V.D. Ambeth Kumar et al. (Eds.)

doi:10.3233/APC210031

A Comprehensive Survey on Privacy-Security and Scalability Solutions for Block Chain Technology

Puneeth R P [a,1] and Parthasarathy G [b]
[a] *Department of Computer Science and Engineering, N.M.A.M Institute of Technology (Visvesvaraya Technological University, Belagavi), Karnataka, India*
[a]*Research Scholar, School of C&IT, REVA University, Karnataka, India*
[b]*Associate Professor, Dept of CSE, REVA University, Karnataka, India*

Abstract: Blockchain has various merits such as decentralization, greater transparency and improved traceability. Nowadays blockchain is used at various numbers of applications such as financial related services, business & industry, integrity verification, governance, health and education sectors. Even though the blockchain technology has promising approaches for the building the future of internet systems and also extensive research is going on about the technical challenges. In this paper we presented the comprehensive survey on blockchain and the techniques that can be used to address the scalability issues with respect to storage and also different privacy preserving techniques that can be incorporated during the implementation of blockchain application.

Keywords: Blockchain, Cryptography, Distributed Ledger Technologies, Security, Privacy, Scalability

1. Introduction

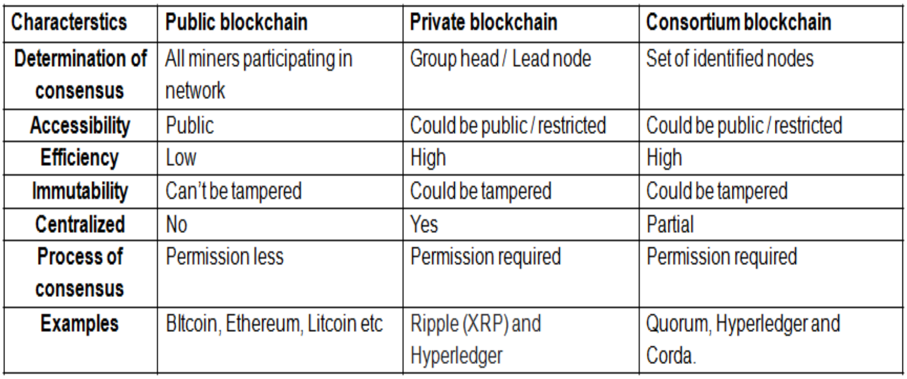
Blockchain technology is predicted to account 10% of Global Gross Domestic Product (GDP) by 2025 as per the information from World Economic Forum (WEF). Around top 10 promising global IT market research organization will include and continue with blockchain technology reported from United Nations Future Report by the year 2025. Blockchains are generally focuses on financial services but it is gradually expanding to various services as well [3]. Inadequate attention has been dedicated to issues related to the scalability & privacy preserving techniques. However, security attacks, scalability, and privacy concerns could cause a great trouble against the global IoT network [7]. A main functionality of the blockchain is to serve as a distributed system and perform transactions securely. Certain important capabilities are supported by blockchain technology firstly the hash chained storage, next is the use of digital signatures and the suitable consensus technique to add a new block to the

[1]Puneeth R P, Dept of CSE, N.M.A.M Institute of Technology, Karnataka, India.
Email: puneeth.rp@nitte.edu.in [1]

existing chain. Mainly digital signatures, merkel hash and hash chain are some of the main features that enhance the security of a blockchain.

2. Key Characteristics of blockchain

Decentralization, Security, Accountability, Anonymity and Persistency are the core characteristics of blockchain technology. The Blockchain architecture is distributed in nature. Each node (only miners) within a network has authority to approve, to maintain and to updates the new block entries in to a distributed ledger. The system is usually controlled by everyone within the blockchain network and it is varied based on the type of architecture [1]. Fig.1 provides the comparison between different types of blockchain architecture. It also helps to identify the type of architecture required for the application based on its features.



Characterstics	Public blockchain	Private blockchain	Consortium blockchain
Determination of consensus	All miners participating in network	Group head / Lead node	Set of identified nodes
Accessibility	Public	Could be public / restricted	Could be public / restricted
Efficiency	Low	High	High
Immutability	Can't be tampered	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Process of consensus	Permission less	Permission required	Permission required
Examples	BItcoin, Ethereum, Litcoin etc	Ripple (XRP) and Hyperledger	Quorum, Hyperledger and Corda.

Figure 1. Comparison between various types of blockchain architecture

3. Consensus algorithms

During the process of creation of a new block in a blockchain network, initially the new block is broadcasted to all the nodes of a network, and then each node has the choice whether to consider or to ignore it. So the consensus mechanism is used to take a decision to avoid fraudulent attempts or malicious attacks. The consensus process can be achieved by broadcasting of message between nodes and majority of the nodes has to approve the received message based on the consensus policy. The major consideration is to have a network that should be potential to avoid the degradation of services [1][7].

