IJCSE International Journal of Computer Sciences and Engineering Open Access

Technical Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

A Primer on Blockchain Technology

Vikas Thada[1*], Utpal Shrivastava[2]

[1,2]Department of Computer Science & Engineering, Amity University Gurgaon

DOI: https://doi.org/10.26438/ijcse/v7i5.246250 | Available online at: www.ijcseonline.org

08/May/2019, Published: 31/May/2019

Abstract- Blockchain, the foundation technology behind Bitcoin, has gotten wide attention starting late. Blockchain fills in as an immutable record where trades happen in a decentralized manner Basically, a blockchain is a database incorporating a physical chain of blocks each of which is of fixed size that incorporate many transactions, where every transaction is added to another block is approved and after that embedded into the block.. Applications of blockchain are hopping up, covering different fields including financial organizations, reputation structure and Internet of Things (IoT), food industry, cyber security and many more. This paper is an introduction on blockchain innovation covering able issue for a tyro on blockchain advancement. The paper presents a layout of blockchain building directly off the bat alongside its different applications.

Keywords—Blockchain, block, bitcoin, consensus, decentralized,miner

I. Introduction

These days digital money has turned into a trendy expression in both industry and the scholarly community. As a standout amongst the best cryptographic money, Bitcoin has appreciated an enormous accomplishment with its capital market achieving 10 billion dollars in 2016 [1]. With an exceptionally planned information stockpiling structure, exchanges in Bitcoin system could occur without the need of any outsider[9,10]. Bitcoin is driven by blockchain technology, which was first proposed in 2008 and actualized in 2009 [2]. Blockchain could be viewed as an open record and every single submitted exchange are put away in a rundown of blocks. This chain develops as new blocks are appended to it seamlessly. Public key cryptography and distributed consensus algorithm have been actualized for client security and record consistency. The blockchain innovation for the most part has key attributes of decentralization, persistency, obscurity and auditability. With these qualities, blockchain can enormously spare the expense and improve the proficiency. Use of decentralized network and a timestamping server which is distributed , a public blockchain database is managed without any external control.

.The open blockchain is likewise a distributed program with one critical distinction: In addition to the fact that it moves documents (information) from distributed, it additionally guarantees that every one of the companions have the equivalent definite information. In the event that the information changes on one machine, it changes on all the . machines. There are rules determining precisely how a change can be made, and on the off chance that somebody doesn't tailly them and adjusts their duplicate unlawfully, they're ignored. At the end of the day, information is just composed, never erased that is records can only be added but never deleted. This is the manner by which it gets the name blockchain, in light of the fact that new information is included in batches or blocks, and attached to the current blocks, shaping a chain of blocks. In addition to the fact that everyone has a similar database (blockchain), yet everybody gets a storage inside the blockchain that no one but only they can have access to[4,5].

There is a great deal of writing on blockchain from different sources, for example, sites, wikis, discussion posts, codes, gathering procedures and diary articles. our paper centres around state of the art blockchain examines including ongoing advances and future patterns. The remainder of this paper is composed as pursues. Section II presents architecture of blockchain. Section III shows applications of blockchain and segment IV finishes up the paper.

II. Architecture of Blockchain

Blockchain architecture is a decentralized architecture. It is sequence of blocks having number of transaction records. The first block is known as genesis block. Each next block contains hash of previous block and is stored into the block header. Lets discuss various components of a blockchain.

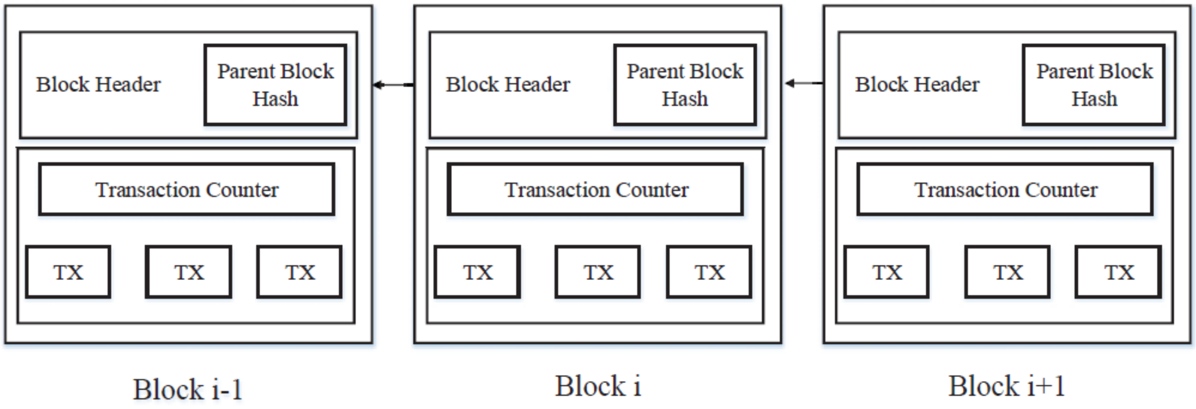

Fig. 1: An example of blockchain

2.1 Block

A block is made up of header and the body. Block header comprises metadata. This help in the verification of validity of the block. The metadata consist of following parts.

