Blockchain Technology

Shubham Ghodke [1], Aniruddh Sarkar [2], Aditya Shinde [3], Sanjog Rathod [4], Namrata Naikwade [5]

[1, 2, 3, 4] Bachelor of Technology Student, [5] Assistant Professor

Department of Computer Science and Engineering, MIT Art Design and Technology University

Abstract

A blockchain is a public ledger, or distributed ledger, containing all completed transactions or functions that may be shared among participants. A majority of the system's participants double-check each transaction in the shared ledger. Once data has been input, it cannot be removed. Every single transaction that has ever taken place is recorded in the blockchain, which is both secure and verifiable. Bitcoin, a decentralized peer-to-peer digital money, is the most well-known application of blockchain technology. Despite the fact that the virtual currency bitcoin is divisive, the blockchain technology that underpins it has functioned well and has a wide range of applications in both the financial and nonfinancial sectors. The underlying notion is that in the digital internet age, the blockchain now creates a smart contracts system. Involved parties can already see that a digital event occurred by creating an unequivocal log in a public ledger. It lays the path for a digital economy that is democratic, open, and resilient to emerge from a centralized one. This cutting-edge technology has enormous potential, and the revolution in this field has just begun. This white paper provides an overview of blockchain technology and some of its most favorable environments in the monetary and nonfinancial sectors. Then we examine the issues and opportunities that this basic technology, which has the potential to transform our modern society, brings.

Keywords: Blockchain, Decentralized Ledger, Consensus Mechanisms

1. Introduction

A chain of blocks of records, or public ledger, of all transactions or impact the operations that have been completed and shared among participants. Each activity in the public blockchain is double-checked by a percent of the system's members. Once data has been input, it cannot be removed. Every transaction that has ever taken place is logged in the network, which is both secure and verifiable. To provide a simple example, snatching a biscuit out of a cookie jar kept in a remote position is significantly easier than grabbing a biscuit from a biscuit tin kept in a central location. In a marketplace when hundreds of people are watching. Bitcoin is the most well-known example of a cryptocurrency that is inextricably linked to blockchain technology. It is also the most contentious since it contributes to the creation of a multibillion-dollar worldwide industry of anonymous transactions that is free of official regulation. As a result, it is responsible for a variety of regulatory concerns involving governments and banking institutions. However, Blockchain technology is uncontroversial, has performed admirably over time, and is being successfully utilized to both monetary and non-applications. The blockchain - based distributed consensus model was named its most important breakthrough since the Internet itself by Marc Andreessen, the leading light of Silicon

Valley's capitalists, last year. BNP Paribas' Johann Polychaeta stated in Quintessence magazine that bitcoin's blockchain, the software that enables the digital money to function, should be viewed as an invention similar to the steam or combustion engine, with the potential to alter the financial world and beyond. The blockchain innovation comes in helpful here. It has the potential to transform the digital world by facilitating a distributed consensus in which each and every digital payments involving digital assets, both past and present, can be confirmed at any moment in the future. It accomplishes this without jeopardizing the digital assets' and parties' privacy. Blockchain technology has two crucial characteristics: distributed consensus and anonymity. The benefits of Blockchain technology overshadow the technical and organizational challenges. "Smart Contracts" are a prominent emerging use case for blockchain technology. Smart contracts are computer systems that can automatically carry out a contract's terms. When a smart contract's pre-configured condition among system is an active is met, the parties to a contractual obligation can be automatically paid according to the contract in a transparent manner. In this paper, we look at how the introduction of blockchain technology is causing upheaval in every industry in today's digital economy. Blockchain technology has the potential to become the next growth engine in the digital economy, as we increasingly use the Internet to conduct digital retail and share our personally identifiable and life events. This field offers huge prospects, and the change in this arena has only just begun. In this paper, we will look at a few significant Blockchain applications in the areas of notary, insurance, private securities, and a few other non-financial applications. We'll start by going over some background information and the new tech itself.

2. Blockchain Hyperledger Architectural Diagram

Like a traditional public ledger, a blockchain is a series of blocks that carry a detailed set of transaction data. A block has just one parent block if the block header contains a preceding block hash. Uncle blocks' hashes (children of the block's forebears) would likewise be kept on the Ethereum blockchain. The genesis block is the initial block in a blockchain that has no block header. The components of the system of blockchain are then explained in detail. The genesis block and indeed the block body make up a block. The block header, in particular, contains the following information:

(1) **Block Cersion:** Specifies which set of blocks validation criteria should be applied.

(2) **Merkle Tree Root Hash:** The sum of all transactions in the block's hash value.

