IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 7.047 ⁜ Vol. 10, Issue 4, April 2022

DOI: 10.17148/IJIREEICE.2022.10437

Review on Blockchain Technology

Rushikesh Bhusari[1], Suraj Paswan[2], Tushar Parate[3], Sandip Neware[4], Prabhakar Khandait[5]

KDK College of Engineering Nagpur, India[1-5]

Abstract: As a decentralized ledger, blockchain is the foundation that supports Bitcoins. Due to its immutability, Blockchain has garnered extensive attention recently. In numerous fields such as financial services, reputation ‘systems and Internet of Things (IoT), blockchain-based applications. In this paper we have present a comprehensive overview on blockchain technologies, detailing the different blockchain architectures and explaining the algorithms used in each of them. Moreover, we describe recent technological advances and technological challenges for blockchain as well as possible future trends..

Keywords: Blockchain , Decentralize .

I. INTRODUCTION

Cryptocurrencies have become a buzzword in business and academia today. Bitcoin is one of the most successful bitcoins, and its market capitalization is projected to reach 700 billion dollars by 2022 [1]. The blockchain is the core technology of Bitcoin, which was first proposed in 2008 and implemented in 2009. Transactions can happen without a third party in the Bitcoin network thanks to a specially designed data storage system. In a blockchain, all transactions are recorded in blocks, which grow continuously as new blocks are added. Asymmetric cryptography is used to safeguard user data, along with distributed consensus algorithms.

Decentralization, persistence, anonymity, and auditability are key characteristics of blockchain technology. With these traits, blockchain technology can save the cost and improve the efficiency of transactions .The blockchain can be used in a wide variety of financial services including digital assets, remittance and online payment. In addition, smart contracts, public services, IOT and other fields can be incorporated into the blockchain as well. Those fields can benefit from blockchain in several ways, including immutability. Once data is stored in the blockchain, transactions cannot be manipulated. Businesses that require high trustworthiness and integrity can benefit from blockchain technology, Additionally, blockchain is distributed and can prevent a situation where a single point of failure exists. As for spart contracts, once they have been deployed on the blockchain the contracts can be executed automatically by the miners. Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges.

Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading(2). Additionally, larger blocks take up more storage space, and the network propagates the data slower. As a result, centralization will take place gradually as fewer users will be interested in maintaining such a large blockchain.

Due to this trade off between block size and security, there has been a big challenge. Secondly, it has been proven that selfish mining strategies can result in major revenues beyond what miners are entitled to. Miners hide their mined blocks in order to gain more revenue. In order to address this problem, some proposals must be put forward. Moreover, it has been shown that privacy leakage can also occur when users transfer funds simply using their public keys and private keys. Further, current consensus algorithms such as Proof of work (pow) or Proof of stake (pos) all suffer from this flaw.

There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. [13] made a technical survey about decentralized digital currencies 2017 IEEE 6th International Congress on Big Data including Bitcoin. Our paper examines state-of-the-art blockchain researches and recent developments and future trends, rather than digital currencies. Nomura Research Institute made a report on blockchain technology. Throughout the paper, we describe blockchain architecture and suggest typical consensus algorithms used in blockchains, highlighting technical challenges and progress, and suggesting some potential future directions.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 7.047 ⁜ Vol. 10, Issue 4, April 2022
DOI: 10.17148/IJIREEICE.2022.10437

