WORLD JOURNAL OF PHARMACEUTICAL RESEARCH
SJIF Impact Factor 8.084
Volume 10, Issue 1, 526-546. Review Article ISSN 2277– 7105

BLOCKCHAIN TECHNOLOGY FOR COUNTERFIT DRUGS

Ramaish*, Dr. Hemraj Vashist and Shivani Dogra

Department of Pharmacy, LR Institute of Pharmacy Solan H.P. 173223.

Article Received on
03 Nov. 2020,

Revised on 24 Nov. 2020,
Accepted on 14 Dec. 2020

DOI: 10.20959/wjpr20211-19458

***Corresponding Author**
Ramaish
Assistant Professor, LR Institute of Pharmacy Solan H.P. 173223.

ABSTRACT

Pharmaceutical Research & Development is a complex process that takes several years from drug discovery to drug development and regulatory approval. When all the method is done and a standard item is created, the following challenge for producers is to provide the item to the aiming client in its unique shape and to guarantee that the client gets the honest to goodness item that's created by the true blue producer, not by counterfeiter. But the current Supply Chain Management (SCM) framework of pharmaceutical industry is obsolete and doesn't give perceivability and control for producers and administrative specialist over drugs dispersion and it not withstand the 21st century cyber-security threats. In this study the use of blockchain technology in healthsupervision is explained and pointed out the issues in current pharmaceutical supply chain management and explained how blockchain can be used to add traceability and visibility to drugs supply and overcome the issue of counterfeiting. How the identity mechanism of blockchain works and how is it helpful to exchange medical data while keeping the patient's private data secrete is explained. We highlight the possible techniques, blockchain types and third-party solutions that can be used to implement a blockchain base supply chain for pharmaceuticals. In the last we explained the working of the suggested organization with an example that shows how the organization will be easily used by different participants. Theblockchain technology have great potential in creating secure and effective healthsupervision ecoorganizations with its inherent unique properties. Overall, blockchain has a wide range of possibilities in healthsupervision, which invites many research opportunities in this space.

KEYWORDS: Blockchain, Counterfit drugs, Cyber Threat, Hash Value, Suppply Chain, Cryptography.

1. INTRODUCTION

Pharmaceutical Research & Development is a complex process that takes several years from drug discovery to drug development and regulatory approval. When all the method is done and a standard item is created, the following challenge for producers is to provide the item to the aiming client in its unique shape and to guarantee that the client gets the honest to goodness item that's created by the true blue producer, not by counterfeiter. But the current Supply Chain Management (SCM) framework of pharmaceutical industry is obsolete and doesn't give perceivability and control for producers and administrative specialist over drugs dispersion and it not withstand the 21st century cyber-security dangers circumstance of SCM leads to the generation, dispersion, and utilization of fake drugs. Counterfeit pills have created an especially hazardous public fitness danger and increasingly acute worldwide difficulty particularly in developing countries.[1]

These counterfeit drugs directly and indirectly adversely affect health. Indirectly, these drugs do now not contain the dosage or energetic agent required to kill the disease, that sooner or later purpose drug-resistant strains, and then even the use of the original tablets are useless. More directly, such counterfeits may incorporate active ingredients, but the amount is too low or too high, or produced in an impure manner that incorporate poisonous ingredients, in this case it can cause very serious health problems.[1] Counterfeit pills producers every so often use the brand brand of official producers and make fake products used in daily life, that's less harmful. But in many cases, they have an effect on the pills for the remedy of cancer, painkillers, cardiovascular disorders, antibiotics, contraceptives and different prescription drugs, that can lead to very serious results. Estimates of the numbers of counterfeit prescribed drugs change from 10 to 15 percentage of the world drug supply.30% of the drugs sold in creating nations are counterfeit.[2]

WHO estimates that of the 1 million passings that happen each year due to jungle fever, 0.2 million of them are the result of fake anti-malarial drugs.[3] Fake drugs for tuberculosis and jungle fever slaughter 0.7 million individuals each year1. Forging is maybe one of the most seasoned and most profitable businesses, but the progression in innovation have much encouraged the commerce of forgers, that's why FBI calls forging the wrongdoing of the 21st century, since generation and dispersion of forged merchandise is expanded, and they can be created in a huge amount in brief sum of time.[4] Agreeing to the International Anti-Counterfeiting Coalition (IACC), falsifying has gotten to be one of world's biggest and quick

developing criminal commerce, with an evaluated esteem of more than US$ 600 billion annually.[4]

For the prevention of counterfeit drugs, pharmaceutical industry wants an environment friendly grant chain management organization, and the exceptional available answer to enhance a ideal SCM organization is the Blockchain technology. Blockchain could be a disperse record framework (firstly presented by a nom de plume Satoshi Nakamoto in 2008)[5] that has appeared far reaching flexibility in later a long time and an assortment of advertise divisions looked for ways of joining its capacities into their operations. In spite of the fact that, so distant most of the center has been on the money related administrations industry, but presently ventures in other service-related zones, such as healthsupervision, vitality and lawful firms moreover begun utilizing this wonder. Supply chain security is one viewpoint that has as of late won consideration. Any item subject to a delicate generation handle and widespread reputational issues are related with the ultimate item, the benefits of Blockchain are apparent. Blockchain is the leading fit in those scenarios where protection security and information security are the most noteworthy need. Therefore, pharmaceutical supply chain presents a further use of Blockchain technology.

2. PURPOSE

Whereas looking at the issues the pharmaceutical industry needs an upgraded supply chain framework. The reason of the modern framework is to join the highlights of blockchain innovation and include traceability, and security to the drugs supply chain, and to supply perceivability to producers and drugs administrative specialist of the SCM organization.[6] In such scenarios where we require information security and information availability both at the same time blockchaintechnology is the leading choice. Every time an item changes hands, the replace can be archived to form a changeless history of an item, from make to deal. This will drastically decrease time delays, costs, and human blunder that happens in replaces nowadays. The purpose and elements of the blockchain based SCM device for pharmaceutical industry are summarized as follows.

