IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 8, August 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

Public Ledger: The Blockchain Technology

Manisha Bagri[1]

[1] Computer Science Department, Atma Ram Sanatan Dharma College, University Of Delhi, New Delhi, India

Abstract

A blockchain is a linked sequence of blocks. The blocks are connected in chronological order in the blockchain. They are distributed and decentralized in nature, .i.e. anyone over the network can access a block and there's no centralized authority is present. This paper gives a brief explanation of how it was used in cryptocurrency like Bitcoin. This paper also gives a clear understanding of blockchains' architecture, some of its key characteristics that it possesses and lists its benefits and limitations. The paper gives a concise clarification of different types of blockchains and their comparisons. Blockchains technology can also be implemented in other fields such as Internet of Things (IoT), Apartment Rentals/Real Estate, Financial services, Supply chain management, Healthcare, Internet of Things (IoT), Cloud computing etc
A technique is also proposed for online voting system to cast the votes in real time.

Keywords: Block, Blockchain, Hash, Decentralized, Distributed.

1. Introduction

The Blockchain is currently a buzzword in public ledger technology world. The reason of this interest is the Bitcoin system, the decentralized peer to peer cryptocurrency. Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 [1]. The technology used to build bitcoin is called blockchain.
As the success of Bitcoin has demonstrated, blockchain technology is useful for projects that require real-time collaboration between mutually-suspicious contributors over the Internet [10].
Blockchain is an open distributed ledger. It is simply a collection of blocks linked together as a chain. Each block keeps the record of the transactions which cannot be modified. This chain grows when a new block is appended to the end. Each block contains a cryptographic hash of the previous block except the first block, a transaction and a timestamp. The Blockchain has some key characteristics includes Security, Consensus, Immutability, Decentralization, Digital Data and Audibility.
Apart from financial transactions blockchain can be used in other fields such as smart contracts [5], public services [6], Internet of Things (IoT) [7], Reputation Systems [8] and Security Services [9].
The purpose of this paper is to purpose an idea to implement blockchain technology in voting system. This paper includes concise explanation of Blockchain, its types, architecture, key characteristics, merits, limitations and some possible future scope.

2. Blockchain: Categories, Architecture, Characteristics, Merits and Demerits

2.1 Architecture

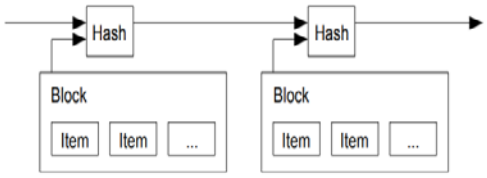

Fig. 1 Connection of Blocks in a Blockchain [3].

Blocks are connected in the system and hence the name Blockchain. Each block contains a hash of its own, a hash of the pervious block, timestamp and a transaction to which the blocks belongs (Fig. 1). Blocks in a blockchain are connected in chronological fashion. Blocks are decentralized and distributed over the blockchain network, so anybody on a network can see the content of blocks leading it to impossible to hack. Each block is cryptographically secured. As the blocks are connected together in a chain using the hash of the pervious block, any minute change in a block leads to a different hash and hence the block becomes invalid in the chain.

If an error is made by the legitimate user in the process of creating a block, he/she can't change the originally created block, even though they were rightful owner. The only way to rectify an error is to create a new block to the chain that contains the error information of the originally created block and is connected by using a hash of original block.

2.2 Categorization of Blockchain System

Blockchain systems are of three types:-

1. **Public Blockchains**

It is open source and not permissioned, means anyone with an internet connection can download a source code and read/write the blocks on their devices, hence participating in the verification process of transaction over the network as well as in the consensus process. To ensure security, this type of blockchain uses cryptography and consensus mechanisms such as proof of work (POW) and proof of stake (POS). Examples: Bitcoin and Ethereum.

2. **Private Blockchains**

It is permissioned and owned by an organization. Accesses of read/write of blocks are restricted by the company's network administrator. Consensus is achieved by the incharge hence; it makes the blockchain as distributed and not decentralized. It is still cryptographically secured as far as company's is concerned. Examples: Multichain, Blockstack.

3. **Consortium Blockchains**

It is permissioned but here number of companies owns the blockchain. Access of write into the block is given to a set of participants and read access may be made public or restricted to the participants only. Consensus process is also controlled by the pre selected nodes. It is partially decentralized. Example: R3 (Banks), EWF (Energy).

Comparisons among the three types of blockchains (Table 1)

Table 1: Comparisons among the three types of Blockchains

Basis	**Public**	**Private**	**Consortium**
Read permission	Public	Restricted	Public or Restricted
Decentralized	Yes	No	Partial
Owner	Open source	One organization	Selected set of companies
Consensus method	No permission	Permissioned	Permissioned

2.3 Key characteristics

Blockchain has become a revolution now and has some fancy characteristics:-

- ***Security*:** All the nodes share the copies of same information over a decentralized network. There is no chance of shutting down of the entire system. It is nearly impossible to hack the system since the blockchain network is secured by many computers on the network and these nodes/computers validate the transaction on this network.

