International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072

Blockchain Technology A Literature Survey

Ibrar Ahmed[1], Shilpi[2], Mohammad Amjad[3]

[1,2]D/o Computer Engineering, Jamia Millia Islamia University, New Delhi, India
[3]Associate Professor, D/o Computer Engineering, Jamia Millia Islamia University, New Delhi, India

---

Abstract:- *Evolved from the Merkle Tree, Blockchain Technology is a fully decentralized digital register which keeps a secure history of data exchanges. The decentralization aspect of Blockchain Technology does away the need of any central authority for managing it. In this paper we present a comprehensive overview on blockchain technology. We first begin by shedding light on the fundamentals of Blockchain Technology then we analyse some typical algorithms used in various blockchains. Blockchain, the foundation of Bitcoin, has received extensive attention recently. Being an ineradicable data storing technology, Blockchain can be used not only in financial assets but anything which has some value. However, being a human invention, downsides are even here in the blockchain technology such as scalability issues, security problems, and not-so-user-friendly for non-technical people. Next, with common technical issues we have talked about the recent advances. We lastly conclude this paper by laying out possible future developments of blockchain technology.*

Key Words: Blockchain, Ledger, Bitcoin, Application

1. INTRODUCTION

Blockchain may well be viewed as a public ledger and each submitted dealings is place during a list of blocks. This chain develops as new blocks are mounted to that incessantly. With an awfully designed data storage structure, transactions in Bitcoin system might occur with no any third party and therefore the core innovation to construct Bitcoin is blockchain, that was initial planned in 2008 and dead in 2009 [1]. These days digital cash has become a stylish expression in each trade and profound world. In concert of the foremost eminent digital cash, Bitcoin has delighted an enormous success with its capital market achieving ten billion greenbacks in 2016 [2]. Asymmetric cryptography and distributed accord calculation are dead for consumer security and record consistency. The blockchain technology has key qualities of decentralization, persistence, anonymity and auditability. With these attributes, blockchain will considerably spare the price and enhance the productivity. As a matter of 1st importance blockchain is permanent. Dealings cannot be altered once it's stuffed into the blockchain. Organizations that need high responsibility and honesty will utilize blockchain to draw in purchasers. Moreover, blockchain is distributed and may avoid the only purpose of disappointment circumstance. Blockchain are often utilised in several money services as an example, advanced resources, settlement and on-line payment [3], [4]. Additionally, it may be applied into alternative fields as well as sensible contracts [5], public services [6], web of Things (IoT) [7], name systems [8] and security services [9]. Those fields favour blockchain in multiple ways in which. It's been proved that miners might come through larger revenue than their justifiable share through inconsiderate mining strategy [10]. Moreover, it's been shown that privacy escape might additionally happen in blockchain even users solely create transactions with their public key and personal key [11] Tschorsch et al. [12] created a technical survey regarding suburbanized digital currencies as well as Bitcoin. Nomura analysis Institute created a technical report regarding blockchain [13].

The rest of this paper is organized as follows. Section II introduces blockchain design. Section III shows typical agreement algorithms employed in blockchain. Section IV summarizes the technical challenges and therefore the recent advances during this space. Section V discusses some potential future directions and section VI concludes the paper.

2. BLOCKCHAIN ARCHITECTURE

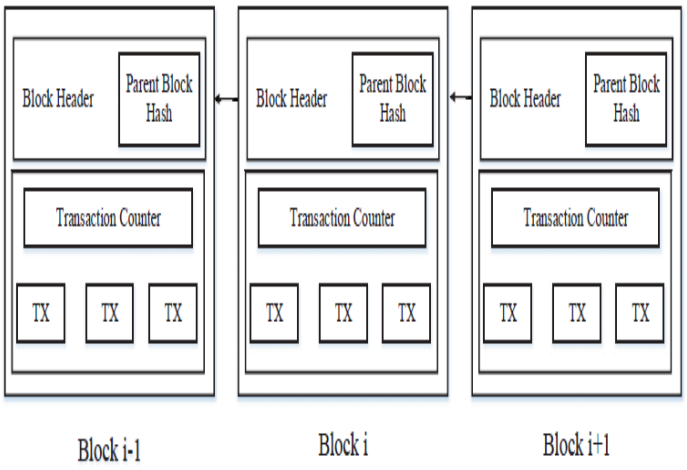

Figure – 1

Blockchain could be a sequence of blocks, that holds an entire list of dealing records like standard public ledger [14]. Figure one illustrates associate degree example of a blockchain.

With a previous block hash contained within the block header, a block has just one parent block. Its price noting that uncle blocks (children of the block's ancestors) hashes would even be hold on in ethereum blockchain [15]. The primary block of a blockchain is named genesis block that has no parent block. We tend to then justify the internals of blockchain in details.

2.1 Blocks

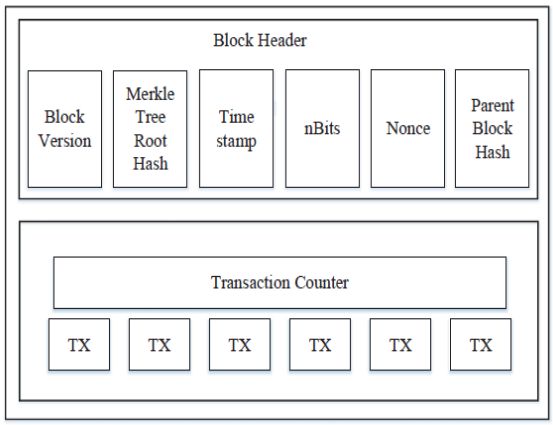

Figure – 2

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 that set of block validation rules to follow.

