区块链技术应用的安全与监管问题

王俊生[1,2] 李丽丽[1,2] 颜 拥[3] 赵 微[4] 徐 彧[1,2]
(国网汇通金财(北京)信息科技有限公司 北京 100053)[1] (国网电子商务有限公司 北京 100032)[2]
(国网浙江省电力公司 杭州 310014)[3] (北京鑫苑科技有限公司 北京 100080)[4]

摘 要 区块链技术由于具有分布式高冗余存储、时序数据且不可篡改与伪造、去中心化信用等显著特点,因此得到了广泛的应用,但其自身和应用的安全性以及监管问题也日益受到重视。文中对区块链技术的安全问题和监管问题作了剖析,首先收集和分析了各类区块链安全事件,对事件的成因进行归类,并给出了相应的安全防范措施;其次,分析了中国区块链监管的现状,并借鉴了国际上对区块链的监管政策,提出了适合中国国情的区块链监控模式;最后,总结了区块链在监管模式下的技术发展需求。

关键词 区块链,分布式存储,安全事件,防范措施
中图法分类号 T-01 **文献标识码** A

Security Incidents and Solutions of Blockchain Technology Application

WANG Jun-sheng[1,2] LI Li-li[1,2] YAN Yong[3] ZHAO Wei[4] XU Yu[1,2]
(Beijing Huitong Financial Information Technology Co., Ltd., Beijing 100053, China)[1]
(State Grid Electronic Commerce Co., Ld., Beijing 100032, China)[2]
(State Grid Zhejiang Electric Power Co., LTD., Hangzhou 310014, China)[3]
(Beijing Xinyuan Technology Co., Ltd., Beijing 100080, China)[4]

Abstract Blockchain technology has been widely used. It has many advantages, such as distributed storage, high redundant data, centering and so on. The safety of its application and regulatory issues has been paid attention to. Firstly, this paper collected and analyzed all kinds of blockchain security incidents, and the causes of the incident were classified, corresponding safety precautions were put forward. Secondly, the present situation of China blockchain supervision was analyzed. Referring to the international policy on blockchain supervision, the model for China blockchain monitoring situation was put forward. Finally, the technology development needs of blockchain were summarized in the pattern of supervision.

Keywords Blockchain, Distributed storage, Security incident, Precautionary measures

1 概述

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用模式[1-6],近年来已成为联合国、国际货币基金组织等国际组织以及许多国家政府研究讨论的热点[7-10]。国内对区块链技术的关注度也日趋上升,北京、上海、深圳等城市先后成立了不同形式的联盟,并在以金融技术为代表的领域展开了实践。区块链技术的应用并非一帆风顺,而是机遇和挑战并存,动力和障碍共同作用。各国对区块链技术的发展基本持开放态度,法律上处于空白状态,近期发生的一系列与区块链相关的安全事件透露出区块链技术不仅面临安全风险,还面临着监管缺失问题。本文对区块链技术的安全和监管问题作了剖析,首先,收集和分析了各类区块链安全事件,对事件的成因进行了归类,并给出了相应的安全防范措施;其次,分析了中国区块链监管的现状,并借鉴了国际上对区块链的监管政策,提出了适合中国国情的区块链监控模式;最后,总结了区块链在监管模式下的技术发展需求。

2 区块链技术应用的安全事件及防范措施

由于区块链技术能够大幅节约成本,因此主流的大型银行都在参与研究和开发区块链技术。但是也有专家警告说,分布式的总账技术也许会有“大而不倒”的问题,也很可能会导致前台交易变得缓慢,以及由于安全保护技术的不完善而导致其技术发展受到阻碍[7]。虽然区块链是基于现有的成熟密码学算法进行设计的,但是其安全仍是一个非常引人重视的话题。以下几个方面还需要重点关注。

