[32] Mihaylov M, Razo-Zapata I, Radulescu R, Nowe A. Boosting the renewable energy economy with NRGcoin. ICT for Sustainability, 2016. [doi: 10.2991/ict4s-16.2016.27]

[33] Murkin J, Chitchyan R, Byrne A. Enabling peer-to-peer electricity trading. ICT for Sustainability, 2016. [doi: 10.2991/ict4s-16.2016.30]

[34] Zhang N, Wang Y, Kang CQ, Cheng JN, He DW. Blockchain technique in the energy Internet: Preliminary research framework and typical applications. CSEE, 2016,36(15):4011–4022 (in Chinese with English abstract). [doi: 10.13334/j.0258-8013.pcsee.161311]

[35] Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. In: Proc. of the IEEE Int'l Conf. on Intelligent Transportation Systems. 2016. 2663–2668. [doi: 10.1109/ITSC.2016.7795984]

[36] Wang YD, Yang JH, Xu C, Ling X, Yang Y. Survey on access control technologies for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1129–1150 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4820.htm [doi: 10.13328/j.cnki.jos.004820]

[37] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1):71–83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[38] Zhang YQ, Zhou W, Peng AN. Survey of Internet of Things security. Journal of Computer Research and Development, 2017,(10):2130–2143 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2017.20170470]

[39] Feng DG, Zhang M, Li H. Big data security and privacy protection. Chinese Journal of Computers, 2014,37(1):246–258 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2014.00246]

[40] Lin JQ, Jing JW, Zhang QL, Wang Z. Recent advances in PKI technologies. Journal of Cryptologic Research, 2015,2(6):487–496 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000095]

[41] Fromknecht C, Velicanu D. CertCoin: A NameCoin based decentralized authentication system. Technical Report, 6.857 Class Project, Massachusetts Institute of Technology, 2014.

[42] Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. Technical Report, 803, Massachusetts Institute of Technology, 2014.

[43] Lewison K, Corella F. Backing rich credentials with a blockchain PKI. Technical Report, Pomian & Corella, LLC, 2016.

[44] Axon L. Privacy-Awareness in blockchain-based PKI. Technical Report, 21-15, University of Oxford, 2015.

[45] Axon L, Goldsmith M. PB-PKI: A privacy-aware blockchain-based PKI. In: Proc. of the Int'l Conf. on Security and Cryptography. 2017. 311–318. [doi: 10.5220/0006419203110318]

[46] Matsumoto S, Reischuk RM. IKP: Turning a PKI around with decentralized automated incentives. In: Security and Privacy. 2017. 410–426. [doi: 10.1109/SP.2017.57]

[47] Faisca JG, Rogado JQ. Personal cloud interoperability. In: World of Wireless, Mobile and Multimedia Networks. 2016. 1–3. [doi: 10.1109/WoWMoM.2016.7523546]

[48] Zhu JM, Fu YG. Supply chain dynamic multi-center coordination authentication model based on block chain. Chinese Journal of Network and Information Security, 2016,2(1):27–33 (in Chinese with English abstract). [doi: 10.11959/j.issn.2096-109x.2016.00019]

[49] Kuo TT, Hsu CN, Ohno-Machado L. ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. Technical Report, University of California San Diego, 2018.

[50] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town Crier: An authenticated data feed for smart contracts. In: Proc. of the ACM Conf. on Computer and Communications Security. 2016. [doi: 10.1145/2976749.2978326]

[51] Al-Bassam M. SCPKI: A smart contract-based PKI and identity system. In: Proc. of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017. 35–40. [doi: 10.1145/3055518.3055530]

[52] Sanda T, Inaba H. Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0. In: Proc. of the 2016 IEEE Global Conf. on Consumer Electronics. 2016. 1–5. [doi: 10.1109/GCCE.2016.7800479]

[53] Raju S, Boddepalli S, Gampa S, Yan Q, Deogun JS. Identity management using blockchain for cognitive cellular networks. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2017. 1–6. [doi: 10.1109/ICC.2017.7996830]

[54] Hardjono T, Alex. Verifiable anonymous identities and access control in permissioned blockchains. Technical Report, Massachusetts Institute of Technology, 2016.

[55] Hardjono T, Smith N. Cloud-Based commissioning of constrained devices using permissioned blockchains. In: Proc. of the ACM Int'l Workshop on Iot Privacy, Trust, and Security. 2016. 29–36. [doi: 10.1145/2899007.2899012]

[56] Ateniese G, Faonio A, Magri B, Medeiros BD. Certified bitcoins. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. 2014. 80–96. [doi: 10.1007/978-3-319-07536-5_6]

[57] Bui T, Aura T. Application of public ledgers to revocation in distributed access control. Technical Report, Aalto University, 2016.