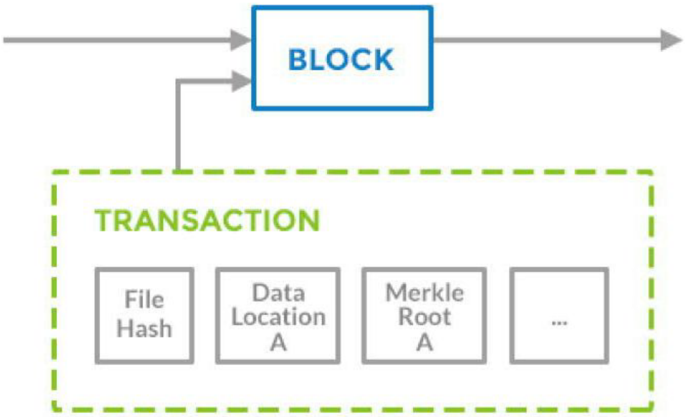
(3) **Timestamp:** From January 1, 1970, the current time has been expressed in seconds in universal time.

(4) **Bits:** A valid block hash's target threshold.

(5) **Once:** A 4-byte field that starts with 0 and rises with each hash computation.

(6) **Parental Block Hash:** A SHA-256 hash value that refers to the block before it.

Figure 1: Metadata Insertion in the Blockchain



3. Digital Signatures

The user has a pair of both encryption keys. The transactions are signed with a private key, which must be kept secret. The digitally signed transactions are disseminated over the whole network. A typical digital signature comprises two phases: the signing phase and the verification phase. For example, user Alice intends to send a message to user Bob.

(1) Alice vaults her content with her private key during the signing step and delivers the encrypted result as well as the original data to Bob.

(2) Bob verifies the value with Alice's public key during the verification phase. Bob could simply check if indeed the data had been manipulated with this way. The invertible digital signature technique is the most common digitally signed procedure used in blockchains (ECDSA).

4. Important Characteristics

In conclusion, the fundamental properties of blockchain are as follows:

(1) **Decentralization:** Each transaction in traditional centralized transaction systems must be validated by a central entity authority (e.g., the central bank), resulting in cost and performance bottlenecks at the centralized servers. In contrast to the centralized option, blockchain does not require a third party. Consensus algorithms are employed in blockchain to keep data consistent across a distributed network.

(2) **Persistency:** Transactions can also be authenticated fast, and honest miners would not accept invalid transactions. Once a transaction is incorporated in the blockchain, it is nearly hard to erase or rollback the transaction. Blocks containing incorrect transactions might be found right away.

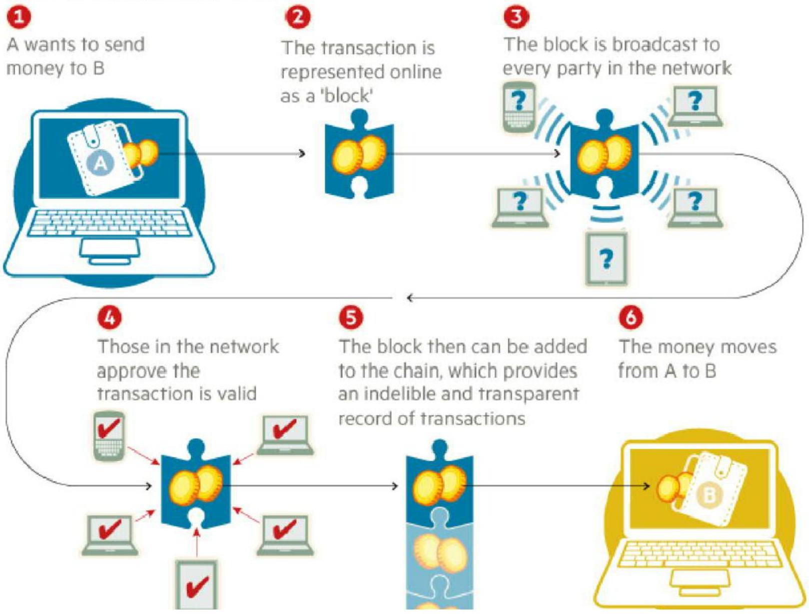
(3) **Anonymity:** Each user interacts with the blockchain using a randomly generated address that hides the user's true identity. Due to the inherent restriction, blockchain cannot ensure full privacy preservation.

(4) **Auditability:** The Unspent Transaction Output (UTX-O) paradigm is used to store data on user balances on the Bitcoin blockchain: Any transaction must reference some previously unspent funds. The state among these referred unspent transactions changes from unspent to spend once the present transaction is verified into the blockchain. As a result, trades could be easily tracked and validated.

