www.ijecs.in
International Journal of Engineering and Computer Science
Volume12 Issue 05, May2023, PageNo.25722-25728
ISSN:2319-7242DOI: 10.18535/ijecs/v12i03.4671

Implementation Of BlockChain Technology

Manju Sharma
College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Abstract

Transaction volumes throughout the world are growing very fastly and that result in the complexities, vulnerabilities, inefficiencies, and higher costs of current transaction systems. The growth of ecommerce, online banking, and in-app purchases, is increasing and is more popular among the people around the world. And transaction volumes are increasing with the advent of the Internet of Things (IoT). Objects, such as laptop, washing machines and groceries are running low and cars that deliver themselves to your door. To meet these challenges and others we need faster payment methods that are trustworthy and require no specialized equipment with no chargebacks or monthly fees and offer a good bookkeeping solution for ensuring transparency.

Keywords: Bitcoin, Block, Blockchain, Digital transaction.

Introduction

One solution that’s been developed to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems is Bitcoin — the digital currency launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto. Unlike traditional currencies issued by central banks, Bitcoins have no central monetary authority. No one controls it. Bitcoins aren’t printed like dollars or euros; they’re “mined” by people (and increasingly by businesses) running computers all around the world who use software to solve mathematical puzzles. Rather than relying on a central monetary authority to monitor, verify, and approve transactions and manage the money supply, Bitcoin is enabled by a peer-to-peer computer network made up of its users’ machines, akin to the networks that underpin BitTorrent and Skype.

Bitcoin has several advantages over other current transaction systems, including

» Cost-effective: Bitcoin eliminates the need for intermediaries.

» Efficient: Transaction information is recorded once and is available to all parties through the distributed network.

» Safe and secure: The underlying ledger is tamper-evident. A transaction can’t be changed; it can only be reversed with another transaction, in which case both transactions are visible.[1]

The idea of Bitcoin was conceptualized by Satoshi Nakamoto, an anonymous figure. In May 2008, he shared a white paper about Bitcoin. He did not disclose who he was. He outlined how the currency would work. The first major blockchain innovation was bitcoin, a digital currency experiment. The second innovation was called blockchain, which was made keeping in mind that the technology that operated the Bitcoin should be separated from the currency and used for all kinds of other inter organizational cooperation. Almost every major financial institution in the world is doing blockchain research at the moment, and 15% of banks are expected to be using blockchain in 2017. The third innovation was called the "smart contract," embodied in a second-generation blockchain system called ethereum, which built little computer programs directly into blockchain that allowed financial instruments, like loans or bonds, to be represented, rather than only the cash-like tokens of the bitcoin. The fourth major innovation, the current cutting edge of blockchain thinking, is called "proof of stake."[2]

Figure 1. Bitcoin[2]

A block consists of the block header and the block body. In particular, the block header includes: • Block version: indicates which set of block validation rules to follow. • Parent block hash: a 256-bit hash value that points to the previous block. • Merkle tree root hash: the hash value of all the transactions in the block. • Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC. • nBits: current hashing target in a compact format. • Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculationThe block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions (NRI, 2015). A digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature. [6]

What is Blockchain?

Blockchain is a distributed database over a network of computers where data can be safely stored, making it impossible to change or manipulate. In other words, a blockchain is simply a digital record of transactions replicated and spread across the blockchain's network of nodes or computer systems. Each block on the chain contains several transactions, and whenever a new transaction takes place on the blockchain, a trace of that transaction is added to the ledger of every participant. Distributed Ledger Technology is a decentralized database administered by several individuals (DLT).[4]. Blockchain technology is computer software or a protocol for the transfer of unique instances securely for value which can be money, property, contracts etc via the internet without need of a third-party intermediacies like bank or government.Bitcoin, a crypto currency and payment system firstly introduced in the year 2008, is one of the most common implementations of blockchain. The transfer of digital assets, such as bitcoin, within a block chain is initiated when a seller or payer submits a transaction.In general, the BC represents a continuously maintained and controlled database considering growing factors and collected data sample sets. The key elements of BC are participant created transactions, and the recorder blocks of such transactions. Here, the recorder block checks whether, transaction details were maintained in the correct sequence or not. This does not allow any tampering of the data available. If the recorded data must be maintained in sequential order, the need for chain approach arises.This maintained transactionwas shared with the network of participated nodes. This eliminates the concept of central server by identifying each node that is participated in the transaction sharing process by using the cryptography.[8]

