计算机科学
COMPUTER SCIENCE

一种量子安全拜占庭容错共识机制

任畅，赵洪，蒋华

引用本文

任畅，赵洪，蒋华. 一种量子安全拜占庭容错共识机制[J]. 计算机科学, 2022, 49(5): 333-340.

REN Chang, ZHAO Hong, JIANG Hua. Quantum Secured-Byzantine Fault Tolerance Blockchain Consensus Mechanism[J]. Computer Science, 2022, 49(5): 333-340.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400154

一种量子安全拜占庭容错共识机制

任 畅[1,2] 赵 洪[1] 蒋 华[1,2]
1 北京电子科技学院 北京 100070
2 西安电子科技大学通信工程学院 西安 710071
(vinochange@foxmail.com)

摘 要 针对经典区块链共识机制面临量子计算机攻击的问题,提出了一种量子安全拜占庭容错共识机制。首先,对于公钥数字签名存在的安全隐患问题,采用QKD网络进行量子密钥分发,通过经典网络传输消息和签名等信息,提出了一种基于量子密钥分发(Quantum Key Distribution,QKD)和多线性哈希函数族的无条件安全签名方案(Multilinear Hash-Unconditionally Secure Signature,MH-USS),该方案中的签名具备不可伪造性、不可抵赖性以及可传递性,并且该方案可在现有设备上实现,具有较高的实用价值。然后,针对经典拜占庭容错共识机制PBFT共识效率相对较低的问题,提出了一种QS-BFT(Quantum-Secured Byzantine Fault Tolerance)共识机制。最后,通过增设"快速-标准"双共识模式以及允许节点对空区块投票的方式,减少系统通信次数并消除视图转换过程,使方案不仅具备安全性与活性,还能够有效降低消息复杂度,提高共识效率。对所提方案进行仿真实现与性能测试,结果表明,与改进后基于MH-USS签名方案的PBFT共识机制相比,所提方案吞吐量更高、时延更短。

关键词:区块链;共识机制;量子密钥分发;无条件安全;数字签名
中图法分类号 TP391

Quantum Secured-Byzantine Fault Tolerance Blockchain Consensus Mechanism

REN Chang[1,2],ZHAO Hong[1] and JIANG Hua[1,2]
1 Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 College of Communication Engineering,Xidian University,Xi'an 710071,China

Abstract Aiming at the problem that the classical blockchain consensus mechanism is under the threat of quantum computing attacks,a quantum-secured Byzantine fault tolerant consensus mechanism is proposed. Firstly,to solve the security threat of public key digital signature,this paper proposes a multilinear hash-unconditionally secure signature(MH-USS) signature scheme based on quantum key distribution (QKD) and multilinear hash function family. In this scheme,quantum keys are distributed through QKD network,messages and signatures are transmitted through classical network,and the simplified USS signature scheme is adopted as the main framework,combined with the family of multiple linear hash functions,to generate a new USS scheme. This signature scheme has the characteristics of unforgeability,non-repudiation and transferability. Moreover,this scheme can be implemented on existing equipment and has high practical value. Secondly,in view of the relatively low consensus efficiency of the classical Byzantine fault-tolerant consensus mechanism PBFT,this paper proposes the quantum secured-byzantine fault tolerance (QS-BFT) consensus mechanism. By adding "fast-normal" consensus mode and allowing nodes to vote on empty blocks,the system communication times are reduced and the view conversion process is avoided. It has been proved that this scheme not only guarantees the safety and liveness,but also effectively reduces message complexity and improves consensus efficiency. The simulation and performance test for this scheme indicate that the throughput of this scheme is higher and the delay is lower compared with the PBFT consensus mechanism which is based on the MH-USS signature scheme.

Keywords Blockchain,Consensus protocol,Quantum key distribution,Unconditionally secure,Digital signatures

到稿日期:2021-04-15 返修日期:2021-09-07
基金项目:国家重点研发计划(2018YFE0200600)
This work was supported by the National Key R&D Program of China(2018YFE0200600).
通信作者:赵洪(zh@besti.edu.cn)

1 引言

2008年，中本聪首次提出比特币[1]概念，并采用区块链技术作为其底层技术支撑。区块链发展至今，已成为当今科技领域的热门话题，被认为是人类历史上的第四次工业革命。区块链融合密码学、共识机制、分布式数据存储、点对点通信等新型技术体系，可构建具备去中心化和不可篡改等特性的分布式系统，改变传统依托中心化模式的分布式体系。

区块链架构根据功能可划分为4层，依次为用户层、服务层、核心层和基础层[2]，其中基础层和核心层为区块链系统提供基础运行环境和共识服务。区块链是一种基于密码学原理的分布式账本技术，数字签名用于保护区块链数据的完整性和不可伪造性等，哈希指针使区块按顺序首尾相连。当前主流区块链系统，如比特币、以太坊[3]等，均使用经典密码学算法和共识机制来维护系统的稳定性、安全性和可用性。系统采用依赖于数学困难问题的经典密码算法，并且假设敌手节点能力有限，不能破解数字签名和哈希函数。系统的安全性取决于系统中最薄弱的环节，上述假设会在量子计算攻击环境下失效，使区块链系统面临严重的安全威胁。例如，在使用传统公钥签名算法的区块链系统中，存在被攻击方利用Shor算法[4]破解其公钥系统的风险；在比特币系统中，存在被攻击方利用Grover算法[5]实现51%攻击的风险。因此，如何将区块链技术与抗量子攻击技术相结合，令区块链平台具备抗量子计算攻击的安全性，并根据区块链应用场景设计和优化共识机制，提高共识效率，是当今量子安全区块链技术应用中的研究前沿与热点。

