量子区块链：融合量子信息技术的区块链能否抵御量子霸权？

张俊[1,2]，袁勇[1]，王晓[1]，王飞跃[1]

（1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室，北京 100190；
2. 武汉大学电气与自动化学院，湖北 武汉 430072）

摘　要：区块链的广泛应用使越来越多的学者聚焦到安全加密这一重大问题上。然而，随着电子计算机技术的飞速发展，远超传统计算速度和数据处理容量的量子计算机已经逐步从理论走向实践，它的极大算力将给区块链的链内安全带来巨大和根本性的挑战。介绍了量子信息的两大核心应用，分析了量子霸权对区块链现行的共识方式和加密算法的破解方式。同时，针对目前区块链的漏洞，提出量子区块链以防止量子计算带来的攻击威胁，并阐述了量子通信技术的原理与应用方法，举例说明了量子区块链的安全性与可行性。最后，对目前量子计算存在的几大技术挑战进行了分析。

关键词：区块链；加密算法；量子霸权；量子信息技术；量子区块链

中图分类号：TN918.91

文献标识码：A

doi: 10.11959/j.issn.2096−6652.201945

Quantum blockchain: can blockchain integrated with quantum information technology resist quantum supremacy?

ZHANG Jun[1,2], YUAN Yong[1], WANG Xiao[1], WANG Fei-Yue[1]

1. The State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China
2. School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China

Abstract: Quantum computers, which substantially exceed traditional computing speed and data processing capacity, are gradually moving from theory toward practice. The tremendous computing power of quantum computers will bring fundamental challenges to current information encryption mechanism. Two key applications of quantum information technology were introduced, followed by comments on how quantum supremacy threatens the current blockchain consensus and encryption mechanisms. Meanwhile, considering loopholes existing in the current blockchain technology, a blockchain system integrating quantum technology was discussed aiming to prevent the threat of quantum supremacy.

Key words: blockchain, cryptographic algorithms, quantum supremacy, quantum information technology, quantum blockchain

1　引言

1.1　区块链

随着比特币等数字加密货币的普及，区块链作为一种全新的去中心化架构与分布式计算范式逐渐兴起，受到国内外各行业的广泛关注与高度重视[1]。区块链通过密码学原理、分布式存储、共识机制与智能合约四大核心技术为数据存储提供了一种全新的可信任分布式解决方案。总体来说，区块链通过块链式结构来验证和存储数据，通过非对称加密算法保障数据访问与传输安全，通过各分布式节点的工作量证明（proof-of-work，POW）等共识算法保障数据安全更新，并通过广义执行脚本操作和处理数据。

区块链作为一种普适性技术框架，已在数字金融、物联网、智能制造等多个领域引发深刻变革[2]。

收稿日期：2019−11−01；修回日期：2019−11−29
通信作者：张俊，jun.zhang.ee@whu.edu.cn

自 2008 年中本聪发布《比特币：一种点对点的电子现金系统》以来，区块链已经发展了 11 年。2015 年，中国区块链应用研究中心首次在北京成立；2016 年，我国发布《中国区块链技术和应用发展白皮书（2016）》[3]，将区块链列为国家重点关注技术；2019 年 10 月 24 日，中共中央政治局第十八次集体学习中，习近平总书记强调“把区块链作为核心技术自主创新的重要突破口”，将同时具备开放、共享、安全、可信的区块链技术列为未来发展的重点。这一系列事件体现出我国对区块链技术的重视程度及区块链技术本身蕴含的巨大潜力和广阔前景。

1.2 区块链与信息加密技术

区块链的核心是通过密码学保障的链式分布式数据库，因此可以说密码学是区块链安全的最根本保障。节点间通信用到的双向加密算法通常可分为对称加密算法和非对称加密算法[4]。

（1）对称加密

对称加密方案也称为对称密钥、秘密密钥和单密钥，它通过使用一对相同的密钥对数据进行加解密，该方法的特点是计算工作量小、执行速度快，但安全隐患大，至今仍广泛应用于数据加密和消息完整性检查等方面。经典的对称加密算法包括数据加密标准（data encryption standard，DES）、高级加密标准（advanced encryption standard，AES）等。

