参考文献

[1] M.S. Ali, M. Vecchio, M. Pincheira, et al., Applications of blockchains in the internet of things: a comprehensive survey, IEEE Communications Surveys and Tutorials 21 (2) (2019) 1676–1717.

[2] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 19 (5) (2017) 653–659.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[4] D. Chaum, Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups, Ph.D Thesis, University of California, Berkeley, CA, USA, 1982.

[5] S. Haber, W.S. Stornetta, How to time-stamp a digital document, J. Cryptol. 3 (2) (1991) 99–111.

[6] D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, in: R. Capocelli, A. De Santis, U. Vaccaro (Eds.), Sequences II, Springer, New York, NY, USA, 1993.

[7] R. Sharma, Bit gold, Investopedia, 2021. Available online: https://www.investopedia.com/terms/b/bit-gold.asp. (Accessed 24 October 2021).

[8] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. https://bitcoi n.org/bitcoin.pdf, October 2008.

[9] R. Sheldon, A timeline and history of blockchain technology. https://whatis.techtarget.com/feature/A-timeline-and-history-of-blockchain-technology, 2021.

[10] V. Buterin, Ethereum whitepaper. https://ethereum.org/en/whitepaper/, 2013.

[11] A. Groetsema, A. Groetsema, N. Sahdev, N. Salami, R. Schwentker, F. Cioanca, Blockchain for Business: an Introduction to Hyperledger Technologies, The Linux Foundation, 2019.

[12] P. Vasin, BlackCoin's Proof-of-Stake Protocol v2. https://blackcoin.org/blackco in-pos-protocol-v2-whitepaper.pdf. Accessed March 21, 2021.

[13] Crushcrypto, WHAT IS DELEGATED proof-OF-STAKE? Crushcrypto (2018). Available online: https://crushcrypto.com/what-is-delegated-proof-of-stake/. (Accessed 21 March 2021).

[14] Intel Corporation, PoET 1.0 Specification, 2016. Available online: https ://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html. (Accessed 21 March 2021).

[15] M. Castro, B. Liskov, Practical Byzantine Fault tolerance, in: Proceedings of the Third Symposium on Operating Systems Design and Implementation; 22–25 Feb 1999; New Orleans, LA, USA, USENIX Association, Berkeley, CA, USA, 1999, pp. 173–186.

[16] S. Popov, The Tangle. https://whitepaper.io/document/3/iota-whitepaper, 2018. Accessed March 21, 2021.

[17] Academy Binance, What is a Directed Acyclic Graph (DAG) in Cryptocurrency? Academy Binance, 2020. Available online: https://academy.binance.com/en/artic les/what-is-a-directed-acyclic-graph-dag-in-cryptocurrency. (Accessed 29 April 2021).

[18] OpenEthereum, Proof of Authority Chain. https://openethereum.github.io/Proofof-Authority-Chains. Accessed March 21, 2021.

[19] J. Kwon, Tendermint: Consensus without Mining. https://tendermint.com/static/docs/tendermint.pdf, 2014. Accessed March 21, 2021.

[20] B. Chase, E. MacBrough, Analysis of the XRP ledger consensus protocol, arXiv, 2018, preprint.

[21] L. Luu, V. Narayanan, K. Baweja, et al., SCP: a computationally-scalable byzantine consensus protocol for blockchains, IACR Cryptology ePrint Archive, 2015, p. 1168.

[22] M. Ghosh, M. Richardson, B. Ford, R. Jansen, A TorPath to TorCoin: Proof-ofBandwidth Altcoins for Compensating Relays, 2021. https://dedis.cs.yale .edu/dissent/papers/hotpets14-torpath.pdf. Accessed March 21, 2021.

[23] NEM, NEM Technical Reference. https://nemplatform.com/wp-content/uploads/2020/05/NEM_techRef.pdf, 2018. Accessed March 21, 2021.

[24] K. Karantias, A. Kiayias, D. Zindros, Proof-of-Burn, in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science, vol. 12059, Springer, Cham, 2020, pp. 523–540.

