International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ELSEVIER SSRN

COPY RIGHT

IJIEMR Transactions, online available on 17 Oct 2020.

Link :

https://papers.ssrn.com/sol3/JELJOUR_Results.cfm?form_name=journalbrowse&journal_id=3206923&dgcid=EngRN-PIP-IJIEMR_email_netann

Title:- BLOCKCHAIN PROLIFERATION IN THIS DIGITAL EPOCH.

Volume 09, Issue 10, Pages: 20 - 28.

Paper Authors

[1]B.V.SATISH BABU, [2]DR.K.SURESH BABU.

Associate Professor of CSE, School of IT, JNUTH

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Blockchain Proliferation in this Digital Epoch

[1]B.V.Satish Babu, [2]Dr.K.Suresh Babu

[1]Research scholar, JNTUH, vsatish.phd@gmail.com
[2]*Associate Professor of CSE, School of IT, JNUTH, kare_suresh@yahoo.co.in*

Abstract:
In this digital epoch, the block chain is the correct choice to solve many digital societal problems. Block chain proliferations are just not constricted to digital currencies like bitcoin. Different attributes like immutability, decentralized, no need for third parties, and automatic access policy realization using smart contracts, etc. made block chain as a quintessential framework to solve manifold problems in our society. In this paper, we made a look over on block chain proliferation in different applications and finally we analyze to understand it's suitability in this digital epoch

Index Terms – ***block chain, distributed, ledger, paradigms, attacks, Merkle tree, hashing, time stamping, ledger***

1. Introduction

The name "Blockchain" was coined by "S.Harber and W.scott" in the journal of cryptology, 1991.[1]. In 1993 Dave Bayer et al. [2] adjoined the concept called "Merkle Trees". The data structure "Merkle tree used to maintain the hashes of multiple transactions in the blockchain. In 2008, Blockchain as substratum, "Satoshi Nakamoto" introduced the concept of the cryptocurrency called "Bitcoin".

In 2009, the block chain was implemented as the communal version 1.0. [4]. In 2015, the concept of smart contracts incorporated in the 2nd colossal cryptocurrency called "Ethereum" as block chain version 2.0. From that point, blockchain is not just constricted to the cryptocurrency realm.

Different characteristics like immutable, decentralized, no need of third parties, and automatic access policy realization using smart contracts, etc. made block chain as a quintessential framework to solve manifold problems in our society.

There are many complications like scalability, interoperability, privacy, adoption, etc. that are involved in both the communal version of 1.0 and 2.0. To overcome also all these issues many innovations and researches are conducted,

and the result is Blockchain 3.0. The concept of Blockchain 3.0 has made many enterprises adopt the blockchain as a foundation for their decentralized software and applications.

II Related Work

In this paper, after referring to 187 journals, we have identified almost 88 different applications as part of the block chain 3.0. Our main focal point is to identify the proliferation of block chain so that we can plainly understand its applicability and challenges.

We have organized our paper in the following way. Section III contains information about blockchain and its attributes. In Section IV, is about understanding block chain proliferation and application analysis. Section V and Section VI are dedicated to various attacks on the blockchain and implementation challenges in the blockchain. Section VII is the conclusion of this paper.

III Blockchain and its attributes

The block chain is a decentralized peer-to-peer network that maintains the same copy of the distributed ledger in all participating peer systems. “Ledger” is a table of transactions generated by participants in the block chain network. A block is created by combining a set of transactions that are happened on a particular scale of time.

Inside the block, for every transaction hash value is calculated using the SHA-256 algorithm. These hash values of all the transactions in a block are reduced to a single root hash using the data structure “Merkle tree”. This single hash value will be placed in “block header” and used as a link between two blocks in the blockchain [5]. Likewise, all blocks in the block chain are linked together. Any modification in the previous block breaks links between all the blocks in block chain from that block

The first block in the block chain is called “Genesis block”. A new block is generated by a special peer called “Miner”. Generally, miner systems are equipped with huge computing power. The block chain network contains several miners along with ordinary peer participants. To generate a block, miners will compete with each other to solve the puzzle called Proof of Work (PoW). During this puzzle, the miner has to calculate a special hash value called “Nonce”.