- **To Increase Trust and Transparency** – Producer and clients being able to track pharmaceutical items all through the supply chain, they will believe each other. Producers will be able to see that the items they need to convey is securely gotten by the expecting client. On the other hand, client will be able to see that the item he needs to purchase is created by a true legiimate producer, and he got it in its unique form.

- **Traceability** –Once the producer produces an item, he will enlist it on the blockchain, and here after the drugs will be followed, followed and verified at each arrange of their travel. As the drugs proprietorship alter physically, its possession will be replaced at the same time on the blockchain technology. Drugs manufacturers can be able to see the journey of their products at any of time, from manufacturing to packagers, and from packagers to distributers.
- **Add Visibility and Protect Privacy** - Visibility and privacy are mostly opposite to each other and to obtain one we might lose the other. Blockchain is the leading technology for the trade-off that can guaranty to confirm the originality of a chunk of information that's made accessible freely whereas keeping the private information of a substance discharge and without any compromise on security. In a pharmaceutical supply chain framework, the items will be irrefutable without any data around the producers discharge procedures. On the other hand, the patient's therapeutic record will be open to distinctive members on the organize without knowing the private information of the quiet.
- **Extended Security** – Blockchain is considered as one of the foremost secured record frameworks on the planet. Blockchain is an unchanging database and the data once put away on it, it not be deleted or adjusted. Within the proposed organization, a permissioned blockchain will be utilized that's more secure at that point the open blockchain, in which as it were authentic members will be allowed benefits to thrust information to the blockchain.
- **Database for Future Statistics** –The impact of drugs on persistent will be recorded, that record will be modest bunch for specialist to recommend dosage to an understanding in future. Utilizing routine databases, this sort of record keeping was not secure, and patient's protection was at hazard, but utilizing blockchain, patient's information can be put away without sharing his private record.[6]

HISTORY OF BLOCKCHAIN

Blockchain was designed by an individual (or bunch of people) utilizing the title Satoshi Nakamoto in 2008 to serve as the open replace record of the cryptocurrency bitcoin.[5] The character of Satoshi Nakamoto is obscure. The innovation of the blockchain for bitcoin made it the primary computerized money to unravel the double-spending issue without the require of a trusted specialist or central server. The bitcoin plan has motivated other applications, and blockchains that are clear by the open are broadly utilized by cryptocurrencies. Blockchain is considered a sort of installment rail. Private blockchains have been proposed for commerce

utilize. A blockchain is basically a dispersed database of records or open record of all replaces or advanced occasions that have been executed and exchanged among partaking parties. Each replace within the open record is confirmed by agreement of most of the members within the framework. And, once entered, data can never be deleted. The blockchain contains a certain and irrefutable record of each single replace ever made. To utilize an essential sameity, it is simple to take a cookie from a cookie jostle, kept in a disengaged put than taking the cookie from a cookie bump kept in a commercial center, being watched by thousands of people.

3. BLOCKCHAIN TECHNOLOGY

A blockchain, could be a developing list of records, called blocks, that are connected utilizing cryptography and these block contains a cryptographic hash of the past block, and timestamp, and information.

By design, a blockchain is safe to adjustment of the information. It is "an open, disseminated record that can record replaces amoung two parties proficiently and in an unquestionable and changeless way". For utilize as a conveyed record, a blockchain is regularly overseen by a peer-to-peer organize collectively following to a convention for inter-node communication and approving modern blocks.[5] Once recorded, the information in any given square not be modified retroactively without change of all ensuing squares, which needs agreement of the arrange lion's exchange. In spite of the fact that blockchain records are not unalterable, blockchains may be considered secure by plan and represent a conveyed computing framework with tall Byzantine blame resistance. Decentralized agreement has subsequently been claimed with a blockchain.

3.1 CENTRALIZED VERSUS DISTRIBUTED LEDGER

Data entered onto the blockchain are "hashed", i.e. converted into a latest digital string of a exact length using a mathematical function, and encrypted to ensure data integrity, prevent forgery, and guarantee that the information was created and sent by the declare sender and was not changed in transit.[7] If the sender of the information does not wish other participants in the network to see the content of the message itself, i.e. the plaintext data contained in the documents submitted, sender can choose to encrypt the message itself, thereby rendering the data unintelligible to individuals without authorized access.

Once validated, information is save in "blocks" that are then "chained" to each other in chronological order using cryptographic techniques. Data, once added to a blockchain, are time-stamped and near impossible to modify the data. However, while blockchains can help prevent fraud on the ledger, the tamper resistance of the technology not prevent false information from being put into the ledger.