[25] A. Hayes, Proof of Capacity (cryptocurrency), Invest, 2020. Available online: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp. (Accessed 21 March 2021).

[26] L.S. Sankar, S. M, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017); 6–7 Jan 2017; Coimbatore, India, IEEE, Piscataway, NJ, USA, 2017, pp. 1–5.

[27] Z. Zheng, S. Xie, H. Dai, et al., An overview of blockchain technology: architecture, consensus, and future trends, in: IEEE 6th International Congress on Big Data; 25–30 Jun 2017; Honolulu, HI, USA, IEEE, Piscataway, NJ, USA: IEEE, 2017, pp. 557–564.

[28] A.P. Joshi, M. Han, Y. Wang, A survey on security and privacy issues of blockchain technology, Mathematical Foundations of Computing 1 (2) (May 2018) 121–147.

[29] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generat. Comput. Syst. 107 (June 2020) 841–853.

[30] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchainbased strategies for healthcare, ACM Comput. Surv. 53 (2) (2021) 1–27.

[31] H.T.M. Gamage, H.D. Weerasinghe, N.G.J. Dias, A survey on blockchain technology concepts, applications, and issues, SN Computer Science 1 (114) (2020).

[32] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A survey on blockchain for information systems management and security, Inf. Process. Manag. 58 (1) (January 2021).

[33] S. King, S. Nadal, PPCoin: peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf, August, 2012.

[34] D. Schmidt, Delegated proof of stake. https://www.benzinga.com/money/delega ted-proof-of-stake/, July, 2020.

[35] J. Frankenfield, Proof of Elapsed Time (PoET) (Cryptocurrency), Invest, October 16, 2020. Available online: https://www.investopedia.com/terms/p/proof-elapse d-time-cryptocurrency.asp. (Accessed 21 March 2021).

[36] IOTA. https://www.iota.org/. Accessed March 23, 2021.

[37] T. Kozak, Consensus Protocols that Meet Different Business Demands, Part I, Intellectsoft, 2018. Available online: https://blockchain.intellectsoft.net/blo g/consensus-protocols-that-meet-different-business-demands/. (Accessed 21 March 2021).

[38] CrushCrypto, WHAT IS proof OF WORK?. https://crushcrypto.com/what-is-proof -of-work/, 2021.

[39] CrushCrypto, What is practical byzantine fault tolerance (PBFT)? Crushcrypto, 2018. Available online: https://crushcrypto.com/what-is-practical-byzantinefault-tolerance/. (Accessed 21 March 2021).

[40] S. Zhang, J.-H. Lee, Analysis of the main consensus protocols of blockchain, ICT Express 6 (2020) 93–97.

[41] R. Santos, K. Bennett, E. Lee, Blockchain: Understanding its Uses and Implications, The Linux Foundation, 2021. Available online: https://www.edx.org/course/b lockchain-understanding-its-uses-and-implications. (Accessed 5 October 2021).

[42] A.M. Antonopoulos, Mastering Bitcoin, second ed., O'Reilly Media, Inc., Sebastopol, CA, USA, June 2017.

[43] W. Chen, Z. Xu, S. Shi, Y. Zhao, J. Zhao, A survey of blockchain applications in different domains, in: International Conference on Blockchain Technology and Applications (ICBTA); 10–12 Dec; Xi'an, China, ACM, New York, NY, USA, 2018, pp. 17–21.

[44] D. Dave, S. Parikh, R. Patel, et al., A survey on blockchain technology and its proposed solutions, Procedia Comput. Sci. 160 (2019) 740–745.

[45] A.A. Monrat, O. Schelen, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.

[46] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: a review, IEEE Access 6 (2018) 10179–10188.

[47] Cryptoslate, Coin rankings. https://cryptoslate.com/coins/, February 28, 2021.

[48] L. Conway, The 10 most important cryptocurrencies other than bitcoin, Invest (Jun 1, 2021).

[49] S. Kovach, Tesla Buys $1.5 Billion in Bitcoin, Plans to Accept it as Payment, CNBC, February 8, 2021. Available online: https://www.cnbc.com/2021/02/08/tesla-b uys-1point5-billion-in-bitcoin.html. (Accessed 23 March 2021).

