Review on Effectivity of Consensus Algorithms

Ashish Dhillon[1], Dr.Khushboo Tripathi[2], Neha Bhateja[3]
[2, 3]Assistant Professor
[1, 2, 3]Amity University, Haryana.

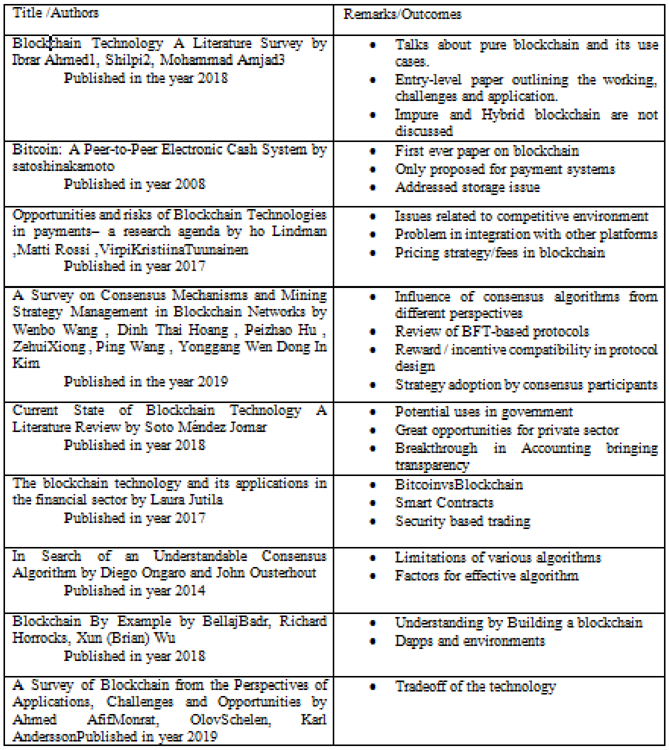
Abstract- *The past decade has witnessed the rapid evolution in blockchain technologies, which has attracted tremendous interests from both the research communities and industries. The blockchain network was originated from the Internet financial sector as a decentralized, immutable ledger system for transactional data ordering. Nowadays, it is envisioned as a powerful backbone/framework for decentralized data processing and data-driven self-organization in flat, open-access networks. This survey is motivated by the lack of a comprehensive literature review on the development of decentralized consensus mechanisms in blockchain networks. In this survey, we provide a systematic vision of the organization of blockchain networks. By emphasizing the unique characteristics of incentivized consensus in blockchain networks, our in-depth review of the state-of-the-art consensus protocols is focused on both the perspective of distributed consensus system design and the perspective of incentive mechanism design. From a game-theoretic point of view, we also provide a thorough review of the strategy adopted for self-organization by the individual nodes in the blockchain backbone networks. Consequently, we provide a comprehensive survey on the emerging applications of the blockchain networks in a wide range of areas. We highlight our special interest in how the consensus mechanisms impact these applications. Finally, we discuss several open issues in the protocol design for blockchain consensus and the related potential research directions.*

Keywords- Blockchain, Decentralization, incentive, Consensus

I. INTRODUCTION

The blockchain technology is the technology that powers the bitcoin cryptocurrency and other crypto coins but the blockchain is bigger than the Bitcoin. Evolved from the Merkle Tree, Blockchain Technology is a fully decentralized digital register which keeps a secure history of data exchanges .All of the major resources say that technology has groundbreaking nature, having potential in multiples areas government and the private sector .The accounting potential still looks unresolved but accounting firms have an interest in the technology. The technology can reduce costs in multiple areas of the private sector and government, increase transparency and security thanks to an advanced security mechanism. There are technical challenges still to resolve. The law lag must be minimized to keep up with the technology and its implementations. Generally, the term “blockchain networks” can be interpreted from two levels, namely, the “blockchains” which refer to a framework of immutable data organization, and the “blockchain networks” on top of which the approaches of data deployment and maintenance are defined. The two aspects Authentication and immutability, are considered as the major innovation of blockchain technologies. blockchains are able to provide the proofs of authentication for asset (i.e., token) transfer and then the proofs of asset ownerships using several consensus mechanisms and use off-the-shelf cryptographic techniques and hashing to provide immutability. Furthermore, a blockchain maintains an arbitrary order of the transactional records by cryptographically chaining the record subsets in the form of data “blocks” to their chronic predecessors. With the help of cryptographic references, any attempt of data tampering can be immediately detected.