The “Nonce” hash value should start with a specified number of zeros as mentioned in PoW. Generating nonce requires a huge amount of computing power. The Miner who generates the nonce is going create the block and distribute that block to all the peers in the block chain network. All peers agreed to consensus accept that block. A newly created block will be linked to the existing block chain by every peer. Finally, miners will be rewarded for the new block generation.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Peers inside the block chain organized in the form of groups called "Organizations". The entire block chain arrangement depicted in Figure .1 and Figure .2 represent individual block inner structures

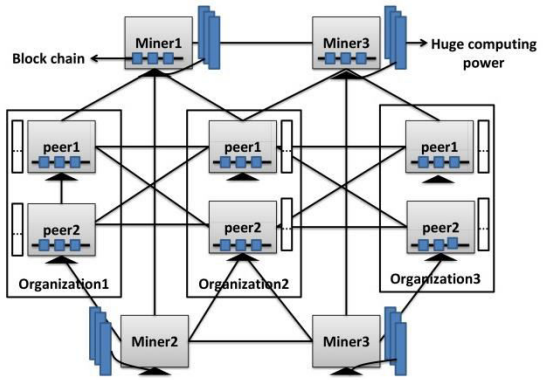

Figure.1 Block chain and its attributes

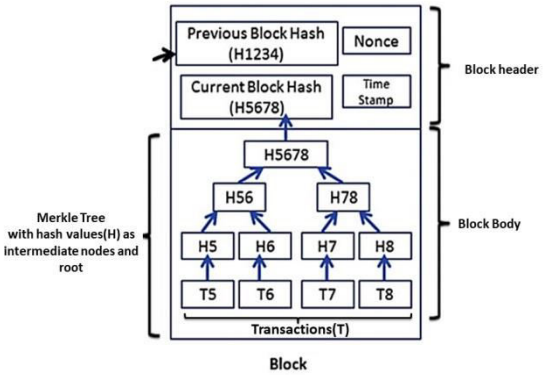

Figure.2 Individual block inner structure

We have four different types of block chains

a) Public domain: Completely decentralized, and anyone can participate without permission. Peer transaction is visible to all participants without disclosing peer identity. It has the following cons:

- Transaction confirmation and block formation takes more time
- Consensus protocols are generally computationally intensive

b) Private domain: It is a permission-based blockchain and limited to one particular enterprise. Verifies the transactions immediately when compared to the public domain.

- Not truly decentralized
- Due to fewer numbers of nodes, security is unpredictable

c) Consortium (or) Federated: It is a cross-organizational block chain established in between multiple organizations.

- Less transparent
- Need lots of regulations

d) Hybrid: It is the combination of public, private, and federated blockchain with greater control.

- Less transparent
- Contribution to the block chain network does not support incentives

IV Blockchain Proliferation and Analysis

After referring to 187 journals, we have identified almost 88 different applications that take advantage of the blockchain in a variety of domains. Table.1 represents the application domain type and name of these applications.

Table.1: Domains and corresponding applications

Application domain	Block chain based application name
Data Security Applications	1. User Authentication. [6] 2. Data Steganography. [7] 3. User Privacy. [8] 4. User Identity. [9] 5. Access Control Policies. [10] 6. Identifying breaches using Log System [11]