本文受国家电网公司基金资助项目(52110417000G)资助。

王俊生(1978-),男,高级工程师,主要研究方向为电力物联网、互联网金融,E-mail:wangjunsheng@sgec.sgcc.com.cn;**李丽丽**(1983-),女,工程师,主要研究方向为电力物联网、互联网金融,E-mail:lilili@sgec.sgcc.com.cn(通信作者);**颜 拥**(1986-),男,博士生,主要研究方向为区块链技术及其应用、电力市场、互联网+电力营销,E-mail:55682381@qq.com;**赵 微**(1984-),男,主要研究方向为区块链技术、房产金融产品、互联网金融,E-mail:wei.zhao@ftcrdit.com;**徐 彧**(1974-),男,高级工程师,主要研究方向为通信和信息领域技术以及互联网技术,E-mail:2443835553@qq.com。

首先是立法。如何对区块链系统进行监管，攻击区块链系统是否属于犯罪，攻击银行系统是否要承担后果等，目前还没有任何法律作出明确规定。

其次是软件的实现存在潜在漏洞。对于金融系统来说，无论是客户端还是平台侧，即便是很小的漏洞，都可能造成难以估量的损失。另外，公有区块链的所有交易记录都是公开可见的。作为一套完全的分布式系统，公有链缺乏有效的调整机制，一旦运行起来，出现问题后难以修正。

此外，运行在区块链上的智能合约应用的种类繁多，必须进行安全管控，在注册和运行前需要有相应的机制进行探测，以规避恶意代码的破坏。2016 年 6 月 17 日，攻击者利用智能合约存在的重大缺陷，对区块链界最大的众筹项目 TheDAO(被攻击前有约 1 亿美元的资产)进行攻击，直接导致 300 多万以太币资产被分离出 TheDAO 资产池。导致该事件发生的最主要的原因在于 TheDAO 编写的智能合约中的一个 splitDAO 函数，攻击者通过此函数中的漏洞重复利用自己的 DAO 资产来不断从 TheDAO 项目的资产池中分离 DAO 资产给自己。此次攻击事件中，DAO 系统漏洞被利用，直接导致了价值 6000 万美元的数字货币被利用者获取，给区块链历史上留下了沉重一笔。2016 年 8 月 4 日，全球最大的数字资产交易平台之一 Bitfinex 被盗走了价值超过 6000 万美元的比特币[11]。2017 年 4 月 22 日，韩国比特币交易平台 yapizon 成为了黑客攻击的最新受害者，该交易所的员工在社交媒体上发布通知，确认有 3831 BTC 被盗，市场价值约合 500 万美元。2017 年 7 月 19 日，多重签名钱包 Parity1.5 及以上版本出现了安全漏洞，导致 15 万个价值 3000 万美元的以太坊 ETH 被盗。这些事件的发生，引发了大家对数字资产安全性的担忧，区块链从业人员应吸取教训，加强对平台安全的管理，以尽可能减少类似的安全事故。事实证明，目前基于区块链技术进行生产应用时，务必要细心、谨慎地进行设计验证。

随着区块链应用范围的扩大，区块链应用和技术的安全成为了重点关注对象，一旦相关软件存在漏洞，将造成巨大的财产损失。本文通过研究国内外区块链领域的安全事件，结合这些安全事件背后的区块链应用运行机制，对区块链的安全态势进行分析，感知区块链的潜在风险和安全影响，以对区块链的安全问题进行思考，并尝试建立起针对这些安全问题的防范思路。

在分析了各类区块链的安全事件之后，发现区块链技术的安全问题非常严重，并且在各个环节均存在不同的安全风险。总结以上经验，在后续的区块链技术应用产品上设法规避各类风险十分重要。根据安全事件形成的原因，可以将安全事件分为 4 类：底层机制安全风险、实现风险、环境漏洞风险、管理风险。