为应对量子计算对区块链平台的安全威胁，量子通信研究领域已在区块链技术中引入量子密码技术方案。文献[6]在加密货币区块链平台中引入了量子货币协议。文献[7]首次提出将经典智能合约与量子闪电相结合的经典-量子混合支付区块链系统。文献[8]设计了一种在区块链数据结构中引入时间纠缠的新型量子区块链。但上述方案中涉及的量子技术大多仍处于理论研究阶段[9]，实现难度大，可行性低。量子密钥分发(Quantum Key Distribution，QKD)技术是目前发展得最为成熟的量子密码技术，已进入规模化商用阶段。QKD技术结合量子真随机性和量子不可克隆原理，基于物理安全设计出“一次一密”加密系统，成功实现了点对点安全通信，是一种具备无条件安全特性的通信方案。文献[10]提出了量子安全区块链解决方案(Quantum-secured Blockchain，QB)，该方案构建了量子-经典两层区块链网络模型，即在量子网络层使用QKD方式进行对称密钥分发，其余通信均在经典网络层进行，与其他量子区块链方案相比，QB区块链的可行性更高。QB区块链采用基于QKD和Toeplitz哈希函数的无条件安全消息认证方案框架，但缺乏对该认证方案具体内容的详细描述。由于QB区块链采用了基于原始状态机复制的共识机制[11]，使得系统内的通信复杂度很高，如果系统中存在较多作恶节点，则会导致节点间的通信次数呈指数级增长，共识效率很低，不具备可扩展性。文献[12]以QB区块链框架为基础，提出了量子安全区块链方案(Logicontract，LC)，其中数字签名采用基于QKD的无条件安全Toeplitz群签名方案，但Toeplitz函数与其他主流Universal哈希函数[13]相比，其运算速度较慢且需要占用较大的存储空间[14]。LC区块链采用一种具备抗碰撞性的哈希函数，用于计算哈希指针的哈希函数，但该方案仍面临被量子计算攻击的风险。LC区块链采用简化后的YAC(Yet Another Consensus)[15]共识机制，该共识机制要求拜占庭节点比例小于1/4，即容错率低于主流拜占庭容错共识机制的1/3，且该共识机制的网络通信复杂度较高。

结合上述研究与分析，本文提出了一种可以抵抗量子计算攻击的区块链共识机制。在区块链架构的基础层，采用量子-经典两层对等网络。在核心层，提出了基于QKD的无条件安全签名MH-USS方案，并引入可以抗量子计算攻击的参数哈希函数[16]，在保证区块链哈希指针和数字签名安全的前提下，优化实用拜占庭容错共识机制(PBFT)[17]，并设计了量子安全拜占庭容错(Quantum-Secured Byzantine Fault Tolerance，QS-BFT)共识机制，通过动态选择共识模式来消除传统视图转换过程，以有效减少通信次数，提高共识效率，降低通信资源开销。

2 预备知识

2.1 多线性哈希族

文献[13]首先提出Universal哈希函数，用于构造对称加密签名方案。多线性哈希函数族(Multilinear Hash Family)[18]是一种Universal哈希函数族，具有计算速度快、占用存储空间小等优点。

定义1 设$H=\{h:X\to Y\}$，假设输入字符串x、随机数r和大素数M。将x以n维向量的形式表示为$x=[x_1,x_2,\cdots,x_n]$，其中，x_i表示x的第i位，$x_i\in\{0,1,\cdots,M-1\}$；将密钥r以$n+1$维向量的形式表示为$r=[r_1,r_2,\cdots,r_{n+1}]$，其中$r_i$表示$r$的第$i$位，$r_i\in\{0,1,\cdots,M-1\}$。定义多线性哈希函数族为：

$$h(x)=r_1+\sum_{i=1}^{n}r_{i+1}x_i \bmod M \tag{1}$$

当输入值x的长度小于n时，剩余位置补0占位。多线性哈希函数族属于强Universal哈希函数族[13]，满足以下两个条件。

(1)对于每一个$x\in X,y\in Y$，满足：

$$|\{h\in H:h(x)=y\}|=|H|/|Y|$$

(2)对于每一个$x_1,x_2\in X,x_1\neq x_2,y_1,y_2\in Y,y_1\neq y_2,\tau\in R^+$，满足：

$$|\{h\in H:h(x_1)=y_1,h(x_2)=y_2\}|\leqslant\tau|H|/|Y|$$

2.2 参数哈希函数

在主流区块链中，常采用SHA-256，Scrypt等经典哈希函数来构建哈希指针，并用于构建区块链数据结构和Merkle树。目前认为经典哈希函数能够抵抗量子计算攻击，因为量子算法尚未解决NP-hard问题[19]，所以通常采取将经典哈希函数输出长度增加一倍的方式来抵抗量子计算攻击，但此

方法目前只适用于抵抗 Grover 算法攻击，其仍存在被其他量子算法攻击的风险。

本共识机制采用由文献[16]提出的参数哈希函数(Parametric Hash Function)来构建哈希指针，该函数是专门为区块链设计的，可以抵抗量子计算攻击，具备抗碰撞性，且雪崩效应明显，当输入改变 1 比特的信息时，输出结果将产生 50%的变化。该函数基于希尔伯特第十问题，即在未知数个数大于整数多项式方程个数且方程组含有 3 次以上的多项式时，求解该整数多项式方程的整数根。该问题无算法可解[16]，因此理论上可以抵抗量子攻击。