- ***Consensus*:** A transaction can only be added if it is unanimously approved by all the parties on the network (node) [2]. Using consensus, all the nodes in a network are synchronized with each other.

- ***Immutability*:** Transactions once recorded can never be changed. If an error occurs a new transaction will be added. One cannot delete or rollback the already recorded transactions.

- ***Decentralization*:** Blockchain supports decentralized system. In decentralization, no third party is needed. The communication is based on peer to peer network in contrast to centralized system where, there is a single authority that does and manages all the work.

- ***Digital Data*:** Data are stored in digital format. Therefore no paper work will be needed.

- ***Audibility*:** Blocks in a blockchain are transparent in nature i.e. all the blocks in a blockchain are public. The authenticity of each transaction can be verified by any individual.

2.4 Blockchains: Merits

Below is list of some of important benefits of blockchain technology:-

- ***Distributed:*** There are number of computers that can take part in blockchain, making the blockchain distributed over a network. This property reduces the risk of cyber crime, tempering and fraud.

- ***Disintermediation:*** It eliminates the need of third party organization. In the third party system, even if it is a trusted one, if anyone somehow gains the access of the centralized system, he/she can easily corrupt the data. Blockchains on the other hand are decentralized and doesn't require any mediator.

- ***Transparency:*** It is an open source technology. That means any developer can modify the code and can use it for their specific application. Since everybody can see the data, manipulating logged data in a blockchain is difficult.

2.5 Blockchains: Demerits

Although blockchains are popular and it reduces the need of third party, it has some disadvantages too. Some of them are listed below:-

- ***Storage:*** The blocks in a blockchain are only in appended mode. Furthermore, every node in a decentralized system has a copy of actual database. With increasing transactions the size of this database will also increase. Therefore, every node in a network stores a large amount data, which leads to a problem of storage.

- ***Security:*** The 51% attack, which says, *If 51% of the nodes lie, the lie will become the truth.* [3]. If somehow more than half of the logged blocks get successfully changed in a blockchain, then the changed blocks may appear as a legitimate blocks to the nodes over the network.

- ***Redundancy:*** The total amount of computation required in blockchain is relatively higher than a centralized system. Processing of a transaction in a blockchain environment is done by each and every node connected over the network. Every node is doing the same thing to achieve the same end result, resulting in redundancy.

3. Proposed Method for Online Voting System

The blockchain technology can be used in voting system too like they were used in Bitcoin system. Following is the proposed algorithm for the same:-

1. Firstly, number of voters must be known in advance.

2. All the voters should have some form of identification to ensure the valid votes, so that only those will be considered in the final voting count that pass the test.

3. To ensure security of voters, separate blockchain will be designed using private blockchain technology that can be owned by an individual organization or a government.

4. Only those voters are eligible to vote whose identification is true.

5. Once the identification part is done, a voter will be entered in a network that implements the public blockchain technology and also hides the individuals' identity. So, that voter can cast his/her vote anonymously.

6. Now, in this network all the nodes can cast their vote and can also see the votes of others.

The casting of votes and counting is done in real time.
The blockchain for identification of valid voters can use a RSA cryptography algorithm. An RSA uses a pair of keys; a public key and a private key.
The blockchain for actual casting a vote can use an AES cryptography algorithm.

4. Conclusions

Blockchain technology is used in popular cryptocurrency named Bitcoin. The same technology can also be used in other fields like Healthcare, Apartment Rentals/Real Estate, Financial services, Supply chain management, Internet of Things (IoT), Cloud computing etc. Relating to this matter, in this paper we demonstrate that the same technology can be used to cast a vote, more precisely, an e-vote. A technique is proposed to illustrate the same.
The information on a blockchain is virtually unforgeable, and this is what makes it particularly suitable for information validation and storage. The fundamental element of blockchain is cryptography; in particular the hash functions which provide a unique fingerprint to any block of recorded information [4].

References

[1] State of blockchain Q1 2016: "Blockchain funding overtakes bitcoin", 2016.http://www.coindesk.com/state-of-blockchain-q1-2016/

[2] Deloitte, Convergence 2017. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf

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

[4] Nicola Dimitri, "The Blockchain Technology: some theory and applications", October 2017.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.

ISSN (Online) 2348 – 7968

www.ijiset.com

[6] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy", 2013.

[7] Y. Zhang, and J. Wen, "An iot electric business model based on the protocol of bitcoin", 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", 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] Morgen Peck, reviewers and advisors- William R. Tonti, Angelos Stavrou, Jason W. Rupe, Chunming Rong and Tim Kostyk, "Reinforcing The Links of the Blockchain", November 2017.