中，再下一个区块也是一样，如此继续，建立一连串的交易块，即区块链。恶

意节点对前期交易块的任何修改都会转化为对所有后续区块的修改，这将很快被诚实节点发现并拒绝。

2.2 它是如何开始的:比特币和加密货币

从历史上看，第一个区块链也是现在应用最广泛的区块链应用是比特币。比特币中每一笔交易都是以货币形式出现。比特币是第一个加密货币。此后，基于类似的原理，人们发明了许多其他加密货币。加密货币的主要优点是去中心化、有限的匿名化和公开验证的交易的不可篡改性。

2.3 新范式：智能合约

区块链结构还可以应用于不同类型的交易。例如，在以太坊区块链中，交易也可以由一些软件支持，这些软件可以在满足一组条件时执行。这就是“智能合约”的基础，它是新兴应用程序的核心。

2.4 新兴区块链应用

区块链技术的内在特征使其成为一种颠覆性技术，能够跨多个细分市场进行创新业务转型。它的去中心化和不可篡改的特性可以使交易双方超高可信的执行交易、验证交易和审计历史交易。虽然过往区块链技术一直是以比特币为代表的加密货币的代名词，但智能合约的功能为自动化业务流程和工作流提供了最大的变革潜力。简要回顾一下其他细分市场中的一些新兴应用案例，可以帮助说明区块链应用程序在未来的量子计算机攻击中所面临的风险越来越大。

- **金融服务——清算和结算。**使用区块链技术可以大幅减少金融资产交易或兑换的清算和结算时间。一个基于区块链的服务可以自动更新数据库/注册表以及相关的工作流，可以将这个时间间隔从几天缩短到几分钟。更多细节可参见惠普关于金融行业区块链的技术意见书，以及 CSA 发表的另一篇关于区块链用例的论文。

- **身份管理服务。** 区块链技术特别适合支持分布式身份管理服务。 可以在区块链上为每个人创建一个加密的安全“数字身份”。 然后，双方可以使用身份“证明”或来自数字身份的属性来证实该用户的身份。 最近 NIST 在有关身份管理的技术意见书中对此进行了明确的说明。

- **医疗健康。** 区块链技术潜在地支持各种医疗健康用例（例如，安全访问患者健康记录，对医疗健康交易进行安全审计，减轻或防止欺诈性处方药的流动）。 有兴趣的读者可以咨询医疗健康中有关区块链的介绍，以及医疗健康中有关区块链的技术意见书。

- **智能家居和物联网。**家庭环境中具有区块链功能的物联网(IoT)设备可以以安全的方式远程控制和管理(如家用电器、消费电子产品)。例如，参见物联网中基于区块链的安全访问控制以及CSA 在物联网区块链上发表的另一篇论文。

- **供应链和物流。** 启用了区块链的 IoT 设备（例如运动传感器，GPS 传感器，温度传感器，车辆信息传感器）可以在货物穿越复杂的供应链时提供详细的状态更新。 还可以部署智能合约来自动执行任务（例如，当冷藏卡车内的温度降得太低时，可以自动启动补救措施）。 世界经济论坛的一份技术意见书以及 CSA 发布的一份文件都提到了这一点。

- **汽车行业。**目前正在评估区块链技术在支持自动驾驶汽车、自动加油支付、智能停车和自动交通控制方面的适用性。可以在 Cube 的技术意见书中找到示例。

在不同细分市场中创建的关键业务区块链应用可能会在同一攻击面出现相同的量子安全漏洞。一旦这一攻击面成为未来量子计算机攻击的目标，整个行业范围的区块链安全风险敞口将迅速超过其他归因于比特币加密货币的安全风险敞口。潜在的，恶意的参与者可能正在收集这些被量子脆弱的加密方案保护的数据，以待量子硬件可用时解密数据。因此，尽早制定合适的量子安全对策变得越来越迫切。

3. 量子时代

完整的区块链框架依赖其底层密码流程的安全性。没有可信的哈希函数和公钥签名就不会有区块链。 量子计算机(Quantum Computer)可以执行传统计算机无法执行的计算，威胁到区块链中使用的几种密码学原语(Cryptographic Primitive)。要攻破密码学原语背后的数学问题，通用且可扩展的量子计算机是必不可少的。虽然目前尚不可用，但一些公司和世界各国政府已经建造了具有有限输入规模和计算量有限的小型量子计算机。有些量子计算机甚至可以通过互联网访问，并可用于测试量子算法。量子霸权(Quantum Supremacy)描述了量子计算机明显优于传统计算机