定义 2　参数哈希函数的定义如下。

(1)参数包括 n 维系数 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$，素数 p，系数 $a_i=\sigma_1 a_1+\sigma_2 a_2+\cdots+\sigma_n a_n$，以及由 $m(m>n)$ 个系数 a_i 构成的矩阵 $\boldsymbol{A}=(a_1,a_2,\cdots,a_m)$。

(2)构建参数哈希函数：

$$f(x)=[a_1 f_1(x)+a_2 f_2(x)+\cdots+a_m f_m(x)]\bmod p \quad (2)$$

其中，f_i 的定义形式不限，例如 f_i 可以取：

$$f_i(x)=[a_1 x_1 x_2 x_3+a_2 x_2 x_3 x_4+\cdots+a_m x_m x_1 x_2] \bmod p \quad (3)$$

3　签名方案设计

3.1　MH-USS 签名方案

无条件安全量子签名方案将量子真随机性、量子不可克隆原理与一次一密相结合，以保证方案的无条件安全性[12]。本文提出了基于 QKD 和多线性哈希函数族的 MH-USS 签名方案。该方案通过量子网络进行量子密钥分发，在经典网络中传输消息和签名等信息，并采用简化后的 USS(Unconditionally Secure Signature)签名方案[20]作为主要框架，结合多重线性哈希函数族，建立一套适用于 QS-BFT 共识机制的 MH-USS 签名方案。该方案中的签名具备不可伪造性、不可抵赖性、可转移性以及无条件安全性[21]。

与 LC 群签名方案[12]采用的 Toeplitz 哈希函数族相比，本文方案采用的多线性哈希函数族的摘要计算速度比 Toeplitz 快 8 倍，更适合用于通信次数较多的投票式拜占庭容错共识机制，可缩短计算时间，提高签名效率。

MH-USS 签名方案主要包括 3 个部分：密钥分发、签名生成以及签名验证。

3.1.1　密钥分发

假设签名方案中有 1 个签名者和 K 个验签者。签名者和验签者均使用量子网络，并通过 QKD 方式进行密钥分发。

(1)签名者生成 K^2 个密钥 $r=(r_1,r_2,\cdots,r_{K^2})$，用于构建多线性哈希函数 $h(x)$。

(2)签名者进行密钥分发：将 $r_i=(r_{(i-1)K+1},\cdots,r_{iK})$ 发送给验签者 P_i。

(3)每个验签者 P_i 将密钥 $r_j\in r_i$ 分别发送给其他验签者 P_j，P_j 将全部验签者发来的密钥记为 $r_{i\to j}$。

3.1.2　签名生成

(1)签名者按照式(1)计算签名，其中的 $h(m)$ 采用式(1)中的多线性哈希函数。

$$Sign(m)=(h_1(m),h_2(m),\cdots,h_{K^2}(m))=(t_1,t_2,\cdots,t_{K^2}) \quad (4)$$

(2) 签名者使用经典信道将$(m,Sign(m))$发送给各个验签者。

3.1.3　签名验证

(1)验签者 P_j 通过密钥 $r_{i\to j}\in R_{i\to j}$ 计算 $h_{i\to j}(m)$，若满足 $t_{i\to j}=h_{i\to j}(m)$，则 $T^m_{i\to j}=1$，否则 $T^m_{i\to j}=0$。

(2)验签者 P_j 计算 $\sum_{i=1}^{K} T^m_{i\to j}$。若满足 $\sum_{i=1}^{K} T^m_{i\to j}>K\delta$，则表示签名有效，接受该签名，否则拒绝该签名。其中，$\delta=\frac{1}{2}+d$，d 表示全部节点中拜占庭节点所占的比例，本文中 $d=\frac{1}{3}$。

3.2　安全性分析

MH-USS 签名方案满足不可伪造性、不可抵赖性、可转移性以及无条件安全性[21]。USS 签名方案[20]基于强哈希函数族的特性，证明了 USS 方案满足上述特性。MH-USS 采用的多重线性哈希函数族也属于强哈希函数族，且对 USS 的简化过程只涉及系数调整，不影响签名安全性，故 USS 证明方法同样适用于 MH-USS 方案，此处省略其证明过程。

4　QS-BFT 共识机制设计

PBFT(Practical Byzantine Fault Tolerance)是最经典的共识机制之一，其能够保证系统各节点按相同的顺序执行相同的命令，有效避免区块链分叉问题，是强一致型拜占庭容错共识机制的基础，但 PBFT 在视图转换过程中显著增加了通信复杂度，因此，Zyzzyva[22]，SBFT[23]，Hot-stuff[24] 和 Tendermint[25]等共识机制均在 PBFT 基础上分别从用户角色、签名方案等角度优化共识方案，但均不具备抵抗量子计算攻击的能力。因此，本文提出了 QS-BFT 共识机制，与 PBFT 相比，QS-BFT 具有以下优点。

(1)QS-BFT 共识机制中，密码方案采用了 MH-USS 签名方案与参数哈希函数，具备抗量子计算攻击能力。

(2)优化共识策略，加入快速模式。QS-BFT 将共识过程分为快速模式和标准模式，引入 speculation 技术[12]，将主节点作为消息和投票的收集者，令每个从节点将投票消息发送给主节点。当主节点收到所有节点对同一区块的投票时，进入快速模式，否则进入标准模式。进入快速模式后，直接由主节点广播快速决议消息，有效减少了通信次数。与 PBFT 不同，从节点可避免进入通信复杂度较高的广播交互阶段。