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

	7. Anonymous File sharing. [12] 8. Malware Containment. [13] 9. Secure Data Auditing. [14] 10. Intrusion detection. [15]
Data Management Applications	11. Data sharing with others. [16] 12. Data exchanging between two parties. [17] 13. Representing big data along with distributed databases like Apache Cassandra and IPFS. [18] 14. Supporting Database Management System. [19] 15. Data archive system. [20] 16. Data Analysis. [21] 17. Data Integrity. [22] 18. Trust Management by consensus. [23] 19. Integration to Distributed databases. [24] 20.Document time stamping without the possibility of changing the time stamp to
Applications on Computing paradigms	21. Cloud Applications. [26] 22. Edge Computing. [27] 23. Fog Computing. [28] 24. IoT / VoIT / Ubiquitous computing. [29] 25. Big data Computing. [30] 26. Grid Computing. [31] 27. Mobile Computing. [32] 28. Quantum Computing. [33]
Community-based Applications	29. Disaster Management. [34] 30.Education-Online Quiz. [35] 31. Education-Credit Management. [36] 32. Education Certificate verification. [37] 33. Health care Management. [38] 34. Medical field. [39] 35. Pharmaceuticals. [40] 36. Railways. [41] 37. Smart cities. [42] 38. Smart grids. [43] 39. Water Control System. [44] 40. Agriculture supply chain. [45] 41. E-waste Management. [46] 42. Volunteer service time record system. [47] 43. Social Welfare Maximization. [48] 44. Electricity Trading. [49]
	45. Solar Power Management. [50] 46. Electric Vehicle Charging Station. [51]
Industry based Applications	47. E-Commerce. [52] 48. Automation. [53] 49. Package Delivery System. [54] 50. Human Resource Management. [55] 51. Online Advertising. [56] 52. Customer services. [57] 53. Trust management between multiple organizations. [58] 54. Product reviews. [59] 55. Rideshare services. [60] 56. Product supply chain. [61] 57. Measurement of integrity in logistics. [62]
Financial Firms	58. Insurance systems. [63] 59. Crypto trading. [64] 60. Payment systems. [65] 61. Incentive distribution. [66] 62. Trust Management. [67] 63. Cryptocurrency. [68] 64. Fraud prevention. [69] 65. Leftover currency exchange. [70] 66. Inter-bank application. [71]
Government based Applications	67. Government data auditing. [72] 68. Voting based applications. [73] 69. Crowdsensing systems. [74] 70. Defence Applications. [75] 71. Criminal Records. [76] 72. Government services. [77] 73. Auction based applications. [78] 74. Legal Metrology. [79] 75. Bidding systems. [80] 76. Procurement based applications. [81] 77. Land record management. [82] 78. National ID management. [83]
Multimedia Applications	79. Multimedia Privacy. [84] 80. Protecting Intellectual property rights. [85] 81. Ownership Management. [86] 82. OTT Services. [87] 83. Identifying the source of

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

	news. [88] 84. Catalogue CCTV video evidence. [89]
Other domains	85. Virtualization (VM Migration) . [90] 86. Artificial Intelligence. [91] 87. Machine Learning. [92] 88. Image and Video Processing. [93]

As you can see in Table .1, it conspicuous that the proliferation of blockchain technology in a variety of domains. Based on the above table, the overall analysis represented using the doughnut chart Figure .1

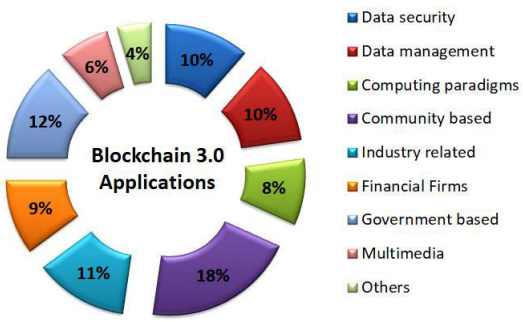

Figure .3 Mapping of application percentage and domain

According to the analysis, almost 18% of block chain applications are community-based applications. It manifests importance of the block chain and its adaptability in solving societal problems.

V Attacks on the block chain

Apart from its immutable and completely decentralized nature, the block chain is still prone to different attacks. In this section, we will try to list out some of these attacks [94].

Eclipse attacks: In eclipse attacks, the attacker will manage the victim to connect malicious nodes controlled by the attacker. From that instant victim is influenced, and all inbound and outbound connections are blocked for the victim.

Sybil attacks: It is similar to an eclipse attack, but it targets the entire network of nodes. In this attack, the attacker introduces several malicious nodes with a fictitious identity to take control of the network during the consensus process.

Selfish Mining: In the block chain, the rule is to accept the longest chain i.e. more blocks. In this attack self-seeking miner is going to secretly maintain the longest chain parallel to the current chain.

51% attack: In this type of attack, a particular miner is going to control other miners and their computing power that leads to a monopoly on the block chain network. This attack leads to a double-spending attack.

