ISSN 2395-1621

Current State of Blockchain Technology Research, It's Future Trends, with reference to a Health sector application

[#1]Indranil Choudhury, [#2]Prof. Manjusha Tatiya

[1]indranil82@gmail.com,
[2]manjusha.tatiya@indiraicem.ac.in

[#12]Department of Computer Engineering
Indira College of Engineering and Management, Pune, India

ABSTRACT

Blockchain, the base of Bitcoin, has gotten broad considerations as of late. Blockchain fills in as an unchanging ledger which permits exchanges happen in a decentralized way. The explanation behind the enthusiasm for Blockchain is its focal traits that give security, obscurity and data integrity with no outsider association responsible for the exchanges, and hence it makes intriguing research areas, particularly from the point of view of specialized difficulties and confinements. Blockchain innovation is ready to change about each feature of our advanced lives, from the manner in which we send cash to the manner in which we heat our homes. By hindering outsiders, blockchains guarantee to make our frameworks progressively productive. By bypassing oversight, they guarantee to make our frameworks progressively fair. Also, if appropriately actualized, they could make our frameworks progressively solid and secure. Blockchain-based applications are jumping up, covering various fields including monetary administrations, notoriety framework and Internet of Things (IoT, etc). Be that as it may, there are as yet numerous difficulties of blockchain innovation, for example, versatility and security issues holding on to be survived. This report introduces a far reaching diagram on blockchain innovation and it's difficulties. A blockchain application is proposed vis a vis a health monitoring application using cloud.

Keywords: Blockchain, Bitcoin, Cryptography, Network security, Cryptocurrency, Distributed computing.

ARTICLE INFO

Article History

Received: 28th April 2019

Received in revised form :

28th April 2019

Accepted: 01st May 2019

Published online :

02nd May 2019

I. INTRODUCTION

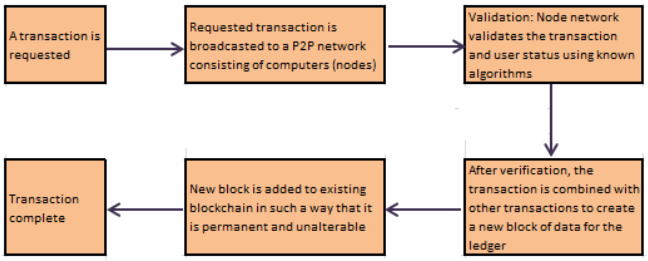
Blockchain is a computerized, decentralized record that tracks all exchanges that happen over a shared system. It is an interlinked and consistently extending rundown of ledgers put away safely over various interconnected frameworks. This makes blockchain innovation flexible since the system has no single point of failure. Also, each block is exceptionally associated with the past blocks through a computerized mark/digital signature which implies that creation a change to a record without irritating the past records in the chain is not possible, hence rendering the data carefully designed. The key advancement in blockchain innovation is that it enables its member to exchange resources over the Internet without the requirement for a outsider or third party. Blockchain innovation was created as the basic innovation behind the digital currency called bitcoin. The outcome of the 2008 subprime emergency diminished trust in the current financial system. This is the point at which an individual called Satoshi Nakamoto composed a white paper containing the 'bitcoin convention' which utilized a distributed ledger and accord working to compute algorithms. The bitcoin convention was composed to render conventional financial intermediaries useless, as a method for encouraging direct P2P exchanges. Since the introduction of the Internet, there have been endeavours to make virtual monetary standards, yet those attempts flopped due to the 'double spend' issue, in particular the hazard that an advanced resource, for example, a money can be spent twice. The present answer for dispose of the double spend issue is through the presentation of 'middle people of trust, for example, banks. Be that as it may, the utilization of blockchain innovation makes it conceivable to take care of

the key issue of twofold spending without the requirement for such delegates of trust, in this way encouraging the exchange of advantages, for example, virtual monetary standards over the Internet safely. This idea can be reached out to non-cash related territories and that is the guarantee of blockchain innovation.

Cash exchanges between people or organizations are centralized by third party. Making cash transfer via digital means requires a bank or card provider as a broker to finish the exchange. Likewise, an exchange causes an expense from a bank or a Mastercard organization. A similar procedure applies additionally in a few different spaces, for example, recreations, music, programming and so forth. The exchange framework is ordinarily brought together, and all information and data are controlled and overseen by a third party, instead of the two end parties engaged with the exchange. Blockchain innovation has been created to tackle this issue. The objective of Blockchain innovation is to make a decentralized domain where no outsider is responsible for the exchanges and information. Blockchain is a distributed database arrangement that keeps up a continuously growing list of ledgers or records that are verified by the hubs taking part in it. The information is recorded in an open ledger, including data of each exchange at any point finished. Blockchain is a decentralized arrangement which does not require any third party interference. The data about each exchange at any point finished in Blockchain is shared and accessible to all hubs. This characteristic makes the framework more straightforward than concentrated exchanges including a middle-man. What's more, the hubs in Blockchain are for the most part anonymous, which makes it secure for different hubs to affirm the exchanges. Bitcoin was the principal application that presented Blockchain innovation. Bitcoin made a decentralized environment for cryptocurrency, where the members can purchase and trade products with digital cash. Nonetheless, despite the fact that Blockchain is by all accounts an appropriate answer for leading exchanges by utilizing digital forms of money, it has still some specific difficulties and constraints that should be contemplated and tended to. High integrity of exchanges and security, just as protection of nodes are expected to anticipate assaults and attempts to aggravate exchanges in Blockchain. Furthermore, affirming exchanges in the Blockchain requires a computational power. It is imperative to recognize what subjects have been as of now considered and tended to in Blockchain and what are right now the greatest difficulties and restrictions that need further examinations.