II. ARCHITECTURE

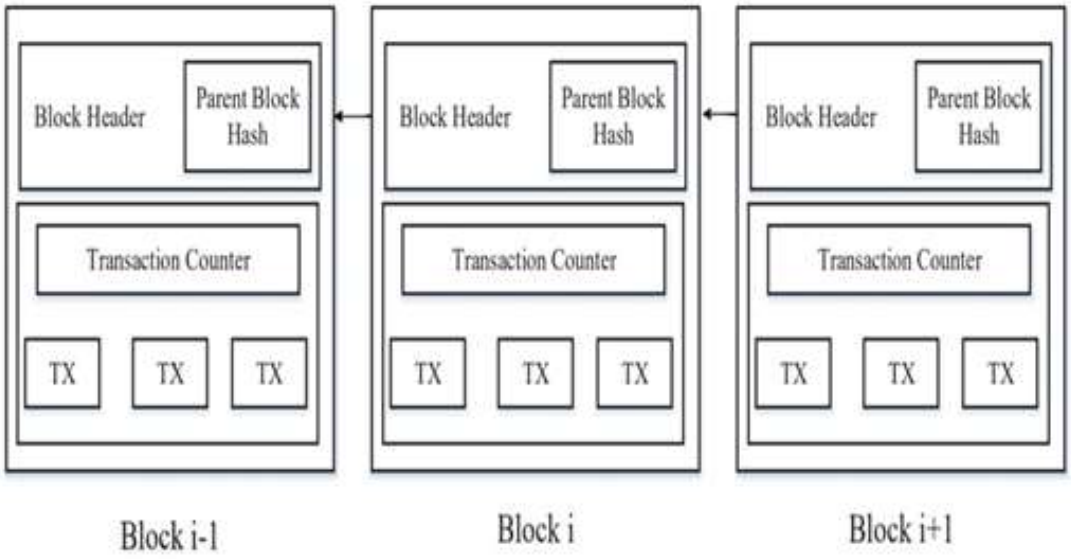

Fig 1- Blockchain Architecture[2]

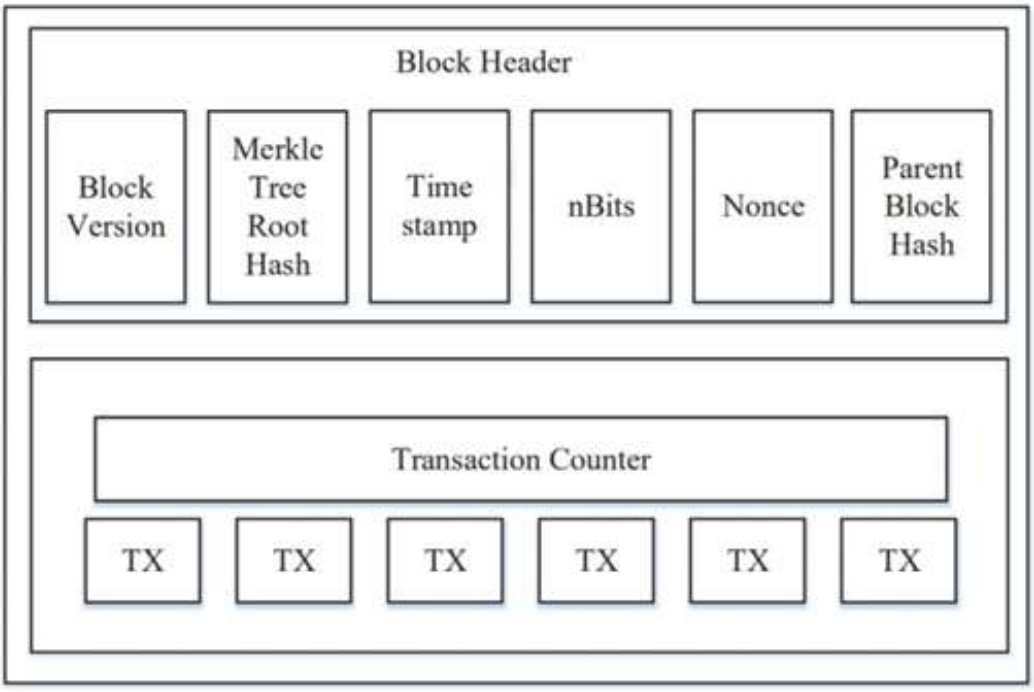

Fig 2- Block Structure[2]

A blockchain is composed of blocks containing a list of transactions like traditional ledgers, illustrating a blockchain. A block has only one parent block, as it contains the previous block's hash. A. Block A block consists of the block header and the block body as shown in Figure 2. In particular, the block header includes: (i) Block version: indicates which set of block validation rules to follow. (ii) Merkle tree root hash: the hash value of all the transactions in the block. (iii) Timestamp: current time as seconds in universal time since January 1, 1970. (iv) nBits: target threshold of a valid block hash. (v) Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III). (vi) Parent block hash: a 256-bit hash value that points to the previous block.[2] A transaction counter and transactions make up the block body. The maximum number of transactions that can be stored in a block is determined by the block size and the transaction size. To validate transaction authentication, Blockchain employs an asymmetric cryptography technique.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 7.047 ⁜ Vol. 10, Issue 4, April 2022

DOI: 10.17148/IJIREEICE.2022.10437

In an untrustworthy environment, a digital signature based on asymmetric cryptography is used. After that, we'll show you how to create a digital signature.

