ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.2

BlockChain- An Open Distributed Ledger

Kazi Abdul Samad Maheboob
Lecturer
Department of Computer Engineering
Vishweshwarayya Abhiyantriki Padvika Mahavidyalay, Almala, India

Abstract:
A blockchain is a singly Linked List of block, with each block containing a number of transactions. It provides a decentralized, immutable data store that can be used across a network of users, create assets and act as a shared black book that records all transactions. Each transaction can be easily queried, affording greater transparency and trust to all parties involved. With the original creator, or creators, being anonymous the true motivations behind blockchain are arguably unknown. However it has proven to be a more than adequate solution to the many issues.

Keywords: Cryptocurrency**,** Digital ledger, Public Key, Transaction

I. INTRODUCTION

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block. The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted party. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network. In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016. Smart contracts which run on a blockchain, for example ones which "creat[e] invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level."Require an off-chain oracle to access any "external data or events based on time or market conditions [that need] to interact with the blockchain." IBM opened a blockchain innovation research center in Singapore in July 2016.A working group for the World Economic Forum met in November 2016 to discuss the development of governance models related to blockchain. According to Accenture, an application of the diffusion of innovations theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce. In May 2018, Gartner found that only 1% of CIOs indicated any kind of blockchain adoption within their organisations, and only 8% of CIOs were in the short-term 'planning or [looking at] active experimentation with blockchain'.

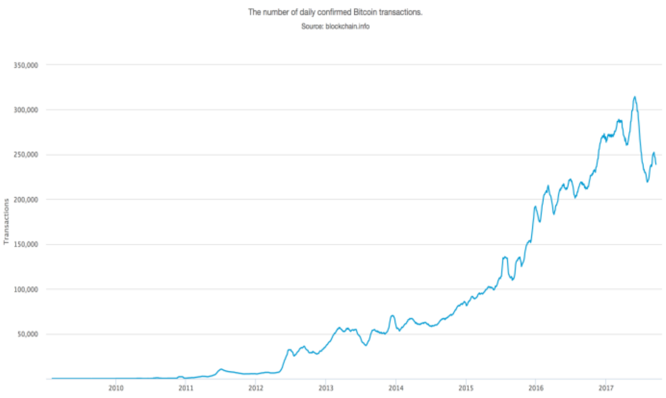
The number of daily confirmed Bitcoin transactions.
Source: blockchain.info

Figure.1. Bitcoin transactions (January 2009–September 2017)

II. FUNDAMENTALS 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. This allows the participants to verify and audit transactions independently and relatively inexpensively. 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. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a value-exchange protocol. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

A. Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bit coin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

B. Block time

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is 10 minutes.

C. Hard forks

A hard fork is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid. In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software. If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur. For example, Ethereum has hard-forked to "make whole" the investors in The DAO, which had been hacked by exploiting vulnerability in its code. In this case, the fork resulted in a split creating Ethereum and Ethereum Classic chains. In 2014 the Nxt community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment. Alternatively, to prevent a permanent split, a majority of nodes using the new software may return to the old rules, as was the case of bit coin split on 12 March 2013.

III. BLOCKCHAIN WORK

The function of a blockchain is straightforward. As it is a peer-to-peer network, a user needs to start a transaction. Once done, a block is allocated to the said transaction. The transaction block is also broadcasted to the network, and all the nodes in the network get the said information. The block is then mined and validated. It is also added to the chain, followed by a successful transaction.

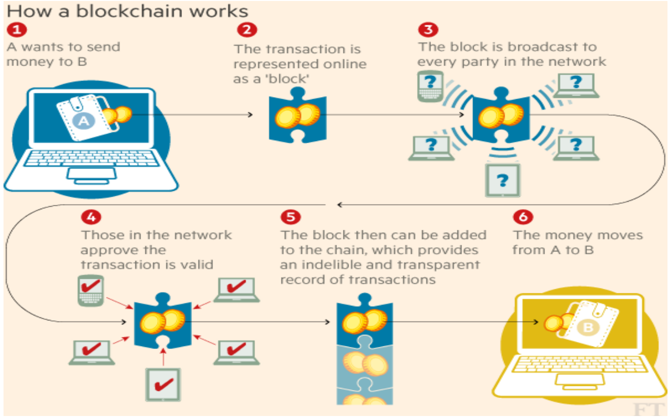
How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent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

Figure. 2. Working of Blockchain

IV. TYPES OF BLOCKCHAINS

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

A. Public blockchains

A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol).Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm. Some of the largest, most known public blockchains are Bitcoin and Ethereum.