[50] J. Leng, P. Jiang, K. Xu, Q. Liu, J.L. Zhao, Y. Bian, R. Shi, Makerchain: a blockchain with chemical signature for self-organizing process in social manufacturing, J. Clean. Prod. 234 (2019) 767–778.

[51] J. Leng, S. Ye, M. Zhou, J.L. Zhao, Q. Liu, W. Guo, W. Cao, L. Fu, Blockchainsecured smart manufacturing in industry 4.0: a survey, IEEE Transact. Syst. Man Cybernet.: Systems 51 (1) (2021) 237–252.

[52] J. Leng, G. Ruan, P. Jiang, K. Xu, Q. Liu, X. Zhou, Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: a survey, Renew. Sustain. Energy Rev. 132 (2020), 110112.

[53] J. Leng, D. Yan, Q. Liu, K. Xu, J.L. Zhao, R. Shi, L. Wei, D. Zhang, X. Chen, ManuChain: combining permissioned blockchain with a holistic optimization model as Bi-level intelligence for smart manufacturing, IEEE Transact. Syst. Man Cybernet.: Systems 50 (1) (2020) 182–192.

[54] H. Poston, Mapping the OWASP top ten to blockchain, Procedia Comput. Sci. 177 (2020) 613–617.

[55] Ji.H. Park, Jo.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164.

[56] J. Frankenfield, Mt. Gox, Investopedia, 2021. Available online: https:// www.investopedia.com/terms/m/mt-gox.asp. (Accessed 26 March 2021).

[57] E. Yu, Anonymous Website Disappears with $100M in Bitcoin, ZDNet, December 5, 2013. Available online: https://www.zdnet.com/article/anonymous-websi te-disappears-with-100m-

in-bitcoin/. (Accessed 26 March 2021).

[58] J. Horwitz, I. Kar, One of the World's Largest Bitcoin Exchanges Lost $65 Million in a Hack, QUARTZ, August 3, 2016. Available online: https://qz.com/748995 /one-of-the-worlds-largest-bitcoin-exchanges-lost-65-million-in-a-hack/. (Accessed 26 March 2021).

[59] F. Erazo, Hackers Steal Over $1.3M from European Crypto Trading Platform, Cointelegraph, Aug 03, 2020. Available online: https://cointelegraph.com/ne ws/hackers-steal-over-13m-from-european-crypto-trading-platform. (Accessed 26 March 2021).

[60] V. Buterin, Bitfloor Hacked, $250,000 Missing, Bitcoin Magazine, September 5, 2012. Available online: https://bitcoinmagazine.com/business/bitfloor-hac ked-250000-missing-1346821046. (Accessed 26 March 2021).

[61] C.K. Elwell, M.M. Murphy, M.V. Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, Congressional Research Service, July 15, 2014. Available online: https://www.everycrsreport.com/reports/R43339.html. (Accessed 26 March 2021).

[62] R. Chirgwin, Android Bug Batters Bitcoin Wallets, The Register, August 12, 2013. Available online: https://www.theregister.com/2013/08/12/android_bug_batter s_bitcoin_wallets/. (Accessed 26 March 2021).

[63] B. Grubb, Australian Bitcoin Bank Hacked: $1mþ Stolen, Brisbane Times, November 8, 2013. Available online: https://www.brisbanetimes.com.au/tech nology/australian-bitcoin-bank-hacked-1m-stolen-20131108-hv2iv.html. (Accessed 26 March 2021).

[64] W. Zhao, $30 Million: Ether Reported Stolen Due to Parity Wallet Breach, Coindesk, Jul 20, 2017. Available online: https://www.coindesk.com/markets/2017/07/19/30-million-ether-reported-stolen-due-to-parity-wallet-breach/. (Accessed 26 March 2021).

[65] Parity Technologies, Security Alert. https://www.parity.io/security-alert-2/, November 08, 2017. Accessed April 11, 2021 from.

[66] N. Popper, A Hacking of More than $50 Million Dashes Hopes in the World of Virtual Currency, N. Y. Times, June 17, 2016.