DES 算法使用 56 位密钥对 64 位分组数据进行加密，其加密过程和解密过程使用相同的密钥。DES 是一种迭代算法，对明文中每个分组的加密过程都包含 16 轮，且每轮的操作完全相同。DES 通过迭代执行分组密码的 2 种本源操作——混淆与扩散，达到数据加密的目的。混淆可以尽量模糊密钥与密文之间的关系，实现混淆的常用操作就是替换；扩散是为了消除密文所反映的明文的统计结构，常用的操作为位置换。在进行 DES 加密时，每个分组数据都会进行 16 轮的加密，其中每一轮的密钥 k_i 都由主密钥 k 推导得来。随着计算能力的不断提升，56 位的密钥已无法保证机密数据的安全，故 DES 被逐渐淘汰。

AES 是目前使用较为广泛的加密算法之一，已在各大行业系统中得到大规模应用。到目前为止，针对 AES 最有效的破解方式是蛮力攻击。AES 通过 128 位、192 位、256 位密钥对 128 位分组数据进行加密。加密过程涉及字节替换、行位移、列混淆和轮密钥加 4 种操作，由于每一步都是可逆的，对密文按照相反的顺序操作即可恢复明文。密钥长度的不同，AES 加密的轮数也随之不同，例如 128 位对应的轮数是 10 轮，而 192 位对应的轮数是 12 轮。相比 DES 来说，AES 具有更高效的异或运算、更低耗的资源需求、更灵活的编程兼容[5]等优势。到目前为止，在抵抗主流的暴力破解方面，AES 几乎是牢不可破的，如果以现阶段市场主流的 CPU 的计算能力来衡量，大概需要 225 年才能攻破 AES 加密。

对称加密的使用历史至少已有 4 000 年，技术也已十分成熟，但对称加密中密钥分配通信模式问题是其固有的弱点，而非对称加密模式则解决了该问题。

（2）非对称加密

对称密码的目标通常是使输入和输出之间不存在紧凑的数学描述关系，非对称算法与对称算法完全不同。公开密钥基础设施（public key infrastructure，PKI）是一种网络基础服务设施，它充分利用公钥密码学的理论基础，为密钥和证书建立了一个安全的网络环境，为各种网络应用提供了全面的安全服务[6]。非对称加密通过生成 2 个密钥，即公/私钥对来对数据进行加密/解密，当一个密钥用作加密时，另一个密钥就用作解密。私钥是由被认证过的用户独自掌管的，该用户发布或传递的信息会用私钥加密，只有对应的公钥才能对其进行解密，进而完成信息接收的身份认证；而公钥是在网络上公开的，公私钥体制的密钥管理主要针对公钥进行。非对称加密可以在不直接传递密钥的情况下完成解密，这样能够确保信息的安全性，避免直接传递密钥被破解造成的风险。目前。最广泛使用的算法包括 RSA（Rivest, Shamir, Adleman）算法[7]和椭圆曲线密码学（elliptic curve cryptography，ECC）算法等。

RSA 算法是一种非对称加密算法，由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）在 1977 年共同提出，因此以三人姓氏的首字母命名了该非对称加密算法。RSA 算法是目前十分有影响力的公钥加密算法，它的安全性依赖于大数的因式分解，具有数学原理简单、工程应用易实现等特点。RSA 算法能抵抗现阶段已知的绝大多数密码攻击，已被国际标准化组织（international organization for standardization，ISO）推荐为公钥数据加密标准。目前，

RSA 算法常用于小片段数据加密与数字签名领域，由于非对称加密涉及大量计算，实际运行效率较低，故常与对称加密配合来加密对称加密的密钥。

ECC 算法主要用于解决有限域上的椭圆曲线离散对数问题，其单位安全强度相对 RSA 算法较高，但在工程应用中比较难以实现。而且，ECC 算法可以通过国际上公认的 PollardRho 方法破解，虽然它的破解难度基本上是指数级的，但也为它的安全性埋下了隐患。目前，ECC 算法只能完成密钥的生成和解析，在工程应用中需要调用硬件完成加密/解密才能实现，这个过程复杂程度较高。