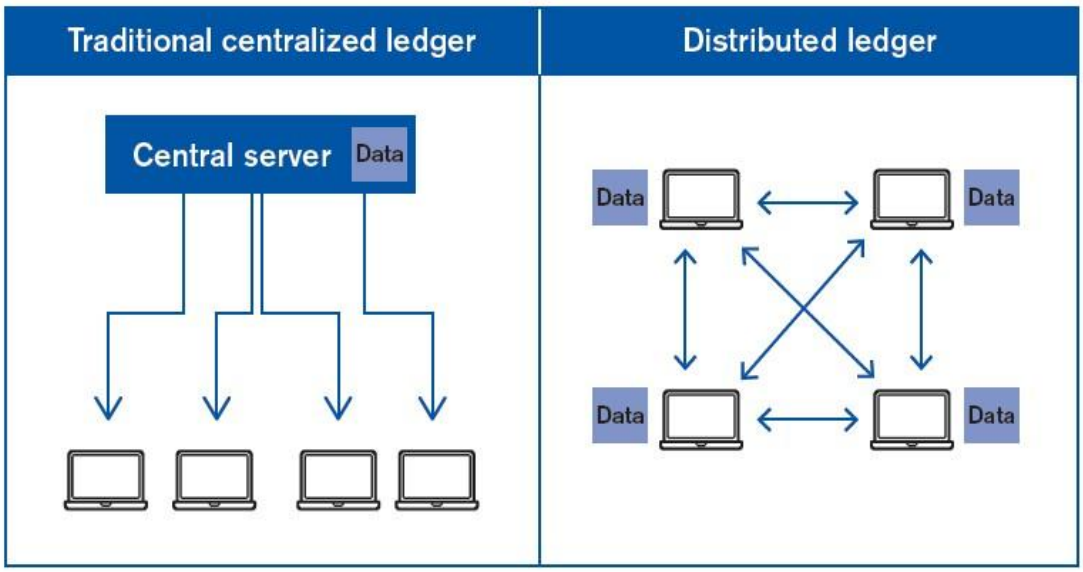

Figure 1: Centralized versus distributed ledger.[7]

In a blockchain, each peer keeps a complete copy of the information (or as close to it as possible), and updates are exchanged with all participants simultaneously. Components in a blockchain therefore all have access to the same information at any time. In other words, a blockchain is a exchanged and trusted ledger that all participants can access and check at any time, but that no single party can control (unless it is fully private – see next section), which allows people with no particular trust in each other to collaborate without relying on trusted intermediaries.[7]

As data are replicated as many times as there are nodes, falsifying data or compromising the whole network would require compromising a large number of nodes, which would be difficult in practice, although not impossible. In theory, a blockchain network can be compromised if a validator or pool of validators control more than 50 per cent of the network's computing power, which is called a "51 per cent attack". While the 51 per cent attack is a problem common to all types of blockchains, it is particularly dengrous in the case of public blockchains, given the difficulty of determining who is effectively validates blocks.

A particular feature of public blockchains is the considerable quantity of computational power that most of them require to validate informations, in particular those using the Proof of Work consensus mechanism, such as Bitcoinin spite of the fact that inefficient in terms of vitality cost, Verification of Work is required to guarantee the security of the agreement prepare. It makes the open blockchain scientifically exceptionally difficult to hack as the fetched of hacking gets to be as well tall for a framework where each hub associated is synchronized with the whole blockchain arrange. Hence, although hacking the framework isn't outlandish, it is financially wasteful and essentially amazingly difficult... However, computing power capacity is increasingly being aggregated. The 51 per cent vulnerability is, to date, still subject to heated debates regarding the severity of its potential consequences.

3.2 TYPES OF BLOCKCHAINS

Behind the simple and catchy term of "Blockchain", there are various different dummy that change in terms of the degree of decentralization and access, the identity of participants, the consensus mechanism, speed, level of privacy, energy consumption, fees and scalability. Blockchains are often classified as public versus private. Under the private blockchain there is a sub-type called consortium or federated blockchain, sometimes considered as a type of blockchain in its own right. Another commonly used classification of blockchain applications is permission less versus permissioned platforms, i.e. the extent to which access to the platform is restricted – or not – to those with permission. These two classifications are sometimes conflated, and it is not uncommon for people to associate public with permission less and private/consortium blockchains with permissioned blockchains. The reality is, however, slightly more complicated as some public blockchains can be permissioned. The world of Blockchain is nebulous, complex and fast-changing, and definitions and classifications are not cast in stone. As technology matures and latestdummy of information flows and applications are being developed, definitions and classifications continue to evolve.[8]

3.2.1 PUBLIC BLOCKCHAINS

In a public platform, no specific entity/entities manage the platform, platform are public and individual users can maintain anonymity. No user is given special privileges on any decision. As such, it is a completely thrustless organization, in that it does not rely on a trusted party to validate the informations but instead relies on the nodes to come to a consensus before any data (information record, block, etc.) are kept on the ledger.[9]

Public blockchain platforms, however, need to ensure that users are incentivized to reach consensus. On the Bitcoin blockchain, for example, the verification process requires the performance of complex mathematical problems. The miner, i.e. "validator", who first solves the mathematical problem, is rewarded through Bitcoins. Fees charged in return on users differ significantly amoung platforms. They are, by far, the highest on the Bitcoin platform.14 In early November 2017, the average fee charged for Bitcoin informations reached more than US$ 11 per information, leading some in the community to argue that the organization had reached its limit.[8]

Most public blockchains are permission less, i.e. they are open to everyone. Thus.

- Any individual can download the required software on their device without permission and start running a public node, validating informations and thereby participating in the consensus protocol. The protocol that determines which blocks get added to the chain.
- Anyone can send informations through the network.
- Any individual can read and write relevant data on the blockchain.

  Because of their highly decentralized nature, public blockchains are considered particularly secure and resistant to malicious attacks, with no single point of failure, but they face issues of scalability.

3.2.2 PRIVATE BLOCKCHAINS

In fully private blockchains, the permissions to validate and write data onto the blockchain are controlled by one entity which is highly trusted by the other users, and participants are identified. In some situations, the entity may restrict the read permission to some users. Restricted read permissions provide a largerlevel of privacy to the users, a feature not available in public blockchains. The entity in control has the power to change the rules of the private blockchain and may decline informations based on its established rules and regulations.

In a private blockchain, verification of the informations is carried out by a very restricted number of nodes (according to the rules of the blockchain), which allows for largerefficiency and much faster processing of informations than public blockchains, while requiring much less computing power. Information fees may apply for information validation as per the rules of the blockchain.

In addition, given that the validators are known, it is easier for human intervention to fix faulty nodes and risks of a 51 or 99 per cent attack arising from miner collusion do not apply; but the more centralized nature of these networks makes them less resilient to outside attacks, and there is a largerrisk of human tampering of data.