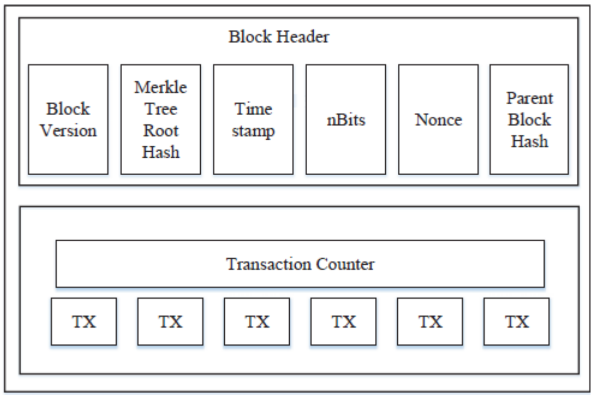

Fig 2: Components of a block in blockchain

(i) Block version: current block structure version.
(ii) Merkle tree root hash: the cryptographin sha256 hash value of all the transactions in the block.
(iii) Timestamp: time at which block was created
(iv) nBits: the mining difficulty
(v) Nonce: anrandom number which is used only once and is of 4byte
(vi) Parent block hash: a pointer to previous block(sha256 hash value)

transaction counter (number of transactions) and transactions are part of body of block.Remaining portion of the block contains transactions verified and validated by the miner.
Users transactions are created and submitted to the network and after validation they are included in a block. Blockchain utilizes public key cryptography system to approve the verification of transactions.[13]. To verify the identity of the owner/user concept of digital signature (hash encrypted by private key) is used in an untrustworthy environment of blockchain.

2.2 Other components [5]

- Node –it is computer having a copy of blockchain ledger
- Transaction - smallest building block or unit of work of a blockchain system
- Chain –ordered listing of blocks
- Miners - specific nodes responsible for creation of block, verifying them for cryptographically correct and later appending to the end of the blockchain.
- Consensus (consensus protocol) –used to achieve on an agreement for a data value.
- UTXO (Unspent Transaction Output):- It can be spent as input to the new transaction. For a payment to be valid, it must only use UTXOs as inputs.
- POW(Proof of Work)- Original consensus algorithm. With PoW, miners compete against each other to complete transactions on the network and get rewarded

III. Key Characteristics of Blockchain [1][5][8]

Major attributes/characteristics of blockchainare :

- Decentralization.:The entire distributed database is access ed by each member of the blockchain structure. Unlike th e central system, the consensus algorithm enables networ k control
- Persistency: Transactions are validated quick and miners would allow only valid transactions. Once they are included in the blockchain, it cannot be deleted or rollbacked.

- Anonymity:Every user can interact with a generated address with the blockchain which does not uncover the genuine personality of the client. Because of the intrinsic constraint, blockchain can not guarantee perfect privacy
- Auditability: The user balances in Bitcoin blockchain are stored in the form of Unspent Transaction Output (UTXO) model [2]: Transactions always point to some previous UTXO. The state of transaction changes to spent from unspent after it is validated and added as part of block in blockchain. It makes easy to verify and track the transactions.
- Immutability: No alteration or deletion of any records in a blockchain
- Transparency – Infeasible to corrupt the blockchain as each block in the whole system need to be overwritten which demand large computing power.
- Provenance –origin of every transaction can easily be tracked.

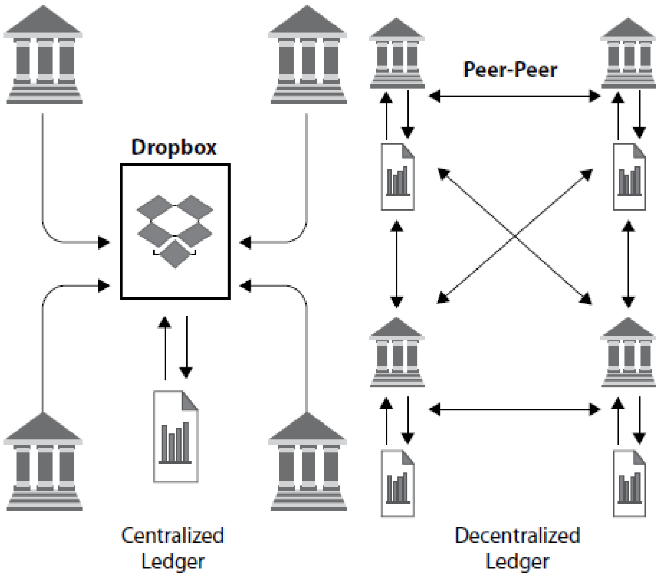

Fig 3: Centralized Vs Decentralized Store[8]

IV. How Blockchain Works

As can be seen from the figure 4 in step 1 a transaction is to be requested by some node. Step 2 creates a block consisting of that transaction. The block thus created and before adding as new block to the blockchain has to be verified and validated by miner nodes so it is send to every other node in the network. In step 4 miners validates the transactions and in turn gets some reward for the proof of the work (POW). After this the block gets added to the blockchain network.

