IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

Blockchain

Taniya Kashinath Bant and Sanjana M. S.
Alva's Institute of Engineering and Technology, Mijar, Moodbidire, India

Abstract: *Blockchain is another innovation with solid ramifications for the eventual fate of how we trade data and money as a comprehensively organized society. It is new to the point that there is moderately minimal scholastic work done on it, yet this is evolving rapidly. For this writing survey, we have started by gathering an example of principally peer-inspected sources, and additionally an educational diagram of articles from different channels. Our determination of articles enables us to give an agent perspective of three essential points. In the first place, a portion of the essential current themes being talked about with respect to blockchain innovation. Second, the agent classifications of said points. Third, the potential fate of blockchain improvement alongside its effect on society and innovation.*

Keywords: Blockchain

I. INTRODUCTION

A blockchain is a growing list of records, called *blocks*, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks. Although blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

The blockchain was popularized by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin, based on work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The identity of Satoshi Nakamoto remains unknown to date. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double- spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain is considered a type of payment rail.

Private blockchains have been proposed for business use. *Computerworld* called the marketing of such privatized blockchains without a proper security model "snake oil"; however, others have argued that permissioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

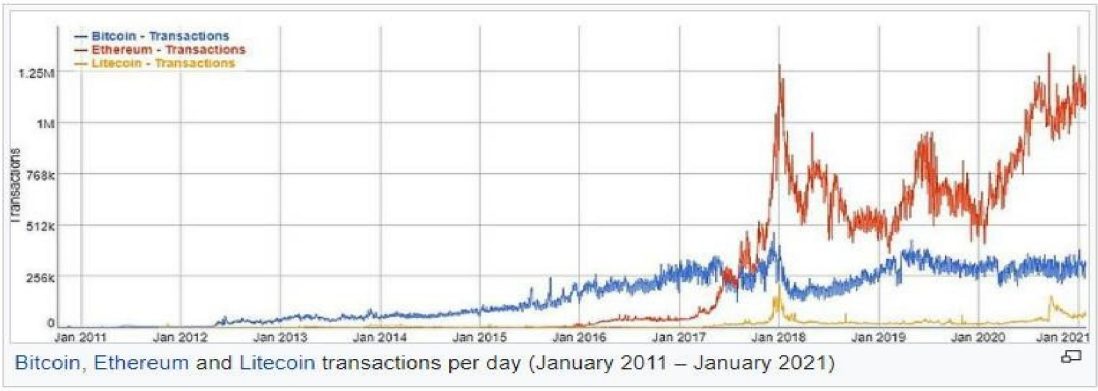
II. HISTORY

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups." Further 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 wherein document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block. Under their company Surety, their document certificate hashes have been published in *The New York Times* every week since 1995.

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 ledger size had exceeded 200 GB by early 2020.

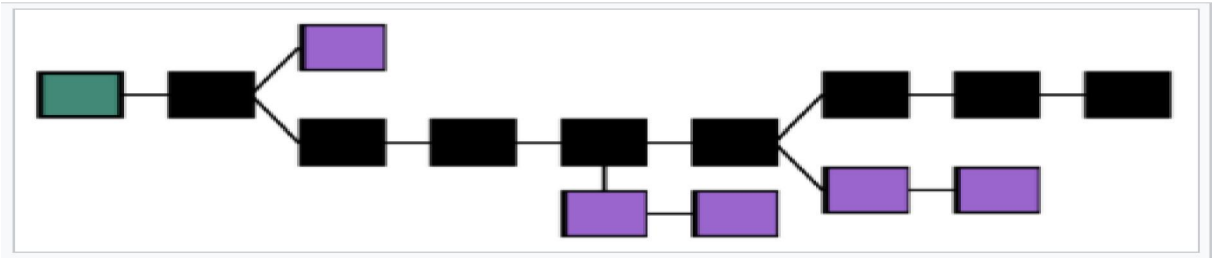
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

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.



