International Journal of Disaster Recovery and Business Continuity
Vol.11, No. 1, (2020), pp. 3002-3007

Blockchain Technology a new era: Architecture and its Core Components

Dr.Vidya Gavekar, Dr.Manisha Kumbhar, Prof.Aparna Kulkarni

Abstract

Blockchain technology has become very trendy and penetrated different domains, mostly due to the popularity of cryptocurrencies.Blockchain, the foundation of Bitcoin, has received wide attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture and compare some types of blockchain. Furthermore, core components of blockchain architecture and features briefly listed. We also lay out applications of block chain in differnt domain.

Keywords*: Architecture ,Blockchain, Bitcoin, cryptocurrencies ,decentralization, etc.*

1. INTRODUCTION

Blockchain is a digital, secure, public record book of transactions (a ledger). Block describes the way this ledger organizes transactions into blocks of data, which are then organized in a "chain" that links to other blocks of data. The links make it easy to see if anyone has changed any part of the chain, which helps the system protect against illegal transactions. It can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. It as a chain or records stored in the forms of blocks which are controlled by no single authority. A block chain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it.

A. Creation of trust through Block chain:

There are three key elements needed to establish trust: 1) identity, or who's who; 2) ownership, or who owns what; and 3) verification, or what's true. Blockchains allow users to easily prove their identities, protect ownership of digital assets, and verify transactions without a high-cost intermediary.[4]

- **Who's Who:** Blockchains solve the identity problem with theb help of digital signatures. Each user is given a set of two digital codes 1.private key – It is similar to an account number, and a Blockchains allow users to easily prove their identities, protect ownership of digital assets, and verify transactions without a high-cost intermediary. 2.public key-It is similar to a password that allows them to easily prove an identity and issue authorized transactions.
- **Who Owns What**: Blockchains solve the ownership problem through a technology called "cryptographic hashing." A cryptographic hash is simply a piece of data that has been run through a math function and transformed into a shorter piece of data. In a blockchain,each block contains a hashed representation of the data in the previous block. If you change any previous pieces of data, that change will get reflected throughout the chain, making it easy for the system to see and reject fraudulent attempts to manipulate the data. This allows blockchains to create "immutable" data, otherwise known as tamper-proof records.[9]
- **What's True**:Finally, blockchains solve the verification problem by making it feasible for a group of people to publicly verify that a transaction is true, without the need for a trusted intermediary. In blockchain terminology, this is called "distributed consensus." The ability for blockchains to verify transactions with fewer intermediaries is a key benefit that can lead to lower costs.

B. Backbround

ISSN: 2005-4289 IJDRBC

Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party

In order to understand blockchain better, consider an example where you are looking for an option to send some money to your friend who lives in a different location. A general option that you can normally use can be a bank or via a payment transfer application like PayPal or Paytm. This option involves third parties in order to process the transaction due to which an extra amount of your money is deducted as transferring fee. Moreover, in cases like these, you cannot ensure the security of your money as it is highly possible that a hacker might disrupt the network and steal your money. In both the cases, it is the customer who suffers. This is where Blockchain comes in.[9]

Instead of using a bank for transferring money, if we use a blockchain in such cases, the process becomes much easier and secure. There is no extra fee involved as the funds are directly processed by you thus, eliminating the need for a third party. Moreover, the blockchain database is decentralised and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized. Since the information is not stored in a single place, there's no chance of corruption of the information by any hacker.

C. Working of block chain:

A blockchain is a chain of blocks that contain data or information. Despite being discovered earlier, the first successful and popular application of the Blockchain technology came into being in the year 2009 by Satoshi Nakamoto. He created the first digital cryptocurrency called Bitcoin through the use of Blockchain technology. [1]

Each block in a blockchain network stores some information along with the hash of its previous block. A hash is a unique mathematical code which belongs to a specific block. If the information inside the block is modified, the hash of the block will be subject to modification too. The connection of blocks through unique hash keys is what makes blockchain secure.

While transactions take place on a blockchain, there are nodes on the network that validate these transactions. In Bitcoin blockchain, these nodes are called as miners and they use the concept of proof-of-work in order to process and validate transactions on the network. In order for a transaction to be valid, each block must refer to the hash of its preceding block. The transaction will take place only and only if the hash is correct. If a hacker tries to attack the network and change information of any specific block, the hash attached to the block will also get modified.

The breach will be detected as the modified hash will not match with the original one. This ensures that the blockchain is unalterable as if any change which is made to the chain of blocks will be reflected throughout the entire network and will be detected easily.[5]

In a nutshell, here's how blockchain allows transactions to take place:[10]

- A blockchain network makes use of public and private keys in order to form a digital signature ensuring security and consent.
- Once the authentication is ensured through these keys, the need for authorization arises.
- Blockchain allows participants of the network to perform mathematical verification and reach a consensus to agree on any particular value.
- While making a transfer, the sender uses their private key and announces the transaction information over the network. A block is created containing information such as digital signature, timestamp, and the receiver's public key.
- This block of information is broadcasted through the network and the validation process starts.
- Miners all over the network start solving the mathematical puzzle related to the transaction in order to process it. Solving this puzzle requires the miners to invest their computing power.
- Upon solving the puzzle first, the miner receives rewards in the form of bitcoins. Such kind of problems is referred to as proof-of-work mathematical problems.
- Once the majority of nodes in the network come to a consensus and agree to a common solution, the block is time stamped and added to the existing blockchain. This block can contain anything from money to data to messages.
- After the new block is added to the chain, the existing copies of blockchain are updated for

ISSN: 2005-4289 IJDRBC

all the nodes on the network.

