IJCAT - International Journal of Computing and Technology, Volume 7, Issue 3, March 2020
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

Blockchain Technology: An Overview and Areas of Application

[1] Afolashade Kuyoro; [2] Deborah Aleburu; [3] Olujimi Alao; [4] Akinniyi Akingbile

[1, 2, 3] Computer Science Department
Babcock University, Ilishan-Remo, Ogun State, Nigeria

[4]Information Technology Development Services Department
Babcock University, Ilishan-Remo, Ogun State, Nigeria

Abstract - Blockchain is considered to be an emerging technology and was introduced through bitcoin. Blockchain can be described as a distributed ledger technology capable of recording safe and continuous transactions between parties. Attempts have been made to adapt the technology to other fields of implementation, outside finance, so that the interesting characteristics of blockchain could benefit other sectors and use cases. Blockchain is now regarded as a general-purpose technology that has discovered applications in various sectors and applications, such as identity management, conflict resolution, contract management, supply chain management, insurance and healthcare, to name a few. This paper presents an overview of blockchain technology and its application areas.

Keywords- Blockchain, Immutability, Transparency, Integrity

1. Introduction

Blockchain can be described as a distributed ledger technology capable of recording safe and continuous transactions between parties. Blockchain fundamentally eliminates the need for intermediaries who were earlier needed to behave as trusted third parties to check, record and coordinate transactions by' sharing' databases between various parties. By enabling the transition from a centralized scheme to a decentralized and distributed system (see Fig 1), blockchain efficiently releases information earlier stored in protected silos [3]. At their basic level, they allow a group of users to record transactions within that group in a shared ledger, so that no transaction can be altered once it is published under the normal operation of the blockchain network.

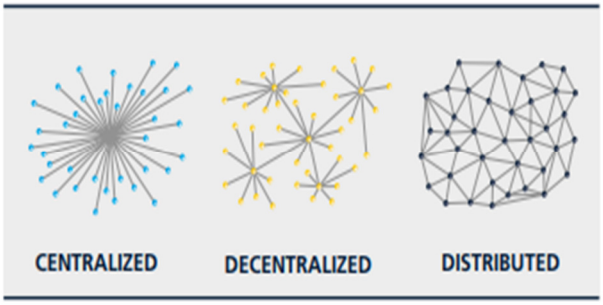

Fig 1: Going from centralized to a decentralized, distributed database using blockchain [3]

In 2008, to generate contemporary crypto currencies, the blockchain concept was merged with several other techniques and computational ideas: digital money protected by cryptographic processes rather than a central repository or power. Blockchain is not a regular database. This means that tables with rows and columns do not exist, rather, a directory of previous activities exists [4]. This paper presents an overview of blockchain technology and its areas of application. It is arranged as follows: Section One presents an introduction to the study, Section Two discusses a brief background of Blockchain technology, chaining of blocks in blockchain is presented in Section Three. Key characteristics and category of blockchain is presented in section four and five respectively, applications of blockchain is presented in section six while conclusion is presented in section seven.

2. Brief Background of Blockchain

In 1991, as an electronic ledger, a signed chain of information was used to digitally sign documents in a way that could easily show that none of the signed documents in the collection had been changed. These ideas were merged and introduced to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System, pseudonymously published by Satoshi Nakamoto, and later in 2009 with the establishment of the Bitcoin blockchain cryptocurrency network. The paper by Nakamoto contained the blueprint

followed by most contemporary cryptocurrency systems (although with differences and changes). Bitcoin was the first of many applications for blockchain [4]. Its main advantage was to allow direct user-to-user transactions without the need for a trusted third party. It also allowed those users who manage to post fresh blocks and keep copies of the ledger to issue fresh cryptocurrency in a specified way; such users are called miners in Bitcoin. The miners ' automated payment allowed the system to be distributed without the need to organize. A blockchain and consensus-based maintenance mechanism were developed to ensure that only valid transactions and blocks were added to the blockchain [4]. Other technologies for blockchain 1.0 include Monero, Dash and Litecoin, to name just a few.