不同于传统公钥算法，ECC 加密算法的安全原理并非基于大质数因子的分解困难性，而是基于椭圆曲线上有理数构成的加法群对椭圆离散对数的计算困难性，通过使用较短的操作数就可提供与 RSA 算法同等的安全等级。一般情况下，ECC 算法在性能和带宽上均优于 RSA 算法。目前我国居民二代身份证采用的就是 256 位的 ECC 算法，此外比特币也采用了该加密算法。

1.3　量子信息技术

量子理论经过一百多年的曲折发展，已经成为现代物理学的两大基石之一，并为描述自然界提供了新的方向与思考。其揭示了微观世界的基本规律，为现代信息技术、原子物理学等奠定了理论基础，并衍生出了许多新兴学科。量子信息技术是在量子物理与信息技术基础上发展出来的交叉学科，近年来多应用在信息安全[8]与加密[9]等方面，主要方向包括量子计算与量子通信。2019 年 11 月，华为创始人任正非在访谈中表示：就信息安全问题来说，区块链技术在量子计算机面前不值一提，这体现出量子信息技术在信息安全与加密领域起着变革性作用。

（1）量子通信

量子通信最早由 Bennett 等在 20 世纪 90 年代提出，是用量子纠缠效应来传递信息的一种新型通信方式。量子通信的关键技术有量子密钥分发（quantum key distribution，QKD）、量子隐形传态（quantum teleportation，QT）、量子安全直接通信、量子机密共享等，针对区块链面临的加密方式安全性问题，量子密钥分发和量子隐形传态是可以应用在区块链中的重要技术。QKD 将量子状态作为信息加密和解密的密钥，以量子态为信息载体，通过量子信道使通信双方共享密钥，现阶段较为通用的 QKD 协议为 Bennett-Brassard（BB84）协议。QT 利用量子纠缠理论，通过一对纠缠态量子实现远距离量子信息传输，不需要直接传输量子比特信息即可实现量子纠缠态的转移。

（2）量子计算

量子计算是通过量子力学规律控制量子信息进行并行计算的新型计算模式，是基于量子力学方法对通用图灵机的重新构建。与传统计算机的基本单元——比特相对应，量子计算的基本单元是量子比特。与传统的物理比特存储的 0/1 逻辑状态相似，量子比特也拥有 2 个状态，记作 $|0\rangle$ 和 $|1\rangle$。与传统比特一个时刻只能存储一个状态不同的是，量子比特可以是状态的线性叠加，也称为叠加态[10]。例如 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$，其中 α 和 β 均为复数。这意味着 N 个量子比特可以存储 2^N 个比特的信息，因此量子计算机的处理能力将随着比特数的增长呈指数型增长，可以解决经典计算机无法解决的大规模计算难题。

2　量子霸权对区块链的威胁

量子霸权是对量子计算机远超于经典计算机的强大计算能力的描述，它的实现与否直接标志着量子计算能否从理论走向实验甚至实践。2019 年 9 月 20 日，谷歌公司研究人员架设出一台名为“悬铃木”的计算机，它成功地在 3 分 20 秒内解决了传统超级计算机可能耗时 1 万年才能处理的问题，这是声称全球首次实现了“量子霸权”的量子计算机。

量子霸权对区块链的第一个威胁主要来源于 Grover 算法，这是一种能显著加快函数反演的量子搜索算法[11]。Grover 算法可以通过 2 种方式攻击区块链。

- 搜索 Hash 冲突：在传统的密码学中，Hash 算法被计算的数据是无限的，但不可否认的是，计算后的结果范围是有限的，因此区块链中不同区块的 Hash 值存在 Hash 冲突的可能。如果可以生成完全冲突的 Hash 值，可能就可以采用修改后的块内容和给定的 Hash 值，并在记录中添加琐碎的数据，以使给定的 Hash 值与块的内容一致。Grover 算法通过给定的 Hash 值去搜索 Hash 冲突，利用 Hash 冲突生成一个不同于原映射的预映射，从而修改已签名的数据区块。一般情况下，Grover 算法会对源数据进行暴力搜索，直到找到 Hash 空间内与目标 Hash 值相匹配的 Hash 冲突为止。这种算法在理想情况下搜索所需的时间与 Hash 空间的大小呈线性