2.1　区块链的底层机制安全风险

区块链底层涉及数据存储、网络传输和分布式共识等方面，为价值的存储和转移提供支撑。交易的有效验证和状态的合理判断，是保证价值安全、可靠流通的基础。Mt. Gox 交易平台事件便是由于区块链底层不完善而造成的。由于 Mt. Gox 的底层技术存在可锻造性漏洞，导致攻击者可重复提现，受此影响，Mt. Gox 一度停止用户提现，并禁止用户向其他平台转移比特币。这一消息导致 Mt. Gox 上的比特币价格暴跌，最终使 Mt. Gox 破产。

针对区块链底层机制安全风险的防范策略：在设计应用程序时，对可锻造性漏洞进行规避；交易验证时，不能仅根据一个哈希值来判断交易的状态，应该使用双因素或多因素进行验证。比如，可以根据用户比特币钱包的余额来判断用户是否有足够的余额进行交易，或者通过追踪每笔交易的信息来判断是否真正交易成功。

2.2　区块链应用的实现安全风险

区块链的安全问题除了其自身底层协议和机制的安全性外，还包括其上层应用的安全性[12]。与智能手机中的应用程序漏洞或恶意应用程序造成的系统安全问题类似，把区块链作为某种应用的底层技术时，区块链自身的安全性并不能保证区块链之上的应用的安全性。如运行于以太坊区块链基础上的 The Dao 应用被攻击而造成大量资金被盗事件，就很好地证明了区块链本身的安全性并不能保证以区块链为基础的应用的安全性。

区块链的应用多数与资产、货币交易相关，软件一旦出现漏洞，就可能会导致财产损失的严重风险。与区块链应用相关的安全事件主要包括：1)Bitstamp 被攻击，损失约 500 万美元；2)The Dao 被劫事件；3)Bitomat 文件丢失。

针对此类风险的安全防范策略：在应用程序设计及代码实现过程中进行安全规划，在上线前进行充分的安全测试。对业务流程及业务周边的信息进行处理，反复推敲演练，避免在程序设计上出现安全风险。

2.3　区块链应用的环境漏洞安全风险

与攻击银行机构相比，攻击区块链平台能获得更高的“回报”且风险更低，其主要原因是可以采用匿名方式设置区块链的帐户。区块链在交易的过程中，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。因此，虽然能够看到每一笔转账记录的发送方和接收方的地址，但无法对应到现实世界中的具体个人，这就为一些不法分子带来了可乘之机，黑客能够以更加隐蔽的方式进行攻击。当前，区块链应用环境漏洞的安全事件包括：

1)Blockchain 遭遇 DNS 劫持攻击；

2)Bitfinex 遭黑客入侵；

3)云挖矿平台 ScryptCC 被黑，大量比特币被盗；

4)MyBitcoin 遭黑客攻击而丢失了全部钱包数据；

5)Bitfloor 交易中心遭黑客入侵；

6)比特币云采矿平台 Cloudminr. io 遭入侵，用户数据被黑客低价“大甩卖”。

针对此类风险的安全防范策略：对应用程序运行的各个层面的环境进行充分的安全测试，包含所有软件版本(尽量采用高版本)、服务器安全测试、网络安全测试、数据安全测试、渗透测试等，以确保应用程序中各个层面环境的安全。

2.4　区块链应用的管理安全风险

完善的协议与架构设计，构筑了区块链安全、可信的存储与交易网络。然而，一系列私钥被盗、比特币丢失的事件折射出：影响区块链网络可信任的重要环节就是用户私钥的安全保护问题。在区块链网络中，私钥唯一标识数字资产的拥有者，一旦私钥丢失或者泄漏，数字资产则无法找回，因此私钥是确保区块链可信的基石。若保管不善，造成数据泄露或私钥被盗，将使得用户的资产面临着高度的危险。区块链应用的管理安全事件包括：1)MtGox 用户证书被盗用；2)Bitcoin