The introduction of intelligent characteristics and smart contracts is connected with the second generation of blockchain technology (blockchain 2.0). The intelligent properties are those digital properties or assets whose property can be governed by a blockchain-based platform, whereas smart contracts are software programs that encode the guidelines of how intelligent properties are controlled and managed. Ethereum, Ethereum Classic, NEO and QTUM are examples of blockchain 2.0 cryptocurrencies.

Building on the above, blockchain technology's third generation (blockchain 3.0) is now involved with blockchain's non-financial applications. To this end, attempts were made to adapt the technology to other fields of implementation, outside finance, so that the interesting characteristics of blockchain could benefit other sectors and use cases. Consequently, blockchain is now regarded as a general-purpose technology that has discovered applications in various sectors and applications, such as identity management, conflict resolution, contract management, supply chain management, insurance and healthcare, to name a few [2].

3. Chaining Blocks

Block chaining is accomplished through another primitive cryptography involving the use of hash functions. A hash function takes an arbitrary length message and crunches it into a set length hash output called a digest message or a digital fingerprint. An intriguing hash function property is that it is collision-resistant, i.e. the same hash output will not be produced by two distinct messages. This property is the foundation of the chaining of blocks. The hash of the prior block header is included in the fresh block header to chain a fresh block to the blockchain. The last block in the blockchain thus contains the fingerprint of the transactions in the preceding block, which in turn contains the fingerprint of the transactions in the preceding block, etc. [2].

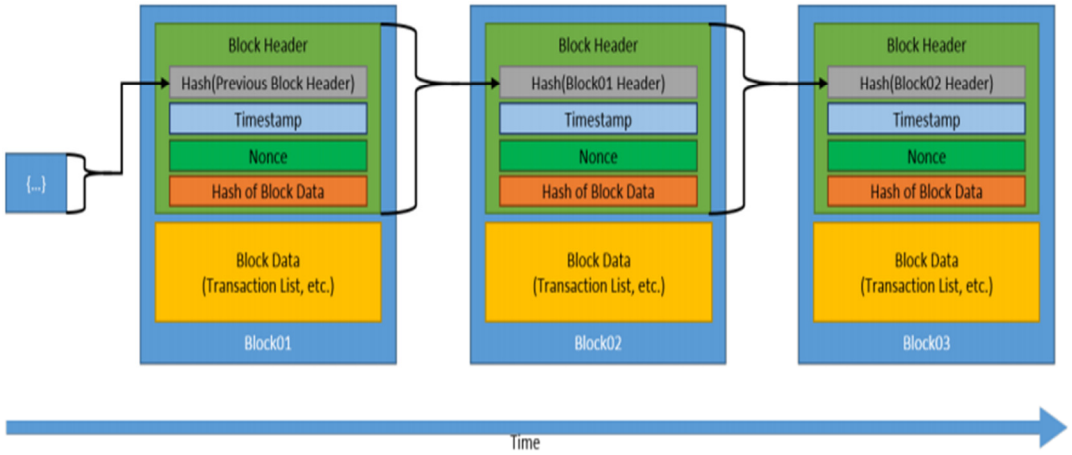

Fig 2: Generic Chain of Blocks[2]

A streamlined instance of how blocks are linked into a blockchain is shown in Fig 2. Note that there is a header and a number of transactions in each block. The transactions in a block are hashed to produce a fixed-length hash output that is appended to the header of the block. After the first block has been created, each subsequent legitimate block must contain the prior block header's hash output. The hash of the prior block header contained in each block serves as the chain that connects each valid block to the preceding ones. Thus, a chain of blocks (blockchain) is created by connecting each block with the past blocks.

4. Key Characteristics of Blockchain Technology

Decentralized: It is a network-connected database system with open access control. The information on various devices can be accessed, tracked, stored and updated.

Transparent: Blockchain information recorded and stored is transparent to prospective customers, which can be readily updated further. Blockchain's transparent nature could definitely avoid altering or stolen information.

Immutable: Once stored, the records become permanently reserved and cannot be easily modified without controlling more than 51 percent of the node at the same time.