3.1 Approaches to consensus

Proof of Work (PoW): It's a consensus mechanism used in an application of Bitcoin network. Basically it requires high computational nodes for solving a challenging puzzle/hard mathematical problem to create a new block. This process is known as "mining", the participants involved in this mining process are called as "miners". The miner who manages to solve the problem will be rewarded and adds the block into the blockchain. The complexity of the mathematical problem and verify the correctness of solution are the two main features that contributed to wide popularity.

Proof of Stake (PoS): It's an energy saving technique alternate to PoW. The Participant nodes should own a cryptocurrency stake to become candidate for validating the new block and to earn a reward fee from it. To create and to validate new block the algorithm chooses the candidate from pool of candidates. During the selection process the algorithm combines the certain factors to make selection fair and to make sure everyone should get a turn.

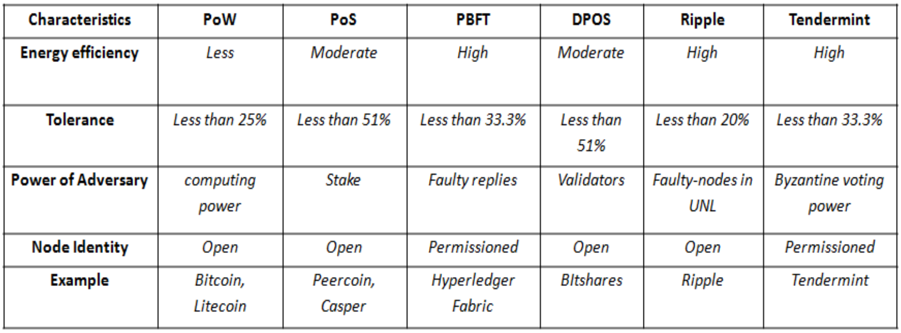
Practical Byzantine Fault Tolerance (PBFT): In PBFT the nodes are sorted in an order with one node acts as a leader (called a primary node) and other nodes referred as backup nodes (called secondary nodes). In case of any failure in the primary node then any one of secondary node can become the primary by transitioning from secondary to primary. PBFT algorithm can work effectively till the set of malicious nodes are not greater than or equal to $1/3^{rd}$ of total nodes in the blockchain system. As the participant node increases there is a less chances of being attacked and it leads to more secure network.

Delegated Proof of Stake (DPoS) which is an advanced form of PoS, priority based mining process is followed to generate new blocks based on their stake. To generate a new block and to perform the validation a representative is elected by the stake holders. This leads to fewer numbers of nodes to validate the block and transactions are completed early.

Ripple is another consensus algorithm that make uses of accumulatively trusted sub-networks within the group of networks. Especially during the process there will be two types of nodes, mainly the Client-node: used for transferring of only funds and server-node to take part in consensus process. Every ripple server-node has a unique node List(UNL), with the help of UNL ripple server ask every other node and determine whether to put the transaction in to the global /distributed ledger or not.

Tendermint is a consensus algorithm similar to PBFT, to become a validator the tendermint nodes have to lock their coins, if the validator is found to be fraudulent then it would be punished. The new block is identified in a round fashion, initially the proposer broadcast an unconfirmed block, based on the successful completion of pre-vote-step, pre-commit-step, and commit-step, new block is added to ledger.

In Fig 2. Summary of the different consensus algorithms based on certain characteristics is discussed [1].



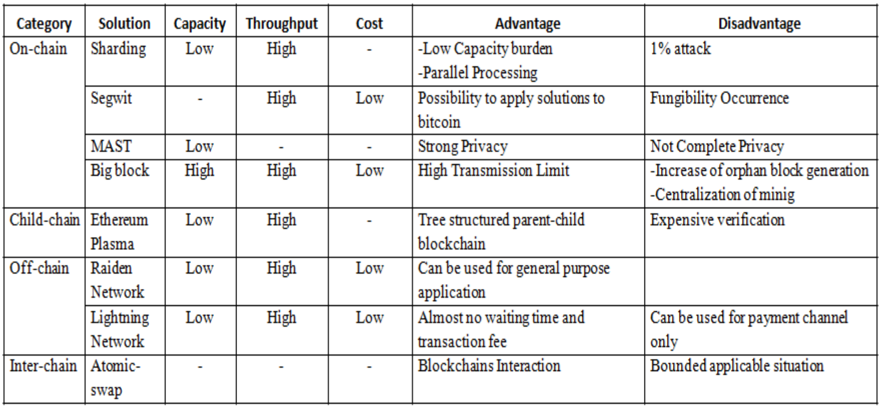
Characteristics	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Energy efficiency	Less	Moderate	High	Moderate	High	High
Tolerance	Less than 25%	Less than 51%	Less than 33.3%	Less than 51%	Less than 20%	Less than 33.3%
Power of Adversary	computing power	Stake	Faulty replies	Validators	Faulty-nodes in UNL	Byzantine voting power
Node Identity	Open	Open	Permissioned	Open	Open	Permissioned
Example	Bitcoin, Litecoin	Peercoin, Casper	Hyperledger Fabric	BItshares	Ripple	Tendermint