The term "Blockchain" in the context of private ledgers is controversial and disputed, as such highly centralized ledgers have little in common with the original idea behind Blockchain.

3.2.3 CONSORTIUM BLOCKCHAINS

A consortium blockchain is a type of private blockchain that operates under the leadership of a group rather than a single entity and in which participants are identified. It is a "partially decentralized" platform.

Instead of allowing anyone with an internet connection to participate in the information verification process or letting a single entity having full control, a few selected nodes are predetermined. These nodes control the consensus process. They can read and/or write the data and can decide who has access to the blockchain ledger. The right to read the blockchain may be public, or restricted to the participants.[9]

For example, a consortium blockchain could be formed among 10 companies, each of which operates a device connected to the blockchain network. If Company 2 only trades and exchanges its invoices with Companies 3, 4 and 5, it could be decided that permissions to read the exchanged data be given only to these companies.[8]

Private and consortium blockchains are usually permissioned blockchains, i.e. access to the platform is limited to those with permission, which allows participating institutions to maintain a certain level of control and privacy.

4. HOW DOES BLOCKCHAIN WORK?

Blockchain is only one type of distributed ledger technology (DLT). The technology is evolving rapidlyand latestdummy of information flow are being developed to enhance speed and security and to lower energy consumption, which are moving away from the concept of "blocks", and even from both the concepts of "block" and "chain". "Latest kids not on the blocks" include IOTA, Ripple and Hash graph. Although these latestdummy are not blockchains the term "blockchain" is commonly used to refer to distributed ledger technology

in general and to the phenomenon surrounding it. Figure 2 illustrates the typical steps involved in blockchain informations.

Step 1

The sender submits or requests aninformation. A blockchain/DLT information can involve any type of asset digital (e.g. cryptocurrency, digital painting), tangible (e.g. a transfer of property or funds, or areplace of documents such as a customs declaration or certificates of origin), or intangible (e.g. provision of a service). Which is replaced amoung participants in the network.[9] It can involve documents, contracts, cryptocurrencies or any other type of asset.

When a information is submitted, various processes take place to guarantee the security of the information.

- First, the sender generates a key pair, including a public key and a private key. These keys are mathematically related. The public key is made available to the receiver.
- The sender then hashes the data to be sent, i.e. converts it into a latest digital string of a predefined and fixed length using a mathematical function a hash. Hashing ensures data integrity and prevents forgery.1 The resulting hash value is encrypted using the sender's private key. The encrypted hash forms the digital signature of the data, i.e. the digital fingerprint of an electronic record. It guarantees that the message was created and sent by the claimed sender and was not altered in transit. The sender not deny having sent the message.
- The sender then transmits the digital signature together with the plaintext data to participants in the peer-to-peer network the receivers.

If the sender does not wish other participants in the network to see the message itself, i.e. the plaintext data contained in the documents submitted, receiver can choose to encrypt the message.

Step 2

Once the digital signature has been generated and the message has been hashed and encrypted, they are transmitted to participants in the peer-to-peer network receivers, also called nodes and added to an unvalidated information pool.

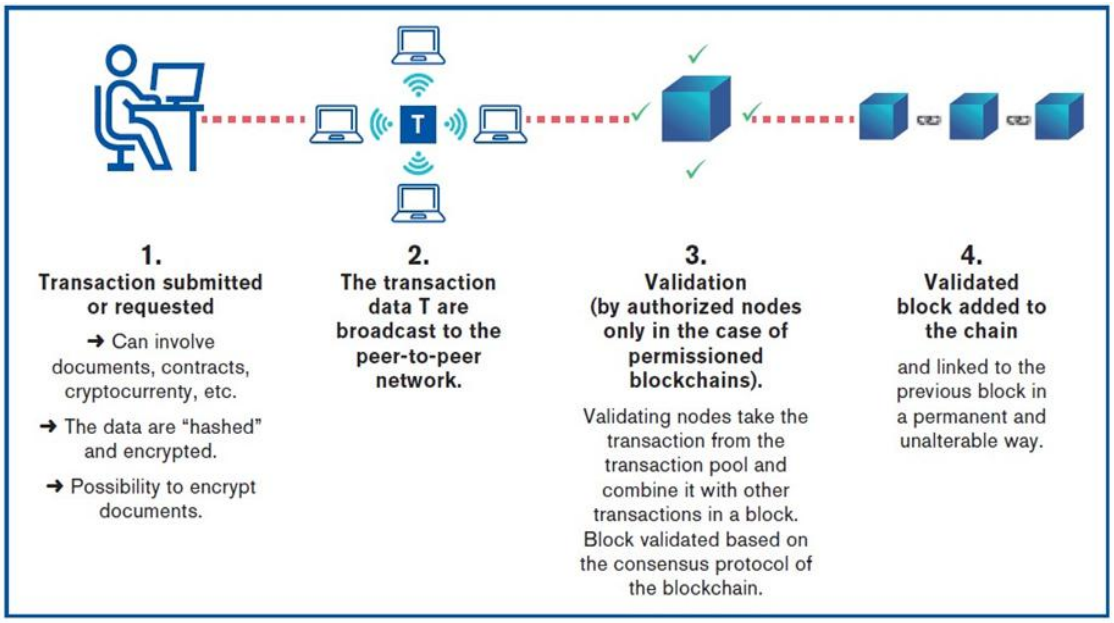

Figure 2: Working of Blockchain.[8]

Step 3: Validation

Receivers in the case of permissioned blockchains, authorized nodes validate the information using the sender's public key to decrypt the information. A successful decryption confirms that the information originates from the claimed sender.[8] The receiver can then verify the integrity of the data by comparing the decrypted hash value sent by the sender with the hash value that he computed when applying the same hash algorithm on the plain data transmitted by the sender. If both hash values coincide, the receiver has the guarantee that the data were not altered in transit. The information can then thus be validated.