5. Consensus Algorithms

The Byzantine Generals (BG) Dilemma, which also was proposed in, is a transformation of how to obtain consensus among untrustworthy nodes in blockchain. A gang of generals who supervise a section of the Byzantine forces circle the city in the BG issue. Some generals would rather assault, while others would rather retreat. However, if only a portion of the commanding officers attack the city, the attack will fail. As a result, they must decide whether to assault or retreat. It's difficult to reach a quorum in a dispersed setting. It's also a problem for blockchain because the network is spread. There is no main server in blockchain that assures all distributed node ledgers are identical. The Bitcoin network employs a consensus mechanism known as PoW (Proof of Work). Someone must be chosen to record transactions in a decentralised network. Random selection is the simplest method. Random selection, on the other hand, is open to attacks. As a result, if a node wishes to disseminate a transactions on the network, it must first establish that it is likely to invade the network. In most cases, the work entails computer computations. Each network node calculates a hash value for the block header in PoW. A nonce is included in the block header, and miners would modify it regularly to obtain different hash values. PoS (Proof of Stake) is a less energy-intensive form of PoW. In a PoS system, miners must demonstrate that they hold the money in question. People with even more currencies are thought to be a little less likely to assault the network. Since this single richest participant is bound to be prominent in the network, the relying solely on income statement is highly unjust. As a result, numerous techniques using a mix of stake size to determine which one should manufacture the next block have been presented. Black coin, in particular, employs randomness to forecast the next generator. It employs a formula that considers the low hash value as well as the stake size. Peer coin prefers to select coins depending on their age. Older and larger groups of tokens have a higher chance of processing the next block in Peer coin. PoS preserves significant resources and is more efficient than PoW. Unfortunately, because the cost of mining is so low, attacks may occur as a result. Many blockchains start with PoW and then transition to PoS over time. Ethereum, for example, is intending to switch from Ethash (a type of PoW) to Lucid (a kind of PoS).

Figure 2: How a Blockchain Works


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

6. Advances on Consensus Mechanisms

Efficiency, safety, and ease are all attributes of a good consensus algorithm. A number of efforts have recently been undertaken to improve blockchain consensus algorithms. Different consensus algorithms are being developed in order to address some specific blockchain issues. The fundamental principle underpinning Peer Census is to dissociate chain formation and transaction confirmation in order to significantly boost consensus speed. Aside from that, Kraft presented a novel consensus mechanism to guarantee that such a block is processed at a somewhat constant speed. High block production rates are well recognized to jeopardize Bitcoin's security. To overcome this problem, the Greedy Heaviest-Observed Sub-Tree (GHOST) network selection rule is proposed. Instead of using the longest branch strategy, GHOST measures the branches so that miners can pick the best one. Chepurnoyet et al. proposed a new peer-to-peer blockchain consensus process in which anyone who presents non-interactive evidence of irretrievability for previous state snaps is agreed to construct the block. Miners simply have to save outdated block headers rather than complete blocks in such a system.

7. Challenges and Recent Advances

Due to immense potential, blockchain faces various constraints that hinder its broader use. The following are the significant barriers and rapid advances:

(1) **Scalability:** The blockchain is becoming increasingly hefty as the number of transactions increases. Because they must evaluate if the provenance of the current session is unspent or not, each node must record all transactions in order to confirm them on the blockchain. Furthermore, the Bitcoin protocol can now only perform about 7 operations per second due to the initial block size restriction and the time interval required to construct a new block, which is insufficient to meet the need of handling money transfers in real-time. Meanwhile, because blocks have a limited capacity, many minor transactions may be delayed because miners prefer transactions with a high transaction fee. There seem to be a number of approaches to tackle the bottleneck of blockchain that can be categorized into two:

(1.1) **Blockchain Storage Optimization:** Because it is more difficult for a node to maintain a full copy of the blockchain, Bruce proposed a revolutionary cryptocurrency system in which the network removes (or forgets) old transaction records. The account of all non-empty aliases is kept in a database called account tree. Aside from that, a lightweight client may be able to assist in the resolution of this issue. VerSum is a revolutionary system that was developed to include another way for lighter weight consumers to exist. VerSum enables lightweight clients to offload costly computations with big inputs. By evaluating results from multiple servers, it assures that perhaps the computational result is correct.