Autonomy: The blockchain system is independent and autonomous, which means that each node on the blockchain system can safely access, transfer, store and update the data, making it reliable and free from any external interference.

Open Source: The blockchain technology is developed in a manner that offers open-source access to all network linked. This inimitable versatility enables anyone not only to openly inspect the documents, but also to create multiple applications that are imminent.

Anonymity: As information transfer takes place between node and node, the individual's identity stays anonymous, making it a safer and more reliable system.

5. Blockchain Categorization

Blockchain networks can be classified based on their model of permission, which determines who can manage them (e.g. publish blocks).

5.1 Permissionless blockchain

Permissionless blockchain networks are decentralized ledger platforms that are accessible to anyone who publishes blocks without any authority's consent. Any user of the blockchain network can read and write to the ledger within a permissionless blockchain network. Allowable blockchain networks frequently use a multiparty contract or ' consensus ' scheme that needs customers to spend or retain funds when trying to post blocks [4].

5.2 Permissioned blockchain

Permissioned blockchain networks are those where some power (whether centralized or decentralized) must authorize users to publish blocks. Because only approved customers maintain the blockchain, read access can be restricted and who can issue transactions can be restricted.

Accordingly, permissioned blockchain networks can allow anyone to read the blockchain or limit read access to approved persons. They can also allow anyone to include transactions in the blockchain or, again, limit that access only to authorized people [4].
A permitted blockchain may also be classified as a Blockchain private or consortium. The difference between Blockchain private and consortium is based on the amount if nodes are allowed to be miners. It is more appropriately referred to as private blockchain if only one node is allowed to be a miner. Consortium blockchain is one that allows two or more nodes to participate in the mining process, but the blockchain network remains allowed in the sense that only approved consumers can be part of the network [2].

6. Applications of Blockchain

The following are some of the areas in which blockchain has been/can be used amongst many others:

6.1 Digital Identities

About one-sixth of the world's population is unable to engage in political, economic and social life because they lack the most basic information which is documented evidence of their existence. Blockchain technology offers a huge opportunity to solve this challenge by developing cryptographically secure digital identity systems. Governments and NGOs can use digital identity to provide a variety of citizen services and eliminate certificates forgery and identity theft [3].

ID2020, a United Nations-affiliated organization, aims to provide people with proof of identity who are without an official form of identification. ID2020 basically uses blockchain technology to provide global IDs–its system allows registered users to control their personal data to share access and adequate information without worrying about the use or loss of paper documentation. Blockchain allows system security and promotes trusted transactions, enabling people with digital IDs to access a variety of activities such as education, health care, voting, banking, housing, and other social benefits [1].

6.2 Retail

Retailers and consumer goods producers use blockchain technology to drive honest and responsible business. For instance, by offering more data on how each item was manufactured, it empowers customers, especially by defining whether a product was sourced in an ethical and sustainable manner.

In the United Kingdom, fashion designer Martine Jarlgaard is working on a pilot program with Provenance and other associates to make fashion supply chains completely transparent. This solution promotes and allows customers and distributors to purchase products from fashion supply chains where each stakeholder follows ethical and sustainable business procedures. Users can scan their QR code or NFC-enabled label with a smartphone app to look up the supply chain history of a garment on the blockchain-based scheme. Provenance is now working towards an open traceability protocol, building on this effective pilot program. This would enable anyone to monitor the location of origin for anything, from coffee beans to a fabric roll, and hopefully speed up the motion towards sustainable usage [3].

Everledger in the UK is another instance of ethical sourcing. Everledger is creating a blockchain-based scheme to provide evidence of origin and ethical sourcing for valuable products such as diamonds, wine, and even fine art. It utilizes blockchain to store millions of valuable products with a digital record. For diamonds, this scheme would substitute the faulty paper-based certification method that diamond providers, intermediaries, and buyers are presently using. This digital thumbprint includes unique identifiers consisting of over 40 metadata points, the four Cs (colour, clarity, cut, and carat weight) of the diamond, as well as the certificate number that can be laser-inscribed on the physical diamond if necessary. This thumbprint is then produced visible and stored on the blockchain-based scheme with all respondents [5].