(ii) Merkle tree root hash: the hash worth of all the transactions within the block.

(iii) Timestamp: current time as seconds in Greenwich Mean Time since Jan one, 1970.

(iv) nBits: target threshold of a legitimate block hash.

(v) Nonce: associate degree 4-byte field, that sometimes starts with zero and will increase for each hash calculation (will be explained in detail in Section III).

(vi) Parent block hash: A 256-bit hash worth that points to the previous block.

2.2 Characteristics of Blockchain

In summary, blockchain has following key characteristics:

- ***Decentralization***. In standard centralized group action systems, every group action must be valid through the central trustworthy agency (e.g., the central bank), inevitably ensuing to the value and therefore the performance bottlenecks at the central servers. Distinction to the centralized mode, third party is not any longer required in blockchain. Accord algorithms in blockchain are accustomed maintain information consistency in distributed network.

- ***Persistency***. Transactions are often valid quickly and invalid transactions wouldn't be admitted by honest miners. It's nearly not possible to delete or rollback transactions once they're enclosed within the blockchain. Blocks that contain invalid transactions may well be discovered directly.

- ***Anonymity***. Every user will act with the blockchain with a generated address, that doesn't reveal the $64000 identity of the user. Note that blockchain cannot guarantee the proper privacy preservation thanks to the intrinsic constraint (details are going to be mentioned in section IV).

- ***Auditability***. Bitcoin blockchain stores knowledge regarding user balances supported the unexpended dealings Output (UTXO) model [2]: Any dealings must ask some previous unexpended transactions. Once this dealing is recorded into the blockchain, the state of these referred unexpended transactions switch from unexpended to spent. Therefore, transactions may well be simply verified and tracked.

3. CONSENSUS ALGORITHMS

Pow: (Proof of work) could be a accord strategy employed in the Bitcoin network [2]. In PoW, every node of the network is shrewd a hash worth of the block header. The block header contains a nowadays and miners would modification the nowadays often to induce completely different hash values. The accord needs that the calculated worth should be adequate to or smaller than a specific given worth.

PoS: (Proof of stake) is a vitality sparing option in contrast to PoW. Diggers in PoS need to demonstrate the responsibility for measure of money. Specifically, Blackcoin [16] utilizes randomization to anticipate the next generator. It utilizes an equation that searches for the most minimal hash an incentive in blend with the span of the stake. Numerous blockchains embrace PoW toward the start and change to PoS bit by bit.

PBFT: (Practical byzantine fault tolerance) is a replication calculation to endure byzantine issues [17]. Hyperledger Fabric [18] uses the PBFT as its accord calculation since PBFT could deal with up to 1/3 malignant byzantine reproductions.

DPOS: (Delegated proof of stake) is agent fair. Partners choose their agents to produce and approve squares. casted a ballot out effectively. DPOS is the foundation of Bitshares [19].

Ripple: Ripple [20] is an accord calculation that uses by and large confided in subnetworks inside the bigger system. In the system, hubs are separated into two kinds: server for taking an interest accord process and customer for just exchanging assets.

4. CHALLENGES

There is no doubt about the capability and capacity of Blockchain, yet it does suffer from some serious problems. The magnitude of transaction is magnifying with every passing day and so does the workload of blockchain. Excessive transactions make the system bulky. The size of blocks is also a issue while carrying bigger transaction. Being tiny in size, it can only contain a small amount of data at a

time. That results in delay in small transactions. Although the privacy is guaranteed in blockchain technology however to be precise, the keys of public and private transaction can only preserve a limited amount of privacy. While making the transaction, the anonymity of the users is maintained. However, it is shown in [21], [5] that blockchain cannot guarantee the *transactional privacy* since the values of all transactions and balances for each public key are publicly visible.

5. BLOCKCHAIN APPLICATIONS

The very first application and use of Blockchain was Bitcoin. In the current scenario, financial sphere has felt the presence of blockchain technology the most. Another application is "Smart Contracts". As the name suggests, a smart contract is an automated exchange protocol that executes the terms of an agreement [22]. The idea of making contracts and agreements smart was though of long back, now with the advent of blockchain technology, this can be realized. The reason of Finance being the largest user of blockchain is the transparency it provides to the parties of traders and businessmen while trading and making transaction. Transactions taking place in any entity be it Private or Public can be stored in the blocks and legitimacy of the same can be later verified. For doing away the corrupt and malafied practices and realizing the dream of corruption free nation can be realised by bringing Blockchain in the mainstream and widely using it in all the domains eg. Elections and Banking Sectors.

6. CONCLUSION

Blockchain is a revolutionary technology which has changed the way people interact with the Internet. In this cyber world, where nothing is private, and no data is safe, Blockchain has shown promising potentials of being the best bet of people dealing with the value-sensitive commodities. In this paper we have discussed about the basics of blockchain technology which can be used as a reference for people new in this field. We have also outlined its possible application and the challenges it faces. The aim of this paper is to provide a comprehensive readymade idea of the working of blockchain technology which can be used by students or whoever interested in getting familiar with this revolutionary technology.

REFERENCES

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

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

[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 applications 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 (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.

[9] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward 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, "Deanonymisation 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 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/0531 01f.pdf

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

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

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

[17] 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.

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

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

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

[21] 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 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013.

[22] N. Szabo, "The idea of smart contracts," 1997.

AUTHORS

Ibrar Ahmed is a student of M.Tech (Computer Engineering), Jamia Millia Islamia, University New Delhi, India.

Shilpi is a student of M.Tech (Computer Engineering), Jamia Millia Islamia, University New Delhi, India.

Mohammad Amjad is an Associate Professor in the Department of Computer Engineering, Jamia Millia Islamia University, New Delhi, India.