Ethereum:

Ethereum is the next step in the blockchain evolution. Created in 2013, it is considered to be Blockchain 2.0 and allows for the running of arbitrary code to complete computational processes, rather than just record transactions. It is a Turing-complete virtual machine, and is runs as a public blockchain. Ether is then the fuel of Ethereum, and it is associated with a wallet and address file that is unique to each account. However each user may have multiple accounts, so although one unique account belongs to a single user, it cannot be known how many other IDs link back to that same user.

B. Private blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks. Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

C. Consortium blockchains

A consortium blockchain is often said to be semi-decentralized. 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.

V. USES

Blockchain technology can be integrated into multiple areas. The primary use of blockchains today is as a distributed ledger for cryptocurrencies, most notably bitcoin. There are a few operational products maturing from proof of concept by late 2016. As of 2016, some observers remain skeptical. Steve Wilson, of Constellation Research, believes the technology has been hyped with unrealistic claims. To mitigate risk, businesses are reluctant to place blockchain at the core of the business structure.

A. Cryptocurrencies

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 which will be headed by David Marcus who previously was in charge of Messenger. According to The Verge Facebook is planning to launch its own cryptocurrency for facilitating payments on the platform.

B. Smart contracts

Blockchain-based smart contracts are proposed contracts that could be partially or fully executed or enforced without human interaction.One of the main objectives of a smart contract is automated escrow. An IMF staff discussion reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general. But "no viable smart contract systems have yet emerged." Due to the lack of widespread use their legal status is unclear.

C. Financial Services

Major portions of the financial industry are implementing distributed ledgers for use in banking, and according to a September 2016 IBM study, this is occurring faster than expected. Banks are interested in this technology because it has potential to speed up back office settlement systems. Banks such as UBS are opening new research labs dedicated to blockchain technology in order to explore how blockchain can be used in financial services to increase efficiency and reduce costs. Berenberg, a German bank, believes that blockchain is an "overhyped technology" that has had a large number of "proofs of concept", but still has major challenges, and very few success stories.

D. Blockchain with video games

Some video games are based on blockchain technology. The first such game, Huntercoin, was released in February, 2014.Another blockchain game is CryptoKitties, launched in November 2017. The game made headlines in December 2017 when a cryptokitty character - an-in game virtual pet - was sold for US$100,000. CryptoKitties illustrated scalability problems for games on Ethereum when it created significant congestion on the Ethereum network with about 30% of all Ethereum transactions being for the game. Cryptokitties also demonstrated how blockchains can be used to catalog game assets (digital assets). The Blockchain Game Alliance was formed in September 2018 to explore alternative uses of blockchains in video gaming with support of Ubisoft and Fig, among others.

E. 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.

In the past when a claim is made, all checks would be carried out by humans, which can be time-consuming and leaves room for human error. This will become unnecessary, as checks to ensure that all criteria have been met, and can be done automatically using the Blockchain. Once all obligations are fulfilled, the resulting payout is automatic. This can all be done using minimum human involvement. One of the solutions offered by Deloitte is the inclusion of a QR-code in a receipt. The QR-code is set to contain all the relevant information regarding the purchase: item, serial number, date of purchase and so on. With it, the QR-code also holds instructions on how to find a ‘warranty bot’ on Facebook Messenger. The user can then send a picture of the receipt to that bot, the engine unwraps the QR-code and stores all the product information on the Blockchain.