[67] A. Lewis, A Gentle Introduction to Ethereum, Bits on Blocks, October 2, 2016.

[68] V. Buterin, Thinking about Smart Contract Security, ethereum foundation blog, June 19, 2016. Available online: https://blog.ethereum.org/2016/06/19/thinkin g-smart-contract-security/. (Accessed 11 April 2021).

[69] Spartak_t, HackerGold (HKG) has a SERIOUS bug. https://bitcointalk.org/ind ex.php?topic¼1744115.0, January 08, 2017. Accessed April 11, 2021.

[70] J. Solana, \500K hack challenge backfires on blockchain lottery SmartBillions, Available online: https://calvinayre.com/2017/10/13/bitcoin/500k-hackchall enge-backfires-blockchain-lottery-smartbillions/, 2017. (Accessed 11 April 2021).

[71] L. Brent, A. Jurisevic, M. Kong, et al., Vandal: A scalable security analysis framework for smart contracts, arXiv, 2018 preprint.

[72] A. Roan, How Spankchain Got Hacked. https://medium.com/swlh/how-spankch ain-got-hacked-af65b933393c, March 27, 2020. Accessed April 9, 2021.

[73] P. Litke, J. Stewart, BGP Hijacking for Cryptocurrency Profit, Secureworks, 7 August 2014. Available online: https://www.secureworks.com/research/bgp-h ijacking-for-cryptocurrency-profit. (Accessed 9 April 2021).

[74] J. Wilcke, The Ethereum Network is Currently Undergoing a DoS Attack, Ethereum Foundation Blog, September 22, 2016. Available online: https://blog.e

thereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/. (Accessed 9 April 2021).

[75] Aruba, 10 Blockchain and New Age Security Attacks You Should Know, January 22, 2019. Available online: https://blogs.arubanetworks.com/solutions/10-bloc kchain-and-new-age-security-attacks-you-should-know/. (Accessed 9 April 2021).

[76] Waqas, The Pirate Bay Caught Running Cryptocurrency Mining Script, HackRead, September 17, 2017. Available online: https://www.hackread.com/the-piratebay-caught-running-cryptocurrency-mining-script/. (Accessed 9 April 2021).

[77] K. McCarthy, CBS's Showtime Caught Mining Crypto-coins in Viewers' Web Browsers, The Register, September 25, 2017. Available online: https://www.ther egister.com/2017/09/25/showtime_hit_with_coinmining_script/. (Accessed 9 April 2021).

[78] M. Beedham, Hackers secretly ran cryptocurrency mining malware on Indian government sites, 17 Sep 2018. Available online: https://thenextweb.com/n ews/indian-government-cryptocurrency-coinhive. Accessed: 9 Apr 2021.

[79] T. Claburn, Crypto-jackers Enlist Google Tag Manager to Smuggle Alt-coin Miners, The Register, November 22, 2017. Available online: https://www.theregister .com/2017/11/22/cryptojackers_google_tag_manager_coin_hive/. (Accessed 9 April 2021).

[80] M. Maunder, WordPress Plugin Banned for Crypto Mining, Wordfence, November 8, 2017. Available online: https://www.theregister.com/2017/11/22/cryptojac kers_google_tag_manager_coin_hive/. (Accessed 9 April 2021).

[81] T. Mursch, Over 100,000 Drupal Websites Vulnerable to DRUPALGEDDON 2 (CVE-2018-7600), Bad Packets, June 4, 2018. Available online: https://badpack ets.net/over-100000-drupal-websites-vulnerable-to-drupalgeddon-2-cve-2018- 7600/. (Accessed 9 April 2021).

[82] T. Cantisano, YouTube Ads Hijacked Visitors Computers to Mine Cryptocurrency, Neowin, January 26, 2018. Available online: https://www.neowin.net/news/yout ube-ads-hijacked-visitors-computers-to-mine-cryptocurrency/. (Accessed 9 April 2021).