III. STRUCTURE

A blockchain is a decentralized, distributed, and oftentimes public, digital ledger consisting of records called *blocks* that are used to record transactions across many computers so that any involved block 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 autonomously using a peer-to-peer network and a distributed timestamping 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.



Logically, a blockchain can be seen as consisting of several layers:

- Infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- Data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

3.1 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 initial block, which is known as the ***genesis block***. To assure the integrity of a block and the data contained in it, the block is usually digitally signed.

3.2 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 on average 10 minutes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

3.3 Decentralization

By storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad hoc message passing and distributed networking. One risk of a lack of decentralization is a so-called "51% attack" where a central entity can gain control of more than half of a network and can manipulate that specific blockchain record at will, allowing double-spending.

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. A *public key* (a long, random-looking string of numbers) is an address on the blockchain.

Value tokens sent across the network are recorded as belonging to that address. A *private key* is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

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

as proof-of-work, to serialize changes. Alternative consensus methods include proof-of-stake. The growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

3.4 Types

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 the bitcoin blockchain and the Ethereum blockchain.

B. Private Blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. To distinguish between open blockchains and other peer-to- peer decentralized database applications that are not open ad-hoc compute clusters, the terminology Distributed Ledger (DLT) is normally used for private blockchains.

C. Hybrid Blockchains

A hybrid blockchain has a combination of centralized and decentralized features. The exact workings of the chain can vary based on which portions of centralization decentralization are used.

D. Sidechains

A sidechain is a designation for a blockchain ledger that runs in parallel to a primary blockchain. Entries from the primary blockchain (where said entries typically represent digital assets) can be linked to and from the sidechain; this allows the sidechain to otherwise operate independently of the primary blockchain (e.g., by using an alternate means of record keeping, alternate consensus algorithm, etc.).

3.5 Uses

Blockchain technology can be integrated into multiple areas. The primary use of blockchains is as a distributed ledger for cryptocurrencies such as bitcoin; there were also a few other operational products that had matured from proof of concept by late 2016. As of 2016, some businesses have been testing the technology and conducting low-level implementation to gauge blockchain's effects on organizational efficiency in their back office.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

Individual use of blockchain technology has also greatly increased since 2016. According to statistics in 2020, there were more than 40 million blockchain wallets in 2020 in comparison to around 10 million blockchain wallets in 2016.

A. Cryptocurrencies

Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. On 8 May 2018 Facebook confirmed that it would open a new blockchain group which would be headed by David Marcus, who previously was in charge of Messenger. Facebook's planned cryptocurrency platform, Libra (now known as Diem), was formally announced on June 18, 2019.

The criminal enterprise Silk Road, which operated on Tor, utilized cryptocurrency for payments, some of which the US federal government has seized through research on the blockchain and forfeiture.

Governments have mixed policies on the legality of their citizens or banks owning cryptocurrencies. China implements blockchain technology in several industries including a national digital currency which launched in 2020. To strengthen their respective currencies, Western governments including the European Union and the United States have initiated similar projects.

B. Smart Contracts

Blockchain-based smart contracts are proposed contracts that can be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is automated escrow. A key feature of smart contracts is that they do not need a trusted third party (such as a trustee) to act as an intermediary between contracting entities - the blockchain network executes the contract on its own. This may reduce friction between entities when transferring value and could subsequently open the door to a higher level of transaction automation. An IMF staff discussion from 2018 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 was unclear.

C. Financial Services

According to *Reason*, many banks have expressed interest in implementing distributed ledgers for use in banking and are cooperating with companies creating private blockchains, and according to a September 2016 IBM study, this is occurring faster than expected.

Banks are interested in this technology not least because it has the potential to speed up back office settlement systems. Moreover, as the blockchain industry has reached early maturity institutional appreciation has grown that it is, practically speaking, the infrastructure of a whole new financial industry, with all the implications which that entails.

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.

The blockchain has also given rise to initial coin offerings (ICOs) as well as a new category of digital asset called security token offerings (STOs), also sometimes referred to as digital security offerings (DSOs).