F. Other uses

Blockchain technology can be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments to content creators, such as wireless users or musicians. In 2017, IBM partnered with ASCAP and PRS for Music to adopt blockchain technology in music distribution. Imogen Heap's Mycelia service has also been proposed as blockchain-based alternative "that gives artists more control over how their songs and associated data circulate among fans and other musicians." Everledger is one of the inaugural clients of IBM's blockchain-based tracking service. Walmart and IBM are running a trial to use a blockchain-backed system for supply chain monitoring—all nodes of the blockchain are administered by Walmart and are located on the IBM cloud. New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and micro insurance following the adoption of blockchain. The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers. Online voting is another application of the blockchain.

VI. CONCLUSION

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. Read how blockchain provides these benefits to learn more about using blockchain in your industry. There are several ways blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded. After a transaction is approved, it is encrypted and linked to the previous transaction. This, along with the fact that information is stored across a network of computers instead of on a single server, makes it very difficult for hackers to compromise the transaction data. In any industry where protecting sensitive data is crucial—financial services, government, healthcare — blockchain has an opportunity to really change how critical information is shared by helping to prevent fraud and unauthorized activity.

ACKNOWLEDGMENT

The Our thanks to the Computer Department of Vishweshwarayya Abhiyantriki Padvika Mahavidyalay, Almala (India) for their guidance and cooperation.

VII. REFERENCES

[1]. Nir Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017, Available: http://ieeexplore.ieee.org/document/8012302/

[2]. Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017,

[3]. Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.

[4]. Maaruf Ali and Mahdi H Miraz, "Cloud Computing Applications," in Proceedings of the International Conference on Cloud Computing and eGovernance - ICCCEG 2013, Internet City, Dubai, United Arab Emirates, 2013, pp. 1-8, Available: http:// www.edlib.asdf.res.in/2013/iccceg/paper001.pdf

[5]. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[6]. Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

[7]. Raval, Siraj (2016). "What Is a Decentralized Application?". Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1- 4919-2452-5. OCLC 968277125. Retrieved 6 November 2016 – via Google Books.

[8]."Blockchain may finally disrupt payments from Micro payments to credit cards to SWIFT". dailyfintech.com. 2018 -02 -10. Retrieved 2018-11-18.

[9]. Hampton, Nikolai (5 September 2016). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". Computerworld. Archived from the original on 6 September 2016. Retrieved 5 September 2016.

[10]. Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. 3 (2): 99–111. CiteSeerX 10.1.1.46.8740. doi:10.1007/bf00196791.

[11].Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences. 2. pp. 329–334. CiteSeerX 10.1.1. 71.4891. doi:10.1007/978-1-4613-9323-8_24. ISBN 978-1 -461 3-9325-2.

[12]. Nian, Lam Pak; Chuen, David LEE Kuo (2015). "A Light Touch of Regulation for Virtual Currencies". In Chuen, David LEE Kuo. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press. p. 319. ISBN 978-0-12-802351-8.

[13]. Project Bletchley Whitepaper Archived 11 January 2017 at the Wayback Machine, Microsoft, 2016-09-19. Retrieved 2016-12-24.

[14]. Williams, Ann (12 July 2016). "IBM to open first blockchain innovation centre in Singapore, to create applications and grow new markets in finance and trade". The Straits Times. Singapore Press Holdings Ltd. Co. Archived from the original on 14 November 2016. Retrieved 13 November 2016.

[15]. "The future of blockchain in 8 charts". Raconteur. 27 June 2016. Archived from the original on 2 December 2016. Retrieved 3 December2016.

[16]. "Hype Killer- Only 1% of Companies Are Using Blockchain, Gartner Reports| Artificial Lawyer". Artificial Lawyer. 2018 -05-04. Retrieved 2018-05-22.

[17].Armstrong, Stephen (7 November 2016). "Move over Bitcoin, the blockchain is only just getting started". Wired. Archived from the original on 8 November 2016. Retrieved 9 November 2016.

[18]. Catalini, Christian; Gans, Joshua S. (23 November 2016). "Some Simple Economics of the Blockchain". SSRN Electronic Journal. doi:10.2139/ssrn.2874598. SSRN 2874598.

[19]. Tapscott, Don; Tapscott, Alex (8 May 2016). "Here's Why Blockchains Will Change the World". Fortune. Archived from the original on 13 November 2016. Retrieved 16 November 2016.