的时间点，这一点已经或即将实现。 因此，最重要的是了解量子计算对区块链构成的威胁并提出可能的解决方案。

4. 区块链使用的主要密码学工具

未来的量子计算机攻击将针对区块链的区块构件，因此必须更详细地分析每个威胁。

4.1 随机数生成

随机数生成(Random Number Generation)是大多数密码流程的核心。 由于传统计算机是确定性的，因此生成良好的随机性并不容易。 在许多情况下，不良的随机性会导致灾难，后面最近的案例证明了这一点。 对于在协议的各个级别应用随机数的区块链来说尤其如此。 对于隔离的服务器，问题更加严重，因为在隔离的服务器中，大多数计算都是在没有人工干预的情况下执行的。

在这里量子技术实际上可以提供帮助。 量子理论本质上是不确定的，因此基于量子生成随机数是提供良好随机性更安全的方法。

现在，量子随机数生成器(Quantum Random Number Generator, QRNG)的外形尺寸非常小，如 ID Quantique 的 Quantis QRNG 芯片。 这样的小型 QRNG 可以轻松集成到服务器中，维护区块链的节点，甚至可以集成到各种终端，如用户端的 PC 和智能手机中。

4.2 哈希函数

密码哈希函数(Hash Function)确实是实现区块链密码流程的主力军。哈希函数将任意长度的文本输入转换为固定长度的输出。输出确定地对应到输入，除非使用暴力尝试每个输入直到找到正确的输出，否则不可能从输出恢复输入。

哈希函数在区块链中用于两个目的。一是保证区块的不可篡改性。最常用的哈希函数 SHA256 具有 256 位输出， 对该函数进行暴力攻击需要运行 2^{256} 次操作，甚至超过了最大的超级计算机的能力。使用 Grover 算法进行量子攻击会将操作减少到 2^{128} 次，但仍然是不可行的。量子计算机无

法破坏区块链的不可篡改性，但可能需要将哈希函数的运算级别加倍。

许多区块链哈希函数的第二个目的是提供所谓的工作量证明(Proof-of-Work, PoW)，网络中的节点必须完成工作才能添加新的区块(Block)。这个想法是，当准备在网络上添加新的区块时，矿工(Miner)竞相在该区块上执行计算。第一个完成计算的矿工可以添加该区块并获得奖励。该计算精确地转化了具有较短输出的哈希函数。同样，在量子计算机上实现的 Grover 算法将实现更快的计算。

4.3 公钥签名

公钥密码学(Public-key Cryptography)用于验证在区块链上完成的交易。发送方 Alice 使用她的私钥对交易进行数字签名。然后，接收者和任何感兴趣的一方都可以使用 Alice 的公钥验证数字签名是否有效。公钥密码学机制还用于支持区块链上的数字钱包(Digital Wallet)操作。 数字钱包通过对用户的公钥进行某种形式的哈希运算，与区块链上的公开地址关联。数字钱包通常用于安全地存储区块链用户的私钥以及交易的相关数据，这些交易可能与区块链应用程序有关。对于比特币(Bitcoin)或以太坊(Ethereum)，该数据可能是用户当前的加密货币余额。

[1] 通过以下方式实现这一点：对区块进行哈希，然后将该哈希与一个随机数(nonce)再次进行哈希，直到获得具有给定数量的前导零的哈希值。实现这一目标唯一的已知方法是暴力破解。通过发送随机数的值并要求其他节点检查可以很容易地验证这一点。

5. 几种区块链技术的风险分析

尽管所有区块链技术都依赖于相同的密码学原语，但实现细节是不同的。因此，量子威胁在不同的层面产生作用。我们通过简要分析几个现有的区块链来举例说明这一点。这就要求我们对区块链结构及其技术细节进行相对深入的探索。其目的是通过一些选定的例子来说明风险的性质，以及如何降低风险。更完整的分析超出了本文的范围。

5.1 比特币

比特币是第一个也是最流行的区块链。对于那些不熟悉比特币工作原理的读者来说，最好的信息来源是中本聪的原著（中本聪是整个比特币体系发明者的化名），尽管这个著作有些过时。在这里，我们将简单列出与量子计算机攻击可能有关的基本问题。