快速模式表示网络中的所有节点均收到消息，诚实从节点可以确认全部节点已认证该区块有效，不会出现“分叉”等问题，可以直接进行决议阶段的投票。当主节点未收到至少 $2f+1$ 条有效投票时，进入标准模式，与 PBFT 相同，表示至少 $f+1$ 个诚实节点收到区块消息，进入“预备”状态，并且对该区块进行“预备阶段”的投票，表明此时已进入预备状态。随后进入承诺阶段，当主节点收到至少 $2f+1$ 条有效确认“预备状态”的投票后，再进行决议阶段的投票，对该区块达成

共识，防止出现“分叉”问题。

(3)消除 PBFT 视图转换过程。当节点未收到有效消息时，与 PBFT 不同，QS-BFT 共识机制中的节点可对空区块投票，无需启动复杂度较高的视图转换。在决议阶段，若节点对空区块投票达成一致，直接进入新一轮决议，对下一个新区块进行新一轮投票，保证了系统内各阶段间的连续性，减少了从节点需要接收和验证的消息数量，通信效率更高。

4.1 系统模型

4.1.1 网络模型

如图 1 所示，QS-BFT 共识网络分为量子网络层和经典网络层，且节点之间均采用点对点技术来传输数据。在量子网络层，节点间传输 MH-USS 签名方案所需的密钥，其余信息均在经典网络层中传送。网络共有 $N=3f+1$ 个节点，在 N 个节点中，有 f 个节点是拜占庭节点[17]，其余节点均为诚实节点，每个节点的索引号 $i\in\{0,1,\cdots,N-1\}$。本共识机制是一种拜占庭容错机制，网络模型为同步网络，可以实现状态机复制。

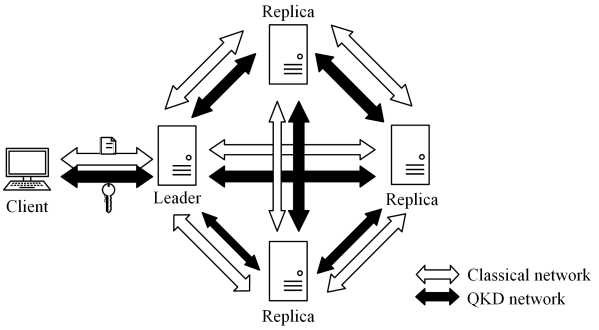

图 1 网络结构图

Fig. 1 Network structure diagram

QS-BFT 共识网络内的节点角色分为主节点和从节点，该网络以轮转机制运行，以客户端将请求消息发送至主节点为开始，以客户端接收主节点反馈消息为结束，这一过程为一轮。每一轮有一个主节点，其余节点皆为从节点。主节点不仅负责在本轮网络中的各阶段接收、整合与传达消息，还可切换为从节点角色，即负责消息的验证、投票、执行和记录。每一轮都会采用轮转机制进行主节点的选举和更替，每一轮的主节点编号 $L=r \bmod N$，r 表示当前轮编号。

4.1.2 消息格式

各节点均配置计时器，设置节点接收消息的最大窗口时间为 T，即节点发出消息 M 后计时开始，直到 T 结束。主节点发送消息的格式为$\langle \text{phase}, r, Cert(\sigma)\rangle_{\sigma_l}$，phase 表示当前阶段，$r$ 表示当前轮数，$Cert(\sigma)$表示主节点的消息凭证，是将全部有效投票中的签名整合为一个签名集合。σ_l表示主节点 L 对该消息进行 MH-USS 签名。从节点发送消息的基本格式为$\langle \text{phase}, r, x\rangle_{\sigma_i}$，其中，当 $x=h(p)$时，该消息表示从节点为新区块 p 投票，$h(p)$表示使用参数哈希函数计算新区块 p 的哈希值；当 $x=\perp$时，该消息表示从节点为空区块投票。

收到消息 M 后，节点首先对消息 M 进行有效性验证：1)是否在规定时间 T 内收到消息 M；2)验证签名 σ 的有效性；3)验证轮编号 r 是否等于当前轮编号；4)验证消息凭证 $Cert$ 的有效性；5)计算哈希值 $h(p)$是否正确。如果消息 M 通过验证且格式符合规定，则节点判定该消息有效，接受该消息。

图 2 给出了 QS-BFT 共识机制分别在快速模式和标准模式下的消息分发流程。

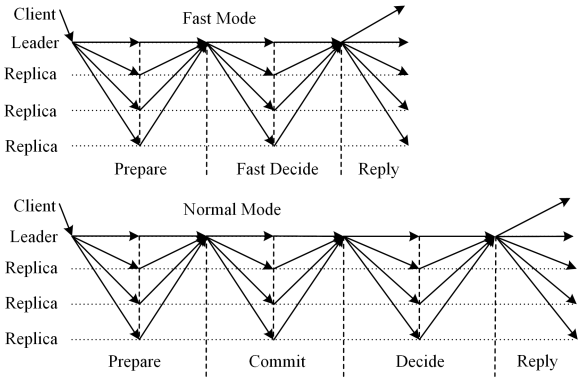

图 2 QS-BFT 共识过程消息分发流程

Fig. 2 Message distribution process of QS-BFT consensus

4.2 QS-BFT 共识机制流程

4.2.1 准备阶段

客户端将已进行 MH-USS 签名的请求消息发送至主节点，主节点将收到的全部有效请求整合为新区块，写入预准备消息中，再将已进行 MH-USS 签名的预准备消息进行广播。如果从节点收到预准备消息且成功验证该消息有效，则向主节点发送对新区块的投票；否则对空区块投票。