Savings and Trust 关闭;3)Bitcoinica 数据泄露;4)ShapeShift 数据泄露;5)MtGox 比特币失窃案。

针对由密钥引起的安全事件的防范策略:1)对私钥运行环境的各个层面进行充分的安全测试,包含所有软件版本(尽量采用高版本)、服务器安全测试、网络安全测试、数据安全测试、渗透测试等,以确保应用程序各个层面环境的安全;2)通过私钥的生命周期确保其安全性,包括私钥的生成、存储、使用、找回、销毁、更新六大环节,保证每个环节的安全性;3)积极对现有私钥进行改造,并替换现有的密钥机制。

3 区块链技术应用的监管问题

区块链作为一种新兴的技术,采用了去中心化的技术设置,颠覆了传统互联网的许多特点,在许多领域具有广泛的应用前景,足以解决现实中的很多问题,引起了世界各国的密切关注[12-13]。然而,技术具有中立性,在带来便利的同时也带来了许多新问题,各国普遍意识到如果法律动辄予以规制,极有可能成为区块链技术发展与应用的绊脚石。各国对区块链技术均持开放态度,并表示要在保证市场信心和交易安全的前提下对区块链技术的相关领域的应用采取宽容的态度,着力推进区块链技术在金融领域的运用,致力于培育新的交易模式,并审慎地予以监管,因此各国均无具体的立法行动,尚在观察阶段,待区块链技术应用成熟且全面掌握了相关风险之后,才会采取措施。

美国众议院对区块链技术的发展召开了多次会议,经过深刻的讨论,众议院出台了一项非约束性区块链技术相关决议,鼓励新技术来保护消费者权益。欧盟方面并未对区块链技术进行直接监管,而是对数字货币加强了监管。

国内同样认为区块链在金融领域的应用前景非常可观,决意要推进区块链技术的应用进程,但是基于保护新生事物的考虑,并未专门进行立法。目前,区块链技术的应用并非无法可依,国内法律对区块链技术的规制主要体现在信息安全领域立法、平台监管、电子证据、公司法等方面。

监管的目的是防范风险、维持秩序。为防止区块链应用给其设计的包括金融在内的多个行业带来秩序上的冲击和危害,各国监管机构在区块链技术的发展与落地中势必需要发挥重要作用。

3.1 国际区块链监管模式

从国际上各个国家对区块链的监管态度来看,主流仍然是对区块链技术的发展给予鼓励、支持与引导,在鼓励创新的大背景下对可能暴露的法律风险进行监管。总体来看,可以概括为以下 3 种模式。

1)以发展科技创新为主要目标的“创新中心”模式,即支持和引导机构理解金融监管的框架,识别创新中的监管、政策和法律事项。这种模式不涉及真实测试或虚拟测试,对区块链等技术的发展持相对宽容的态度[14]。

2)政府部门或监管部门与业界建立合作机制的“创新加速模式”,通过提供资金扶持或政策扶持等方式,加快区块链等金融科技创新的发展和运用。

3)“监管沙盒”。其特点是:包括金融机构在内的任何机构都可以申请进入监管沙盒;监管部门需要对申请者提出的创新产品或服务进行个性化的建议或指导;社会监管注重保护消费者的合法权益。以上特点使得沙盒模式具有可操作性。

3.2 国内区块链监管的状态

中国对区块链相关技术应用的监管,经历了从最初的限制比特币的流通到对数字货币的流通性进行了热议的过程。随着越来越多的电子货币的出现,其发行和运行框架、面临的法律风险、监管制度的构建以及对传统经济金融体系的影响等,都需要进行深入研究。2015 年建立的中国互联网金融协会是一个国家级互联网金融行业的自律组织。2016 年 1 月,中国人民银行在京召开了数字货币研讨会,梳理了数字货币的国内发展情况,并研究了国际监管政策。2016 年 6 月 15 日,中国互联网金融协会决定正式成立区块链研究工作组,该工作组主要负责深入研究区块链技术在金融领域的应用及影响,并密切关注创新带来的金融风险和监管问题,对区块链在金融领域应用的风险管理等监管问题进行研究[15-16]。