6.3 Automotive and Manufacturing

Some of the excitement surrounding blockchain technology is related to its implementation in digital twins in the automotive and manufacturing sectors. A digital twin is a dynamic, digital representation of a physical asset that allows businesses to track their past, present, and future performance throughout the life cycle of the asset. The asset sends performance information and occurrences straight to its digital twin, for instance a car or spare parts, even as it passes from the manufacturer's hands to the distributor and eventually to the new owner. Blockchain can be used to document all associated assets safely.

Groupe Renault is experimenting with storing on a blockchain-based system the digital twin of its vehicles that would provide a single source of truth for the maintenance data of each vehicle. The company released a prototype in July 2017, which was created in collaboration with Microsoft and VISEO–using blockchain to connect the maintenance events of each new vehicle to the digital twin of the vehicle. For authorized parties such as the vehicle owner, this data is fully traceable and visible. Since the digital twin is fully transferable on the blockchain-based system, the maintenance history of each vehicle remains connected to the vehicle even when vehicle ownership changes – a very useful and practical data management service that car manufacturers can provide to their clients [3].

6.4 Energy – Eliminating Marketplace Inefficiencies

Many uses for blockchain technology are likely to be found in the energy industry. Transformation examples include enabling self-managing utility grids to operate and facilitating peer-to-peer exchanges of energy–individual households could sell their neighbors surplus energy (self-generated by solar panels). Furthermore, there are many near-term examples of process improvements that could help energy businesses run more efficiently and save money.

Power Ledger, an Australian startup, created a local marketplace for the sale of renewable energy surpluses through cryptocurrencies (see Fig 3 below).

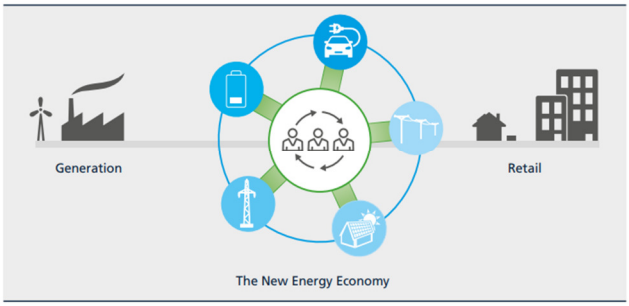

Fig 3: New energy market places based on blockchain [3]

The blockchain-based system allows the sale of excess energy produced in residential and business developments connected to existing or microgrid

electricity distribution networks. This enables owners of renewable energy assets to decide who they want to sell their surplus energy to and at what price, and enables each electricity unit to be tracked securely from the stage of generation to the point of usage.

6.5 Blockchain in Logistics

Logistics is often regarded the backbone of the modern world, with the international shipping industry performing an estimated 90 percent of world trade annually [8]. But the logistics behind international trade is extremely complicated as it often includes many parties with competing interests and priorities as well as using various technologies to monitor shipments. Consequently, achieving new trade logistics efficiencies is likely to have a major effect on the global economy. Blockchain technology can help ease many of the global trade logistics frictions including procurement, transportation management, tracking and tracking, customs collaboration, and trading finance.

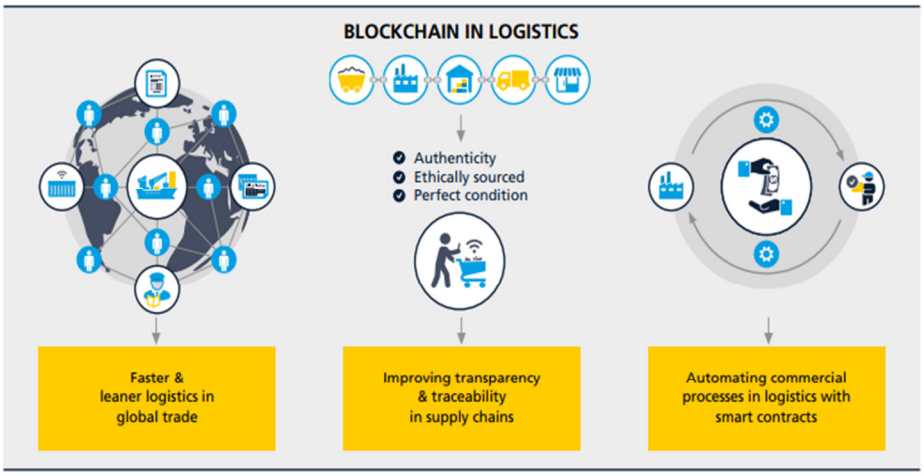

Fig 4: Key blockchain use cases in logistics [3]