4.2.2 模式选择

主节点在发出请求后启动一个计时器 T，记快速模式耗时为 T_1，记标准模式耗时为 T_2，则 $T<T_2-T_1$。在计时器 T 到期前，若主节点接收 $3f+1$ 条新区块有效投票或 $3f+1$ 条空区块有效投票，则进入快速模式；否则切换为标准模式，标准模式的条件为：1)计时器 T 已到期，若主节点接收到至少 $2f+1$ 条且不足 $3f+1$ 条新区块有效投票或空区块有效投票，则进入标准模式，并对该新区块或空区块进入下一阶段投票广播；2)计时器 T 已到期，若主节点未接收到至少 $2f+1$ 条新区块有效投票或空区块有效投票，则进入标准模式，并对空区块进入下一阶段投票广播。

(1)快速模式

主节点将收到的区块投票整合为快速预决议凭证后，广播该区块的快速预决议消息。如果从节点接收到新区块的快速预决议消息且验证有效，则将该区块写入本地，并将更新后的本地状态记入投票消息中，再向主节点发送对新区块的投票；否则从节点只向主节点发送对空区块的投票。最后，从节点锁定当前已投票的区块，并解锁之前已锁定的区块，进入对当前投票区块的锁定状态。

(2)标准模式

1)承诺阶段

主节点将收到的全部投票整合为预承诺凭证，如果主节点接收到至少 $2f+1$ 条对新区块的投票，则广播新区块的

预承诺消息；否则主节点广播空区块的预承诺消息。如果从节点接收到新区块的预承诺消息且验证有效，则向主节点发送对新区块的投票；否则向主节点发送对空区块的投票。最后，从节点锁定当前已投票的区块，并解锁之前已锁定的区块，进入对当前投票区块的锁定状态。

2）决议阶段

主节点将收到的全部投票整合为预决议凭证，如果主节点收到至少 $2f+1$ 条对新区块的承诺投票且验证有效，则广播新区块的预决议消息；否则主节点广播空区块的预决议消息。如果从节点接收到新区块的决议消息且验证有效，则将新区块写入本地区块链，并将更新后的本地状态记入投票消息中，再向主节点发送对新区块的投票；否则只向主节点发送对空区块的投票。

4.2.3　反馈阶段

主节点收到至少 $f+1$ 条决议投票并验证消息有效后，将收到的全部投票整合为反馈凭证并广播反馈消息。从节点和客户端接收反馈消息后，所有节点进入下一轮。

QS-BFT 共识流程如图 3 所示。

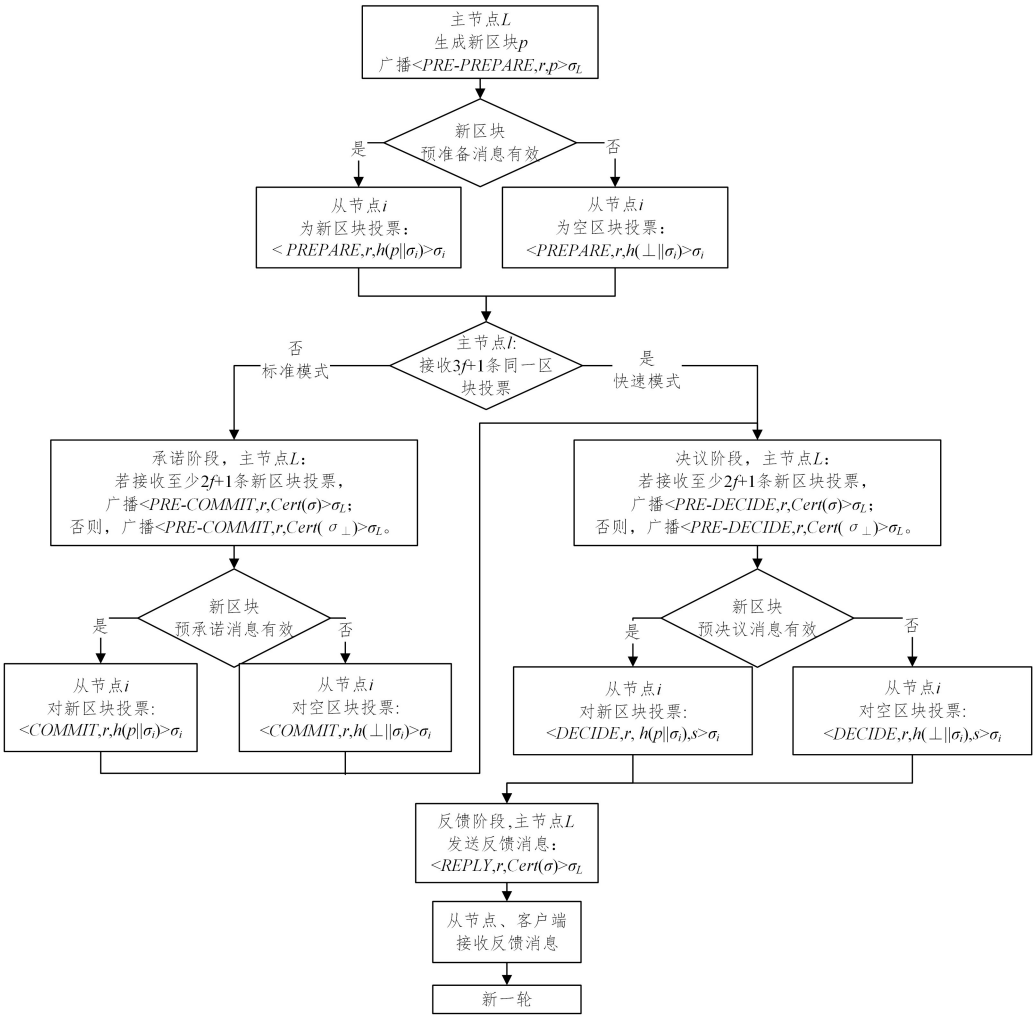

图 3　QS-BFT 共识机制流程图

Fig. 3　Flow chart of QS-BFT consensus mechanism

5　QS-BFT 共识机制分析

5.1　安全性证明

（1）QS-BFT 共识机制采用了抗量子计算攻击的密码算法，即参数哈希函数和 MH-USS 签名方案，且该签名方案具备不可伪造性、不可抵赖性、可转移性以及无条件安全性。即使敌手具有无限计算资源，仍可保证区块链中数字签名和哈希指针的安全性。

