Introduction to Blockchain

Sneha Prajapati[1], Pragyansh Dwivedi[2] , Ashutosh Dhar Dubey[3], Mayur Singh[4], Sachidanand Chaturvedi[5]

[1]Student , CSE Department , Buddha Institute of Technology
[2]Student , CSE Department , Buddha Institute of Technology
[3]Student , CSE Department , Buddha Institute of Technology
[4]Student , CSE Department , Buddha Institute of Technology
[5]Asst. Professor , CSE Department , Buddha Institute of Technology

Abstract

A blockchain is, in the simplest of term, a time-stamp series of immutable records of data that is managed by cluster of computers not owned by any single entity. Each of these block of data or say, "Block" are secured and bound to each other using cryptographic principles say, "Chain". Blockchain technology was first developed for Bitcoin Crypto-currency. As a revolutionary new technology, it has been widely concerned by the business community and academia and study. Blockchain has the advantages of transparency, data integrity, tamper-proofand so on, in the financial; insurance government. Military and other fields have important application values. Blockchain is poised to become the most exciting invention after the Internet; while the latter connects the world to enable new business models based on online business processes, the former will help resolve the trust issue more efficiently via network computing.In this paper, we provide a complete overview to this technology. It deals with the types of blockchain and its structure. At the same time the paper deals with the working of the blockchain, its benefits and the downside of this technology.

Objective

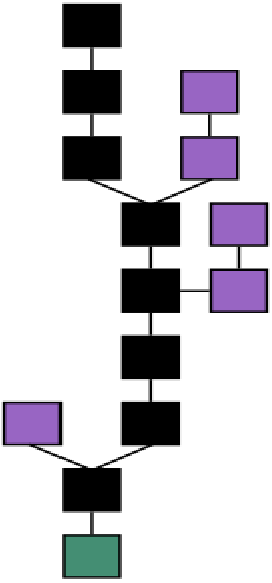
This research paper is mainly focused on the technology named Blockchain. We aim to cover all the basic aspects of this technology. The history and the reason of development is mentioned. The paper deals with the architecture, the type, uses, and the future application. Blockchain is been called as the "new internet", how much this is true has also been mentioned along with the working. Every technology has its advantage and its disadvantage and yes the blockchain do have the same, this paper goes through this too.

Introduction

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography.[1] Each block contains a cryptographic hashof the previous block[1], timestamp, and transaction data.It is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of amajority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.

Blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".[2]

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.” – Don & Alex Tapscott, authors Blockchain Revolution (2016).



[figure-1] *Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.*

History and the Inventor of blockchain

The idea behind blockchain technology can be traced to 1991 when Stuart Haber and W.Scott Stonetta described the work on a cryptographically secure chain of blocks. In 1992, they incorporated Merkle trees into the design allowing several documents to be collected into a block. However, blockchain technology as we know it today gained significance from 2008 when pseudonymous Satoshi Nakamoto published the Bitcoin white paper. Satoshi Nakamoto gave practical impetus to blockchain technology and solved the problem of double spending.

Blockchain was conceptualized in 2008. Nakamoto improved the design in an important way using Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted party[1].The design was implemented the following year by Nakamoto as a core component of the crypto-currency bitcoin, where it serves as the public ledger for the transaction on the network[3].

Structure of blockchain

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks[4]. This allow the participants to verify and audit transactions independently and relatively inexpensive[5]. A blockchain database is managed autonomously using a peer-to-peer network and a distributed time-stamping server. They are authenticated by mass collaboration powered by collective self-interests[6].

- **Blocks:**

  Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree[3]. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form chain[3]. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block[7].

- **Decentralization:**

  By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally.

  Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography[8].

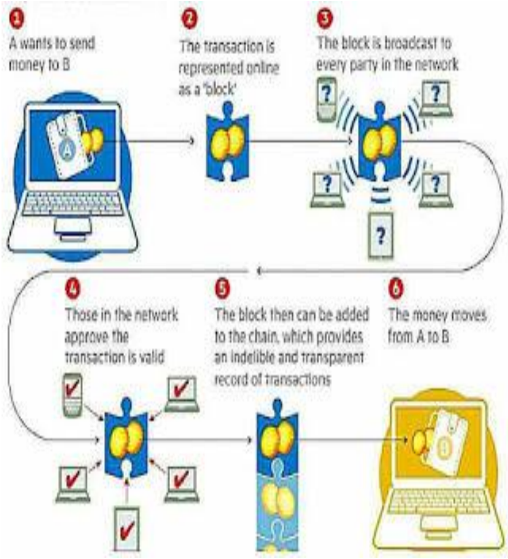
  Every node in a decentralized system has a copy of the blockchain. Data qualityis maintained by massive database replication[9] and computational trust. No centralized "official" copy exists and no user is "trusted" more than any other.[8] Transactions are broadcast to the network using software. Messages are delivered on a best-effort basis. Mining nodes validate transactions,[7] add them to the block they are building, and then broadcast the completed block to other nodes.[10]

- **Openness:**

  Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view. Blockchains serve as a distributed version of multi-version concurrency control(MVCC) in databases[11]. Just as MVCC prevents two transactions from concurrently modifying a single object in a database, blockchains prevent two transactions from spending the same single output in a blockchain[12].