3.3 态度上开放,行为上加强对区块链技术的跟踪和研究

区块链技术相对与当下的业务模式具有多种优势,但由于受金融业自身规律的限制,区块链难以快速改造金融业。当下,应该重视区块链人才与技术的快速培养与累积,强化对区块链技术发展及其应用中的最新成果的了解,深入对区块链技术体系的探索,及时跟踪国内外的重大发展,并对其进行归纳和总结,以夯实区块链应用的基础。各金融机构还要进一步强化协调与合作,力避各自闭门造车,并尽快推出金融行业的区块链标准。

具体工作可以分为以下方面:1)支持民间区块链研究机构的发展,鼓励民间区块链技术企业开展区块链模拟实验室,建立区块链应用技术项目投资基金,探索区块链领域的政府购买服务模式;2)加快组建专门的研究力量,并与国外区块链技术研究公司建立合作交流,动态评估技术应用的成熟度,并及时分析其可能给金融业造成的影响;3)积极参与区块链国际标准和规则的制定,鼓励国内商业银行和金融交易所开展区块链技术合作,共同研究与制定区块链的行业标准,探索应用场景,争取在未来的区块链国际应用合作中取得更大的话语权。

3.4 中国环境中的监管模式建议

中国必须抓住区块链技术带来的机遇,及早制定战略并积极参与区块链的投资布局与实际应用,这样才能在行业重塑中占据有利地位。区块链技术应用并无现成的模式,其在解决现有问题的同时,有可能对现行的金融交易带来较大的挑战。在我国推荐普惠金融的大背景下,要注重平衡新技术的发展与监管之间的关系。在加强风险防范的同时,用新技术来保障金融业的安全和效率的提升[17]。

1)在弹性范围内对区块链进行监管

区块链本身的技术特点与传统金融监管技术和模式的结合,带来了洗钱、诈骗、隐私保护和偷税、漏税等一系列监管新难题。另外,区块链技术与现行法律中的诸多制度可能会存在冲突,这也给监管者提出了新的难题。监管者应该探索利用区块链新技术来改进监管方式,完善监管手段,加强保护投资者权益和市场平衡,在合适的透明度下采取较为宽松的监管政策,培育新的交易模式,以免成为新技术发展的绊脚石。具体来说,首先,要避免监管过度,建立一个可预见、一致、简单的合法环境,尊重区块链技术“自上而下”的特点以及在全球市场的发展;其次,回顾并检视现行的规则,以确保区块链技术的发展不受必要的限制;再次,必要时,国际政策的制定者应该协调不同国家死板的区块链技术规则,提供一些灵活

的管理原则来适应不同国家的监管，以避免企业陷入复杂的监管环境；最后，待区块链的应用较为成熟时，再确定具体的监管政策。

2）由事前监管转向事中监管和事后监管

我国传统的监管手段过度重视事前监管，这在一定程度上会阻碍市场的创新。对于区块链技术与金融的融合，应该采用平衡技术创新与监管的“沙盒监管”模式[18]，具体可以从以下几个方面来构建新型监管体制：

①改变现有的立法体制，将区块链技术与金融的结合纳入到法律的框架下，并加强动态立法，紧跟技术发展的节奏，争取立法与技术的发展同步；

②建立金融消费者保护委员会，统一监管包括区块链技术在内的创新领域，确立以行为监管和金融消费者保护为核心的监管体制；

③考虑到区块链技术的专业性以及该技术在其他领域的广泛应用，可以对其应用进行真实测试或虚拟测试，并在一些法律适用领域给予适当的豁免，以在保证市场大环境相对稳定与安全的基础上促进技术的持续创新[19]。

④在国际化的区块链网络执法过程中，可以考虑建立全球的区块链执法联盟，不同国家的监管者之间进行合作监管，争取在监管的基本理念与手段上达成共识，进而确立一个基础的监管架构[20]。