Digital signature

Every user has a private and public key pair. The transactions are signed with the private key, which must be kept secret. The digitally signed transactions are disseminated over the whole network. A typical digital signature comprises two stages: the signing phase and the verification phase. For example, user Alice wishes to send a message to user Bob. Alice encrypts her data using her private key during the signing step and delivers the encrypted result as well as the original data to Bob. Bob verifies the value with Alice's public key during the verification step. Bob could simply check if the data had been tampered with in this manner. The elliptic curve digital signature technique is the most common digital signature algorithm used in blockchains (ECDSA).

Key Characteristics

- Decentralization.- Each transaction in traditional centralised transaction systems must be certified by a central trusted agency (e.g., the central bank), resulting in cost and performance bottlenecks at the central servers. In contrast to the centralised option, blockchain does not require the use of a third party. Consensus algorithms are employed in blockchain to keep data consistent across a distributed network.
- Persistency- Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately.
- Anonymity. Each user interacts with the blockchain using a randomly generated address that hides the user's true identity. Due to the inherent constraint of blockchain, it cannot ensure absolute privacy protection
- Transparency. The Unspent Transaction Output (UTXO) model is used to store data on user balances on the Bitcoin blockchain: Any transaction must reference some previously unspent funds. The state of those referred unspent transactions changes from unspent to spent once the present transaction is recorded into the blockchain. As a result, transactions could be easily tracked and validated.

III. ALGORITHM

The Byzantine Generals (BG) Problem, which first raised in [20], is a question of how to obtain consensus among untrustworthy nodes in blockchain. A group of generals who command a section of the Byzantine army circle the city in the BG issue. Some generals would rather assault, while others would rather retreat. However, if only a portion of the generals attack the city, the attack will fail. As a result, they must decide whether to assault or retreat. It's difficult to reach a consensus in a dispersed setting. It's also a concern for blockchain because the network is spread. There is no central node in blockchain that assures all distributed node ledgers are identical. To ensure that ledgers in multiple nodes are consistent, some protocols are required. Following that, we'll go over a few different ways to obtain a blockchain consensus.

Approaches

Proof of work (Pow) -It's also a concern for blockchain because the network is spread. There is no central node in blockchain that assures all distributed node ledgers are identical. To ensure that ledgers in multiple nodes are consistent, some protocols are required. Following that, we'll go over a few different ways to obtain a blockchain consensus. Each network node calculates a hash value for the block header in PoW. A nonce is contained in the block header, and miners would change the nonce regularly to obtain different hash values. The estimated value must be equal to or less than a specific value, according to the consensus. When one node reaches the target value, it broadcasts the block to all other nodes, who must all mutually validate that the hash value is correct. Other miners will attach this new block to their own blockchains if the block is validated. Miners are nodes that calculate hash values, and the Pow technique is known as mining in Bitcoin.

Valid blocks may be generated simultaneously in a decentralised network if many nodes identify the appropriate nonce roughly at the same moment. .. But that's unlikely Two competing forks create the next block at the same time. In the Pow protocol, it's a chain that grows longer after that. It is evaluated as genuine. Consider the two forks created by Blocks U4 and B4 verified at the same time. Keep the miner Mining the blocks until you find a longer branch. B4, B5 Form a longer chain that miners switch with U4 The longer branch. Miners have to do a lot of computer calculations with Pow. Nevertheless, these tasks waste too much resources. To mitigate Loss, some Pow logs may work in some A side application has been developed. For example, Primecoin [25] Search for possible special prime chains Used for mathematical research.