How do blockchain work?

When a new transaction or an edit to an existing transaction comes in to a blockchain, generally a majority of the nodes within a blockchain implementation must execute algorithms to evaluate and verify the history of the individual blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.[13]


1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B

[figure-2] *Working of blockchain*

Types of Blockchain

Currently, there are three types of blockchain networks - public blockchains, private blockchains and consortium blockchains.

- **Public Blockchains:**

  A public blockchain as its name suggests is the blockchain of the public, meaning a kind of blockchain which is-***'for the people, by the people and of the people'.***A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator[14].

- **Private Blockchains:**

  Private blockchain as its name suggests is a private property of an individual or an organization.

  A private blockchain is permissioned[15]. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

- **Consortium or Federated Blockchains:**

  A consortium blockchain is often said to be semi-decentralized[16]. This type of blockchain tries to remove the sole autonomy which gets vested in just one entity by using private blockchain. It, too, is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network. The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

Benefits

Across global supply chains, financial services, healthcare, government and many other industries, innovators are exploring ways to use blockchain to disrupt and transform traditional business models. Many industry leaders have already achieved significant business benefits, including greater transparency, enhanced security, improved traceability, increased efficiency and speed of transactions, and reduced costs[17].

Downside

Because of the nature of blockchains, it will always be slower than centralized databases. When a transaction is being processed, a blockchain has to do all the same things just like a regular database does, but it carries three additional burdens[18] as well Signature verification, Consensus mechanisms and Redundancy.

Other disadvantages includes nascent technology, uncertain regulatory status, large energy consumption and so on.

Uses

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. On May 8, 2018 Facebook confirmed that it is opening a new blockchain group[19] which will be headed by David Marcus who previously was in charge of Messenger. According to The VergeFacebook is planning to launch its own cryptocurrency for facilitating payments on the platform[20].

Blockchains are used in cryptocurrencies, smart contracts, financial services, video games, and supply chains. Blockchain technology can also be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments to content creators.

References

[1]Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[2]Iansiti, Marco; Lakhani, Karim R. *"The Truth About Blockchain"*. Harvard Business Review. Harvard University

[3]*"Blockchains: The great chain of being sure about things"*. The Economist.

[4]Armstrong, Stephen. *"Move over Bitcoin, the blockchain is only just getting started"*.

[5]Catalini, Christian; Gans, Joshua S.*"Some Simple Economics of the Blockchain"*.

[6]Tapscott, Don; Tapscott, Alex. *"Here's Why Blockchains Will Change the World"*.

[7]Bhaskar, Nirupama Devi; Chuen, David LEE Kuo. *"Bitcoin Mining Technology"*. Handbook of Digital Currency.

[8]Brito, Jerry; Castillo, Andrea. *Bitcoin: A Primer for Policymakers(PDF) (Report)*. Fairfax, VA: Mercatus Center, George Mason University.

[9]Raval, Siraj."What Is a Decentralized Application?"*Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*

[10]Antonopoulos, Andreas M. . *Mastering Bitcoin. Unlocking Digital Cryptocurrencies*. Sebastopol, CA: O'Reilly Media. ISBN 978-1449374037.

[11]Greenspan, Gideon. "Ending the bitcoin vs blockchain debate". *multichain.com*.

[12]*Tapscott, Don*; *Tapscott, Alex*. The Blockchain Revolution: How the *Technology Behind Bitcoin is Changing Money, Business, and the World. ISBN 978-0-670-06997-2.*

[13]https://www.cio.com/article/3055847/what-is-blockchain-and-how-does-it-work.html

[14]"How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes". *Perfectial*.

[15] Bob Marvin "*Blockchain: The Invisible Technology That's Changing the World*".PC MAG Australia.

[16]https://coinsutra.com/different-types-blockchains/

[17]https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[18]https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

[19]Wagner, Kurt. *"Facebook is making its biggest executive shuffle in company history"*

[20]Gartenberg, Chaim.*"Facebook reportedly plans to launch its own cryptocurrency"*

[figure-1]https://en.wikipedia.org/wiki/Blockchain

[figure-2]https://www.topicsforseminar.com/2018/02/blockchain-technology-seminar-report.html