4　总结

在当今国情下，区块链技术的发展道路比较坎坷，难点较多，解决区块链技术和应用的安全问题是当前的重点。

密钥管理、加密算法和智能合约是区块链安全的核心[21]，因此至少需要从这 3 方面入手来构建区块链应用的安全框架。比如，关注密钥的管理，避免密钥使用的机制逻辑出现漏洞。随着计算机计算能力的不断提升，常规或高强度的加密算法将会被轻易破解，公认的 MD5 算法已经可破解，因而对加密算法的改进也应该有新的突破，否则随着计算机硬件计算能力的提升，区块链技术也就成为空谈。智能合约是机器通过程序自动执行的合约机制，对其合理性和逻辑性应多加关注，而且在计算机程序或硬件发生 BUG 时，智能合约的容错机制都面临潜在风险。区块链应用应更多研究区块链的核心技术，从实现安全、数据安全、管理安全和应用安全等多个维度多管齐下，共同为区块链应用提供坚实的安全基石。

针对区块链技术安全和区块链应用安全，构建图 1 所示的区块链安全体系。

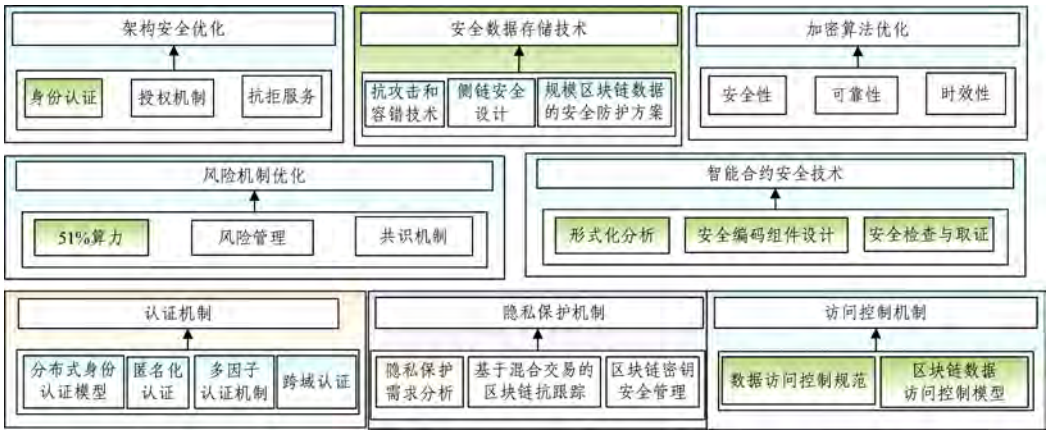

图 1　区块链安全体系

1）区块链架构安全的优化

一方面，区块链系统是开放的，除了交易各方的私有信息被加密外，其他数据对所有人公开；广泛使用的公有区块链和参与交易的个体也是开放的。如何保证区块链自身的安全性，譬如身份认证、授权机制、抗拒绝服务等，是目前一个需要解决的问题。另一方面，电力作为基础设施，其控制系统的安全尚处于整体封闭的状态，这与区块链的总体设计理念相悖，如何在公有链和专有链之间平衡，在系统对接的同时保证原有安全体系的完整性，也是一个需要解决的问题。

2）区块链安全数据存储的优化

区块数据的产生完全依赖于共识机制和智能合约，使得区块链中的所有节点必须在同一网络中实时交互。而在电力行业的大多数应用环境中，特别是配电、用电等直接控制领域，大量的设备处于非稳网络中。当采用分片技术时，部分节点因为网络中断形成网络孤岛，可能会出现数据分叉，与主系统形成两条独立的区块链。在网络再联通后的数据合并过程中，分支区块链被舍弃，从而出现数据丢失的情况，这会对控制系统带来诸多问题。因此，如何解决数据分叉、丢失以及建立一个高度稳定的网络是当前面临的一个挑战。