关系，相比传统的碰撞搜索算法可以提升的速度与 Hash 数量的平方根成正比，该算法相当于仅用 Hash 一半的比特数就可以寻找 Hash 碰撞。因此，Grover 算法将修改后的区块插入链中并不会影响区块的序列一致性。当然，考虑到该算法攻击的提速效果仅为线性，可以考虑扩增 Hash 的长度，但更长的 Hash 带来的随机数计算量会影响区块的吞吐速度，从而限制生成区块链的能力，最终导致区块链无法运行。这一类攻击在保证区块链完整性不发生冲突的同时修改了区块内容的真实性，最终破坏了区块链的去信任环境。

- 缩短挖矿时间：POW 是目前链中形成区块链的主要共识方式，它主要依赖随机数的计算。若要重写区块链，则需要查找部分定义 Hash 的原像，这极大地增加了重写链的计算成本。Grover 算法可以加快随机数的生成，进而加快区块链中区块的生成速度。对于量子计算机来说，在链上生成新区块的速度可以远超经典计算机的算力，这意味着其挖矿耗费的时间比常规计算机短得多。因此，拥有量子计算机的矿工可以通过快速挖矿来获得更多的电子货币，同时主导新区块的生成，最终控制整个区块链的内容。同时，如果随机数的生成速度足够快，那么利用量子计算机可以在非常短的时间内重建一条新的分支链，当分支链的长度超过主链时，分支链就可以取代主链成为一条真正的区块链，从而达到重建区块链的效果。

第二个威胁来源于 Shor 算法，它能用于破坏区块链采用的 RSA 加密[12]。Shor 算法能快速地通过寻找一个合数的 2 个质数因子，而在 RSA 加密算法中合数会被用作公钥，这 2 个质数因子会被当作私钥。对于经典计算机来说，对一个合数进行因式分解非常困难，然而这对量子计算机来说却是一个简单的任务。因而，在用户们交换和验证公私钥的过程中，攻击者可以利用 Shor 算法破解和获取用户的公私钥，从而伪造信息、签名等。这意味着区块链中任何经过签名的内容都可能被伪造，最终通过共识验证后被上传到区块链中。此外，不仅用户之间的交易信息会受到攻击，构建区块链的基础设施中使用的任何加密通信都会受到攻击，丧失了通信加密的可靠性，区块链的链内环境将不再安全。

3　基于量子通信的区块链

量子纠缠是量子力学中一个经典的现象，它指的是量子粒子之间相互作用后，各个粒子的特性不再是独立的，而是具有相互参照的整体性质。因此，2 个处于纠缠态的量子不管分开多远，在不存在任何信息交互的情况下，通过测量其中一个粒子的状态就可以知道另一个粒子在同一时刻的状态。量子通信是利用量子纠缠效应进行信息传递的一种新型通信方式，它主要涉及量子密码通信、量子远程传态和量子密集编码等，近年来逐渐从理论走向实验以及实用化发展。

如上所述，区块链可能被量子计算攻破的原因主要有 2 个：基于 POW 的共识机制和基于 RSA 的加密方式。因此，构建一个基于非 POW 共识机制和量子保密通信的区块链是一个有效的解决方法[13]。对于非 POW 共识机制来说，现在主流的有权益证明机制（proof of stake，POS）、权益授权证明机制（delegated proof of stake，DPOS）等。接下来重点阐述量子通信在区块链中的应用。

针对区块链面临的加密方式安全性问题，QKD 和 QT 是可以应用在区块链中的重要技术。考虑到量子通信技术的特点，利用 QKD 进行信息加密/解密的密钥分发，利用 QT 进行对称密钥的共享，即使攻击者拥有量子计算机，也无法破解或者窃听通信双方的密钥和内容，其 QKD 系统结构如图 1 所示。