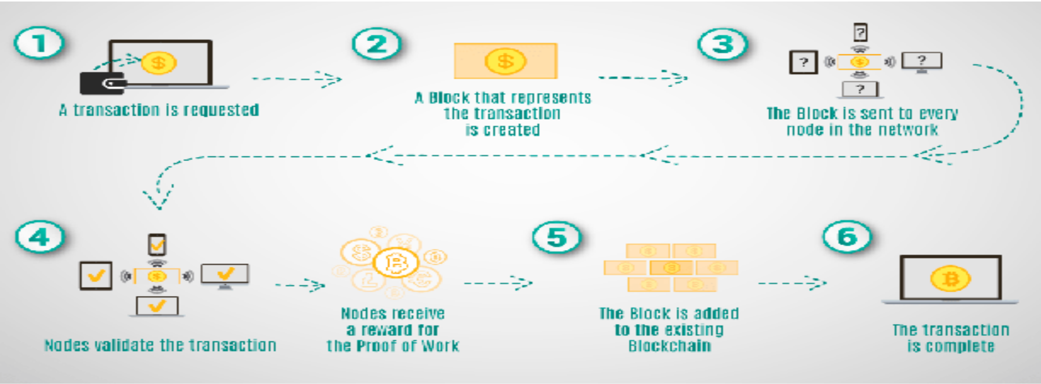
1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Fig 4 : How Blockchain Works[5]

V. TYPES OF BLOCKCHAINS.

There are mainly three types of blockchains:public, private and consortium [1,5,8]. In public blockchain, data and systems access (i.eall records are available to all who is interested in participating. Examples of public blockchain are Ethereum, Bitcoin etc. The private blockchain framework is controlled just by clients from a particular association or approved clients who have a welcome for investment.

A private blockchain is controlled by one organization thus it is centralized. The consortium blockchain developed by a few associations is mostly decentralized. The differences are shown in Table 1.

Table 1: Comparison of public/private/consortium blockchains[1,5,8]

Property	**Public blockchain**	**Consortium blockchain**	**Private blockchain**
Consensus determination	Through All miners	Specific nodes	Private to organization/company
Read permission	All	Public or few permissioned	Public or few permissioned
Immutability level	No tempering	Chances of tempering	Chances of tempering
Efficiency (use of resources)	Less	More	More
Centralization	No	Partial	Yes
Consensus process	No permission is required	Permission required	Permission required

Lets discuss some of the property in detail.

- Consensus determination. In public blockchain, consensus determination is done by each node where in private it is controlled by an organization and in consortium only few specific nodes become part of consensus determination.
- Immutability. This depends upon number of participants which are less in private and in consortium and many in public.
- Efficiency. Transaction propagation takes time in public as compare to other two.
- Centralized. Public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized.
- Consensus process. Every one participates in consensus in public blockchain and in other two only the nodes with permission from group or organization jointhe consensus process.

VI. BLOCKCHAIN APPLICATIONS

As of now most blockchains are utilized in the financial fields, an ever-increasing number of uses for various fields are showing up. Customary businesses could think about blockchain what's more, apply blockchain into their fields to upgrade their frameworks. For instance, client notorieties could be put away on blockchain. In the meantime, the exceptional business could utilize blockchain to improve execution. Other applications are in food industry(everything is transparent), cyber security (trustless system, decentralized and consensus, immutability features),voting blockchain applications, writing smart contract(executable code) and executing on nodes of party involved, land registry (immutability features).

VII. CONCLUSION

Blockchain has appeared potential for changing conventional industry with its key attributes: decentralization, persistency, obscurity and auditability. In this paper, we presented an extensive review on blockchain. We first gave an outline of blockchain innovations including blockchain engineering and key qualities of blockchain. We have talked about various terms identified with blockchain innovation. These days blockchain based applications are jumping up and we have covered them considerably in this paper. Inside and out investigation of agreement calculations and difficulties to blockchain innovation will remain a future work.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564. doi: 10.1109/BigDataCongress.2017.85

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

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

[4] 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

[5] https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture, accessed on 9th April 2019

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

[7] 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.

[8]"Blockchain **A Practical Guide to Developing Business, Law, and Technology Solutions",** Joseph J. Bambara et al. Ist edition, TataMcgraHill,2018

[9] 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 [10] 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.

[11] 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.

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

[13] 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.

[14]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.

[15] 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.

[16] 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