Race attack: This attack is also another type of double-spending attack. Here the trader is going to accept client payment before the validation and confirmation from the block chain

Brute Force attack: This attack is applied to the wallet address to find out the secret keys.

Distributed denial of service (DDoS): In this attack, the attacker is going to adjourn the peer node from receiving services by sending innumerable requests.

Quantum Attacks: These attacks are realized with help of special computers called quantum computers. As quantum computer represents data in the form of 0, 1, and qubit (0,1) at the same time. It takes less amount of time to break cryptographic primitives of block chain [95].

Most of these attacks are already addressed by so many researchers. But still, there is space to improve security aspects of the blockchain.

VI Challenges in implementation

Despite different attacks, the block chain has several implementation challenges when it is applied in a variety of domains and platforms. In this section, we are going to list out some of these challenges.

1. There is a need for quantum-resistant cryptographic primitives for the block chain.
2. Block chain transactions are confirmed slowly.
3. There is a need for sophisticated querying features on the block chain data.
4. There is a need for a light-weight consensus protocols
5. A different type of frameworks with a variety of blockchain implementations leads to reduce/ compromise interoperability.
6. There is a need for parallel algorithms to audit block chain data
7. A block chain is not suitable to support a large number of requests from many IoT devices. It is not suitable for time-critical IoT applications.
8. Pow (Proof of Work) of the block chain is not suitable for resource-constrained Edge devices.
9. Difficult to protect privacy-related confidential information in block chain network because the chain data is available to everyone.
10. It is still uncertain about handling complex data using a block chain.
11. As the blockchain network grows, we need to face big data challenges at any pint of time peers may run out of storage.
12. It is still uncertain the impact of different types of block chain on different computing paradigms.

VII Future work and Conclusion

After listing out 88 different applications of the block chain, we have identified one common thing in the way they were implemented. All these applications are implemented in any one of the following computing paradigms

- Cloud computing
- Edge computing
- Fog computing

- Osmotic computing
- Big data computing
- Ubiquitous computing
- Quantum Computing

Many people adopt a block chain for its immutability nature, even though it is not suitable for a few applications. As future work, we want to survey to discover the appropriateness of block chain in different computing paradigms and we want to address above-mentioned challenges of the block chain.

In this paper, we have explained the proliferation of block chain in this digital era by listing out 88 different applications. In the next decade, the block chain is going to be revolutionary in many digital fields. The block chain itself has few design problems and implementation challenges. When combined with other technologies we can overcome those design problems and challenges easily.

VIII References

1]. Stuart Haber & W. Scott; "How to time-stamp a digital document", Journal of Cryptology", vol-3, pp. 99–111, 1991

[2]. Dave Bayer; "Improving the Efficiency and Reliability of Digital Time-Stamping", Springer link, pp 329-330, 1993

[3]. Satoshi Nakamoto; "Bitcoin: A Peer-to-Peer Electronic Cash System", pp. 1-9, 2008

[4]. A.Cornel-Cristian, M.Arhip-Calin, Al.Zamfirescu; "Cloud Storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Block chain technology", UPEC, 2019

[5]. B. V. Satish Babu, K. Suresh Babu; "Materializing Block Chain Technology to Maintain Digital Ledger of Land Records" , vol 1090,pp 201-212, 2018

[6].BlockCAM: A Block chain -Based Cross-Domain Authentication Model, IEEE transactions.

[7].AI Basuki, D.Rosiyadi; "Joint Transaction-Image Steganography for High Capacity Covert Communication", ICCIA, pp. 41-46, 2019

[8].VH.Hoang, E.Lehtihet, YG.Doudane; "Privacy-Preserving Block chain-Based Data Sharing Platform for Decentralized Storage Systems", IFIP, 2020

[9].G.Malik et al; "Blockchain Based Identity Verification Model", ViTECoN , 2019

[10]. S. Wang, Xu Wang, Y.Zhang; "A Secure Cloud Storage Framework with Access Control Based on Block chain",2019

[11]. H.Wang, Desheng Yang, Nian Duan,Yang Guo, Lu Zhang; " Medusa: Block chain Powered Log Storage System" , ICSESS,2018