（2）假设在第 r 轮中，诚实节点 i 接收到主节点发来的快速预决议消息或预承诺消息后，节点 i 会对新区块 p 加锁，直至下一轮收到上述消息后再解锁，在此期间节点 i 不再接收主节点发来的其他新区块 q，新区块 q 不能被节点 i 写入本地。进入新一轮 r 后，节点 i 接收到主节点发来的预准备消息后，才会进入准备阶段。因此，一个诚实节点在一轮决议中只能对一个新区块进行投票。

假设一个诚实节点 i 在第 r 轮将新区块 p 写入本地日志，则在承诺阶段至少有 $2f+1$ 个节点向主节点提交了关于新区块 p 的承诺消息，使得主节点可以生成承诺凭证发给节点 i。假设另一个区块 q 同样在第 r 轮被节点 i 写入日志，则至少有 $2f+1$ 个节点向主节点提交了关于新区块 q 的承诺投票。由于每条消息均由 MH-USS 签名方案签署，保证了消息的完整性、不可篡改和不可伪造，使拜占庭节点无法成功地伪造其他节点签名后的消息，因此每个节点最多发送一条有效承诺投票。由于系统内节点总数目为 $N=3f+1$，因此

可以推出，至少有 $f+1$ 个节点在同一轮中分别对两个不同的区块进行了投票操作，与“一个诚实节点在一轮中只能对一个新区块进行投票”矛盾，本假设不成立。如果 p 和 q 是两个不同的新区块，那么它们不能在第 r 轮被同时写入区块链。

由上述结果可推出，在同一轮决议中，一个诚实节点只能针对一个区块进行操作，且不同区块不能在第 r 轮决议中被同时写入区块链。因此，在同一轮决议中的任意两个诚实节点只能将同一个区块写入本地区块链，保证了共识机制的安全性。

5.2 活性证明

同步网络避免了出现诚实节点已发出消息但接收方未收到的故障情况。由于系统中至少存在 $2f+1$ 个诚实节点，因此主节点一定会收到至少 $2f+1$ 条投票消息。对于主节点来说，当接收到的同类型有效投票数量大于 $2f+1$ 时，主节点生成有效投票凭证发给从节点。当主节点没有收集到足量投票或投票凭证，以及当主节点超时无响应时，系统不必进入复杂的视图转换过程，而是由从节点提交对空区块的投票以及主节点生成空区块投票凭证，这表明当前节点没有就新区块达成一致，因此共识流程不会停滞在此阶段，所有节点均正常进入下一阶段继续完成投票、收集等任务，直至本轮决议结束，然后通过正常的轮转方式更换新节点，进入新一轮共识流程。本共识机制是确定性共识，在新区块的生成、提交等环节中满足强一致性，避免区块链出现不能达成一致或分叉的问题，保证了区块链的活性。

5.3 消息复杂度分析

依次计算 QS-BFT，QSYAC 和 PBFT 完成单次共识需要的消息复杂度。每种共识机制只计算一次共识过程中的前 3 个核心阶段，通过对比各共识机制的消息复杂度来分析通信效率。

首先计算 QS-BFT 的消息复杂度。假设 N 个节点参与 QS-BFT 共识，在每个阶段，主节点广播发送 $N-1$ 条消息，从节点向主节点发送 1 条消息。当系统处于快速模式时，即所有节点均正常工作时。在准备阶段，主节点广播预准备消息，从节点向主节点发送投票，该阶段的复杂度为 $(N-1)+(N-1)=2(N-1)$。在快速决议阶段，主节点广播含有准备凭证的快速决议消息，从节点向主节点发送相应投票，该阶段的复杂度为 $N(N-1)+N-1=N^2-1$。因此快速模式下的消息复杂度为 $2(N-1)+N^2-1=N^2+2N-3\approx N^2$。当系统处于标准模式时，与快速模式计算复杂度方法相同，易得该模式的消息复杂度约为 $2N^2$。QSYAC 和 PBFT 的核心流程消息复杂度的计算方法与 QS-BFT 相同，在忽略常量和低次幂后的复杂度计算结果如表 1 所列。

表 1 共识机制核心流程消息复杂度

Table 1 Complexity of selected protocols

Consensus protocol	Model	No faulty nodes's complexity	f faulty nodes's complexity
QS-BFT	$N=3f+1$	N^2	$2N^2$
QSYAC	$N=4f+1$	$2N^2$	$2N^2$
PBFT	$N=3f+1$	$2N^2$	N^3