The chain is then updated via the "consensus protocol". Consensus protocols ensure a common, unambiguous ordering of informations and blocks, and guarantee the integrity and consistency of the blockchain across geographically distributed nodes.

In the case of blockchain technology, validated informations are first combined with other informations to create a block that is then validated based on the consensus protocol of the blockchain. If validated, the latest block is linked to the chain as the "true state of the ledger". Each block contains several informations. A block is composed of a block header and of records of informations. The block header contains the following elements.

• The block number.

• The current timestamp that captures the date and time to ensure a record of the chronological sequence.

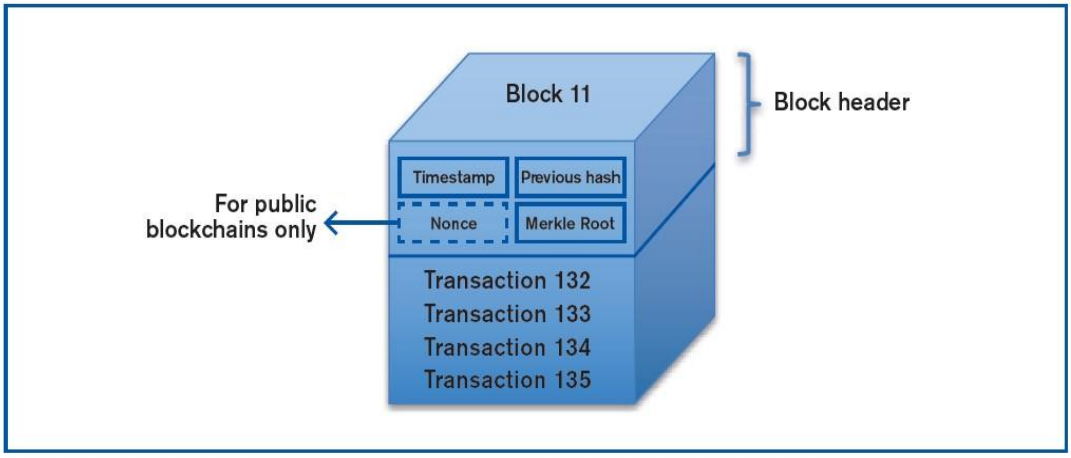

Figure 3: Composition of a block.[8]

• The hash of the previous block – also referred to as a hash pointer – to link the blocks together.

• The hash of what is called the "Merkle Root", which allows easy comparison and verification of large data sets of informations without the need to include the complete set of data of every information in the block header, thereby making the size of blocks more manageable.

In addition, for public blockchains such as Bitcoin, the block header includes the "nonce" i.e. a random sequence of numbers that the miners must find in order to validate the block and the difficulty target associated with it.

Step 4

Once a block is validated or, in the case of DLTs that do not combine informations in blocks, once the information has been validated, it is time-stamped and linked to the preceding blocks/informations with a "hash pointer" a hash of the previous block/ information. thereby forming a linear chronological chain of blocks/informations.

The informations are then confirmed and the block/informationnot be altered or removed – thus, the block/information is immutable. Each time a block/information is added to the chain, the digital ledger is updated on all the participating nodes. The organizationatic update of the ledger on all the nodes is an efficient way to ensure that there are no divergent versions of the ledger in the participating nodes.

Other distributed ledger technologies follow a different process. In IOTA, for example, informations are not grouped into blocks and each information is linked to two previous informations as part of the validation process to form a "Tangle"

5. BLOCKCHAIN BASED APPS FOR HEALTHSUPERVISION

This segment presents the structure and usefulness of a case ponder DApp for Smart Health (DASH)a we created to investigate the adequacy of applying Blockchain innovation to the healthsupervision space. This model was actualized on an Ethereum test Blockchain to imitate a negligible form of a individual HER framework. It gives a web-based entry for participants to self-report and get to their therapeutic records, as well as yield medicine demands. Sprint too incorporates a staff entry for suppliers to audit understanding information and satisfy medicine demands based on authorizations given byparticipants.[10] Fig. 5 shows the structure and working of DASH.

The inernal user features present in DASH can be summarized as the follows.

1. Participants can allow a supplier authorization to get to their health records or prescription requests through the Dash portal.
2. Participants can add a health record through a standardized, preformatted form via the DASH portal.
3. Health related activities (i.e., prescription and health record additions)related to a patient are sent to suppliers with authorized access to the patient's information with secure notice messages.
4. Supplier with authorized get to to a patient's records can inquiry, make changes, and transfer doctor notes to the information, as well as satisfy the patient's medicine demands.
5. Participants will get notification of any update to their health record performed by the supplier.

Dash uses a Patient Registry contract to store a mapping, or relationship that joins interesting quiet identifiers to their related Patient Account contract addresses (areas). Each Patient account contract keeps up a list of healthsupervision suppliers (through unique supplier identifiers) who are allowed read/write get to to the patient's therapeutic records. At its current state, Dash is restricted to as it were give information get to administrations to two sorts of clients: participants and suppliers. Quiet wellbeing records are put away off-chain in a secure database, executing the FHIR information measures. The reason for putting away understanding information in a centralized database is to mimic an information storehouse,

because it is in today's wellbeing frameworks, to afterward on work out information integration with other siloed databases. Our database server makes a secure attachment to supplant permission-based tokenized get to to quiet information utilizing standard open key cryptography.

