IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

A Survey of Security of Blockchain

Dr. S. Sobana[1], Akshay K K[2], Adithya[3], Sahin[4], Ginnu George[5]
EPA, Coimbatore[1]
Students, Department of Computer Science & Engineering[2,3,4]
Assistant Professor, Department of Computer Science & Engineering[5]
Vedavyasa Institute of Technology, Malappuram, Kerala, India

Abstract: *The blockchain technology witnessed a wide adoption and a swift growth in recent years. This ingenious distributed peer-to-peer design attracted several businesses and solicited several communities beyond the financial market. There are also multiple use cases built around its ecosystem. However, this backbone introduced a lot of speculation and has been criticized by several researchers. Moreover, the lack of legislations perceived a lot of attention. In this paper, we are concerned in analyzing blockchain networks and their development, focusing on their security challenges. We took a holistic approach to cover the involved mechanisms and the limitations of Bitcoin, Ethereum and Hyper ledger networks. We expose also numerous possible attacks and assess some countermeasures to dissuade vulnerabilities on the network. For occasion, we simulated the majority and the reentrancy attacks. The purpose of this paper is to evaluate Blockchain security summarizing its current state. Thoroughly showing threatening flaws, we are not concerned with favoring any particular blockchain network..*

Keywords: Block chain

REFERENCES

[1]. R. Wattenhofer, Distributed Ledger Technology - The science of Blockchain. Forest Publishing, 2017.
[2]. E. A. Brewer, "Towards robust distributed systems," in PODC, vol. 7, 2000.
[3]. A. Fox and E. A. Brewer, "Harvest, yield, and scalable tolerant systems," in Hot Topics in Operating Systems, 1999. Proceedings of the Seventh Workshop on. IEEE, 1999, pp. 174–178.
[4]. S. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," Acm Sigact News, vol. 33, no. 2, pp. 51–59, 2002.
[5]. Coindesk, "Bitcoin technology," https://www.coindesk.com/ bitcoin-technology-anonymoustor-network-more-powerful/.
[6]. "History of bitcoin," http://historyofbitcoin.org/, 2008.
[7]. V. Buterin et al., "A next-generation smart contract and decentralized application platform," white paper, 2014.
[8]. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, 2014.
[9]. G. Network, "From the winning team at ethwaterloo world's largest ethereum hackathon," https://gonetwork.co/, 2017.
[10]. J. Moubarak, E. Filiol, and M. Chamoun, "Comparative analysis of blockchain technologies and tor network: Two faces of the same reality?" in Cyber Security in Networking Conference (CSNet), 2017 1st. IEEE, 2017, pp. 1–9.
[11]. C. Dannen, "Introducing ethereum and solidity."
[12]. "Hyperledger fabric blog," http://blockchain-fabric.blogspot.com/2017/ 04/hyperledgerfabric-v10-block-structure.html.
[13]. A. Bahga and V. Madisetti, "Blockchain applications: A hands-on approach," 2017.
[14]. "Hyperledger blog," http://hyperledger-fabric.readthedocs.io/en/latest/ arch-deepdive.html.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 3, December 2021
Impact Factor: 5.731

[15]. C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in Symposium on SelfStabilizing Systems. Springer, 2015, pp. 3–18.

[16]. M. Scherer, "Performance and scalability of blockchain networks and smart contracts," 2017.

[17]. J. Adelstein, Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox (2016). URL http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-hei st-in-history-inside-the-implosion-of-mt-gox.html

[18]. N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017.

[19]. Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: International Journal of Web and Grid Services, 2016.

[20]. M. Ghosh, M. Richardson, B. Ford, R. Jansen, A torpath to torcoin, proof-of-bandwidth altcoins for compensating relays (2014). URL https://www.smithandcrown.com/open-research/a-torpath-to-torcoin-proof-of-bandw idth-altcoins-for-compensating-relays/

[21]. Intel, Proof of elapsed time (poet) (2017). URL http://intelledger.github.io/

[22]. P. technologies, Proof of authority chains (2017). URL https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains

[23]. E. community, Kovan - stable ethereum public testnet (2017). URL https://github.com/kovan-testnet/proposal

[24]. L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smart pool: Practical decentralized pooled mining, in: USENIX Security Symposium, 2017.

[25]. Karl, Security of blockchain technologies, Ph.D. thesis, Swiss Federal Institute of Technology (2016).

[26]. Karl, Ethereum eclipse attacks, 2016. URL http://e-collection.library.ethz.ch/view/eth:49728

[27]. A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016.

[28]. V. Butterin, "Zk-snarks: Under the hood," https://medium.com/ @VitalikButerin/zk-snarks-under-the-hood-b33151a013f6, year=2017.