International Journal of Research in Engineering, Science and Management
Volume-2, Issue-8, August-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Study of Blockchain Technology

Safal M. Gupta[1], Shubham S. Kharabe[2], Nidhi Rathi[3], Achal M. Rakhunde[4], Dhruvika Shekhawat[5]
[1,2,3,4,5]*Student, Dept. of Computer Science & Engg., Sipna College of Engineering & Technology, Amravati, India*

***Abstract*: Blockchain can be defined as a distributed ledger technology that can record transactions between parties in a secure and permanent way. By 'sharing' databases between multiple parties, blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify, record and coordinate transactions. By facilitating the move from a centralized to a decentralized and distributed system. At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.**

***Keywords*: asymmetric key blockchain, cryptocurrency, cryptography, cryptographic hash function, distributed ledger, distributed consensus algorithm, proof of work**

1. Introduction

A. History of blockchain

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament [2] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [3]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [4], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto's paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications). Bitcoin was just the first of many blockchain applications. Many electronic cash schemes existed prior to Bitcoin (e.g., ecash and NetCash), but none of them achieved widespread use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party.

B. Introduction to blockchain

Blockchain can be defined as a distributed ledger technology that can record transactions between parties in a secure and permanent way. By 'sharing' databases between multiple parties, blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify, record and coordinate transactions. By facilitating the move from a centralized to a decentralized and distributed system. Within the Bitcoin blockchain, information representing electronic cash is attached to a digital address. Bitcoin users can digitally sign and transfer rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is stored, maintained, and collaboratively managed by a distributed group of participants. This, along with certain cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later Blockchain technology is the foundation of modern cryptocurrencies, so named because of the heavy usage of cryptographic functions. Users utilize public and private keys to digitally sign and securely transact within the system. For cryptocurrency based blockchain networks which utilize mining users may solve puzzles using cryptographic hash functions in hopes of being rewarded with a fixed amount of the cryptocurrency. However, blockchain technology may be more broadly applicable than cryptocurrencies. In this work, we focus on the cryptocurrency use case, since that is the primary use of the technology today; however, there is a growing interest in other sectors Blockchain implementations are often designed with a specific purpose or function. Example functions include cryptocurrencies, smart contracts (software deployed on the blockchain and executed by computers running that blockchain), and distributed ledger systems between businesses. There has been a constant stream of developments in the field of blockchain technology, with new platforms being announced constantly – the landscape is continuously changing.

2. Blockchain components

Blockchain technology can seem complex; however, it can be simplified by examining each component individually. At a high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives

(cryptographic hash functions, digital signatures, asymmetric-key cryptography) mixed with record keeping concepts (such as append only ledgers). This section discusses each individual main component: cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and how blocks are chained together.

Table 1
Examples of Input Text and Corresponding SHA-256 Digest Values

Input Text	SHA-256 Digest Values
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Since there are an infinite number of possible input values and a finite number of possible output digest values, it is possible but highly unlikely to have a collision where hash(x) = hash(y) (i.e., the hash of two different inputs produces the same digest). SHA-256 is said to be collision resistant, since to find a collision in SHA-256, one would have to execute the algorithm, on average, about 2128 times (which is 340 undecillions, or more precisely 340, 282, 366, 920, 938, 463, 463, 374, 607, 431,768, 211, 456; roughly 3.402 x 1038).

3. Literature survey

1. Bitcoin by far the most well-known application of blockchain is Bitcoin. It could be argued that blockchain got so well-known because of Bitcoin. Just to make sure everyone is on the same page: Bitcoin is a crypto valuta. The first valuta with no bank and/or nation behind it to organize and maintain it.
2. Bit nation Called into life by Susanne Tarkowski Tempelhof on July 14, 2014. Tempelhof's father was stateless for a decade, which brought her interest into this field. She has spent her life till now studying the topic of 'non-geographically contingent governance service aggregators'. With the launch of Bitcoin, she realized she possibly could make her dream true, of 'providing more services than just health insurance, but also things like education and security, through networks of local subcontractors'. Bit nation offers the same services as those provided by traditional governments, but in a geographically unbound way. Any individual from around.
3. Energy reserve supply market As reported in Computable, power Grid Operator Tennet started a pilot in 2017, to investigate whether blockchain technology can help increase the number of decentralized energy parties on the balancing market. This pilot is a cooperation between Tennet, energy market Vandebron and technology parner IBM. Tennet bears responsibility for the balance on the Dutch energy network. In order to be able to deliver on a continuous base, supply and demand have to be in balance 24/7. Generally, the conventional ways of gaining power are easier to balance everything out. However, with an ever increasing part of the energy originating from sustainable energy, it is getting harder and harder to maintain the balance. The idea behind this pilot is that Vandebron delivers energy from recharging electric cars. IBM created a solution based on blockchain which links small batteries to the larger system of Tennet.