由表 1 可知，QS-BFT 和 PBFT 的拜占庭节点占比大于 QSYAC，容错率更高。在节点均正常工作时，QS-BFT 的消息复杂度低于其他两种共识机制。在有节点发生故障时，QS-BFT 消息的复杂度与 QSYAC 相等，但低于 PBFT。QS-BFT 采用了多线性哈希函数族，其计算速度比 QSYAC 采用的 Toeplitz 哈希函数族快，签名和验签速度也更快。QS-BFT 共识机制与 QSYAC，PBFT 相比，其消息复杂度更低、签名速度更快、通信效率更高且可扩展性更佳。

5.4 协议实现及测试

首先通过 Go 编程语言分别对 QS-BFT 与基于 MH-USS 签名方案的 PBFT 共识机制（以下简称为 PBFT）进行仿真实现，然后进行性能测试，其结果不仅与共识机制相关，还与测试过程中的代码数据结构、生成新区块的方式和共识网络状态等相关。为了保证测试的公平性，对 QS-BFT 与 PBFT 采用相似代码结构，并只对单次交易进行共识，分别从吞吐量、延迟、容错性以及交易提交时间对吞吐量的影响 4 个方面对本文提出的区块链共识机制 QS-BFT 与经典 PBFT 共识机制进行对比测试。由于本地硬件条件有限，共识网络中的节点数量最大值取 13。通过测试结果对比可知，相比 PBFT 共识机制，QS-BFT 共识机制在吞吐量、时延方面均有显著提升，且容错性均满足系统模型 $N=3f+1$ 的要求。

5.4.1 吞吐量测试

吞吐量能够反映出共识机制对事务并发的处理能力。在区块链系统中，交易通常表示需要写入区块中的事务性操作。吞吐量通常用区块链系统在单位时间内处理的交易总量（Transaction Per Second，TPS）表示，单位为 tps。

首先测试 QS-BFT 共识机制与 PBFT 共识机制的网络规模对吞吐量的影响。分别在网络规模最小为 4 个节点、最大为 10 个节点时，进行 QS-BFT 和 PBFT 的吞吐量测试，记录二者对 1000 笔交易的处理时间，并重复进行 10 次的独立对比实验，计算平均吞吐量测试结果后，得到 QS-BFT 与 PBFT 的吞吐量对比图，如图 4 所示。

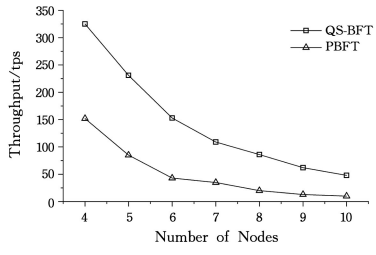

图 4 PBFT 与 QS-BFT 的吞吐量对比图

Fig. 4 Throughput comparison between PBFT and QS-BFT

由图 4 可知，在节点数量相同的情况下，QS-BFT 的吞吐量均高于 PBFT；且 QS-BFT 与 PBFT 的吞吐量均随着节点数量的增多而下降，但 QS-BFT 的下降趋势相对平缓。其原因在于 PBFT 在准备阶段与承诺阶段需要所有副本广播其投票消息，使副本之间产生大量通信开销，而 QS-BFT 通过主节点统一收集主节点投票的方式，减小了从节点之间的广播通信开销；并且由 5.3 节中的消息复杂度与通信次数计算结果

可知，QS-BFT 的消息复杂度和通信次数均小于 PBFT，若节点数量增加，则 QS-BFT 的资源消耗增加幅度小于 PBFT，因此其吞吐量下降幅度更小。

5.4.2　时延测试

时延表示交易从客户端提交到交易被写入区块的时间差。测试 QS-BFT 与 PBFT 共识机制的网络规模与时延的关系，分别在网络规模最小为 4 个节点、最大为 10 个节点时，进行时延测试，并重复进行 10 次的独立对比实验，记录平均时延，测试结果如图 5 所示。

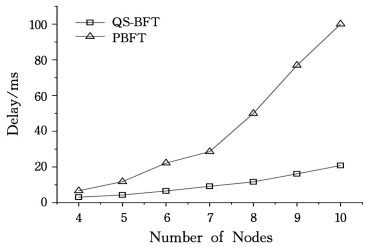

图 5　PBFT 与 QS-BFT 时延的对比图

Fig. 5　Delay comparison between PBFT and QS-BFT

由图 5 可知，在节点数量相同时，QS-BFT 相比 PBFT 时延更小；随着共识节点数量的增加，QS-BFT 与 PBFT 的平均时延均增加。这是因为 QS-BFT 取消了从节点广播，并在快速模式下取消了承诺阶段，有效缓解了主节点与从节点的端口通信压力，并且 QS-BFT 的消息复杂度更低，消耗资源更少，所以与 PBFT 相比，QS-BFT 的时延更低，且消息在低时延情况下，主节点与从节点收、发投票的速度更快，使网络节点达成共识的速度也更快。但随着节点数量逐渐增加，节点在密钥生成与分发、签名与验签、投票等各项环节的时间消耗均增加，导致 QS-BFT 与 PBFT 的总体时延上升。

5.4.3　容错性测试

QS-BFT 共识机制的系统模型为 $N=3f+1$，通过测试系统内无恶意节点与存在最大 f 个恶意节点对系统吞吐量的影响，来检测 QS-BFT 与 PBFT 的共识机制的容错性，其中恶意节点在系统内表现为宕机无响应或发送错误消息。当恶意节点数量大于 f 时，系统无法达成共识。

由图 6 可知，当网络节点数量固定、恶意节点数量取最大时，吞吐量随着恶意节点数量的增加而减少。对于 QS-BFT，当网络中共有 4 个节点时，恶意节点数 f 最大值取 1，此时吞吐量最高。若恶意节点数量大于 f，则系统无法达成共识；若恶意节点数量增多，则用户等待时间更长，而吞吐量随之减少。