2. BLOCKCHAIN ARCHITECTURE

A. Introduction:

The traditional architecture of the World Wide Web uses a client-server network. In this case, the server keeps all the required information in one place so that it is easy to update, due to the server being a centralized database controlled by a number of administrators with permissions.[6,8]

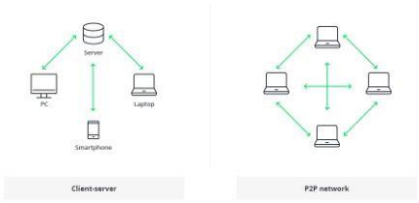

Fig. 1.Data base vs Blockchain Architecture

In the case of the distributed network of blockchain architecture, each participant within the network maintains, approves, and updates new entries. The system is controlled not only by separate individuals, but by everyone within the blockchain network. Each member ensures that all records and procedures are in order, which results in data validity and security. Thus, parties that do not necessarily trust each other are able to reach a common consensus.[3]

To summarize things, the blockchain is a decentralized, distributed ledger (public or private) of different kinds of transactions arranged into a P2P network. This network consists of many computers, but in a way that the data cannot be altered without the consensus of the whole network (each separate computer).

Blockchain architecture is being used very broadly in the financial industry. However, these days, this technology is employed not only for cryptocurrencies, but also for record keeping, digital notary, and smart contracts.

Features of Blockchain architecture :

- **Cost reduction** - lots of money is spent on sustaining centrally held databases (e.g. banks, governmental institutions) by keeping data current secure from cyber crimes and other corrupt intentions.
- **History of data** - within a blockchain structure, it is possible to check the history of any transaction at any moment in time. This is a ever-growing archive, while a centralized database is more of a snapshot of information at a specific point.
- **Data validity & security** - once entered, the data is hard to tamper with due to the blockchain's nature. It takes time to proceed with record validation, since the process occurs in each independent network rather than via compound processing power. This means that the system sacrifices performance speed, but instead guarantees high data security and validity.

B. Working of Core Components of Blockchain Architecture

These are the core blockchain architecture components:

- **Node** - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
- **Transaction** - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
- **Block** - a data structure used for keeping a set of transactions which is distributed to all nodes in the network
- **Chain** - a sequence of blocks in a specific order
- **Miners** - specific nodes which perform the block verification process before adding anything to the blockchain structure

ISSN: 2005-4289 IJDRBC

- **Consensus (consensus protocol)** - a set of rules and arrangements to carry out blockchain operations

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.
The following is a blockchain architecture diagram that shows how this actually works in the form of a digital wallet.

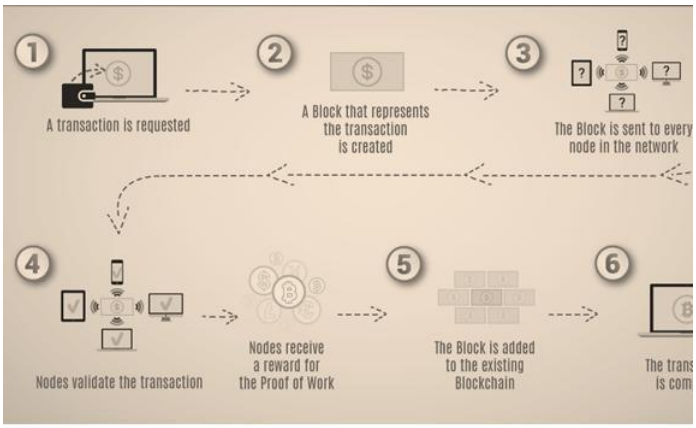

Fig: 2 .Working of Block chain architecture C.Characteristics of Blockchain Architecture

Blockchain architecture possesses a lot of benefits for businesses. Here are several embedded characteristics:[6]

- **Cryptography** - blockchain transactions are validated and trustworthy due to the complex computations and cryptographic proof among involved parties
- **Immutability** - any records made in a blockchain cannot be changed or deleted
- **Provenance** - refers to the fact that it is possible to track the origin of every transaction inside the blockchain ledger
- **Decentralization** - each member of the blockchain structure has access to the whole distributed database. As opposed to the central- based system, consensus algorithm allows for control of the network
- **Anonymity**- each blockchain network participant has a generated address, not user identity. This keeps users' anonymity, especially in a public blockchain structure
- **Transparency** - the blockchain system cannot be corrupted. This is very unlikely to happen, as it requires huge computing power to overwrite the blockchain network completely