Proof of Stake- Pos is a more energy-efficient version of Pow. In a Proof of Stake (Pos) system, miners must demonstrate that they possess the currency in question. People with more currencies are thought to be less likely to assault the network. Because the single richest person is certain to be prominent in the network, the selection based on account balance is

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 7.047 ⁜ Vol. 10, Issue 4, April 2022
DOI: 10.17148/IJIREEICE.2022.10437

highly unjust. As a result, a variety of solutions are presented using a mix of stake size to determine which block to forge next. Blackcoin, in instance, employs randomness to forecast the next generation. . It employs a formula that considers the lowest hash value as well as the stake size. Peercoin [23] prefers to select coins depending on their age. Older and larger groups of coins have a higher chance of mining the next block in Peercoin. Pos saves more energy and is more efficient than Pow. Unfortunately, because the cost of mining is so low, attacks may occur as a result. Many blockchains start with Pow and then transition to Pos over time. Ethereum, for example, is planning to switch from Ethash (a type of Pow) [28] to Casper (a type of Pos) [29].

IV. CHALLENGES & RECENT ADVANCES

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges and recent advances as follows

Scalability

The blockchain is becoming increasingly hefty as the number of transactions increases. Because they must check if the source of the current transaction is unspent or not, each node must record all transactions in order to validate them on the blockchain. Furthermore, the Bitcoin blockchain can only process about 7 transactions per second due to the original block size restriction and the time interval required to construct a new block, which is insufficient to meet the need of processing millions of transactions in real-time. Meanwhile, because block space is limited, many minor transactions may be delayed because miners prefer transactions with a high transaction fee.

There have been several proposals to overcome the scalability problem of blockchain, which can be divided into two categories:

• Blockchain storage optimization Because it is more difficult for a node to maintain a full copy of the ledger, Bruce proposed a revolutionary cryptocurrency system in which the network removes (or forgets) old transaction data [37].

The balance of all non-empty addresses is kept in a database called account tree. Aside from that, a lightweight client may be able to assist in the resolution of this issue. VerSum [38] is a new scheme that was presented to provide another means for lightweight clients to exist. VerSum enables lightweight clients to offload expensive computations with big inputs to the cloud. By comparing results from multiple servers, it assures that the computation result is correct.

Privacy Leakage

Through the use of public and private keys, blockchain may maintain a certain level of privacy. Users transact with their private and public keys without revealing their true identities. However, [40], [5] indicate that blockchain cannot guarantee transactional privacy because all transaction and balance values for each public key are publicly viewable. Furthermore, according to a recent study [41], a user's Bitcoin transactions can be connected to reveal personal information. Furthermore, Biryukov et al. [12] presented a method for linking user pseudonyms to IP addresses even when they are protected by NAT or firewalls. In [12], each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain.

Mining

Blockchain is vulnerable to cooperating selfish miners' attacks. Eyal and Sirer [12], in particular, demonstrated that the network is vulnerable even if only a small amount of the hashing power is cheated. Selfish miners hold their mined blocks without broadcasting in a selfish mining technique, and the private branch is only exposed to the public if certain conditions are met. All miners would accept the private branch because it is longer than the current public chain. Prior to the public release of the private blockchain, honest miners are squandering their energy on a pointless branch, while greedy miners are mining their private chain without competition. As a result, selfish miners tend to make more money.

V . POSSIBLE FUTURE DIRECTION

In both industry and academics, blockchain has proven its worth. We examine four potential future directions: blockchain testing, reversing the trend toward centralization, big data analytics, and blockchain application.

Blockchain Testing

Various types of blockchains have recently appeared, and there are currently over 18000 cryptocurrencies listed in [54]. However, some developers may lie about their blockchain performance in order to entice investors who are looking for a quick return. Furthermore, when consumers wish to incorporate blockchain into their businesses, they must first determine which blockchain best meets their needs. As a result, a blockchain testing process must be in place to test several blockchains.

DOI: 10.17148/IJIREEICE.2022.10437

Testing on the blockchain can be divided into two phases: standardisation and testing. All criteria must be created and agreed upon during the standardisation phase. When a blockchain is created, it can be evaluated against pre-determined criteria to see if it meets the developers' claims. In terms of the testing phase, various criteria must be used to blockchain testing. For example, if a user in charge of an online retail firm is concerned about the blockchain's throughput, the study should look at the average time it takes for a user to transmit a transaction to the transaction being packed into the blockchain, the capacity of a blockchain block, and so on.