Figure 2. Comparison of different consensus algorithms

4. Scalability solutions on blockchain

The blockchain is distributed in nature and the immutability is one of the main features. Nowadays different applications are trying to implement using blockchain technology, but there are certain problems associated with that such as number of transactions processed per second, increased chain size, block size issues, electronic signatures size etc. Solving these problems certainly increases the performance of the blockchain, thus scalability issue is one of the most important issue in the blockchain technology.

Various approaches can be followed to solve the scalability problem in blockchain technology. Firstly, On-chain solution for scalability by increasing the block size of transactions in main-chain, in this technique the propagation speed decreases and it is one of its main disadvantages. Next is Off-chain solution: in this approach the processing of transactions happens at outside of the main chain and result is added to main-chain. Side-chain enables a way to exchanging of different blockchain assets with each other, The issue concerned about this approach is all about how to hand independent cryptocurrencies because the value of each crptocurrencies changes day by day. Child-Chain solution follows parent-child format structure, Processing of the transaction happens at the child chain and the processed information is recorded in the parent-chain. Inter-chain solution enables the communication to happen between one or more blockchain, basically it is similar to side-chain approach. We can say inter-chain technique acts as an infrastructure technology for implementing the side-chain. Finally the Chain-splitter is a solution for storage optimization. In this method main blockchain is stored in the cloud environment and the most recently accessed blocks are stored in the overlay network [4]. The scalability of the blockchain problems are classified into mainly three categories such as Cost involved, storage capacity and throughput.[9] In the Fig 3, we tried to list out the possible solution that can be used during the implementation. [2][3]

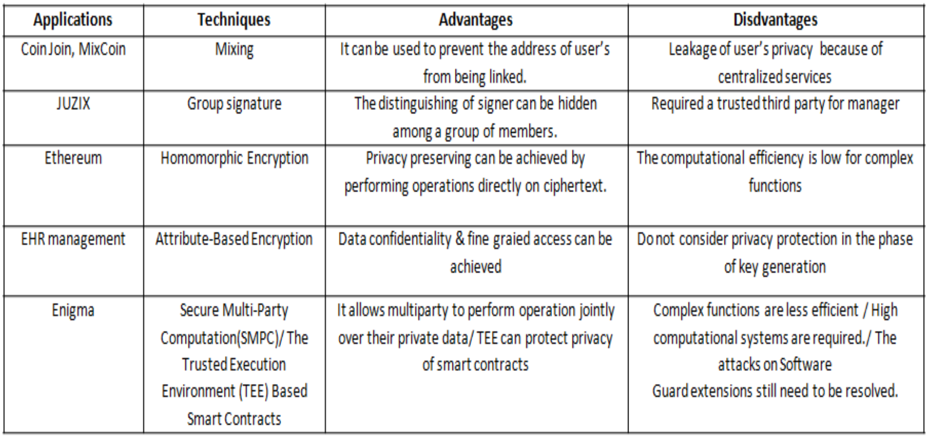


Category	Solution	Capacity	Throughput	Cost	Advantage	Disadvantage
On-chain	Sharding	Low	High	-	-Low Capacity burden -Parallel Processing	1% attack
	Segwit	-	High	Low	Possibility to apply solutions to bitcoin	Fungibility Occurrence
	MAST	Low	-	-	Strong Privacy	Not Complete Privacy
	Big block	High	High	Low	High Transmission Limit	-Increase of orphan block generation -Centralization of minig
Child-chain	Ethereum Plasma	Low	High	-	Tree structured parent-child blockchain	Expensive verification
Off-chain	Raiden Network	Low	High	Low	Can be used for general purpose application	
	Lightning Network	Low	High	Low	Almost no waiting time and transaction fee	Can be used for payment channel only
Inter-chain	Atomic-swap	-	-	-	Blockchains Interaction	Bounded applicable situation

Figure 3. Comparative analysis of scalability issues

5. Security and privacy techniques for blockchain technology

This section provides the summery of different approaches that can be incorporated to improve the security-privacy issues of current system and also for upcoming blockchain systems. Multiple privacy and security properties are required to meet the challenges faced in the complex blockchain system. We would like to highlight three points (i) there is no technology that is perfect in all aspects or that has no defects, whenever we incorporate a new technology to the existing system / complex system, it always bring about new attacks or other problems. (ii) Always there is a compromise between privacy-security techniques and its efficiency. (iii) There is no single technology solution for security and privacy. Many a time's use of multiple technologies can work better than the use of single technology and also incorporate the security-privacy technology that suits to the required application with acceptable performance. [3][8][6].