C. APPLICATIONS OF BLOCK CHAIN TECHNOLOGY IN VARIOUS INDUSTRIES

Blockchain technology can be utilized in multiple industries including Financial Services, Healthcare, Government, Travel and Hospitality, Retail and CPG. Financial Services: In the financial services sector, Blockchain technology has already been implemented in many innovative ways. Blockchain technology simplifies and streamlines the entire process associated with asset management and payments by providing an automated trade lifecycle where all participants would have access to the exact same data about a transaction. This removes the need for brokers or intermediaries and ensures transparency and effective management of transactionaldata. [2,7]
Healthcare: Blockchain can play a key role in the healthcare sector by increasing the privacy, security and interoperability of the healthcare data. It holds the potential to address many interoperability challenges in the sector and enable secure sharing of healthcare data among the various entities and people involved in the process. It eliminates the interference of a third-party and also avoids the overhead costs. With Blockchains, the healthcare records can be stored in distributed data bases by encrypting it and implementing digital signatures to ensure privacy and authenticity.

ISSN: 2005-4289 IJDRBC

Government: Blockchain technology holds the power to transform Government's operations and services. It can play a key role in improving the data transactional challenges in the Government sector, which works in siloes currently. The proper linking and sharing of data with Blockchain enable better management of data between multiple departments. It improves the transparency and provides a better way to monitor and audit the transactions.

CPG and Retail: There is a huge opportunity for Blockchain technology to be applied in the retail sector . This includes everything from ensuring the authenticity of high value goods, preventing, fraudulent transactions, locating stolen items, enabling virtual warranties, managing loyalty points and streamlining supply chain operations.

Travel and Hospitality: The application of Blockchain can radically change the travel and hospitality industry . It can be applied in money transactions, storing important documents like passports/ other identification cards, reservations and managing travel insurance, loyalty and rewards.

4. CONCLUSION

The blockchain technology presents a decentralized network and is regarded as having great potential for use in various sectors. It has sensitive nature of data being processed and managed.Block chain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, and anonymity and audit ability. In this paper, we present a comprehensive overview on blockchain. We first give an overview of block chain technologies including overview on working of block chain and features along with the examples. We discussed detailed architecture and core components of block chain. The revolutionary technology of Blockchain holds a high potential of applications in many different industries and sectors. While some industries have already started adopting blockchain in their businesses, many are still exploring the best possible ways to start with.

REFERENCES:

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [3] G. W. Peters, E. Panayi, and A. Chapelle, "Trends
2. G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain,"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.
3. V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on- public-and-private-blockchains/
4. Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media: Newton, MA, USA, 2015.
5. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture,
6. Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564. [CrossRef]
7. Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H. A critical review of blockchain and its current applications. In Proceedings of the 2017 International
8. Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113. [CrossRef]
9. Greenspan, G. Blockchains Vs Centralized Databases; MultiChain: London, UK, 2016.
10. Lewis, A. A Gentle Introduction to Blockchain Technology.
11. Bits on Blocks. 2018. Available online: https:// bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-
12. technology/ (accessed on 4 September 2018).
13. Wüst, K.; Gervais, A. Do you need a Blockchain? IACR Cryptol. ePrint Arch. **2017**, 2017, 375.
14. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Commun. Surv. Tutor. **2016**, 18, 2084–2123. [CrossRef]

ISSN: 2005-4289 IJDRBC

15. https://www.researchgate.net/publication/318131748_An_Overview_of_B lockchain_Technology _Architecture_Consensus_and_Future_Trend

AUTHORS PFOFILE

Dr.Vidya Gavekar has completed the Master's degree in computer application (2001) from Shivaji Uni versity ,Kolhapur and she is pursuing Master's degree in Business Administration from SPPU,Pune. Also, she has completed Ph. D. in Computer Management. Currently, she is working as Asso Professor of MCA in Sinhgad Institute of Management,Pune. Her research and teaching interest include computer applications. She has authored and co-authored nearly 22 publications in International journals and peer-reviewed conferences.

Dr.Manisha Kumbhar has completed the Master's degree in computer application (1999) from Shivaji Uni versity ,Kolhapur and Master's degree in Business Administration(2019) from SPPU,Pune. Also, she has completed Ph. D. in Computer Management. Currently, she is working as Professor of MCA in Sinhgad Institute of Management,Pune. Her research and teaching interest include computer applications. She has authored and co- authored nearly 35+ publications in International journals and peer-reviewed conferences. She is Ph.D. guide of SPPU,Pune.

Prof.Aparna Kulkarni has completed the Master's degree in computer application from SPPU,Pune. Also she is pursuing Master's degree in Business Administration from SPPU,Pune. Currently, she is working as Asst.Professor of MCA in Sinhgad Institute of Management,Pune. Her research and teaching interest include computer applications. She has authored and co-authored nearly 5+publications in International journals and peer-reviewed conferences. Conferences.

ISSN: 2005-4289 IJDRBC