3）区块链加密算法的优化

随着技术的进步和数学理论的突破，通用的加密算法正逐渐被破解，这势必给基于点对点加密的区块链技术带来挑战。目前，隐私信息虽然经过加密，但都置于公开透明的环境中，一旦加密算法被破解，就存在隐私信息泄漏的风险。

4）广泛应用的智能合约技术，使得区块链需要相应的合约安全保障体系

对区块链中的智能合约进行重点安全防护设计，以形式化分析、安全编码组件设计、安全检查和取证为手段，解决智能合约防伪造、防窃取的问题，保证数据的透明性和公信力。

5）去中心化管理，使得区块链需要具备更加完善和安全的身份认证机制

区块链技术的核心优势是去中心化，在节点无需互相信任的分布式系统中实现点对点交易、协调与协作，解决了中心化机构普遍存在的高成本、低效率和数据存储不安全等问题。研究区块链技术应用的认证机制，基于分布式身份认证模型、匿名化认证、多因子认证和跨域认证等手段，对开放式资源池中的用户进行身份认证，提高系统抗攻击和防伪造的能力。

（下转第 382 页）

私钥，从而无法假冒合法节点。因此，本方案具有更强的容侵能力。

由上述分析可以看出，本方案具有完善的安全特性，并且不存在密钥托管问题，在安全性上优于文献[4-5]中的方案。

3.3 效率分析

本节将对方案的计算开销进行分析，并与文献[4-5]中的方案进行比较。这 3 个方案都是采用基于身份的公钥体制实现的。在分析比较方案的计算开销时，忽略对称密钥操作和普通哈希操作，仅考虑双线性对运算(P)、指数运算(Ex)和椭圆曲线加法群上的点乘运算(Pm)。由文献[7]可知，P 的计算开销约为 Pm 的 9.6 倍，Ex 的计算开销约为 Pm 的 8 倍。由表 1 可以看出，本方案中每个节点只需要进行 6 次椭圆曲线加法群上的点乘运算，不需要进行双线性对运算，因此本方案具有更小的计算开销，更适合在 Ad hoc 网络环境中应用。

表 1 计算开销比较

方案	P	Ex	Pm
文献[4]方案	2	1	1
文献[5]方案	3	1	3
本文方案	0	0	6

结束语 本文结合无双线性对的基于身份的签名算法和 Diffie-Hellman 密钥协商技术，设计了一种新的 Ad hoc 网络认证和密钥协商方案。分析表明，方案在满足安全性要求的前提下，具有较小的计算开销，很好地适应了 Ad hoc 网络的特点和需要。

参 考 文 献

[1] ZHOU L, HAAS Z. Securing Ad Hoc Networks[J]. Microcomputer Applications, 2005, 13(6): 24-30.

[2] YI S, KRAVETS R. MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks[C]// Pki Research Workshop Program. 2004: 65-79.

[3] SEN J, SUBRAMANYAM H. An Efficient Certificate Authority for Ad Hoc Networks[M]// Distributed Computing and Internet Technology. Springer Berlin Heidelberg, 2007: 97-109.

[4] 吴平，王保云，徐开勇. 基于身份的 Ad Hoc 网络密钥管理方案[J]. 计算机工程，2008，34(24)：143-145.

[5] 施荣华，樊翔宇. 基于身份认证的 Ad Hoc 密钥协商方案[J]. 中南大学学报(自然科学版)，2010，41(6)：2236-2239.

[6] DU H Z, WEN Q Y. Efficient traceable identity-based signature scheme[J]. Journal on Communications, 2009, 30(8): 56-61.

[7] 杜红珍，温巧燕. 高效的可追踪的基于 ID 的签名方案[J]. 通信学报，2009，30(8)：56-61.