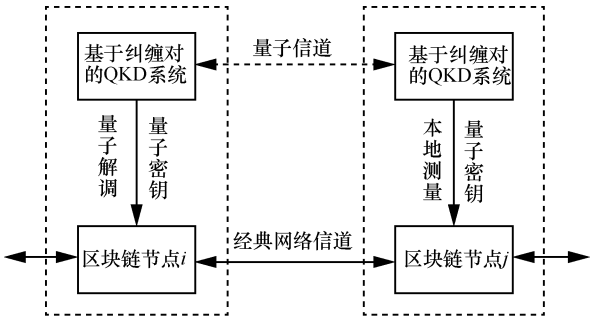

图 1　QKD 系统结构

以密码学的经典例子进行说明。在传统的区块链中，当 Alice 需要在区块链网络中向 Bob 发送数据时，Alice 通过非对称加密对信息进行加密，使用了自己的私钥和 Bob 的公钥，Bob 利用 Alice 的公钥和自己的私钥进行解密，从而获取了 Alice 发送过来的数据。这是典型的非对称加密方式，能在传统网络环境下保证通信的安全，然而其加密原理可以被量子计算攻破，这也是其缺陷所在。然而，在基于量子通信的区块链中，当 Alice 需要在区块链网络中向 Bob 发送数据时，Alice 随机选择纠缠量

子对，在量子信道中发送随机选择的纠缠量子对代号给 Bob，然后利用量子解调形成对称加密密钥，并在经典信道中发布已加密的密文。与此同时，Bob 在本地观测与 Alice 对应的纠缠量子态，利用量子解调生成对应的对称加密密钥，并对 Alice 发起的数据分组进行解密从而获取数据。值得注意的是，即使攻击者在经典信道中窃听且得到了已加密的密文，他仍然无法获取与密文对应的对称密钥，原因主要有 2 个：一是攻击者无法得知纠缠量子对的量子态，从而无法获得密钥；二是攻击者在量子信道中窃听，会引起量子态的改变，被窃听的量子偏振态对应的将是无意义的信息，同时也会被发送双方察觉。这一原理已经被众多科学家所验证，因此，基于量子通信的区块链可以克服传统区块链的缺陷，以应对量子霸权带来的巨大威胁。

4　量子计算的困境与挑战

虽然量子计算机已在某些方面显露出优势，但其仍面临许多艰巨的技术上的困难。这些困难也成为许多学者质疑量子计算可行性的缘由，如法国蒙彼利埃大学的理论物理学家 Michel Dyakonov[14] 就在 *IEEE Spectrum* 发表文章称：实用的通用量子计算机在可预见的未来无法实现。在已有的文献中，对量子计算所处的困境与面临的挑战的总结主要集中在以下几个方面。

4.1　量子纠错

可以快速纠正小型的随机错误是计算机系统正确运行的基础，但却是量子计算面临的一大难题。量子计算机凭借量子特有的相干性与纠缠性，在部分问题的处理上优于传统计算机，然而计算机内电路组件或相干系统与周遭环境的非预期相互作用，很可能使得量子比特受噪声影响而快速失去相干性，即丧失计算能力。目前的技术仅能维持相干性几分之一秒，此外随着量子比特数量的增加，维持相干性的难度还会大大提升，这就对计算速度提出了更高的要求。虽然目前已有针对量子纠错的策略研究，但这些处理手段都会大幅增加计算成本，严重限制计算的规模。因此量子纠错是实现可容错的大规模通用量子计算的核心。

4.2　量子比特质量

以往业界认为 50～60 个量子比特是量子计算机取代经典计算机的关键节点，然而当前研制出的量子计算机早已超过这个阈值，如 2018 年 D-Wave 公司就已推出 2 048 个量子比特的芯片，但这些技术却仍未引发计算能力的变革。这是因为在讨论量子芯片时，不仅要考虑数量，还要考虑质量。美国 IBM 研究院就指出：50 个优质量子比特远远优于 2 000 个劣质量子比特。此外，由于量子单位门及两位量子门的操作存在一定的错误率，多次指令操作后的结果准确度无法保证。因此低容错率的量子计算与实际应用之间还有很大的距离。

4.3　线路设计

量子芯片的扇出问题，即如何增大芯片的量子比特数，也是业界重点关注的问题之一。由于量子芯片的运行条件极为苛刻，需要隔音、隔热、隔绝电磁场，内部温度需接近绝对零度，因此整个芯片外需要包裹一层层的隔离装置，保护与控制结构十分复杂。