II. LITERATURE REVIEW



Title /Authors	Remarks/Outcomes
Blockchain Technology A Literature Survey by Ibrar Ahmed1, Shilpi2, Mohammad Amjad3 Published in the year 2018	• Talks about pure blockchain and its use cases. • Entry-level paper outlining the working, challenges and application. • Impure and Hybrid blockchain are not discussed
Bitcoin: A Peer-to-Peer Electronic Cash System by satoshinakamoto Published in year 2008	• First ever paper on blockchain • Only proposed for payment systems • Addressed storage issue
Opportunities and risks of Blockchain Technologies in payments– a research agenda by ho Lindman ,Matti Rossi ,VirpiKristiinaTuunainen Published in year 2017	• Issues related to competitive environment • Problem in integration with other platforms • Pricing strategy/fees in blockchain
A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks by Wenbo Wang , Dinh Thai Hoang , Peizhao Hu , ZehuiXiong , Ping Wang , Yonggang Wen Dong In Kim Published in the year 2019	• Influence of consensus algorithms from different perspectives • Review of BFT-based protocols • Reward / incentive compatibility in protocol design • Strategy adoption by consensus participants
Current State of Blockchain Technology A Literature Review by Soto Méndez Jomar Published in year 2018	• Potential uses in government • Great opportunities for private sector • Breakthrough in Accounting bringing transparency
The blockchain technology and its applications in the financial sector by Laura Jutila Published in year 2017	• BitcoinvsBlockchain • Smart Contracts • Security based trading
In Search of an Understandable Consensus Algorithm by Diego Ongaro and John Ousterhout Published in year 2014	• Limitations of various algorithms • Factors for effective algorithm
Blockchain By Example by BellajBadr, Richard Horrocks, Xun (Brian) Wu Published in year 2018	• Understanding by Building a blockchain • Dapps and environments
A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities by Ahmed AfifMonrat, OlovSchelen, Karl AnderssonPublished in year 2019	• Tradeoff of the technology

III. BLOCKCHAIN ARCHITECTURE

Blockchain consists of five main components where each of them plays a vital role in the working of the technology. First is the node, where each of the computer systems has its independent copy of the ledger. Then is the transaction that maintains a record of information exchange among the nodes. Then comes the block which contains a set of transaction that is recorded into a data structure called Ledger. Moving on to the next, the miner which is a node, whose function is to verify the transactions thoroughly before adding the information into the chain. Lastly, the consensus protocol consists set of rules that are arranged to carry out blockchain operations.

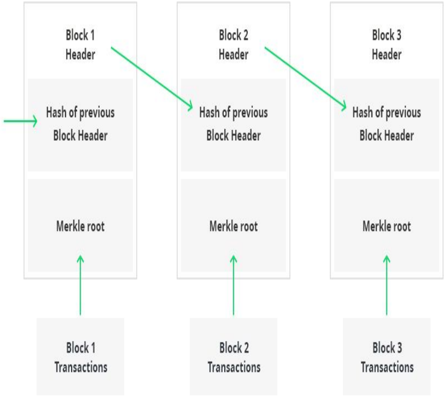
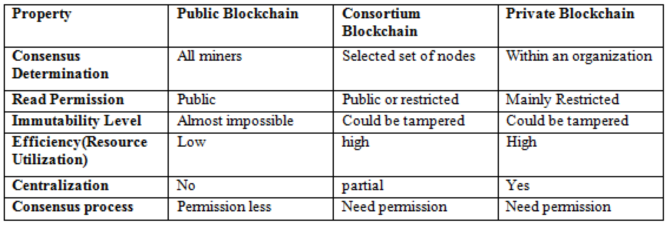


Fig. Blockchain Structure

The verified transactions are requested by the user to be added into the new block. Each block consists of block header, list of transactions, the hash of previous block, Merkle root, hash of current block &nonce. To create a new block, a miner has to solve a puzzle. To solve a puzzle, user has to find hash's value according to the difficulty level. When the requirement is met, new block is created and is added to the chain using hash of the previous block.

IV. TYPES OF BLOCKCHAIN SYSTEMS



Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus Determination	All miners	Selected set of nodes	Within an organization
Read Permission	Public	Public or restricted	Mainly Restricted
Immutability Level	Almost impossible	Could be tampered	Could be tampered
Efficiency(Resource Utilization)	Low	high	High
Centralization	No	partial	Yes
Consensus process	Permission less	Need permission	Need permission

Aspects of effective network

- **Understandability**

Any algorithm that has to be developed for a productive network needs to remain simple and transparent so that it gains the trust of the user and can be further enhanced when developed systematically.

For instance, the proof of work(PoW) needs 51% of nodes to verify a transaction before entering into the block. In this way it is ensured that the ledger remains identical among all the participants of the network.

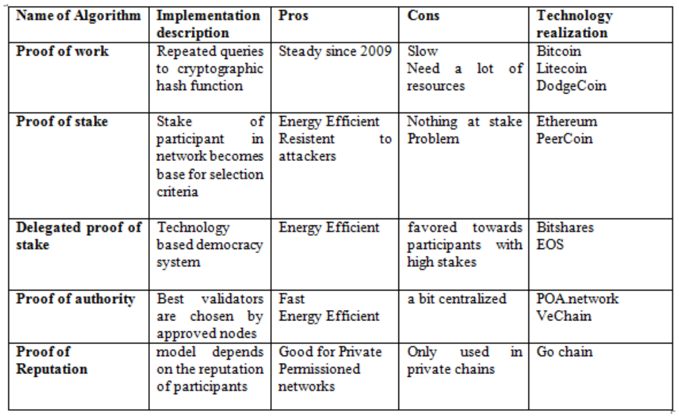
- **Correctness**

This characteristic feature of the algorithm ensures the authentication of the transaction. Referring to the Bitcoin network,authentication takes place by back tracing each coin to its originand also addresses the double spent problem in payment systems.