STO/DSOs may be conducted privately or on public, regulated stock exchange and are used to tokenize traditional assets such as company shares as well as more innovative ones like intellectual property, real estate, art, or individual products. A number of companies are active in this space providing services for compliant tokenization, private STOs, and public STOs.

D. Games

Blockchain technology, such as cryptocurrencies and non-fungible tokens (NFTs), has been used in video games for monetization. Many live-service games offer in-game customization options, such as character skins or other in-game items, which the players can earn and trade with other players using in-game currency. Some games also allow for trading of virtual items using real-world currency, but this may be illegal in some countries where video games are seen as akin to gambling, and has led to gray market issues such as skin gambling, and thus publishers typically have shied

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

away from allowing players to earn real- world funds from games. Blockchain games typically allow players to trade these in-game items for cryptocurrency, which can then be exchanged for money.

The first known game to use blockchain technologies was *Crypto Kitties*, launched in November 2017, where the player would purchase NFTs with Ethereum cryptocurrency, each NFT consisting of a virtual pet that the player could breed with others to create offspring with combined traits as new NFTs. The game made headlines in December 2017 when one virtual pet sold for more than US$100,000. *Crypto Kitties* also illustrated scalability problems for games on Ethereum when it created significant congestion on the Ethereum network in early 2018 with approximately 30% of all Ethereum transactions[*clarification needed*] being for the game.

By the early 2020s, there had not been a breakout success in video games using blockchain, as these games tend to focus on using blockchain for speculation instead of more traditional forms of gameplay, which offers limited appeal to most players. Such games also represent a high risk to investors as their revenues can be difficult to predict. However, limited successes of some games, such as *Axie Infinity* during the COVID-19 pandemic, and corporate plans towards metaverse content, refuse led interest in the area of Game Fi, a term describing the intersection of video games and financing typically backed by blockchain currency, in the second half of 2021. Several major publishers, including Ubisoft, Electronic Arts, and Take Two Interactive, have stated that blockchain and NFT-based games are under serious consideration for their companies in the future.

In October 2021, Valve Corporation banned blockchain games, including those using cryptocurrency and NFTs, from being hosted on its Steam digital storefront service, which is widely used for personal computer gaming, claiming that this was an extension of their policy banning games that offered in-game items with real-world value. Valve's prior history with gambling, specifically skin gambling, was speculated to be a factor in the decision to ban blockchain games. Journalists and players responded positively to Valve's decision as blockchain and NFT games have a reputation for scams and fraud among most PC gamers, Epic Games, which runs the Epic Games Store in competition to Steam, said that they would be open to accepted blockchain games, in the wake of Valve's refusal.

3.6 Supply Chain

There have been several different efforts to employ blockchains in supply chain management.

- **Precious Commodities Mining:** Blockchain technology has been used for tracking the origins of gemstones and other precious commodities. In 2016, *The Wall Street Journal* reported that the blockchain technology company, Ever ledger was partnering with IBM's blockchain-based tracking service to trace the origin of diamonds to ensure that they were ethically mined.[105] As of 2019, the Diamond Trading Company (DTC) has been involved in building a diamond trading supply chain product called Tracer.
- **Food Supply:** As of 2018, Walmart and IBM were running a trial to use a blockchain-backed system for supply chain monitoring for lettuce and spinach — all nodes of the blockchain were administered by Walmart and were located on the IBM cloud.[107] In 2021, scientists from Nosh Technologies and the University of Essex developed a blockchain-based approach named *Food SQR Block* using QR code and cloud computing to digitize food supply chain data to improve traceability of food by the farmers and consumers. Nosh Technologies also developed a blockchain-based multi-layered framework named *Smart Waste* using reinforcement learning- based machine learning to reduce waste in the food supply chain.