Applications	Techniques	Advantages	Disdvantages
Coin Join, MixCoin	Mixing	It can be used to prevent the address of user's from being linked.	Leakage of user's privacy because of centralized services
JUZIX	Group signature	The distinguishing of signer can be hidden among a group of members.	Required a trusted third party for manager
Ethereum	Homomorphic Encryption	Privacy preserving can be achieved by performing operations directly on ciphertext.	The computational efficiency is low for complex functions
EHR management	Attribute-Based Encryption	Data confidentiality & fine graied access can be achieved	Do not consider privacy protection in the phase of key generation
Enigma	Secure Multi-Party Computation(SMPC)/ The Trusted Execution Environment (TEE) Based Smart Contracts	It allows multiparty to perform operation jointly over their private data/ TEE can protect privacy of smart contracts	Complex functions are less efficient / High computational systems are required./ The attacks on Software Guard extensions still need to be resolved.

Figure 4. summary of privacy and security techniques

6. Conclusion

The blockchain can be applied to various fields and it has promising solutions for transforming existing industry with its main characteristics. In this paper initially we presented key characteristics of blockchain followed by consensus algorithms. Then we described the different scalability solutions and security-privacy techniques for achieving the better efficiency in blockchain technology. In future we try to explore the feasibility of using different alternate techniques related to security-privacy and scalability methods for the observation of system behavior. Performance evaluation based on certain parameters is also one of the key research areas in blockchain.

References

[1] Zibin Zheng,shaoan Xie,Hong-Ning Dai, Blockchain Challenges and Opportunities: a Survey, International Journal of Web and Grid Services, *Vol. 14, No. 4, 2018.*

[2] Soohyeong Kim, Yongseok Kwon,Sunghyun Cho, A Survey of Scalability Solutions on Blockchain , ICTC 2018, IEEE Xplore.

[3] RuiZhang and RUI Xue, Security and Privacy on Blockchain , arXiv:1903.07602v2,16 Aug 2019.

[4] Qiheng Zhou , Huawei Huang , (Member, Ieee), Zibin Zheng ,And Jing Bian ,Solutions to Scalability of Blockchain: A Survey, Volume 8,IEEE Access, 2020

[5] Merlinda Andonia,, Valentin Robua, David Flynna, Simone Abramb, Dale Geachc, David Jenkinsd, Peter McCallumd, Andrew Peacockd, Blockchain technology in the energy sector: A systematic review of challenges and opportunities , Elsevier, Renewable and Sustainable Energy Reviews 2019.

[6] Amin Fadaeddini, Babak Majidi, Mohammad Eshghi, Secure decentralized peer-to-peer training of deep neural networks based on distributed ledger technology, The Journal of Supercomputing, Springer-2020.

[7] RUI ZHANG And RUI XUE, Security and Privacy on Blockchain . Association for Computing Machinery,2019 .

[8] Xiaoyan Yan, Qilin Wu, and Youming Sun .A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing, Wireless Communications and Mobile Computing Volume 2020, Article Id 8832341, WILEY-2020.

[9] Ambeth Kumar.V.D (2017).Efficient Routing for Low Rate Wireless Network a Novel Approach. International Journal of Image Mining, Vol. 2, Nos. 3/4, 2017, 2017

[10] B. Aravindh; V.D.Ambeth Kumar; G. Harish; V. Siddartth, " A novel graphical authentication system for secure banking systems", IEEE (ICSTM), Pages: 177 – 183, 2-4 Aug. 2017, DOI: 10.1109/ICSTM.2017.8089147

[11] R. Subha Shini et.al., " Recurrent Neural Network based Text Summarization Techniques by Word Sequence Generation",IEEE International Conference on Inventive Computation Technologies (ICICT), 2021, DOI: 10.1109/ICICT50816.2021.9358764

[12] K. Nanagasabapathy; G. Harish; O. I. Allen Sebastian; N. Sowrabh Chandra; V. D. Ambeth Kumar," Validation system using smartphone luminescence", IEEE International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Pages: 235 – 239, 2017. DOI: 10.1109/ICICICT1.2017.8342566