Stop tendency to centralization

Blockchain is a distributed ledger technology. However, there is a tendency in which the mining pool's miners are centralised.

The top 5 mining pools currently control more than 51% of the total hash power in the Bitcoin network [55]. Apart from that, the selfish mining technique [12] demonstrated that pools with more than 25% of total processing power might earn more than their fair share of money. The selfish pool would attract rational miners, and the pool could easily approach 51 percent of the total power. Because the blockchain is not designed to service a small number of enterprises, some solutions to this problem should be presented.

Big data analytics

Big data and blockchain could work nicely together. We divided the combination into two categories: data management and data analytics. In terms of data management, because blockchain is distributed and safe, it might be utilised to store sensitive information. Additionally, blockchain might confirm that the data is authentic. If blockchain is used to store patient health information, for example, the data cannot be tampered with and it is difficult to steal confidential information. Transactions on blockchain could be utilised for large data analytics when it comes to data analytics. User trading patterns, for example, might be retrieved. With the analysis, users may predict the trading behaviour of possible partners.

The majority of blockchains are being used in the financial sector, but more and more applications for various industries are arising.

Traditional industries could investigate blockchain and incorporate it into their domains to improve their systems. User reputations, for example, might be stored on blockchain. At the same time, blockchain could help the up-and-coming industry boost performance. For example, Arcade City [53], a ridesharing business, uses blockchain technology to create an open marketplace where riders may connect directly with drivers.

A smart contract is a computerised transaction mechanism for carrying out a contract's terms [54]. It has been discussed for a long time, and now it may be executed using blockchain technology. A smart contract is a code fragment in the blockchain that may be automatically executed by miners. Smart contracts have the potential to revolutionise a variety of industries, including financial services and the Internet of Things.

V. CONCLUSION

With its main qualities of decentralisation, persistency, anonymity, and auditability, blockchain has proved its potential to revolutionise traditional industries. We offer a complete review of blockchain in this paper. We begin by providing an overview of blockchain technologies, including their architecture and fundamental attributes. The typical consensus algorithms utilised in blockchain are then discussed. We looked at and compared these techniques in a variety of ways.

We also compiled a list of hurdles and issues that could stymie blockchain growth, as well as a summary of some existing solutions. There are also some suggestions for future directions. Blockchain-based apps are gaining popularity these days, and we intend to do in-depth research on them in the future.

REFERENCES

[1] Market capitalization 2022Available https://coinmarketcap.com

[2]Zheng, Zibin; Xie, Shaoan; Dai, Hongning; Chen, Xiangping; Wang, Huaimin (2017). [IEEE 2017 IEEE International Congress on Big Data (BigData Congress) - Honolulu, HI, USA (2017.6.25-2017.6.30)] 2017 IEEE International Congress on Big Data (BigData Congress) - An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. , (), 557–564.

[3] "State of blockchain q1 2016: Blockchain funding overtakesbitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/

[4] S.Nakamoto,"Bitcoin:A peer-to-peer electronic cash system,"2008.[Online].Available:https://bitcoin.org/bitcoin.pdf

[5] 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.2646618563

[6] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"2015.

DOI: 10.17148/IJIREEICE.2022.10437

[7] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk:blockchain model of cryptography and privacy-preserving smartcontracts," in Proceedings of IEEE Symposium on Security and Privacy(SP), San Jose, CA, USA, 2016, pp. 839–858.

[8] 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

[9] Y. Zhang and J. Wen, "An iot electric business model based on theprotocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015,pp. 184–191.

[10] 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 (EC-TEL2015), Lyon, France, 2015, pp. 490–496.

[11] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.

[12] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on FinancialCryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.

[13] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisationof clients in bitcoin p2p network," in Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, NewYork, NY, USA, 2014, pp. 15–29.

[14] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[15] NRI, "Survey on blockchain technologies and related services," Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[16] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed.Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[17] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.