[83] C. Osborne, MikroTik Routers Enslaved in Massive Coinhive Cryptojacking Campaign, ZDNet, August 3, 2018. Available online: https://www.zdnet.com/arti cle/mikrotik-routers-enslaved-in-massive-coinhive-cryptojacking-campaign/. (Accessed 9 April 2021).

[84] L. Kelion, Starbucks Cafe's Wi-Fi Made Computers Mine Crypto-Currency, BBC News, December 13, 2017.

[85] C. Cimpanu, IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack, Bleepingcomputer, 2018. Available online, https://www.bleepingcompute r.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishin g-attack/ (Accessed: 9 Apr 2021).

[86] L. Cuen, IOTA Being Shut Off is the Latest Chapter in an Absurdist History, CoinDesk, February 26, 2020. Available online: https://www.coindesk.com/bus iness/2020/02/25/iota-being-shut-off-is-the-latest-chapter-in-an-absurdist-histo ry/. (Accessed 9 April 2021).

[87] L. Breidenbach, P. Daian, F. Tramer, A. Juels, Enter the Hydra: towards principled bug bounties and exploit-resistant smart contracts, in: 27th USENIX Security Symposium; 15–17 Aug 2018; Baltimore, MD, USA, USENIX Association, Berkeley, CA, USA, 2018, pp. 1335–1352.

[88] E. Hildenbrandt, M. Saxena, N. Rodrigues, et al., KEVM: a complete formal semantics of the

ethereum virtual machine, in: 2018 IEEE 31st Computer Security Foundations Symposium (CSF); 9–12 Jul 2018; Oxford, UK, IEEE, Piscataway, NJ, USA, 2018, pp. 204–217.

[89] L. Luu, Oyente: An Analysis Tool for Smart Contracts. https://loiluu.com/oyente.h tml, 2016. Accessed April 5, 2021.

[90] P. Tsankov, A. Dan, D. Drachsler-Cohen, et al., Securify: practical security analysis of smart contracts, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS'18); 15–19 Oct 2018; Toronto, ON, Canada, ACM, New York, NY, USA, 2018, pp. 67–82.

[91] S. Kalra, S. Goel, M. Dhawan, et al., ZEUS: analyzing safety of smart contracts, in: Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, USA, NDSS, Reston, VA, USA, 2018.

[92] L. Luu, D.-H. Chu, H. Olickel, et al., Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16); 24–28 Oct 2016; Vienna, Austria, ACM, New York, NY, USA, 2016.

[93] Mythril. https://github.com/ConsenSys/mythril, 2018. Accessed Apr 7, 2021.

[94] J. Frank, C. Aschermann, T. Holz, EthBMC: a bounded model checker for smart contracts, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2757–2774.

[95] M. Mossberg, F. Manzano, E. Hennenfent, et al., Manticore: a user-friendly symbolic execution framework for binaries and smart contracts, in: 34th IEEE/ ACM International Conference on Automated Software Engineering (ASE); 11–15 Nov 2019; San Diego, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 1186–1189.

[96] I. Nikolic, A. Kolluri, I. Sergey, et al., Finding the greedy, prodigal, and suicidal contracts at scale, in: The 34th Annual Computer Security Applications Conference(ACSAC); 3–7 Dec 2018. San Juan, PR, USA, ACM, New York, NY, USA, 2018, pp. 653–663.

[97] N. Grech, M. Kong, A. Jurisevic, et al., MadMax: surviving out-of-gas conditions in ethereum smart contracts, in: Proceedings of the ACM on Programming Languages 2, 2018, pp. 1–27.

[98] C.F. Torres, J. Schütte, R. State, Osiris: hunting for integer bugs in ethereum smart contracts, in: 34th Annual Computer Security Applications Conference (ACSAC); 3–7 Dec 2018; San Juan, PR, USA, ACM, New York, NY, USA, 2018, pp. 664–676.

[99] M. Zhang, X. Zhang, Y. Zhang, Z. Lin, TxSpector: uncovering attacks in ethereum from transactions, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2775–2792.

[100] S. Zhou, Z. Yang, J. Xiang, et al., An ever-evolving game: evaluation of real-world attacks and defenses in ethereum ecosystem, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2793–2810.