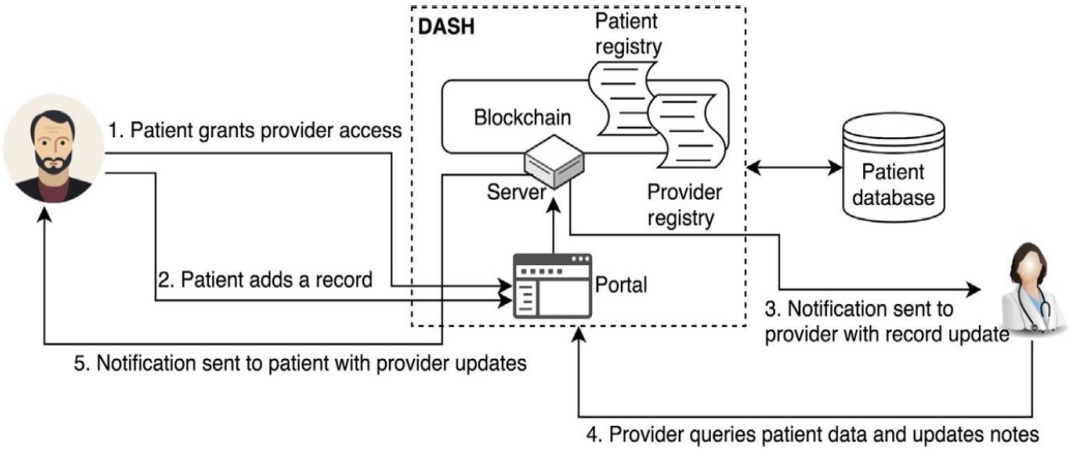

Figure 5: DASH architecture overview.[10]

Supplier and patient users who are members of DASH are each haveing with two different secure cryptographic key pair for encrypting and decrypting data references for authorizing access to a patient dataset and installinglatest health records and verifying signatures to prevent tampering to the data.

6. BLOCKCHAIN APPLICATION IN HEALTHSUPERVISION

6.1 OPIOID PRESCRIPTION DETECT

It is broadly known that there's an opioid epidemic present within the India. While many efforts are being made to address this crisis (e.g., the Drug Supply Chain Safety Act (DSCSA), the President's Commission on Combating Drug Addiction and the Opioid Crisis, and numerous prescription awareness campaigns, our current prescription detectorganization still lacks the technology to do so effectively. Data hoarding, doctor shopping, supplier ignorance, vulnerable and centralized data, and over prescription riddle the current prescription opioid marketplace.[11]

The decentralization and auditability of Blockchain technology provide a promising approach to prescription monitoring that not only makes prescriptions safer, but also provides incentives for writing fewer prescriptions.

Healthsupervisionsuppliers today are incentivized to prescribe opioids to participants. For example, suppliers incur less face time with participants, fewer costs associated with patient supervision, and thus larger profits from higher returns. Likewise, pharmacies are incentivized to produce and distribute opioids since the more they sell, the higher their bottom line, and the largertheir return to exchangeholders. Moreover, participants are incentivized to consume opioids. In the treatment of pain, physical therapy or post-surgeryrecovery can be frustrating and riddled with disappointment. Opioids provide a short-term relief, at the cost of addicting a patient. This self-fulfilling cycle can thus benefit from a technological solution that realigns these incentives.

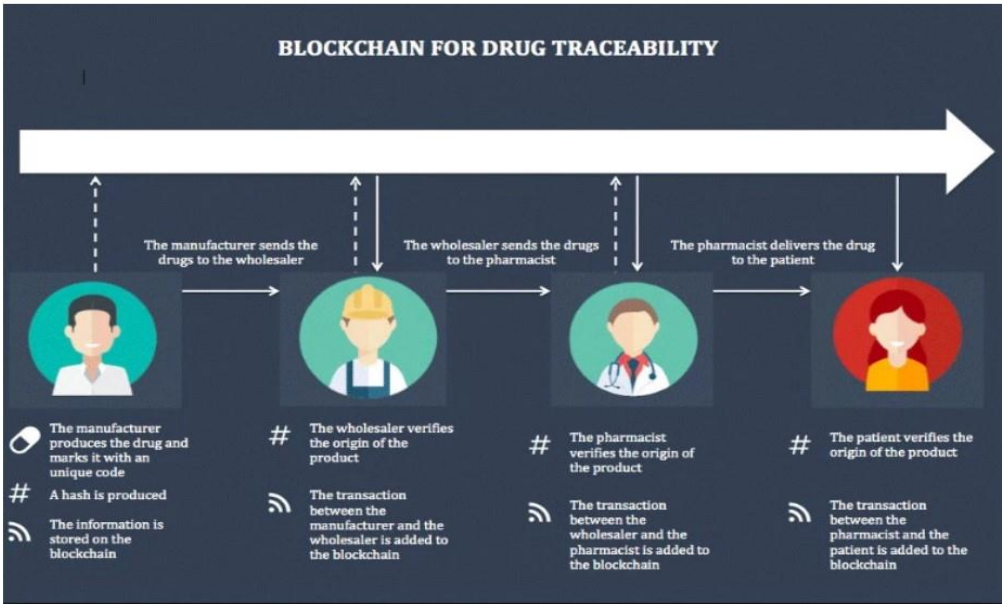

Figure 6: Chain Management by Blockchain.

To offset these incentives contributing to the rise of the opioid epidemic, a Blockchain-based organization can establish a trusted network of hospitals and pharmacies to store opioid-associated informations (including prescriptions, fulfilment, etc.) in a secure and accountable manner. Such a distributed and exchanged permissioned Blockchain platform allows for loosely coupled suppliers to access other data silos without explicit trust relationships amoung each other. Stakeholders within the organization (hospitals, pharmacies, etc.) are likewise incentivized to onboard latest members to the consortium because with each additional member, they can form a more complete dataset. Rules can be mutually predefined so the consortium can securely onboard latestsupplier members to the organization.