[58] Maesa DDF, Mori P, Ricci L. Blockchain based access control. In: Proc. of the IFIP Int'l Conf. on Distributed Applications and Interoperable Systems. Springer-Verlag, 2017. 206–220. [doi: 10.1007/978-3-319-59665-5_15]

[59] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the IEEE Security and Privacy Workshops. 2015. 180–184. [doi: 10.1109/SPW.2015.27]

[60] Ouaddah A, Elkalam AA, Ouahman AA. FairAccess: A new Blockchain—Based access control framework for the Internet of Things. Security & Communication Networks, 2016, 9. [doi: 10.1002/sec.1748]

[61] Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 2017,112:237–262. [doi: 10.1016/j.comnet.2016.11.007]

[62] Ouaddah A, Elkalam AA, Ouahman AA. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. Springer Int'l Publishing, 2017. [doi: 10.1007/978-3-319-46568-5_53]

[63] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing. 2017. [doi: 10.1109/PERCOMW.2017.7917634]

[64] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: Challenges and solutions. Technical Report, University of New South Wales (UNSW), 2016.

[65] Hu V, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K. Guide to attribute based access control (ABAC) definition and considerations. Technical Report, ITLB, 2013. [doi: 10.6028/NIST.SP.800–162]

[66] Li XF, Feng DG, Cheng CW, Fang ZH. Model for attribute based access control. Journal on Communications, 2008,29(4):90–98 (in Chinese with English abstract).

[67] Wang XM, Fu H, Zhang LC. Research progess on attribute-based access control. ACTA ELECTRONICA SINICA, 2010,38(7):1660–1667 (in Chinese with English abstract).

[68] Sinnema R, Wilde E. eXtensible access control markup language (XACML). Technical Report, RFC7061, EMC Corporation, 2013.

[69] Ouaddah A, Bouij-Pasquier I, Elkalam AA, Ouahman AA. Security analysis and proposal of new access control model in the Internet of Thing. In: Proc. of the Int'l Conf. on Electrical and Information Technologies. 2015. 30–35. [doi: 10.1109/EITech.2015.7162936]

[70] Kalam A a E, Benferhat S, Miège A, Baida RE, Cuppens F, Saurel C, Balbiani P, Deswarte Y, Trouessin G. Organization based access control. In: Proc. of the IEEE Int'l Workshop on Policies for Distributed Systems and Networks. 2003. 120–131. [doi: 10.1109/POLICY.2003.1206966]

[71] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access, 2016,4:2292–2303. [doi: 10.1109/ACCESS.2016.2566339]

[72] Kõlvart M, Poola M, Rull A. Smart Contracts. Springer Int'l Publishing, 2016. [doi 10.1007/978-3-319-26896-5_7]

[73] Mcfarlane C, Beer M, Brown J, Prendergast N. Patientory: A healthcare peer-to-peer EMR storage network v1.1. Technical Report, ICObazaar, 2017.

[74] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-Preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities & Society, 2018, 39. [doi: 10.1016/j.scs.2018.02.014]

[75] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. In: Proc. of the Int'l Conf. on Open and Big Data. 2016. 25–30. [doi: 10.1109/OBD.2016.11]

[76] Ekblaw A, Azaria A, Halamka JD, Md†, Lippman A. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Technical Report, 5-56-ONC, Massachusetts Institute of Technology, 2016.

[77] Kim KJ, Hong SP. Study on rule-based data protection system using blockchain in P2P distributed networks. Int'l Journal of Security and its Applications, 2016,10(11):201–210. [doi: 10.14257/ijsia.2016.10.11.18]

[78] Xue PF, Fu QC, Wang C, Wang XY. Study on medical data sharing model based on blockchain. ACTA AUTOMATICA SINICA, 2017,43(9) (in Cinese with English abstract). [doi: 10.16383/j.aas.2017.c160661]

[79] Outchakoucht A, Es-Samaali H, Philippe J. Dynamic access control policy based on blockchain and machine learning for the Internet of Things. Int'l Journal of Advanced Computer Science & Applications, 2017,8(7). [doi: 10.14569/IJACSA.2017.080757]

[80] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations. In: Proc. of the IEEE Int'l Conf. on Distributed Computing. 2017. [doi: 10.1109/ICDCS.2017.241]

[81] Alansari S, Paci F, Margheri A, Sassone V. Privacy-Preserving access control in cloud federations. In: Proc. of the IEEE Int'l Conf. on Cloud Computing. IEEE Computer Society, 2017. 757–760. [doi: 10.1109/CLOUD.2017.108]

[82] European Parliament and of the Council. General data protection regulation. Official Journal of the European Union (OJ), 2016,59: 1–88.

[83] Neisse R, Steri G, Naifovino I. A blockchain-based approach for data accountability and provenance tracking. In: Proc. of the Int'l Conf. on Availability, Reliability and Security. ACM, 2017. 14.

[84] Zhao H, Li XF, Zhang LK, Wu ZC. Data integrity protection method for microorganism sampling robots based on blockchain technology. Journal of Huazhong University of Science & Technology (Natural Science Edition), 2015,43(s1):216–219 (in Chinese with English abstract). [doi: 10.13245/j.hust.15S1052]

[85] Cucurull J, Puiggalí J. Distributed immutabilization of secure logs. In: Proc. of the Int'l Workshop on Security and Trust Management. 2016. 122–137. [doi: 10.1007/978-3-319-46598-2_9]

[86] Huang XF, Xu L, Yang L. A blockchain model of cloud forensics. Journal of Beijing University of Posts and Telecommunications, 2017,(5):1–4 (in Chinese with English abstract).