[101] C.F. Torres, M. Steichen, The art of the scam: demystifying honeypots in ethereum smart contracts, in: 28th USENIX Security Symposium; 14–16 Aug 2019; Santa Clara, CA, USA, USENIX Association, Berkeley, CA, USA, 2019, pp. 1591–1607.

[102] A. Gervais, G.O. Karame, K. Wüst, et al., On the security and performance of proof of work blockchains, in: 2016 ACM SIGSAC Conference on Computer and Communications Security; 24–28 Oct 2016; Vienna, Austria, ACM, New York, NY, USA, 2016, pp. 3–16.

[103] R. Zhang, B. Preneel, Lay down the common metrics: evaluating proof-of-work consensus protocols' security, in: 2019 IEEE Symposium on Security and Privacy; 19–23 May 2019; San

Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 175–192.

[104] B. Jiang, Y. Liu, W. Chan, ContractFuzzer: fuzzing smart contracts for vulnerability detection, in: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering; 3–7 Sep 2018; Montpellier, France, IEEE, Piscataway, NJ, USA, 2018, pp. 259–269. [105] C. Liu, H. Liu, Z. Cao, et al., ReGuard: finding reentrancy bugs in smart contracts, in: The 40th International Conference on Software Engineering: Companion; 27 May–3 Jun 2018; Gothenburg, Sweden, IEEE, Piscataway, NJ, USA, 2018, pp. 65–68.

[106] Y. Fu, M. Ren, F. Ma, et al., EVMFuzzer: detect EVM vulnerabilities via fuzz testing, in: 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering; 26–30 Aug 2019. Tallinn, Estonia, ACM, New York, NY, USA, 2019, pp. 1110–1114.

[107] V. Wustholz, M. Christakis, HARVEY: a greybox fuzzer for smart contracts, in: The 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering; 8–13 Nov 2020; Virtual Event, ACM, New York, NY, USA, 2020, pp. 1398–1409.

[108] L. Luu, Y. Velner, J. Teutsch, P. Saxena, SMARTPOOL: practical decentralized pooled mining, in: 26th USENIX Security Symposium, Vancouver, BC, Canada; 16–18 Aug 2017. Vancouver, BC, Canada, USENIX Association, Berkeley, CA, USA, 2017, pp. 1409–1426.

[109] M. Drijvers, K. Edalatnejad, B. Ford, et al., On the security of two-round multisignatures, in: 40th IEEE Symposium on Security and Privacy; 19–23 May 2019; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 1084–1101.

[110] M. Drijvers, S. Gorbunov, G. Neven, Pixel: multi-signatures for consensus, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2093–2110.

[111] Y. Sun, A. Edmundson, N. Feamster, M. Chiang, P. Mittal, Counter-RAPTOR: safeguarding tor against active routing attacks, in: IEEE Symposium on Security and Privacy; 22–26 May 2017; San Jose, CA, USA, IEEE, Piscataway, NJ, USA, 2017, pp. 977–992.

[112] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: an authenticated data feed for smart contracts, in: 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16); 24–28 Oct 2016; Vienna, Austria, ACM, New York, NY, USA, 2016, pp. 270–282.

[113] A. Mavridou, A. Laszka, Tool demonstration: FSolidM for designing secure ethereum smart contracts, in: International Conference on Principles of Security and Trust; 14–20 Apr 2018; Thessaloniki, Greece, Springer, Cham, Switzerland, 2018, pp. 270–277.

[114] H. Kalodner, S. Goldfeder, X. Chen, et al., Arbitrum: scalable, private smart contracts, in: 27th USENIX Security Symposium; 15–17 Aug 2018; Baltimore, MD, USA, USENIX Association, Berkeley, CA, USA, 2018, pp. 1353–1370.

[115] S. So, M. Lee, J. Park, et al., VERISMART: a highly precise safety verifier for ethereum smart contracts, in: 2020 IEEE Symposium on Security and Privacy; 17–21 May 2020; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2020, pp. 1678–1694.