By distributing knowledge that an opioid information has occurred, rather than the entirety of the specific content of that information, this type of ecoorganization can remedy several the problems in the current opioid organization. More complete opioid prescription history can be available to detect overly prescribed opioid by suppliers and patterns of doctor shopping in participants. Consequently, suppliers will be incentivized to meet the requirements to join the consortium of suppliers through potential access to data that will increase the quality of their supervision. Most importantly, by detect the history of opioid prescriptions, participants will re opioids toward less addictive and supervision more appropriate to their condition and thus be steered away from the dangers of thus longer lasting treatment actions.[11]

7.2 DATA SHARING AMOUNG TELEMEDICINE AND TRADITIONAL SUPERVISION

Traditionally, telemedicine offers widely accessible supervision to participants who are in remote areas far away from local health facilities or in areas of with shortages of medical staff. Today, it has becoming increasing among participants who wish to receive convenient medical supervision. Connected participants can avoid wasting time waiting at a doctor's office and get immediate treatment for minor but urgent conditions on demand. Owing to the growing accessibility to smart mobile and telemedicine devices, many companies offer 24/7 continuous access to supervision, and many user-friendly apps have been created for participants to monitor, manage, and report their health using technology.[12] For example, Apple Health app allows participants to connect to equipment for measuring vitals and store these data on their phones. These records can then be reported to the supplier as needed.

By removing the need for a third-party authority and empowering direct interactions amoung involved participants, Blockchain technology can potentially bridge the communication barrier amoung these suppliers. Blockchain technology alone, however, not address the complex data sharing challenge it must be incorporated into existing disparate health organizations and clinical data standards. Fig 7 shows a high level conceptual framework where a Blockchain is connected to disparate health database organizations.

Each database organization is shown in Fig. 7 opens up a latest secure data channel (as represented by small circles on the ellipse border), same to what is used to exchange data with other akin organizations. A smart contract (the keyed file symbol) is then used to govern the data informations amoung these organizations based on mutual agreements and also

create an immutable history of all the information records.[10] In practice, a robust architecture will include many more design components than what is shown in Fig. 7.

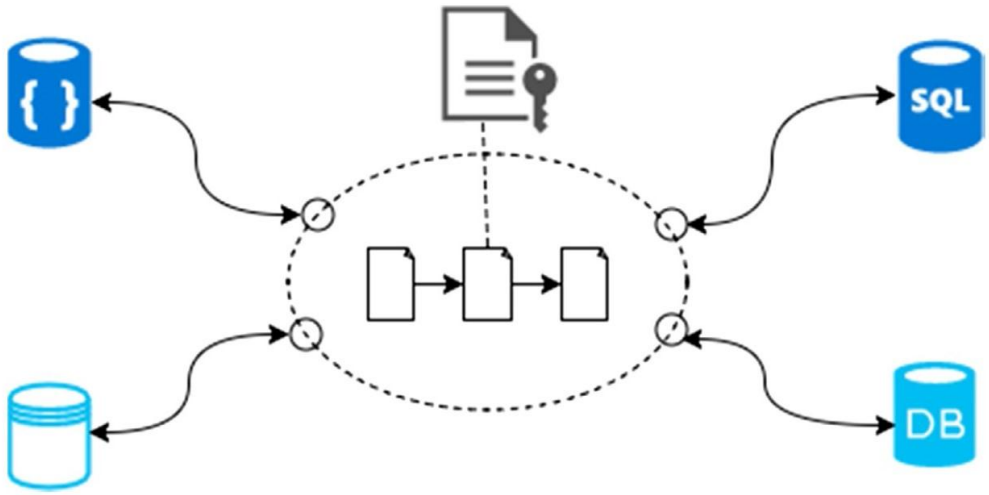

Figure 7: A high-level blockchain based conceptual infrastructure to connect disparate health organization and record data replace history.

7.3 PATIENT DIGITAL IDENTITY

A fundamental component in health information replace is patient identification matching, which finds a patient in a healthsupervision database using a unique set of data. Organizations like the master patient index and enterprise patient master index have been created to manage patient identities within a healthsupervision organization or within a trusted network. Despite the increased development effort, accurately and consistently matching patient data remain hard. Patient identity mismatching has contributed to duplicated patient records and incomplete or incorrect medical data. the study estimated that 195,000 death occur each year due to medical mistakess, with 10 of 17 mistakess being identity or "wrong patient mistakes." There are also significant costs to healthsupervision organizations who maintain these duplicate records and correct mistakenly merged mistakess and also participants who experience repeated tests or treatment delays.[13] In addition, these mistakess also impact reimbursement as claims may be denied due to "out of date or incorrect information", not to mention the security risks involved when participants disclose their personal information.

Without common standards for collecting patient identifying information, even the same patient's identity can change from one supervision facility to another. For instance,

demographics data, such as name, date of birth, address, and Social Security number (SSN) are often used to register a patient. However, names may be kept in various formats, such as legal first and last name, nickname and last name, with or without middle initial, and participants may exchange identical or same names; samely, date of birth can be entered into the organization in multiple ways; address can change as participants move to a latest location; and participants may refuse to provide their SSN or do not have an SSN. Furthermore, patient information manually entered into the organization may contain typos or mistakess, and the more data collected, the more opportunities for mistakes. Although within each organization patient demographics data may be collapsed into a single unique ID, the ID generally does not translate across organizations.