With more than 50,000 merchant vessels engaged in the worldwide shipping industry and various customs governing freight transit, ocean freight is a significant focus for efficiency gains. Blockchain technology has enormous potential to optimize costs as well as time connected with trade paperwork and administrative processing for shipments of ocean freight. One instance of the complexities of ocean freight today is the estimation that a easy shipment of refrigerated products from East Africa to Europe can pass through almost 30 individuals and organizations with more than 200 distinct interactions and communications between these parties [6].

Maersk and IBM have begun a project to set up a worldwide blockchain-based scheme for digitizing trade workflows and end-to-end shipment monitoring to unlock effectiveness in ocean freight. The scheme enables each supply chain stakeholder to view goods ' progress via the supply chain, knowing when a container is in motion. Stakeholders can also see customs documents status and view lading bills and other information. For this documentation, Blockchain technology guarantees safe information exchange and a manipulator-proof repository. The two businesses expect tens of millions of shipping containers to monitor this solution annually. It has the ability to decrease delays and fraud considerably, which could lead to savings in the logistics industry in billions of dollars [6].

6.6 Improving Transparency and Traceability in Supply Chains

Many initiatives use blockchain technology to enhance transparency in the supply chain and monitor provenance. These projects collect data on how products are produced, where they come from, and how they are handled; this information is kept in the system based on blockchain. This implies the information becomes permanent and easy to share, offering supply chain players greater track-and-trace capacities than ever before. For instance, companies can use this data to provide evidence of legitimacy for products in pharmaceutical shipments and evidence of luxury goods authenticity. These initiatives also provide consumer benefits – people can learn more about the products they buy, for instance, if a product has been obtained ethically, is an original item and has it been stored under the right conditions [3].

Companies such as Unilever and Wal-Mart are investigating the use of blockchain technology in the consumer goods and retail industry to enhance transparency in the supply chain and track provenance. In particular, Wal-Mart focuses on food monitoring, traceability and safety (see Fig 5 below).

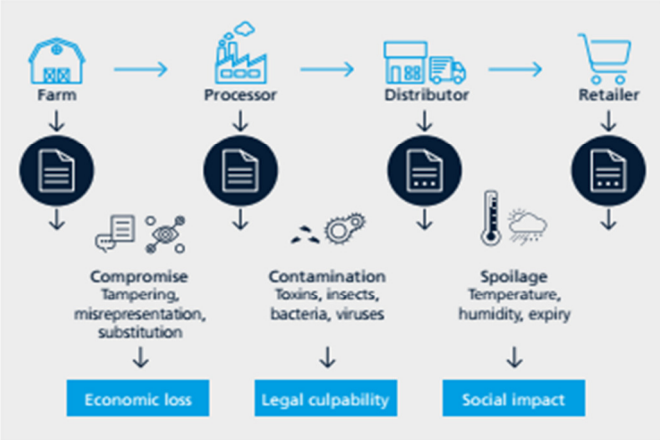

Fig 5: Using blockchain to increase safety and reveal product provenance in food supply chains [3]

6.7 Fighting Counterfeit Pharmaceutical Goods through Blockchain

A main implementation is the use of blockchain technology to tackle today's world's main challenge: drug counterfeiting and fake medicines. According to Interpol, about 1 million individuals die each year from falsified medicines, 50% of pharmaceutical goods sold through rogue websites are deemed falsified, and up to 30% of pharmaceutical goods sold in developing markets are falsified [9]. DHL and Accenture are conducting a blockchain-based serialization project to provide the pharmaceutical industry with advanced track-and-trace functionality (see Fig 6 below).