[87] Siddiqi M, All ST, Sivaraman V. Secure lightweight context-driven data logging for bodyworn sensing devices. In: Proc. of the Int'l Symp. on Digital Forensic and Security. 2017. 1–6. [doi: 10.1109/ISDFS.2017.7916500]

[88] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Security and Privacy. 2016. 839–858. [doi: 10.1109/SP.2016.55]

[89] Lazarovich A. Invisible ink: Blockchain for data privacy [Ph.D. Thesis]. Boston: Massachusetts Institute of Technology, 2015.

[90] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. Computer Science, 2015.

[91] Maymounkov P, Mazières D. Kademlia: A peer-to-peer information system based on the XOR metric. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. 2002. 53–65.

[92] Bissias G, Levine BN, Ozisik AP, Andresen G. An analysis of attacks on blockchain consensus. arXiv:1610.07985, University of Massachusetts Amherst, 2016.

[93] Dhar A, Saxena A, Misra J. Increasing anonymity in bitcoin. Lecture Notes in Computer Science, 2014,8438:122–139. [doi: 10.1007/978-3-662-44774-1_9]

[94] Monaco JV. Identifying bitcoin users by transaction behavior. In: Proc. of the SPIE DSS. 2015. [doi: 10.1117/12.2177039]

[95] Spagnuolo M, Maggi F, Zanero S. BitIodine: Extracting Intelligence from the bitcoin network. Lecture Notes in Computer Science, 2014,8437:457–468. [doi: 10.1007/978-3-662-45472-5_29]

附中文参考文献:

[4] 范捷,易乐天,舒继武.拜占庭系统技术研究综述.软件学报,2013,24(6):1346–1360. http://www.jos.org.cn/1000-9825/4395.htm [doi: 10.3724/SP.J.1001.2013.04395]

[24] 安瑞,何德彪,张韵茹,李莉.基于区块链技术的防伪系统的设计与实现.密码学报,2017,4(2):199–208. [doi: 10.13868/j.cnki.jcr.000174]

[30] 田海博,何杰杰,付利青.基于公开区块链的隐私保护公平合同签署协议.密码学报,2017,4(2):187–198. [doi: 10.13868/j.cnki.jcr.000173]

[34] 张宁,王毅,康重庆,程将南,贺大玮.能源互联网中的区块链技术:研究框架与典型应用初探.中国电机工程学报,2016,36(15): 4011–4022. [doi: 10.13334/j.0258-8013.pcsee.161311]

[36] 王于丁,杨家海,徐聪,凌晓,杨洋.云计算访问控制技术研究综述.软件学报,2015,26(5):1129–1150. http://www.jos.org.cn/1000-9825/4820.htm [doi: 10.13328/j.cnki.jos.004820]

[37] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71–83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[38] 张玉清,周威,彭安妮.物联网安全综述.计算机研究与发展,2017,(10):2130–2143. [doi: 10.7544/issn1000-1239.2017.20170470]

[39] 冯登国,张敏,李昊.大数据安全与隐私保护.计算机学报,2014,37(1):246–258. [doi: 10.3724/SP.J.1016.2014.00246]

[40] 林璟锵,荆继武,张琼露,王展.PKI 技术的近年研究综述.密码学报,2015,2(6):487–496. [doi: 10.13868/j.cnki.jcr.000095]

[48] 朱建明,付永贵.基于区块链的供应链动态多中心协同认证模型.网络与信息安全学报,2016,2(1):27–33. [doi: 10.11959/j.issn.2096-109x.2016.00019]

[66] 李晓峰,冯登国,陈朝武,房子河.基于属性的访问控制模型.通信学报,2008,29(4):90–98.

[67] 王小明,付红,张立臣.基于属性的访问控制研究进展.电子学报,2010,38(7):1660–1667.

[78] 薛腾飞,傅群超,王枞,王新宴.基于区块链的医疗数据共享模型研究.自动化学报,2017,43(9). [doi:10.16383/j.aas.2017.c160661]

[84] 赵赫,李晓风,占礼葵,吴仲城.基于区块链技术的采样机器人数据保护方法.华中科技大学学报(自然科学版),2015,43(s1):216–219. [doi: 10.13245/j.hust.15S1052]

[86] 黄晓芳,徐蕾,杨茜.一种区块链的云计算电子取证模型.北京邮电大学学报,2017,(5):1–4.

刘敖迪(1992－),男,吉林舒兰人,博士生,主要研究领域为区块链安全,云计算安全,网络信息安全.

王娜(1980－),女,博士,副教授,主要研究领域为云计算安全,网络与信息安全.

杜学绘(1968－),女,博士,教授,博士生导师,主要研究领域为大数据安全,云计算安全,信息系统多级安全.

李少卓(1995－),男,硕士生,主要研究领域为网络与信息安全.