Bitcoin: A peer-to-peer electronic cash system S. Nakamoto, 2008, [6], cited by 4707:As per this article and the usage of blockchains as immutable ledgers can be seen as the origin of the blockchain technologies we see today. It is in this paper the bitcoin and blockchain revolution started. Even though the paper was published as a non peer reviewed white paper, it is one of the most cited works in the blockchain research area. The paper itself is short and does not include so many details. It primarily presents the overall idea and structure. Details on the solution, the specific technologies, and the exact properties on how the bitcoin system would be implemented is not included. Another interesting note, is that Satoshi Nakamoto never mentions the term blockchain specifically in his paper. But he does talk about chains of blocks, proof-of-work chains, and lengths of chains.[9]

History of Blockchain Technology

The blockchain technology promises to revolutionize the way of business. It has effects on various sectors, from financial to manufacturing as well as education. Satoshi Nakamoto released the well-known whitepaper about the technology in 2009. In the paper, he provided details of how the technology was well equipped to enhance digital trust given the decentralization aspect that meant nobody would ever be in control of anything. Ever since Satoshi Nakamoto exited the scene and handed over Bitcoin development to other core application developers, the digital ledger technology has evolved resulting in new applications that make up the blockchain history (Url-4, 2018). The evolution of Bitcoin and other cryptocurrencies have both drawn significant attention and also threatened the very foundations of the financial system. After all, this was the intention of Satoshi Nakamoto when the global financial crisis hit not only USA but also the global economy harder than any crisis in history. [7]

KeyFeatures of Blockchain

Blockchain technology isn’t just a backup network for cryptocurrencies, but it offers a lot more. So, what are the key blockchain features that makes it so irresistible? Why is it gaining so much popularity? Let’s dive in a little deeper into the features of blockchain in this guide to answer these questions. Let’s start with the quick Blockchaininfo graphic!he three key technologies that make up the blockchain are a digital ledger, a peer-to-peer network, and cryptographic keys. The two types of cryptographic keys are private keys and public keys. Both of these keys are held by each person or node and are used to generate digital signatures. [3]

The development of block chain technologies seems more beneficial for banking and financial institutions. Block chain technology is very helpful in the current tax system, it reduced the load on management and is easier for the business entity get the information about the cash flows in the bank account. And it is easier to pay off tax.

The use of blockchain technology is also characterized by the ability to protect transactions from cyberattacks. Security problems are addressed in several ways: new blocks are always stored linearly and chronologically. In other words, they are always added to the "end" of the blockchain. Since the block was added to the end of the blockchain, it is very difficult to go back and change the contents of the block. This is because each block contains its own hash, as well as the hash of the block in front of it. Hash codes are created using a mathematical function that turns digital information into a string of numbers and letters.[5]

Advantages of Blockchain

- **Less Failure:** In blockchain everything is organized digitally and it is not dependent on human. So it has lesser or no failure.
- **User Control:** Since everything is organized digitally it doesn’t rely on third party for maintenance.
- **Third-Party not required :** There is no risk in case of third party involvement in this. As everything is organized digitally.
- **Zero or null fraud:** As the system runs on algorithms there are less chances of fraud and scam.
- **System Transparency:** The decentralized nature of technological usage makes it more transparent.
- **Reliability:**Blockchain is considered as the most reliable source for digital transactions currently.
- **Hacking:** Everything is maintained digitally and is organized chances of hacking are less.