Fig 6: Blockchain to ensure product integrity [3]

Pharmaceutical serialization is the mechanism of allocating to each sealable unit a unique identity (e.g., a serial number), that is then connected to key information about the origin, batch number, and expiry date of the product. Serialization efficiently allows a device to be tracked at nearly any time and traced at any point of its lifecycle to its place. A main serialization challenge is to maintain traceability and transparency, particularly when these units are repackaged or aggregated for logistics reasons from unit to case to pallet and then disaggregated back to consumption unit level. To overcome this and other challenges, the DHL / Accenture proof-of-concept was established by demonstrating the efficacy of blockchain technology in product verification. The objective is to demonstrate that pharmaceutical products have come from legitimate producers, are not falsified, and have been treated properly from origin to customer throughout their trip.

Most remarkably, this initiative demonstrates how end clients can check pharmaceutical products legitimacy and integrity, particularly compliance with handling demands. This does not only convinces the end client that their medications are real and in ideal condition at the stage of purchase, but it also has possibly life-saving consequences. To accomplish this, the partners set up a blockchain-based track-and-trace serialization prototype consisting of a worldwide node network across six geographies. The system fully records every step a pharmaceutical product takes to the shop shelf and ultimately the consumer (see Fig 7 below) [3].

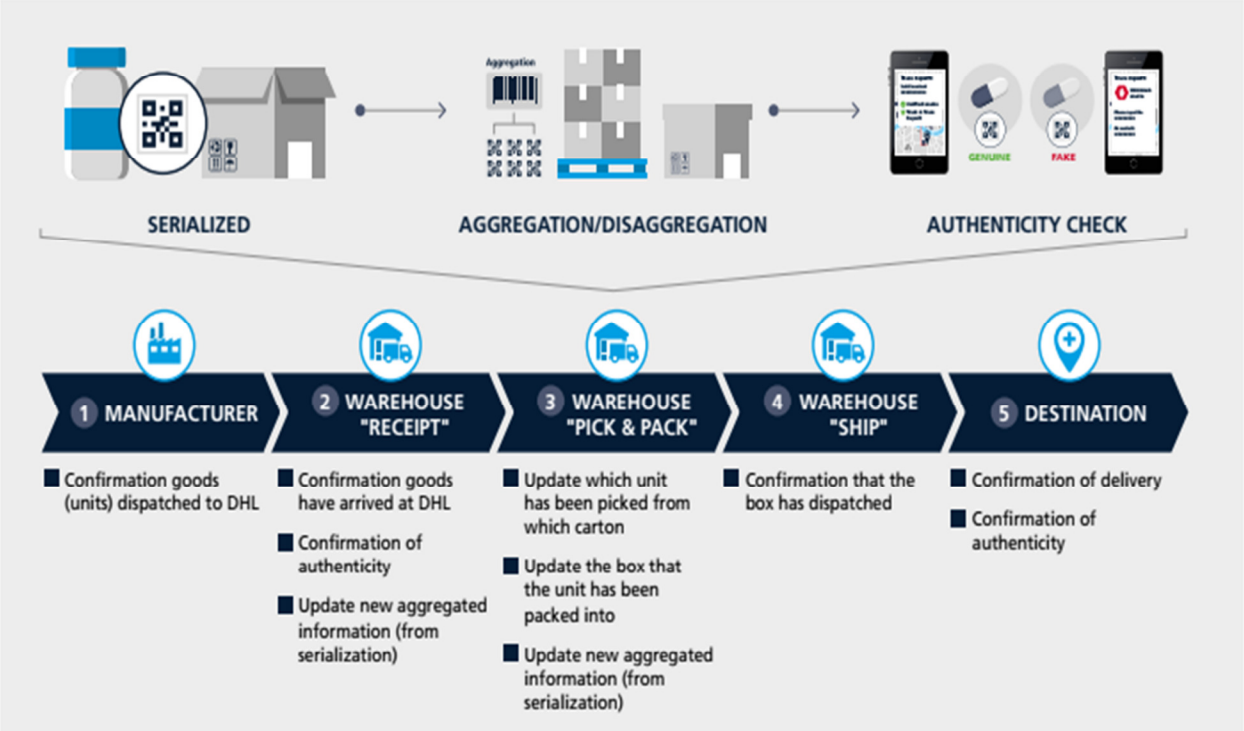

Fig 7: Example of how a blockchain-based track and trace system can be used to monitor pharmaceutical goods from the manufacturer to the user [3]

