

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Mr. Dattaprasad Patil¹ and Mrs. Vijaya Bhosale²

Student, M.Sc. I.T., I. C. S. College, Khed, Ratnagiri, Maharashtra, India¹

Asst. Prof., Department of I.T., I. C. S. College, Khed, Ratnagiri, Maharashtra, India²

Abstract: Blockchain, which is the backbone of Bitcoin, has recently received a lot of attention. Blockchain functions as an immutable ledger that enables decentralized transactions. Numerous fields, such as the Internet of Things (IoT), reputation systems, and financial services, are being covered by blockchain-based applications. However, blockchain technology still faces numerous difficulties, such as scalability and security issues, that need to be resolved. A comprehensive overview of blockchain technology is provided in this paper. First, we compare some common consensus algorithms utilized by various blockchains and provide an overview of the architecture of blockchains. In addition, a brief list of recent advancements and technical difficulties is provided. In addition, we outline potential blockchain trends for the future.

Keywords: Blockchain, decentralization, consensus, scalability

REFERENCES

- [1]. "State of block chain q12016:Block chain funding over takes bitcoin," 2016. [Online]. Available: <http://www.coindesk.com/state-of-blockchain-q1-2016/>
- [2]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [3]. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.2646618>
- [4]. G. Foroglou and A.-L. Tsilidou, "Further application of the blockchain," 2015.
- [5]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
- [6]. B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: <https://ssrn.com/abstract=2394738>
- [7]. Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
- [8]. M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (ECTEL 2015), Lyon, France, 2015, pp. 490–496.
- [9]. C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feed forward scanning," arXiv preprint arXiv:1601.01405, 2016.
- [10]. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
- [11]. A. Biryukov, D. Khovratovich, and I. Pustogarov, "De-anonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
- [12]. F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys and Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
- [13]. NRI, "Survey on blockchain technologies and related services," Tech. Rep., 2015. [Online]. Available: <http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf>

- [14]. D.LeeKuoChuen,Ed.,HandbookofDigitalCurrency,1sted.Elsevier, 2015. [Online]. Available: <http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170>
- [15]. V. Buterin, "A next-generation smart contract and decentralized application platform," whitepaper, 2014.
- [16]. D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.
- [17]. V. Buterin, "On public and private blockchains," 2015. [Online]. Available: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- [18]. "Hyperledger project," 2015. [Online]. Available: <https://www.hyperledger.org/>
- [19]. "Consortium chain development." [Online]. Available: <https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development>
- [20]. L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.
- [21]. S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," Self-Published Paper, August, vol. 19, 2012.
- [22]. "Bitshares-your share in the decentralized exchange." [Online]. Available: <https://bitshares.org/>
- [23]. D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.
- [24]. J. Kwon, "Tendermint: Consensus without mining," URL <http://tendermint.com/docs/tendermintv04.pdf>, 2014.
- [25]. S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," July 7th, 2013.
- [26]. P. Vasin, "Blackcoin proof-of-stake protocol v2," 2014. [Online]. Available: <https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>
- [27]. G. Wood, "Ethereum: A secured decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.
- [28]. V. Zamfir, "Introducing casper the friendly ghost," Ethereum Blog URL: <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost>, 2015.
- [29]. C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.
- [30]. D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," Stellar Development Foundation, 2015.