- **Efficiency**

Performance is measured on the basis of security, time taken per transaction and minimal amount of transaction fee. When compared to master card and visa, Bitcoin networks ensures the payment is sent directly to the address by avoiding third party vendors. The Bitcoin network also ensures the privacy by not taking any user's personal information. Bitcoin network can handle seven transactions per second till date when compared to visa's 65000 per second. Scaling solution are also available in bitcoin in form of use of lightning network which makes bitcoin payment system much superior to the conventional international payments and wire transfers. Moving on to the transaction fee, this network fee ranges from 0.5% to 5% of transaction which is minimal when compared to current payment system which charge 20% to 30% for each transaction.

V. COMPARISONS OF CONSENSUS ALGORITHMS



Name of Algorithm	Implementation description	Pros	Cons	Technology realization
Proof of work	Repeated queries to cryptographic hash function	Steady since 2009	Slow Need a lot of resources	Bitcoin Litecoin DodgeCoin
Proof of stake	Stake of participant in network becomes base for selection criteria	Energy Efficient Resistent to attackers	Nothing at stake Problem	Ethereum PeerCoin
Delegated proof of stake	Technology based democracy system	Energy Efficient	favored towards participants with high stakes	Bitshares EOS
Proof of authority	Best validators are chosen by approved nodes	Fast Energy Efficient	a bit centralized	POA.network VeChain
Proof of Reputation	model depends on the reputation of participants	Good for Private Permissioned networks	Only used in private chains	Go chain

VI. DISCUSSION &FUTURE SCOPES

Influence of distributed system protocols depends on the nature of their use case. Every algorithm has both pros and cons. Owning 51% resources in a network could be beneficial in a private block chain network as it can help in reverting few transactions which is a useful in some cases where as it is considered to be a problem in public block chains which is known as byzantine fault tolerance. Bitcoin network is not suitable for small payments as it is slow. There are lots of scopes in private block chain sector like carbon offsets monitoring, decentralized journalism. Blockchain technology can be used to provide a transparent record of documents like educational certificates and land registry.

VII. CONCLUSIONS

This paper provides a succinct overview of disturbed consensus protocols. The success of a protocol depends on the selection of the application. For instance, proof of work is good in preventing double spent problem whereas less resource consuming protocol will be better in case of Inter planetary file system(IPFS). This paper focuses on three main parameters, i.e. understandability, correctness & performance to measure the viability of the protocol. This information will be handy in developing application specific protocols for blockchain systems. Till now blockchain technology is preferred mostly in financial sectors. But this technology has a lot of scopes in other areas as discussed in future scopes. Booming of the technology depends on the contribution to the other areas of the society.

REFERENCES

[1] Ahmed, Ibrar, and Mohammad AmjadShilpi. "Blockchain Technology A Literature Survey." (2018)

[2] Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system.* Manubot, 2019.

[3] Lindman, Juho, VirpiKristiinaTuunainen, and Matti Rossi. "Opportunities and risks of Blockchain Technologies–a research agenda." (2017).

[4] Wang, Wenbo, Dinh Thai Hoang, Peizhao Hu, ZehuiXiong, DusitNiyato, Ping Wang, Yonggang Wen, and Dong In Kim. "A survey on consensus mechanisms and mining strategy management in blockchain networks." *IEEE Access* 7 (2019): 22328-22370.

[5] Jomar Soto Mendez, JomarCurrent State of Blockchain Technology A Literature Review (2018).

[6] Jutila, Laura. "The blockchain technology and its applications in the financial sector." (2017).

[7] Ongaro, Diego, and John Ousterhout. "In search of an understandable consensus algorithm." In *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)*, pp. 305-319. 2014.

[8] BellajBadr, Richard Horrocks, Xun (Brian) Wu BlockchainBy Example, 2019.

[9] Monrat, Ahmed Afif, OlovSchelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." *IEEE Access* 7 (2019): 117134-117151.

[10] Wahab, Abdul, and WaqasMehmood. "Survey of consensus protocols." *arXiv preprint arXiv:1810.03357* (2018).

[11] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998

[12] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999

[13] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[14] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[15] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[16] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[17] W. Feller, "An introduction to probability theory and its applications," 1957.

[18] https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[19] https://www.investopedia.com/articles/forex/042215/bitcoin-transactions-vs-credit-card-transactions.asp

[20] https://cointelegraph.com/news/research-bitcoin-can-beat-visa-mastercard-to-top-world-payment-system-in-10-years