Without a functional, unified identity management organization, patient identification schemes employed at various supervision sites may continuously experience incompatibility and patient matching problems, unless a patient exclusively receives supervision within one organization. In fact, the very nature of Blockchain incorporates such a decentralized, unified identity organization. Many existing Blockchains use cryptographically secured addresses to represent identities. Each address is mathematically linked with a unique key that is used to easily verify the ownership of an address or an identity yet does not reveal any personal information relating to the individual. The decentralized and auditable characteristics of Blockchain can help enforce standardized verifiable identities for participants via a universal patient index registry sharable across all healthsupervision facilitates within a nation and beyond. In case of lost or stolen keys, latest addresses are also trivial to generate and reassign to participants.[10]

7.4 PERSONAL HEALTH RECORDS (PHRs)

Unlike the current standard practice of using supplier centric EHRs to maintain and manage patient data, PHRs are applications used by participants, the true data owners, to access and manage their health information. The goal for PHRs is to help participants securely and conveniently collect, track, and control their complete health records compiled from various sources, including supplier visit data, immunization history, prescriptions records, physical activity data collected from Smartphone devices, and many more. PHRs enable participants to control how their health information is used and exchanged, verify the accuracy of their health records, and correct potential mistakess in the data. Enterprises and technology companies, such as Apple and Microsoft, have begun exploring centralized solutions with

their Apple Health and Microsoft HealthVault products. Centralized approaches do not resolve the data sharing problem at its core, however, and may therefore face same hurdles as existing disparate EHR organizations.[13]

Blockchains, in contrast, allow distribution of control to individuals viadecentralization enabled by consensus algorithms. By creating a widely accessible and secure data distribution service that connects to existing health organizations, participants can easily aggregate their medical history without requesting a copy from every supplier they have visited. Connections to personal smart devices are also possible as Blockchains remove the "distrust" amoung healthsupervision professionals and third-party health detect apps and services. Furthermore, permission-based data distribution can be set up with smart contracts to guarantee that participants remain in control of their data access, are aware of the origin of aggregated data sources, and are informed when their data are accessed by suppliers. Data origin and access history are made transparent to the participants through immutable audit logs to always keep participants up to date of when and by whom their health information is recover.

7.5 CANCER REGISTRY SHARING

Data sharing is especially censorious in cancer supervision where cases are usually complex, and cures are rarely one-size-fits-all. Being able to exchange cancer data helps ensure the integrity of results obtained from clinical trials by enabling individual confirmation and validation, but it can also agglomerate intelligence gathered to reduce unwarranted repetition in clinical trials.[14] It allows distributed clinical trials to achieve a significant cohort size and thus speeds up the discovery of more effective cancer treatments. In the United States, only about 3% of cancer participants are undergoing clinical trials today. As a result, most cancer participants receive treatments based on observations drawn from this small population of highly selective participants with different demographics, family medical history, secondary diagnoses, etc. Population-based cancer registries are attempts to capture very rudimentary data from cancer incidences across geographic areas and for planning population-wide cancer control. As with EHRs, cancer registries are often siloed and fragmented, which can samely leverage Blockchain technology for expedited information replace. In addition, with increased availability of richer data collected from many participants, artificial intelligence can be used to construct prognostic and predictive dummy for assisting supervisionsuppliers with decision support. A learning ecoorganization can be designed using Blockchain

technologies to exchange predictive dummy and collaboratively improve accuracies of learned medical insights.[10]

7. CONCLUSION

In this study the use of blockchain technology in healthsupervision is explained and pointed out the issues in current pharmaceutical supply chain management and explained how blockchain can be used to add traceability and visibility to drugs supply and overcome the issue of counterfeiting. How the identity mechanism of blockchain works and how is it helpful to exchange medical data while keeping the patient's private data secrete is explained. We highlight the possible techniques, blockchain types and third-party solutions that can be used to implement a blockchain base supply chain for pharmaceuticals. In the last we explained the working of the suggested organization with an example that shows how the organization will be easily used by different participants. Theblockchain technology have great potential in creating secure and effective healthsupervision ecoorganizations with its inherent unique properties. Overall, blockchain has a wide range of possibilities in healthsupervision, which invites many research opportunities in this space.

REFERENCES

1. Fenoff, R.S.; and Wilson, J. M.; Africa's counterfeit pharmaceutical epidemic: The road ahead. *Center Anti-Counterfeiting and Product Protection (A-CAPP)* Paper Series, MichiganStateUniversity.Retrievefrom:http://a-capp.msu. edu/sites/default/files/files/AfricaPharmaPaperFINAL, 2009.
2. Gautam, C.S.*;* Spurious and counterfeit drugs: a growing industry in the developing world. *Postgrad. Med. J,* 2009; *85:* 251-6.
3. Harris, J.*;* Keeping it real: Combating the spread of fake drugs in poor countries. *J. Int. Med. Res,* 2009.
4. Organization, W.H.O, In; Geneva, 1995.
5. Nakamoto, S.; Bitcoin: A peer-to-peer electronic cash organization, 2008.
6. Haq, I.; Esuka, O.M.; Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. *Int. J. Chem. Eng. Appl*, 2018; *975*: 8887.
7. Raval, S.; *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.": 2016.
8. Ganne, E.; *Can Blockchain revolutionize international trade?* World Trade Organization, 2018.

9. Hreinsson, E.M.; Blöndal, S.P.; The future of blockchain technology and cryptocurrencies, 2018.
10. Zhang, P.*;* FHIRChain: applying blockchain to securely and scalably exchange clinical data. *Comput. Struct. Biotechnol. J*, 2018; *16*: 267-278.
11. Nelson, L.S.*; et al.*, Addressing the opioid epidemic. *JAMA*, 2015; *314*: 1453-1454.
12. Ben, M.G.; TECHNOLOGY AND TELEMEDICINE, 2017.
13. Just, B.H.*;* Why patient matching is a challenge: research on master patient index (MPI) data discrepancies in key identifying fields. *Perspect. Health. Inf. Manag*, 2016; *13*.
14. Kinahan, P.E.*;* PET/CT Assessment of response to therapy: Tumor change measurement, truth data and mistakes. *Clin. Transl. Oncol*, 2009; *2:* 223-230.