[116] S. Amani, M. B egel, M. Bortin, M. Staples, Towards verifying ethereum smart contract bytecode in Isabelle/HOL, in: The 7th ACM SIGPLAN International H. G

Conference on Certified Programs and Proofs; 8–9 Jan 2018; Los Angeles. CA. USA, ACM, New York, NY, USA, 2018, pp. 66–77.

[117] T. Abdellatif, K.-L. Brousmiche, Formal verification of smart contracts based on users and blockchain behaviors models, in: The 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 26–28 Feb 2018; Paris, France, IEEE, Piscataway, NJ, USA, 2018, pp. 1–5.

[118] T. Sun, W. Yu, A formal verification framework for security issues of blockchain smart contracts, Electronics 9 (2) (2020), 225.

[119] A. Permenev, D. Dimitrov, P. Tsankov, et al., VerX: safety verification of smart contracts, in: 2020 IEEE Symposium on Security and Privacy; 17–21 May 2020; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2020, pp. 1661–1677.

[120] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy; 22–26 May 2016; San Jose, CA, USA, IEEE, Piscataway, NJ, USA, 2016, pp. 839–858.

[121] M. Tran, L. Luu, M.S. Kang, I. Bentov, P. Saxena, Obscuro: a bitcoin mixer using trusted execution environments, in: 34th Annual Computer Security Applications Conference (ACSAC); 3–7 Dec 2018; San Juan, PR, USA, ACM, New York, NY, USA, 2018, pp. 692–701.

[122] T. Kerber, A. Kiayias, M. Kohlweiss, V. Zikas, Ouroboros crypsinous: privacypreserving proof-of-stake, in: 2019 IEEE Symposium on Security and Privacy; 19–23 May 2019; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 157–174.

[123] S. Matetic, K. Wüst, M. Schneider, et al., Bite: bitcoin lightweight client privacy using trusted execution, in: 28th USENIX Security Symposium; 14–16 Aug 2019; Santa Clara, CA, USA, USENIX Association, Berkeley, CA, USA, 2019, pp. 783–800.

[124] S. Bowe, A. Chiesa, M. Green, et al., Zexe: enabling decentralized private computation, in: 2020 IEEE Symposium on Security and Privacy; 18–21 May 2020; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2020, pp. 947–964.

[125] F. Tramer, D. Boneh, K. Paterson, Remote side-channel attacks on anonymous transactions, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2739–2756.

[126] T. Wright, Four-year Anniversary of Bitfinex Hack, and $12M of Stolen BTC Moved, Cointelegraph, Aug 4, 2020. Available online: https://cointelegraph.com/ news/four-year-anniversary-of-bitfinex-hack-and-12m-of-stolen-btc-moved. (Accessed 7 April 2021).

[127] Ethereum, Upgrading Ethereum to radical new heights. https://ethereum.org /en/eth2/, March 1, 2021.

[128] S. Dziembowski, L. Eckey, S. Faust, et al., Perun: virtual payment hubs over cryptocurrencies, in: 2019 40th IEEE Symposium on Security and Privacy; 19–23 May 2019; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 106–123.

[129] P. Gazi, A. Kiayias, D. Zindros, Proof-of-Stake sidechains, in: 2019 40th IEEE Symposium on Security and Privacy; 19–23 May 2019; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2019, pp. 139–156.

[130] H. Yu, I. Nikolic, R. Hou, P. Saxena, OHIE: blockchain scaling made simple, in: 2020 41st IEEE Symposium on Security and Privacy; 18–21 May 2020; San Francisco, CA, USA, IEEE,

Piscataway, NJ, USA, 2020, pp. 90–105.

[131] Visa, Visa fact sheet. https://usa.visa.com/dam/VCOM/download/corporate/ media/visanet-technology/aboutvisafactsheet.pdf, March 1, 2021.

[132] IBM, IBM Blockchain Suppy Chain Solutiuons. https://www.ibm.com/uk -en/blockchain/industries/supply-chain. Accessed July 31, 2021.

[133] VeChain, VeChain Solution Overview. https://vechain.com/solution/logistics. Accessed July 31, 2021.