[12]. S Pradhan et al; "Block chain based Security Framework for P2P File sharing system", ANTS, 2018

[13]. A.Malvankar, J.Payne; "Malware Containment in Cloud", IPS-ISA, 2019

[14]. H.Yu, Z Yang; "Decentralized Big Data Auditing for Smart City Environments Leveraging Block chain Technology", IEEE Access, pp 6288 – 6296, 2018

[15]. M.Kumar, Ashish Kumar; " Distributed Intrusion Detection System using Block chain and Cloud Computing Infrastructure", ICOEI, 2020

[16]. J.Liu, G.Zhang et al; "A Block chain-based Conditional Privacy-Preserving Traffic Data Sharing in Cloud", ICC, 2020

[17]. J.Chen et al; "Bootstrapping a Block chain Based Ecosystem for Big Data Exchange.", Bigdata congress, 2017

[18]. Deepak Puthal et al; "Proof-of-Authentication for Scalable Block chain in Resource-Constrained Distributed Systems", ICCE,2019

[19].Wang et al; "Research and Analysis on the Distributed Database of Block chain and Non- Block chain", ICCBDA 2020

[20].Wen-xing Lin et al; "A double-block chains based Digital Archives Management Framework and Implementation", ISADS, 2020

[21]. Matthew Dixon et al; "Blockchain Data Analytics", IEEE IS, 2018

[22]. Pratima Sharma et al; "Block chain-based Integrity Protection System for Cloud Storage", TIMES-iCON, 2020

[23]. Marcello Cinque et al; "Trust Management in Fog/Edge Computing by Means of Block chain Technologies", SmartData, 2019

[24]. Eranga Bandara et al; "Mystiko- Block chain Meets Big Data"; IEEE International Conference on Big Data, 2018

[25]. Yuan Zhang et al; "Chronos++: An Accurate Block chain-Based Time-Stamping Scheme for Cloud Storage", pp. 216 – 229, IEEE Transactions on Services Computing, 2019

[26]. MHR Tseng et al; "Using Block chain to Access Cloud Services: A Case of Financial Service Application", FedCSIS, 2019

[27].B. Varghese et al; Realizing Edge Marketplaces: Challenges and Opportunities, Vol 5, Issue 6, pp. 9-20, 2018

[28] Kai Lei; "Groupchain: Towards a Scalable Public Block chain in Fog Computing of IoT Services Computing.", IEEE Transactions on Services Computing, 2020

[29].H Seike et al;" Block chain-Based Ubiquitous Code Ownership Management System without Hierarchical Structure", 2018

[30].CA Alexander et al; "Cybersecurity, Information Assurance, and Big Data Based on Block chain", 2019

[31].G Seriţan et al; "Assessment for Efficient Operation of Smart Grids Using Advanced Technologies", 2018

[32].MD. Abdur Rahman et al; "Block chain-based Mobile Edge Computing Framework for Secure Therapy Applications", 2018

[33].JD Preece et al "Towards Encrypting Industrial Data on Public Distributed Networks", 2018

[34].Mehmet Demir et al; "Utility Blockchain for Transparent Disaster Recovery", 2019

[35].H Shen et al; "Research on Online Quiz Scheme Based on Double-Layer Consortium Blockchain", 2018

[36].M Turkanović et al; "EduCTX: A Blockchain-Based Higher Education Credit Platform", 2018

[37].R Arenas et al ; "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials", 2018

[38].SP Novikov et al; Blockchain and Smart Contracts in a Decentralized Health Infrastructure, 2018

[39]. T Dey et al; "HealthSense: A medical use case of Internet of Things and blockchain", 2017

[40].T Bocek et al; "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain", 2017

[42].F Naser et al; "Review : The Potential Use Of Blockchain Technology In Railway Applications : An Introduction Of A Mobility And Speech Recognition Prototype", 2018

[43]. Assessment for Efficient Operation of Smart Grids Using Advanced Technologies

[44].G Seriţan et al; "A Blockchain-based Water Control System for the Automatic Management of Irrigation Communities", 2018

[45].S Thejaswini et al; "Blockchain in Agriculture by using Decentralized Peer to Peer Networks", 2020