Blockchains in Sustainable Supply Chains

A blockchain is a chain of blocks where blocks are digital pieces of information and the storage in a distributed database. The block stores information about - a) transactions b) participants in transactions, and c) differentiation. It provides electronically decentralized and distributed ledger for all participating actors implemented with its time-stamped data structure. It contains nodes for groups the transactions into blocks. The nodes will determine whether a transaction is valid transaction need to be kept in the blockchain. Tamperproof ledgers, transactions in blocks cannot be altered or erased by a single actor.

CHALLENGES OF BLOCKCHAIN

Some of the major challenges currently faced by blockchain technology are listed as below.

1. Scalability: All transactions are stored in each and every node to get it validated. The current transaction should be validated before the other transactions to be validated.The restricted block size and the time interval used to create another block plays an important role in not fulfilling the requirement of processing each transactions at the same time in real time scenarios.

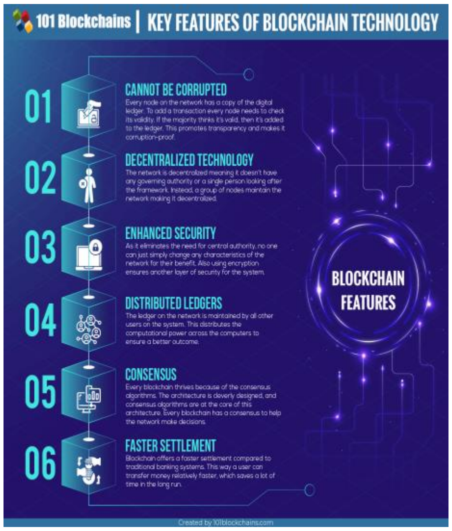
2. Privacy Leakage: The blockchain is mainly vulnerable to transactional privacy leakage due to the fact that the details and balances of all public keys are visible to everyone in the network.

3. Mining: The miners keep the mined blocks without broadcasting it to the network and create a private branch which gets broadcast only after certain requirements are met.

4.Personal Identifiable Information: Personal Identifiable Information (PII) refers to any information that used to remove an individual’s identity.

5. Security: Security can be considered in terms of confidentiality, integrity, reliability and availability. Its always a challenge in case of open networks such as public blockchains.If anyone hack the information about a bank or financial institution. Then a skilled person can do it easily because the number of system to be hacked is only “one”. But in case of blockchain is different if someone want to hack the network of nodes then the person have to hack all the networks, hacking only one system doesn’t work.

6. Future of Blockchain Technology According to York Solutions: By 2022, at least one innovative business built on blockchain technology will be worth $10 billion. By 2026, the business value added by blockchain will grow to just over $360 billion, then by 2030 grow to more than $3.1 trillion.By 2022, at least one innovative business built on blockchain technology will be worth $10 billion. By 2026, the business value added by blockchain will grow to just over $360 billion, then by 2030 grow to more than $3.1 trillion.



101 Blockchains | KEY FEATURES OF BLOCKCHAIN TECHNOLOGY

01 CANNOT BE CORRUPTED
Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

02 DECENTRALIZED TECHNOLOGY
The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

03 ENHANCED SECURITY
As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

04 DISTRIBUTED LEDGERS
The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

05 CONSENSUS
Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

06 FASTER SETTLEMENT
Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

Figure 2: Key features of Blockchain Technogy

BLOCKCHAIN TECHNOLOGY APPLICATIONS

- **A. Internet of Things (IoT):** In IoT biological system the best part of the correspondence is Machine-to-Machine (M2M) cooperation. So, inaugurating trust between the partaking machines is the most challenge for IoT innovation which is yet tomet wide.
- **B. Currency:** Currency is the most common applications of blockchain. Blockchain was mainly designed for bitcoins digital or online currencies. By this way it can be treated as the international currencies. Many researches have been done to make a wide use of blockchain.
- **C. Patents:** Owners have been facilitated by the right to protect patent from exploitation of innovations for specific periods of the patents.
- **D. E-voting System:**Elections are conducted offline even after this advancement in technology. This technology has remarkable results in the voting system as no one can alter the votes and the as well as it is cheap than conducting polls offline.
- **E. Network Operations:** The Blockchain Platform by IBM enables the founders to invite, initiate and configure a network with user interface. Initiating a network creates 3 ordering peers, and two certificate authorities. This facilitates founder with a ready to use foundation for creating their business network