The prototype was a simulation of laboratory efficiency showing how blockchain technology was able to manage quantities of more than 7 billion unique pharmaceutical serial numbers and more than= 1,500 transactions per second. The project demonstrated how blockchain can be used to gather all logistics operations related to a drug product–from manufacturing to purchasing –and guarantee that this data is made safe, transparent and accessible instantly.

6.8 Blockchain for Health Care

Decentralization is a significant characteristic of blockchain that obviously benefits healthcare apps, making it possible to implement distributed healthcare apps that do not depend on a centralized authority. In addition, the fact that the information in the blockchain is duplicated among all the nodes in the network creates an environment of transparency and openness that allows healthcare stakeholders, and patients in particular, to understand how their data is used, by whom, when and how. More importantly, altering any one node in the blockchain network does not affect the ledger's status as the information in the ledger is reproduced between several nodes in the network. Hence, by its design, blockchain can safeguard health information from future information loss, bribery or safety assaults, such as the attack against ransomware [2].

Furthermore, blockchain's immutability property, which makes it impossible to change or alter any record attached to the blockchain, is very well aligned with the requirements for storing health care records— it is very important to ensure the integrity and validity of health records for patients. Moreover, the use of cryptographic algorithms to encrypt the data stored on the blockchain guarantees that they can only be decrypted by users who have legitimate data access permissions, thereby enhancing data security and privacy. In addition, since the identities of clients in a blockchain are pseudonymized by using cryptographic keys, patient health information can be shared among health care stakeholders without exposing patient identities. Blockchain also promotes smart contracts that can be used to program guidelines that enable patients to regulate how they share or use their health records [2].

7. Conclusion

Through its key characteristics such as decentralization, immutability, persistence and auditability, blockchain technology has shown that it has the potential of

transforming various industrial sectors. This paper presented an overview of blockchain technology, its characteristics and areas of applications. In the first section, an introduction to the paper was presented, background of blockchain was briefly discussed in section two, section three discussed the method of chaining the blocks together in blockchain technology. The key characteristics and categories of blockchain was presented in section four and five respectively. Finally, the areas in which blockchain has been/can be applied was presented in section six while conclusion is presented in section seven.

References

[1] Accenture (2017). Accenture, Microsoft Create Blockchain Solution to Support ID2020 | Accenture Newsroom. Retrieved from https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm

[2] C. Agbo, Q. Mahmoud, and J. Eklund. Blockchain Technology in Healthcare: A Systematic Review. Healthcare, Vol7 No2 , 2019

[3] DHL Trend Research (2018). Blockchain in Logistics: Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. Retrieved from https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

[4] D. Yaga, P. Mell, N. Roby, & K. Scarfone. (2018). Blockchain technology overview. National Institute of Standards and Technology: U.S. Department of Commerce.

[5] Gutierrez, C., & Khizhniak, A. (2017). A Close Look at Everledger—How Blockchain Secures Luxury Goods. Retrieved https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/

[6] IBM (2017a). Maersk and IBM Unveil Supply Chain Solution on Blockchain. Retrieved from: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss

[7] IBM (2017b). China Food Safety Efforts Welcome New Collborators. Retrieved from: https://www-03.ibm.com/press/us/en/pressrelease/53487.wss

[8] ICS (2017). ICS | Shipping and World Trade. Retrieved September 9, 2019, from Ics-shipping.org website: https://www.ics-shipping.org/shipping-facts/shipping-and-world-trade

[9] N. Southwick (2017). Counterfeit Drugs Kill 1 Mn People Annually: Interpol. Retrieved from: https://www.insightcrime.org/news/brief/counterfeit-drugs-kill-1-million-annually-interpol/