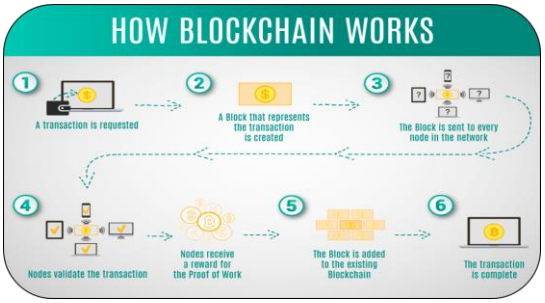

Fig. 1. How blockchain technology works

Where can Blockchain be used?

The Blockchain is ideal for what are known as smart contracts. Smart contracts define the rules and penalties around a specific agreement in the same way as traditional contracts do. However, the big difference is that smart contracts automatically enforce those obligations. The contracts are coded so that they are discharged on the fulfillment of specific criteria.

1. *A warranty claim:* Usually settling warranty claims is expensive, time-consuming and often difficult for those making the claim. It is possible to implement smart contracts using Blockchain that will inevitably make the process a lot easier.
2. *Derivatives:* Derivatives are used in stock exchanges and are concerned with the values of assets. Smart contracts in the trading of stocks and shares could revolutionize current practices by streamlining, automating and reducing the costs of derivatives trading across the industry.
3. *The Internet of Things (IoT):* The Internet of Things (IoT) is the network of physical devices, vehicles and other items embedded with software, actuators, sensors, software and network connectivity, connected to the Internet. All of those features enable such objects to collect and exchange data. Blockchain and its smart contracts are ideal for this.
4. *Identity verification:* Too much time and effort is currently wasted on identity verification. Using the decentralization of Blockchains, the verification of online identity will be much quicker. Online identity data in a central location will vanish with the use of the Blockchain smart contracts. Computer hackers will no longer have centralized points of vulnerability to attack. Data storage is tamper-proof and incorruptible when backed by Blockchain.

4. Applications of blockchain

1. A bitmortgage, some sort of market for mortgages The

University TU-Delft created a working prototype for a blockchain based 'mortgage market'.
2. Loans Quite similar to item 1 but slightly broader. According to Microsoft blockchain can be used for all sorts of loans.
3. Obligations as an obligation can be viewed as a special type of loan, it comes naturally that with item 2 in mind, obligations would go very well with blockchain as well.
4. Voting system One of the things smart contracts on blockchain can be used for. Ethereum already built-in smart contracts which can be easily used for this purpose.

5. Conclusion

Blockchain is a new type of database which solves the double spending problem without a middleman, opening up a whole range of new possibilities. In this database the data is saved in blocks arranged as links in a chain. To secure this block-chain a system called proof-of work is used. In this system so much work (i.e. processing power) is needed to find a block that it is virtually impossible to alter the blockchain afterwards. The work is done by so called miners who get a payment for their effort and the system is set up in such a way that its financially more advantageous for the miners to keep the system in good order than to try and subvert it. blockchain promises to make business processes more efficient and facilitate innovative new services and business models. Blockchain technology is a new tool with potential applications for organizations, enabling secure transactions without the need for a central authority. Starting in 2009-13, with Bitcoin leveraging blockchain technology, there has been an increasing number of blockchain technology-based solutions.

References

[1] Dylan Yaga, "Blockchain Technology Overview."
[2] Keith Turner, "Supply Chain-Blockchain in Logistics."
[3] A. Shanti Bruyn, "Blockchain an introduction."
[4] https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners
[5] Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Xiangping, and Wang, Huaimin, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 6th IEEE International Congress on Big Data, 2017.