[8] 周福才，徐剑，徐海芳，等. Ad hoc 网络中基于双线性配对的 STR 组密钥管理协议研究[J]. 通信学报，2008，29(10)：117-125.

(上接第 355 页)

6)透明化的特点，使得区块链需要具备更完备的隐私保护机制

区块链的开放式存储和数据透明化的特点，使得隐私保护成为重中之重。研究区块链应用的隐私保护问题，有助于解决数据泄露与滥用的问题，兼顾效率性与安全性。

7)点对点交易的模式，使得区块链应具备灵活且安全的访问控制机制

区块链技术对访问控制和身份认证机制提出了新的技术挑战，研究应用于区块链技术的访问控制机制能够有效抵抗外部攻击并避免隐私泄露的问题，从而加强区块链。

最后，随着国家支持政策与监管政策的出台，以及区块链技术的完善，2018 年区块链的应用落地会出现在各行各业。

参 考 文 献

[1] 谭磊，陈刚. 区块链 2.0[M]. 北京：电子工业出版社，2015.

[2] 隐藏在数字货币身后的力量——浅析区块链技术应用场景[EB/OL]. (2015-11-12). http://mingin.baijia.baidu.com/article/228350.

[3] RICHARD D R, GARETH O G. Rep on the block: anext generation reputation system based on the blockchain[C]// Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST). London, Britain: IEEE, 2015.

[4] GUY ZYSKIND G, NATHAN O, ALEX' A S. Decentralizing privacy: using blockchain to protect personal data[C]// Proceedings of the Security and Privacy Workshops (SPW). San Jose, USA: IEEE, 2015.

[5] 赵赫，李晓风，占礼葵，等. 基于区块链技术的采样机器人数据保护方法[J]. 华中科技大学学报，2015，43(S1)：216-219.

[6] 龚鸣. 简单谈谈究竟什么是“区块链”技术[EB/OL]. (2015-10-23). http://mt.sohu.com/20151023/n424005566.shtml.

[7] SWAN M. Blockchain thinking: the brain as a decentral-ized autonomous corporation [J]. IEEE Technology and Society Magazine, 2015, 34(4): 41-52.

[8] 刘孝男，王永涛，白云波. 区块链+时代，行业面临的机遇与挑战[J]. 中国信息安全，2017(8)：100-103.

[9] ANONYMOUS. New kid on the blockchain [J]. New Scientist, 2015, 225(3009): 7.

[10] GODSIFF P. Bitcoin: bubble or blockchain [C]// Proceedings of the 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KES-AMSTA). Sorrento, Italy: Springer, 2015: 191-203.

[11] 谢辉，王健. 区块链技术及其应用研究[J]. 信息网络安全，2016(9)：192-195.

[12] 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.

[13] 邵宇. 区块链技术对金融监管的挑战[J]. 上海政法学院学报(法治论丛)，2017，32(4)：30-40.

[14] 黄锐. 金融区块链技术的监管研究[J]. 学术论坛，2016，39(10)：53-59.

[15] 赵田雨. 区块链技术的监管困境[J]. 经济师，2017(3)：26-27.

[16] 龚鸣. 区块链社会-解码区块链全球应用于投资方案[M]. 北京：中信出版集团，2016(3)：14-16.

[17] 杨东. 保持动态监管体制[J]. 中国经济信息，2016(5)：9-9.

[18] 杨东. 互联网金融的法律规制——基于信息工具的视角[J]. 中国社会科学，2015(4)：107-126.

[19] 杨东. 论金融领域的颠覆创新与监管重构[J]. 人民论坛·学术前沿，2016(11)：30-39.

[20] SAMUL A. Consumer Financial Servicesin Britain: New Approaches to Dispute Resolution and Avoidance[J]. European Business Organization Law Review, 2002, 3(3): 649-694.

[21] 朱岩，甘国华，邓迪，等. 区块链关键技术中的安全性研究[J]. 信息安全研究，2016，2(12)：1090-1097.