3.7 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[116] or musicians. The Gartner 2019 CIO Survey reported 2% of higher education respondents had launched blockchain projects and another 18% were planning academic projects in the next 24 months. 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 a blockchain-based alternative "that gives artists more control over how their songs and associated data circulate among fans and other musicians."
- New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and microinsurance following the adoption of blockchain.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

- The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers. The use of blockchain in libraries is being studied with a grant from the U.S. Institute of Museum and Library Services.
- Other blockchain designs include Hyperledger, a collaborative effort from the Linux Foundation to support blockchain-based distributed ledgers, with projects under this initiative including Hyperledger Burrow (by Monax) and Hyperledger Fabric (spearheaded by IBM). Another is Quorum, a permissionable private blockchain by JPMorgan Chase with private storage, used for contract applications.
- Blockchain is also being used in peer-to-peer energy trading.
- Blockchain could be used in detecting counterfeits by associating unique identifiers to products, documents and shipments, and storing records associated with transactions that cannot be forged or altered. It is however argued that blockchain technology needs to be supplemented with technologies that provide a strong binding between physical objects and blockchain systems.
- The EUIPO established an Anti-Counterfeiting Blockathon Forum, with the objective of "defining, piloting and implementing" an anti-counterfeiting infrastructure at the European level. The Dutch Standardisation organisation NEN uses blockchain together with QR Codes to authenticate certificates.

IV. CONCLUSION AND FUTURE WORK

With blockchain technology possessing such a large appeal, we are already seeing widespread adoption. As nearly every industry utilizes some sort of agile, record keeping practices, it is not unreasonable to expect to see this technology applied to a wide range of applications some of which are hinted at in our previous sections such as the potential for a smart city, while others are either still in development or have yet to be discovered. Furthermore, due to the peer-to-peer nature of the technology this technology and every stakeholder having access to their block of the ledger, cooking the books or falsifying data has never been harder. This alone has the potential to increase consumer confidence in these new technological disruptions. As with any new technology, the underpinnings are not well understood and for that reason it is difficult to say how widely adopted the technology will be. Future research should delve into these topics and new applied applications, as well as study adoption rates of the technology. For those who do adapt blockchain, further study would grant us insights as to what increases (if any) in productivity have been recorded.

Studies may also focus on roadblocks as to why this technology has not been adopted as well as investigate trends in consumer confidence. Additionally, as technology increases, future studies may help shed light on any security issues not initially discovered. With what started as some posted code by an anonymous programmer with a goal of creating a new currency platform, blockchain has skyrocketed in popularity, with nearly every industry from finance and healthcare, all the way to education and city planning. In conclusion, blockchain technology appears to not only improve tasks in current industries, but also hold the potential to revolutionize systems that keep track of the history of artifacts through a vastly improved, transparent ledger system.

REFERENCES

[1]. Ahmed, S., & Broek, N. t. (2017). Food supply: Blockchain could boost food security. (brief article). Nature.
[2]. Chapron, G. (2017). The environment needs cryptogovernance. Nature.
[3]. Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology. Future Internet.
[4]. Huckle, S., & White, M. (2016). Socialism and the blockchain. Future Internet, 8 (4), 49.
[5]. Ishmaev, G. (2017). Blockchain technology as an institution of property. Meta philosophy, 48 (5), 666- 686.
[6]. Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. IEEE Software, 34 (6), 21-27.
[7]. Maxwell, D., Speed, C., & Pschetz, L. (2017). Story blocks: Reimagining narrative through the blockchain. Convergence: The International Journal of Research into New Media Technologies, 23 (1), 79- 97.
[8]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[9]. Pierro, M. D. (2017). What is the blockchain? Computing in Science & Engineering, 19 (5)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, February 2023
Impact Factor: 7.301

[10]. Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2 (1)

[11]. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. New York: Portfolio / Penguin.

[12]. Tranquillini, A. (2016). Blockchain yes, blockchain no: An outsider (non-it expert) view. Journal of Securities Operations & Custody, 8 (4), 287-291.

[13]. Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. Financial Innovation, 2 (1), 1-5.

[14]. Wikipedia, & Contributors. (2018a). Bitcoin — wikipedia, title=Bitcoin & oldid.

[15]. Wikipedia, & Contributors. (2018b). Blockchain — wikipedia, title=Blockchain& oldid.

[16]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? Ă systematic review. PLOS ONE.