5　结束语

区块链将成为物联网的重要支撑技术之一，然而，区块链的共识机制与加密方式依赖于目前的经典计算机信息技术，在量子信息技术的条件下，其局限性渐渐凸显，为未来区块链的实用带来了很大的隐患。量子计算的两大核心算法——Grover 算法和 Shor 算法会给区块链安全性带来严重威胁，但与此同时，利用量子信息技术的特性，加密技术也将变得更加安全。QKD 确保发送的信息只有使用量子密钥解密之后才能阅读信息，QT 保证了密钥共享与信息传输的安全性，且能防窃听，为区块链可信环境的进一步构建提供了一种可行的思路。量子加密通信已经开始在全球进行推广使用，因此，量子区块链将会得到更加长远的发展。

参考文献：

[1] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[2] 张俊, 高文忠, 张应晨, 等. 运行于区块链上的智能分布式电力能源系统: 需求、概念、方法以及展望[J]. 自动化学报, 2017, 43(9): 1544-1554.

ZHANG J, GAO W Z, ZHANG Y C, et al. Blockchain based intelligent distributed electrical energy systems: needs, concepts, approaches and vision[J]. Acta Automatica Sinica, 2017, 43(9): 1544-1554.

[3] 中华人民共和国工业和信息化部. 中国区块链技术和应用发展白

皮书(2016)[R]. 2016.

Ministry of Industry and Information Technology of People's Republic of China. China Blockchain Technology and Application Development White Paper (2016) [R]. 2016.

[4] PAAR C, PELZ J. 深入浅出密码学: 常用加密技术原理与应用[M]. 马小婷, 译. 北京: 清华大学出版社, 2012.

PAAR C, PELZ J. Understanding cryptography: a textbook for students and practitioners[J]. Translated by, MA X T. Beijing: Tsinghua University Press, 2012.

[5] 许重建, 李险峰. 区块链交易数据隐私保护方法[J]. 计算机科学, 2019(12): 1-9.
XU C J, LI X F. Blockchain transaction data privacy protection method[J]. Computer Science, 2019(12): 1-9.

[6] 王煜, 朱明, 夏演. 非对称加密算法在身份认证中的应用研究[J]. 计算机技术与发展, 2020(1): 1-7.

WANG Y, ZHU M, XIA Y. Research on application of asymmetric encryption algorithm in identity authentication[J]. Computer Technology and Development, 2020(1): 1-7.

[7] KIMURA S, YONEYAMA K. Security proof of identity-based signature under RSA assumption, reconsidered[J]. IEEE Conference Publications, 2016(21):86-90.

[8] 汤大彬, 唐宾徽. 量子计算机对信息安全的挑战分析[J]. 科技创新导报, 2018, 15(20): 140-141.

TANG D B, TANG B H. The challenge of quantum computer to information security[J]. Science and Technology Innovation Herald, 2018, 15(20): 140-141.

[9] 李林洋, 卢晓波, 潘岳. 量子加密技术发展研究[J]. 商品与质量, 2011(S5): 230.

LI L Y, LU X B, PAN Y. Research on the development of quantum encryption technology[J]. The Merchandise and Quality, 2011(S5): 230.

[10] WONG R. 量子计算与不确定性原理[J]. 计算机科学, 2019(9): 1-19.

WONG R. Quantum computing and uncertainty[J]. Computer Science, 2019(9): 1-19.

[11] RODENBURG B, PAPPAS S P. Blockchain and quantum computing[R]. Mitre Technical Report, 2017.

[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] ABLAYEV F M, BULYCHKOV D A, SAPAEV D A, et al. Quantum-assisted blockchain[J]. Lobachevskii Journal of Mathematics, 2018, 39(7): 957-960.

[14] DYAKONOV M. The case against quantum computing[J]. IEEE Spectrum, 2019.

[作者简介]

张俊（1981− ），男，博士，武汉大学电气与自动化学院教授，主要研究方向为智能系统、人工智能、知识自动化及其在智能电力和能源系统中的应用。

袁勇（1980− ），男，博士，中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员，主要研究方向为社会计算、计算广告学、区块链技术。

王晓（1988− ），女，博士，中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员，主要研究方向为社会交通、动态网群组织、人工智能和社交网络分析。

王飞跃（1961− ），男，博士，中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任，国防科技大学军事计算实验与平行系统技术研究中心主任，中国科学院大学中国经济与社会安全研究中心主任，青岛智能产业技术研究院院长，主要研究方向为平行系统的方法与应用、社会计算、平行智能以及知识自动化。