[134] X. Yu, H. Guo, System, Device and Method for Blockchain-Base Data Exchange, February 5, 2020. Singaporean Patent Application No. 10202000875X.

[135] W. Zou, D. Lo, P.S. Kochhar, et al., Smart Contract Development: Challenges and Opportunities, IEEE Trans. Software Eng., 47 (10) (2019) 2084–2106.

[136] E. Germany, The Crypto SWOT Team Investigates EOS, steemit, 2018. Available online: https://steemit.com/eosgermany/@eosgermany/the-crypto-swot-team-in vestigates-eos.

[137] P. Daian, S. Goldfeder, T. Kell, et al., Flash Boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability, in: 2020 41st IEEE Symposium on Security and Privacy(SP); 18–21 May 2020; San Francisco, CA, USA, IEEE, Piscataway, NJ, USA, 2020, pp. 910–927.

[138] Y. Zhou, D. Kumar, S. Bakshi, et al., Erays: reverse engineering Ethereum’s opaque smart contracts, in: 27th USENIX Security Symposium; 15–17 Aug 2018; Baltimore, MD, USA, USENIX Association, Berkeley, CA, USA, 2018, pp. 1371–1385.

[139] H. Kalodner, M. Moser, K. Lee, et al., BlockSci: design and applications of a € blockchain analysis platform, in: 29th USENIX Security Symposium; 12–14 Aug 2020; online, USENIX Association, Berkeley, CA, USA, 2020, pp. 2721–2738.

[140] G. Xu, B. Guo, C. Su, X. Zheng, K. Liang, D.S. Wong, H. Wang, Am I eclipsed? A smart detector of eclipse attacks for ethereum, Comput. Secur. 88 (2020).

[141] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: 35th Annual Symposium on Foundations of Computer Science; 20–22 Nov 1994 ; Santa Fe, NM, USA, IEEE, Piscataway, NJ, USA, 1994, pp. 124–134.

[142] A. Bouguera, How will quantum computing affect blockchain? Consensys (December 3, 2019). Available online: https://consensys.net/blog/developers/h ow-will-quantum-supremacy-affect-blockchain/. (Accessed 31 July 2021).

[143] NIST’s Post-Quantum Cryptography Program Enters ‘Selection Round’, National Institute of Standards and Technology (NIST), July 22, 2020. Available online: https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-crypto graphy-program-enters-selection-round. (Accessed 31 July 2021).

[144] I. Barmes, B. Bosch, Quantum Computers and the Bitcoin Blockchain, Deloitte, March 13, 2021. Available online: https://www.nist.gov/news-events/news/202 0/07/nists-post-quantum-cryptography-program-enters-selection-round. (Accessed 31 July 2021).

[145] L. M, IOTA Price Prediction 2021 and Beyond: What to Expect? BigDegree, January 25, 2021. Available online: https://www.bitdegree.org/crypto/tutorials /iota-price-prediction.

[146] S. Sayadi, S.B. Rejeb, Z. Choukair, Blockchain challenges and security schemes: a survey, in: Seventh International Conference on Communications and Networking (ComNet); 1–3 Nov 2018; Hammamet, Tunisia, IEEE, Piscataway, NJ, USA, 2018, pp. 1–7.

[147] M. Saad, J. Spaulding, L. Njilla, et al., Exploring the attack surface of blockchain: a systematic

overview, IEEE Communications Surveys & Tutorials 22 (3) (2020) 1977–2008.

[148] D. Dasgupta, J.M. Shrein, K.D. Gupta, A survey of blockchain from security perspective, Journal of Banking and Financial Technology 3 (2019) 1–17.

[149] J. Leng, M. Zhou, J.L. Zhao, Y. Huang, Y. Bian, Blockchain security: a survey of techniques and research directions, IEEE Transactions on Services Computing, 2020.

[150] W. Chen, Z. Xu, S. Shi, et al., A survey of blockchain applications in different domains, in: International Conference on Blockchain Technology and Applications (ICBTA); 10–12 Dec 2018; Xi'an, China, ACM, New York, NY, USA, 2018, pp. 17–21.