[18] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digitalsignature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[19] V.Buterin, "On public and private blockchains,"2015. [Online].Available:https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[20] "Hyperledger project," 2015. [Online]. Available: https://www.hyperledger.org/

[21] "Consortium chain development." [Online]. Available: https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development

[22] 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.

[23] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," Self-Published Paper, August, vol. 19, 2012.

[24] "Bitshares - your share in the decentralized exchange." [Online]. Available: https://bitshares.org/

[25] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[26] J. Kwon, "Tendermint: Consensus without mining," URLhttp://tendermint. com/docs/tendermint { } v04. pdf, 2014.

[27] S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," July 7th, 2013.

[28] P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[29] G. Wood, "Ethereum: A secure decentralised generalised transactionledger," Ethereum Project Yellow Paper, 2014.

[30] V. Zamfir, "Introducing casper the friendly ghost," Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casperfriendly-ghost, 2015.

[31] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design andImplementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[32] D. Mazieres, "The stellar consensus protocol: A federated model forinternet-level consensus," Stellar Development Foundation, 2015.

[33] "Antshares digital assets for everyone," 2016. [Online]. Available:https://www.antshares.org

[34] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work ´vs. bft replication," in International Workshop on Open Problems inNetwork Security, Zurich, Switzerland, 2015, pp. 112–125.

[35] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN). Singapore, Singapore:ACM, 2016, p. 13.

[36] D. Kraft, "Difficulty control for blockchain-based consensus systems,"Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[37] Y. Sompolinsky and A. Zohar, "Accelerating bitcoin's transaction processing. fast money grows on trees, not chains." IACR Cryptology ePrintArchive, vol. 2013, no. 881, 2013.

DOI: 10.17148/IJIREEICE.2022.10437

[38] A. Chepurnoy, M. Larangeira, and A. Ojiganov, "A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability," arXiv preprint arXiv:1603.07926, 2016.
[39] J. Bruce, "The mini-blockchain scheme," July 2014. [Online]. Available:http://cryptonite.info/files/mbc-scheme-rev3.pdf
[40] J. van den Hooff, M. F. Kaashoek, and N. Zeldovich, "Versum: Verifiablecomputations over large public logs," in Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, NewYork, NY, USA, 2014, pp. 1304–1316.
[41] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoinng: A scalable blockchain protocol," in Proceedings of 13th USENIXSymposium on Networked Systems Design and Implementation (NSDI16), Santa Clara, CA, USA, 2016, pp. 45–59.
[42] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M.Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conferenceon Internet Measurement Conference (IMC'13), New York, NY, USA,2013.
[43] J. Barcelo, "User privacy in the public bitcoin blockchain," 2014.
[44] M. Moser, "Anonymity of bitcoin transactions: An analysis of mixing ¨services," in Proceedings of Munster Bitcoin Conference ¨ , Munster, ¨Germany, 2013, pp. 17–18.
[45] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W.Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," inProceedings of International Conference on Financial Cryptography andData Security, Berlin, Heidelberg, 2014, pp. 486–504.
[46] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in Post onBitcoin Forum, 2013.
[47] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practicaldecentralized coin mixing for bitcoin," in Proceedings of EuropeanSymposium on Research in Computer Security, Cham, 2014, pp. 345–364.
[48] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymousdistributed e-cash from bitcoin," in Proceedings of IEEE SymposiumSecurity and Privacy (SP), Berkeley, CA, USA, 2013, pp. 397–411.
[49] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, andM. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in Proceedings of 2014 IEEE Symposium on Security and Privacy (SP),San Jose, CA, USA, 2014, pp. 459–474.
[50] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in Proceedingsof 2016 IEEE European Symposium on Security and Privacy (EuroS&P),Saarbrucken, Germany, 2016, pp. 305–320.
[51] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," arXiv preprint arXiv:1507.06183, 2015.
[52] S. Billah, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner," 2015.
[53] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088
[54] "Crypto-currency market capitalizations," 2022. [Online]. Available:https://www.investopedia.com ›
[55] "The biggest mining pools." [Online]. Available: https://bitcoinworldwide.com/mining/pools/
[56] N. Szabo, "The idea of smart contracts," 1997.