(1.2) **Blockchain is being Redesigned:** It was proposed that Bitcoin-NG (Next Generation) be used. The primary concept of Bitcoin-NG is to split a standard block into two segments: a key block for consensus process and a micro block for transaction storage. Epochs are used to split time in the protocol. Miners must hash each epoch to obtain a key block. The node becomes the owner after the key block is formed, and it is in charge of generating micro blocks. The longest (longest) chain method, in which micro blocks have no weight, was likewise extended in Bitcoin-NG. The dilemma involving block and network monitoring has been handled in this fashion, and blockchain has been reinvented as a result.

(2) **Privacy Leakage:** Through the use of public and private keys, blockchain may maintain a certain level of privacy. Users transact with the private and public keys without revealing their true identities. However, because the identities of all accounting records for each public key are completely public, blockchain cannot guarantee transactional anonymity. Furthermore, according to a recent study, a user's financial transactions can be connected to revealing personal information. Furthermore, Biryukov et al. demonstrated a method for linking user aliases to IPs even when they are protected by NAT or firewalls. A set of nodes that each client connects to can be used to uniquely identify it. This collection, on the other hand, can be trained and utilized to detect the existence of a transaction. Numerous ways have been proposed to improve blockchain anonymity, which can be classified into two groups: Mixing and Anonymous.

(3) **Selfish Mining:** Blockchain is vulnerable to cooperating selfish miners' attacks. Eyal and Sirer, in particular, demonstrated that the network is susceptible although only a small amount of the computing power is cheated. Selfish miners hold their mined blocks while publicizing in a selfish mining technique, and the private section is only exposed to the public if certain conditions are met. All miners would accept the private branch because it is broader than the existing public chain. Miners are burning their energies on a worthless branch even before private blockchain is published, while selfish miners are processing their internal chain without competition. As a result, selfish miners tend to make more money.

8. Possible Future Directions

In both academic and business communities, blockchain has demonstrated effectiveness. We highlight four possible future directions: blockchain testing, countering the trajectory toward centralization, big data analytics, and blockchain application.

(1) **Blockchain in Testing:** Various types of blockchains have recently appeared, and there are currently over 700 cryptocurrencies listed in. Some developers, on the other hand, may fake their blockchain performance in order to entice investors attracted by the tremendous profit potential. Furthermore, when consumers wish to incorporate blockchain into their businesses, they must first determine which blockchain best meets their needs. As a result, a blockchain testing process must be in operation to test several blockchains. Testing on the blockchain can be divided into two phases: standardization and testing. All criteria must be created and agreed upon during the early stages of implementation. Whenever the blockchain is created, it can be evaluated against pre-determined criteria to see if it meets the developers' claims. In terms of the testing phase, various criteria must be used to blockchain testing.

(2) **Limiting the Tendency to Centralization:** Blockchain is a distributed ledger technology. However, there is a tendency in which the mining pool's miners are centralized. Currently, the top five mining pools control more than 51% of the entire mining power in the Bitcoin protocol. Apart from that, the selfish mining technique revealed that pools with more than 25% of total processing capacity might earn more than their fair share of money. The selfish pool would attract rational miners, and the pooling could easily approach 51% of total power. Because the blockchain isn't designed to serve a single business, some solutions to this challenge should be presented.

(3) **Big Data Analytics:** Big data and blockchain could work nicely together. We divided the integration into two categories: data management and analytics. In terms of data management, because blockchain is distributed and safe, it might be utilized to store sensitive information. The

originality of the data could potentially be ensured using blockchain. If blockchain is used to record patient health information, for example, the data cannot be tampered with, and it is difficult to steal confidential information. Operations on blockchain can be utilized for large data analytics when it comes to data analytics.

9. Conclusion

With its key properties of decentralization, consistency, anonymity and auditability, blockchain has proved its potential to revolutionize traditional industries. We offer a complete review of blockchain in this paper. We begin by providing an insight of blockchain technologies, covering blockchain architecture and essential blockchain properties. The typical consensus protocols utilized in blockchain are then discussed. We examined and contrasted these techniques in a variety of ways. We also outlined some of the hurdles and issues that could stymie blockchain growth, as well as some existing solutions to these issues. There are also some suggestions for future directions. Nowadays, blockchain-based applications are aplenty, and we intend to conduct in-depth investigations into them in the future.

References

1. Garrick Hileman, “State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin”, 2016. https://www.coindesk.com/markets/2016/05/11/state-of-blockchain-q1-2016-blockchain-funding-overtakes-bitcoin/
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf
3. G. W. Peters, E. Panayi, A. Chappelle, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective”, 2015
4. G. Foroglou, A.-L. Tsilidou, “Further applications of the blockchain”, 2015
5. A. Kosba, A. Miller, E. Shi, Z. Wen, 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