• 链的不可篡改性：这个目标是通过散列算法实现的，这被认为是量子安全的。只要使用足够长的哈希值，则这方面风险很小（即，考虑到 Grover 的算法，256 位及以上的位允许降级二分之一）。比特币就是这种情况，它使用 SHA 256 算法。

• 公开地址：交易由地址标识，地址是接收方公钥的散列值。因此，如果一个用户想要接收比特币，他们必须创建一个公钥/私钥对，并计算一个地址，该地址是他们公钥的散列。比特币使用的非对称算法是 ECC（椭圆曲线），这不是量子安全的。但是，只要公钥被哈希函数隐藏，它就会得到很好的保护。当用户需要花费与地址相关联的比特币时，公钥被公布。这是为了保证区块链对交易的确认。然而，在交易中，链接到此地址的所有比特币都必须用完。原则上，剩下的任何“找零”都会发送到一个新地址。如果遵循这一规则，量子计算机带来的唯一风险就是对手拦截交易，破解密钥并执行另一笔交易，所有这一切都在几分钟内完成。量子计算机不太可能在短期内足够快地做到这一点。因此，这种风险微乎其微。然而，出于实用性考虑，许多用户在多个交易中重复使用相同的地址。这不是正确的做法，会让他们的比特币面临量子计算机的风险。

• 对于 PoW（工作量证明）：拥有量子计算机的对手执行 PoW（工作量证明）的速度可能比其他矿工快得多，并获得很大优势。特别是，配备量子计算机的恶意用户可能会尝试 51% 的攻击并控制区块链。然而，这可能不会比比特币初期面临的问题更糟，当时矿工使用定制硬件相比较于依赖通用 PC 的其他人有很大优势。这个问题还需要更详细地研究。

5.2 以太坊

以太坊是第二大受欢迎的区块链平台。 它是一个全球性的开源平台，用于构建和运行去中心化应用程序，并且是流行的以太币的基础平台。 许多商业应用程序基于以太坊构建。 公共以太坊平台用于债券发行和结算，供应链自动化，基于区块链证书的凭证，简化公用事业提供商的付款流程等。 以太坊的一个不错的学习书籍是《精通以太坊》。 在本节中，我们将简单列出它与量子安全相关的基本问题。

- 链的不可篡改性（或 链的不可变性）：与比特币类似，以太坊网络中的不可篡改性（或不可变性）是通过散列算法，具体来讲是 Keccak-256 算法（或以太坊圈子中通常称为 SHA-3）来实现的，具有量子抗性。

- 共识：以太坊使用的共识机制目前是工作量证明（PoW），与比特币一样，拥有量子计算机的对手可以尝试 51%的攻击并控制区块链。

- 资金和合约的所有权：以太坊使用公钥加密技术，利用公私密钥对表示以太坊帐户，包括，可公开访问的帐户句柄（地址）和该帐户中的资金所有权（以太），以及该帐户使用智能合约时所需要的任何身份认证。私钥通过作为创建数字签名所需的唯一性信息片段来控制访问，任何花费该账户中资金的交易都需要这个数字签名来签署。数字签名还用于认证合约的所有者或用户。

- 以太坊当前使用 ECDSA 来签署交易并不具有量子抗性。

- 以太坊地址：这些是唯一性标识，这些标识是使用 Keccak-256 单向哈希函数从公钥或合约生成的，该函数具有量子抗性。

- 目前正在进行的以太坊新版本 Ethereum 2.0 是一个重大升级。计划于 2022 年完成，其中包括开发功能，性能和安全性的升级。此版本将依赖于权益证明（PoS），这是另一类共识机制。在 PoS 中，每个验证节点对新区块的添加进行投票。每个验证节点的权重取决于它愿意承担的资金量份额。 PoS 的优势包括安全性提升，中心化风险降低以及性能提高。这在 PoS 的常见问题（FAQ）中进行了描述。此外，它将包括通过诸如 Lamport 算法(逻辑时钟)，XMSS（扩展 Merkle 签名方案）或 SPHINCS 之类的抗量子签名方案来解决量子威胁。

5.3 超级账本框架 (HLF)

超级账本框架 (HLF)是一个需授权的分布式账本平台，最初由 IBM 和 Digital Asset 开发。它是 Linux 基金会于 2015 年创建的 Hyperledger 项目中的一个特定框架。超级账本框架 (HLF)是用于开发模块化应用程序的企业级平台。它提供了一个可扩展且安全的平台，这个平台支持私有交易和私密智能合约。在这里，我们将确定与量子安全相关的基本问题：