F. Operational Monitoring: Users require tomonitoring the activity on network as it grows in terms of transactions and participants. The IBM Blockchain Platform facilitates Network Traffic Dashboard and Network Health Monitor.

G. Blockchain states: Rethinking about the public services in the context of opening up data, services and decisions in the public sector through digital media and technologies, a new generation of open, transparent, collaborative and accountable e-Government services are under development. Recently a report has been published which outlines how blockchain-based technologies could provide new tools to reduce fraud, avoid errors, boost productivity, cut operational costs, support compliance and force accountability in many public services.

H. Smart contracts:

The blockchain ledgers present several interesting and novel features for the users. It facilitates us to maintain the records with the time and a detail of transactions with an active in the implementation and management. Based upon this self-executing smart contract are being developed rapidly.Smart contracts can be defined as a 'computerized transaction protocol that executes the terms of a contract'.

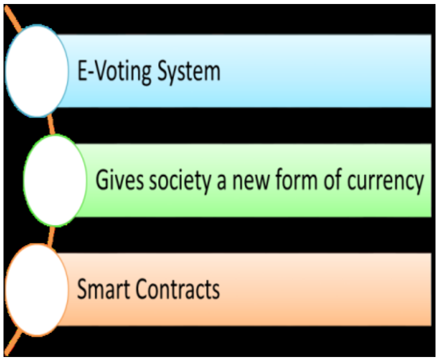


Figure 3. Applications of Blockchain[2]

In simple terms it means that, the terms of an agreement between two or more parties are programmed into set of instructions or say code that are stored on blockchain that are stored on the blockchain [2]

CONCLUSIONS:

This paper is on overview of the blockchain technology and its potential areas. Blockchain technology is database mechanism which facilitates us the transparent information sharing within a business network. The data stored in blocks are linked together in a chain.In other words we can say that Blockchains is the future of all financial and digital transactions currencies.

References:

1. Blockchain For Dummies®, 2nd IBM Limited Edition Published by John Wiley & Sons, Inc. 111 River St. Hoboken, NJ 07030-5774 www.wiley.com Copyright © 2018 by John Wiley & Sons, Inc.
2. A Detailed Study of Blockchain: Changing the World Shweta Singh* , Anjali Sharma* , Dr. Prateek Jain** *Department of Computer Science and Engineering, ManavRachna International Institute of Research and Studies (MRIIRS), Faridabad, India. **Department of Computer Science, Accendere Knowledge Management Services.
3. https://101blockchains.com/introduction-to-blockchain-features/
4. https://shardeum.org/blog/what-are-the-features-of-blockchain/
5. Blockchain technologies characteristics and advantages BegievaRuhshonabegiUtkurovna, Listener of the Banking and Finance Academy,Novateur publicationsJournalNX- A Multidisciplinary Peer Reviewed Journal

ISSN No: 2581 - 4230 VOLUME 6, ISSUE 10, Oct. -2020.

6. Blockchain challenges and opportunities: a survey, ZibinZheng and Shaoan , Hong-Ning Dai , Xiangping Chen*, Huaimin Wang, Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.

7. Blockchain Technology and its NallapaneniManojKumara,Pradeep Kumar Mallickb, International Conference on Computational Intelligence and Data Science (ICCIDS 2018)

8. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

9. Impact on the Global Economy Dr. BurcuSakız (Istanbul Aydın University, Turkey) Prof. Dr. AyşenHiçGencer (Beykent University, Turkey).International conference on Eurasian economies 2019.