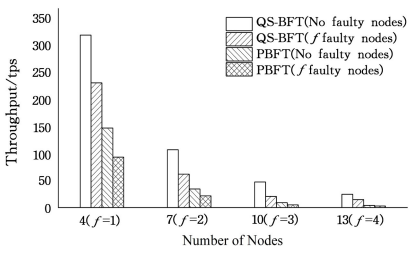

图 6　容错性对比图

Fig. 6　Comparison of fault tolerance

结束语　网络安全形势日益严峻，QS-BFT 共识机制对于保障区块链安全可靠运行有一定的理论价值和实践意义。本共识机制借助 MH-USS 签名方案和参数哈希函数，在不限制敌手计算能力的条件下，可保证区块链系统中哈希指针和数字签名的安全，从而使区块链安全运行。通过 QS-BFT 共识机制来完成状态机复制，以实现拜占庭容错，从而保证区块链的安全性和活性。QS-BFT 共识机制与同类共识机制相比，通过动态选择共识模式，可以降低消息复杂度，提升可扩展性。对本文方案进行仿真实现与性能测试，结果表明，与 PBFT 共识机制相比，本文方案的吞吐量更高、时延更低。未来将尝试研究适用于 QS-BFT 共识机制的量子门限签名，将通信复杂度降为线性，并在共识机制中加入节点信用评分机制，以提高拜占庭节点作恶成本以及区块链的运行效率。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. https://bitcoin.org/en/bi-tcoin-paper.

[2] China Institute of electronic technology standardization. Blockchain reference architecture[EB/OL]. https://www.hackliu.com/w-pcontent/uploads/file/20180305/1520220497223974.pdf.

[3] BUTERIN V. A next-generation smart contract and decentralized application platform[EB/OL]. https://whitepaperdatabase.com/wpco-ntent/uploads/2017/09/Ethereum-ETH-whitepaper.pdf.

[4] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. Siam Journal on Computing, 1997, 26(5): 1484-1509.

[5] GROVER L K. A fast quantum mechanical algorithm for database search[EB/OL]. https://arxiv.org/PS_cache/quant-ph/pdf/96-05/9605043v3.pdf.

[6] LUTOMIRSKI A, ARONSON S, FARHI E, et al. Breaking and making quantum money: toward a new quantum cryptographic protocol[J]. arXiv: 0912.3825, 2009.

[7] COLADANGELO A. Smart contracts meet quantum cryptography[J]. arXiv: 1902.05214, 2019.

[8] RAJAN D, VISSER M. Quantum Blockchain using entanglement in time[J]. ar-Xiv: 1804.05979, 2018.

[9] EDWARDS M, MASHATAN A, GHOSE S. A review of quantum and hybrid quantum/classical blockchain protocols[J]. arXiv: 1912.09280v1, 2019.

[10] KIKTENKO E O, POZHAR N O, ANUFRIEV M N, et al. Quantum-secured blockchain[J]. arXiv: 1705.09258, 2017.

[11] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages & Systems, 1982, 4(3): 382-401.

[12] SUN X, SOPEK M, WANG Q, et al. Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic[J]. Entropy, 2019, 21(9): 887.

[13] CARTER L, WEGMAN M N. Universal Classes of Hash Functions[J]. Journal of Computer and System Sciences, 1979, 18: 143-154.

[14] NEVELSTEEN W, PRENEEL B. Software performance of universal hash functions[C]// Advances in Cryptology-Eurocrypt'99. 1999: 24-41.

[15] MURATOV F, LEBEDEV A, IUSHKEVICH N, et al. YAC: BFT Consensus Algorithm for Blockchain[J]. arXiv: 1809.00554, 2018.

[16] SAZONOVA P, KRENDELEV S. Parametric Hash Function Resistant to Attack by Quantum Computer[C]// 2018 Federated Conference on Computer Science and Information Systems. 2018: 387-390.

[17] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[18] DANIEL L, OWEN K. Strongly universal string hashing is fast [J]. Computer Journal, 2014(11): 1624-1638.

[19] FERNANDEZ-CARAMES T M, FRAGA-LAMAS P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks[J]. IEEE Access, 2020, 8: 21091-21116.

[20] AMIRI R, ABIDIN A, WALLDEN P, et al. : Efficient Unconditionally Secure Signatures Using Universal Hashing[M]// Applied Cryptography and Network Security. Cham: Springer International Publishing, 2018: 143-162.

[21] ARRAZOLA J, WALLDEN P, ANDERSSON E. Multiparty Quantum Signature Schemes[J]. arXiv: 1505.07509, 2015.

[22] KOTLA R. Zyzzyva: Speculative Byzantine Fault Tolerance [C]// ACM Sigops Symposium on Operating Systems Principles. 2007.

[23] GUETA G, ABRAHAM I, GROSSMAN S, et al. SBFT: a Scalable Decentralized Trust Infrastructure for Blockchains[J]. arXiv: 1804.01626v1, 2018.

[24] YIN M, MALKHI D, REITER M K, et al. HotStuff: BFT Consensus with Linearity and Responsiveness[C]// 2019 ACM Symposium. 2019.

[25] KWON J. Tendermint: Consensus without mining [EB/OL]. https://tendermint.com/static/docs/tendermint.pdf.

REN Chang, born in 1994, postgraduate. Her main research interests include quantum secure communication and security of blockchain.

ZHAO Hong, born in 1978, lecturer. His main research interests include cyberspace security and research of cryptographical applications.

(责任编辑:李亚辉)