• 链的不可篡改性：就像比特币一样，框架（Fabric）中的不可篡改性（或不可变性）是通过散列（SHA-256 算法）实现的，这被认为是量子安全的。

• 交易：交易是向超级账本框架 (HLF)提出修改账本状态的请求。密码学通过将交易链接到之前的区块确保交易的完整性，如果受到保护，则通过链接以前链接的块中的密码或哈希值来确保交易的完整性。超级账本框架 (HLF)中的加密模块是可插拔的，因此可以更新模块以确保其量子安全。

• 身份和访问管理：由于 Fabric 是需授权网络，因此它重度依赖于被网络所识别和确认的所有成员。它使用专门的数字证书颁发机构（CA）向区块链网络的成员颁发证书。证书颁发机构基于在 Fabric 中可插拔的加密功能模块，并且可以通过加密模块升级以确保它们达到量子安全的目标。然而，目前在超级账本框架 (HLF)中使用的签名方案本质上并不具有量子抗性。目前正在进行研究以探索基于格结构的数字签名方案(比如 qTESLA)的使用。该数字签名方案已被 NIST 第 2 轮候选数字签名接受，但尚未进入第 3 轮。因此，很可能会提出一种新的签名方案来测试超级账本框架 (HLF)的量子抗性。

5.4 Zcash

Zcash 是比特币的分支，它提供了打开与交易相关的隐私功能的附加功能。支付人和收款人信息以及交易金额受到隐私保护，但同时 Zcash 提供了与任何主流基于区块链的系统相关的不可篡改性和可验证性。隐私特征和交易有效性是通过零知识证明，特别是使用 ZK-SNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）来实现的。 ZK-SNARKs 需要设置受信任方才能启用 ZK 证明系统。

目前，Zcash 加密机制容易受到量子计算机攻击。因此，通过使用已知收款人的地址，可以发现与交易关联的金额以及加密的备忘录。另外，可以操纵验证过程以伪造 Zcash。

目前正在进行大量研究以开发后量子（PQ）Zcash，例如基于格结构的 ZK-SNARKs。一种潜在的后量子方法可能是将 ZK-STARKs（Zero-Knowledge Scalable Transparent Arguments of Knowledge）作为 Zcash 协议的一部分。ZK-STARKs 的另一个优点是不需要设置受信任的实体，从而减轻了这些实体对隐私的任何潜在攻陷可能。

6.未来解决方案

6.1 量子安全签名与加密

量子计算机可能会破坏传统架构下所有的安全连接，解密已加密保存的安全数据库，修改所有已经创建的区块链记录，这可能会对互联网连接的区块链网络的安全性造成大规模的破坏(无论是技术还是经济上的)。量子计算机将破坏大多数现有区块链（即数字签名方案）背后的至少一个基本密码学原语。尽管由于它们的结构，某些区块链，尤其是那些利用对称密钥密码学的区块链，相对具有适应性，而另一些区块链可能会因规则的一些简单更改而变得如此，但必须对此原语进行修改。此外，在大多数区块链实施中，公钥/私钥对由用户存储在数字钱包中。这些钱包中有一些是在线存储的，例如在交易所，而有些则是由用户自己存储的，通常存储在便携式驱动器上。由于这些钱包存储了私钥，因此出现了机密性问题。

在大多数情况下，公钥基础结构还提供了机密性，对通过不安全通道交换的密钥进行加密。这种加密也可能受到量子计算机的威胁。但是，由于可以使加密的钱包独立于区块链本身而具有抗量子性，因此我们将不对其进行进一步讨论。

NIST 的评估目前正在为量子抗性签名和密钥交换机制选择合适的候选方案，这些候选方案可用于加密私钥。我们将仅在下面审查签名方案。

6.2 后量子区块链签名属性

目前，一些行业计划正在制定适用于区块链使用的后量子密码系统。除了提供必要的抵抗未来量子计算机攻击的能力外，这些算法必须从实际部署的角度来看是可行的。一些特别重要的属性包括:

•小的数字签名和哈希值:因为区块链代表了一个不断增长的交易存储库，所以最小化数字签名和哈希值的大小是很重要的。

•小的公钥和私钥大小:合适的后量子算法必须最小化密钥大小，以减少区块链存储需求，并减少与密钥操作相关的计算开销。

•计算速度快:为了支持高性能和可扩展的区块链基础设施，后量子算法的执行速度应该非常快。

6.3 标准化下的后量子签名

目前有三家入围 NIST 签名方案标准化的候选者。两种基于格，一种基于多元密码学。此外有三个备选方案，基于哈希函数、零知识证明以及多元方案。许多其他参加第一轮和第二轮选举的候选人已被淘汰。请参考 IEEE 最近发表的关于领先的后量子算法的评估。这些算法的简要总结如下:

6.3.1 入围基于格的密码系统

基于格结构的密码系统是基于被称为格子的几何结构。格是存在于 n 维空间中的点的周期性结构。像最短向量问题(SVP)这样的问题是 NP-Hard 的，它涉及到确定存在于这样一个格内两点之间的最短非零向量。这个问题和其他相关的问题不能用量子计算机非常有效地解决。由于这些方案的实现在计算上执行起来很简单，因此它们非常适合在区块链中使用。不幸的是，它们目前都需要存储/使用大的密钥键。这些增加的密钥大小引入了大量的传输延迟，即使处理时间通常比 RSA 对应的快。由于共识机制寻求以最佳方式同步验证处理和网络通信，因此减少处理时间和提高传输延迟的影响取决于区块链/DLT。

Crystals-Dilithium 就是这样一种数字签名方案，它的计算难度与基于格的密码系统有关。Crystals (Cryptographic Suite for Algebraic Lattices)组织建议使用 Dilithium -1280x1024 参数集，以实现大约 128 位的安全性，对抗所有已知的经典和量子攻击。Crystals-Dilithium 数字签名方案是 NIST 第三轮数字签名算法的候选方案。Dilithium 方案的优化版本对于区块链的部署非常有意义，因为从执行的角度来看，它们代表了一些最快的方案。为了减少密钥大小，还需要做一些额外的工作。

Falcon 是另一个进入第三轮决赛的基于格的签名方案。与其他基于格的方案相比，它的数字签名尺寸更小。与其他相关方案相比，快速傅立叶采样的使用也使得数字签名的生成和验证操作更快。Falcon 也可能是在区块链中使用的一个有前途的候选者。

6.3.2 最终入选的多元密码系统

多元密码系统被期望达到对量子计算机攻击的有力抵抗，因为它们依赖与求解多元多项式方程组相关的计算难度。基于多变量的签名方案可以以一种相对有效的方式实现，并且只需要相当少量的计算资源。从区块链的角度来看，这些属性是非常需要的。尽管这些方案产生的签名相对较短，但它们可能需要使用相对较大的公钥。然而，这些方案不像基于格的同类方案那样经过审查。

Rainbow 是 NIST 第三轮选出最终入围的多元方案。它是基于求解随机多元二次系统的 NP-Hard 难度。从区块链的角度来看，Rainbow 的使用显示了相当大的前景，因为它非常高效的签名生成和验证操作。

6.3.3 替代候选者

SPHINCS+ (基于哈希的):SPHINCS+是一种无状态的、基于哈希的数字签名方案，因此具有“临时替代”现有数字签名方案的优势。对原始 SPHINCS 方案进行了改进，以减少其数字签名的大小。此方案依赖于一系列单向散列的相关性。此方案的更安全版本可能不具备在区块链环境中使用所需的性能特征。

Picnic (MPC-in-the-head ZKPoK):与许多其他后量子数字签名候选方法相比，Picnic 基于一种不同的方法。它不是基于数论的计算“难度”级别，而是利用零知识证明的概念，结合对称密码学、哈希函数和块密码。尽管基于 Picnic 的方案(如 Picnic2)具有一定的安全优势，但它们可能不具备部署区块链所需的性能特征。

GeMSS (HEv- Multivariate): GeMSS (Great Multivariate Short Signature)是一种基于多变量的

签名方案，它产生的签名相对较小。相关的签名验证过程被认为是快速的，并且它使用了一个中/大型公钥。更安全版本的 GeMSS 的整体性能可能是区块链部署的一个问题。

6.3.4 其他有趣的候选者

qTESLA 是另一种基于格的数字签名方案，它是 NIST 第二轮后量子数字签名的候选方案，但没有入选第三轮。它依赖于带有错误的决策环学习(R-LWE)问题的计算难度。虽然 qTESLA 的实现相对简单，而且被认为是相当快的，但该方案使用的密钥键尺寸相对较大。这是被评估的一种用于保护超级账本框架（Hyperledger Fabric）免受未来量子计算机攻击的方案。

6.4 量子区块链

除了上述的经典解决方案，学术研究目前正在探索利用量子效应来对抗量子计算机对区块链威胁的可行性。以“量子对抗量子”——人们期望由量子技术建立的量子区块链来提供最终的安全性。这些系统不合并后量子算法作为手段来增加对量子攻击的抵抗，而是更原生地采用量子效应，如量子纠缠。

到目前为止，量子区块链还没有真正的实现。Kiktenko 等提议使用现有的量子密钥分发或 QKD 来保护区块链。Del Rajan 和 Matt Visser 的研究描述了一个量子区块链的概念设计，包括将区块链编码到一个时空 GHZ (Greenberger-Horne-Zeilinger)状态的光子，这种光子在空间中不共存。快速量子拜占庭协议已经被数学证明能够在恒定的时间内达成共识。

这些杠杆量子效应为降低 DLT 系统的时间复杂性提供了进一步的机会。就像量子纠缠驱动的 BFT 共识一样，定义了存储链上事务的数据结构的 Merkle 树可能不再需要以顺序方式解密。有点类似于流行的加密“Rollup”解决方案，量子区块链将能够利用高维矩阵来并行化这一过程并批处理 Merkle 树验证。类似地，量子特性使替代机制能够实现零知识证明的特性，就像 ZCash 所必需的那样。这些仍然主要是理论领域。我们离此类区块链的真实用例和部署肯定还有很多年。更详细的量子区块链讨论超出了本文的范围。

7 结论：从前量子到后量子区块链的转变

量子计算的进步已经在 DLT/区块链社区引发了一种越来越紧迫的意识，即确定既有效又能实用部署的后量子算法。从前量子到后量子区块链的转变是保证量子时代区块链安全的必要条件。广泛使用数字签名支持进行区块链交易是一个主要的漏洞。因此，开发和选择合适的后量子数字签名算法受到了广泛关注，这些算法适合于区块链应用程序，并且可以随着时间的推移逐步落地。一些要求概述如下：

首先，当前用于实现区块链节点的某些硬件可能不适合一些计算密集的后量子加密系统。因此，后量子方案应在安全性和计算复杂性之间进行平衡，以便不限制可能与区块链交互的潜在硬件。一种可能性是根据可用的硬件对密钥强度进行分级。

第二，某些后量子密码系统会产生大量开销，可能会影响区块链的性能。为了解决这个问题，未来的后量子开发者将不得不最小化密文开销，并考虑潜在的压缩技术。

最后，为了提高安全性，一些后量子方案可能会限制使用相同密钥签名的消息的数量。因此，有必要不断生成新的密钥，这涉及到投入计算资源和减慢某些区块链进程。

因此，区块链开发者将不得不从速度和交易两个角度来决定如何调整这样的密钥生成机制，以优化区块链的效率。

NIST 后量子密码标准化项目被广泛认为是推动后量子算法选择和采用的权威。截至 2020 年 9 月，基于格结构的密码系统 Crystals-Dilithium 和 Falcon 算法希望很大，因为它们已被选为第三轮数字签名最终的竞争方案。同样的，彩虹多元方案也被第三轮选中可以使用。然而，考虑到区块链应用的具体要求，也可能需要应用其他签名方案。

附录：名词表

Cryptographic	密码的
Immutability	不可篡改性
Cryptography	密码学
Lattice-based	基于格的
Quantum Computer	量子计算机
Cryptographic Primitive	密码学原语
Quantum Supremacy	量子霸权
Quantum-vulnerable	量子脆弱性
Random Number Generation	随机数生成
Quantum Random Number Generator, QRNG	量子随机数生成器
Public-key Cryptography	公钥密码学
Satoshi	中本聪
Hyperledger Fabric	超级账本框架
Multivariate cryptography	多元密码学
NP-Hard	NP-Hard
Entanglement	量子纠缠
Merkle tree	Merkle 树
Stake	权益
ZK-STARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
ZK-SNARK	Zero-Knowledge Scalable Transparent Arguments of Knowledge
Position paper	技术意见书
Public address	公开地址
Rainbow multivariate scheme	彩虹多元方案
Security exposure	安全风险敞口