In spite of the fact that the blockchain innovation has incredible potential for the development of internet systems in future, it faces multiple difficulties. For example, scalability is a big concern. Bitcoin block size is restricted to 1 MB now while a block is mined about at regular intervals. Accordingly, the Bitcoin is confined to a rate of 7 exchanges/second, which is unequipped for managing high rates of trading. In any case, bigger blocks imply bigger space for storage and slower network proliferation. This will prompt centralization progressively as fewer clients might want to keep up such a huge blockchain. Along these lines the trade-off between block size and security has been an extreme test. Besides, it has been demonstrated that blockchain miners could accomplish bigger income than a considerable amount through selfish mining procedure. Miners conceal their blocks mined for more income later on. In that manner, branches could happen much of the time, which impedes blockchain advancement. Subsequently a few arrangements should be advanced to fix this issue. In addition, it has been demonstrated that security spillage could likewise occur in blockchain even clients just make exchanges with their public and private keys. Moreover, current algorithms like proof of work (PoW) or proof of stake (PoS) are confronting some difficult issues. For instance, PoW squanders an excessive amount of energy in terms of electricity while PoS could lead to already rich miners getting wealthier.

Blockchain works by means of validation of exchanges through a distributed network system so as to make a lasting, unchangeable and verified ledger. Figure 1 beneath demonstrates overview of how blockchain functions.



II. CURRENT STATUS OF BLOCKCHAIN RESEARCH

Blockchain is being used in following fields currently:

1. Transfer money

Bitcoin has been portrayed as "blockchain's first use case". For over 40 years, financial analysts have been looking for currency in digital form that can wipe out the issue of double spends and go around the issue of trusting an unknown third party. The Bitcoin blockchain hasn't been hacked yet—and one needs to have a go at utilizing it to acknowledge how basic and how astounding the protocol is. The intermingling of payments via mobile, especially in African market, with cryptocurrency, is a specialty to watch, organizations, for example, BitPesa are driving the charge in this case.

2. Making micropayments

Blockchains use as a means to exchange small amounts of cash is a potential distinct advantage. In the case of discussing app based transfer of few cents or paisas, microgrid exchanges or household electronics moving towards a model more based on paying as per use instead of owning, having the capacity to make little payments utilizing digital money without bringing about bank charges that surpass the first instalment is a tremendous chance.

3. Lend people money

Shared lending is one of the quickest developing areas in finance, with clients are pulled in to make a profit in their investment in a low-interest condition while empowering different clients to obtain at a reasonable rate—and all without giving the bank their cut. Rather than fiat contenders, for example, Zopa and Funding Circle, BTCJam enables clients to do the majority of the abovementioned, however with Bitcoin.

4. Parking fine payment

New York City councilman Mark Levine proposed couple of yours back that headstrong drivers in New York ought to have the capacity to pay for stopping tickets with ApplePay, however with Bitcoin. No news yet on whether this will really occur, however with regards to BitLicense, it's a fascinating proposition.

5. Content Consumption

The rise and rise of ad-blockers has thrown the traditional business model out of the window. All-or-nothing paywalls have proved successful for a few publishers, but research has shown that users are more prepared to reward content creators if the process is seamless and if they can pay only for what they consume. Startups such as London-based Smoogs, Berlin-based SatoshiPay and Yours provide an easy way for writers, film-makers and other content producers to be paid for what they do. The continuous demand for ad blockers has outdone the customary model. Win big or bust paywalls have demonstrated fruitful for a couple of distributers, however as per research demonstrated that clients are progressively arranged to remunerate content makers if the procedure is consistent and in the event that they can pay just for what they devour. New businesses, for example, London-based Smoogs, Berlin-based SatoshiPay and Yours give a simple method to essayists, movie producers and other substance makers to be paid for what they do. The earth shattering Bravebrowser is one more model.

6. Electric car charging

Little, steady instalments are useful for more use cases than simply content utilization. Conventional vehicle charging stations regularly expect drivers to pay in fixed additions, paying little heed to how much power is devoured by the vehicle's battery. Moreover, for electric rental armadas, the contract organization needs to create programming to follow the charge left on the battery, or to do this physically. Envision a framework where each electric vehicle has a chip that enables it to pay legitimately for precisely the power it devours, and where all the driver needs to do is top up the instalment recompense every once in a while. German vitality mammoth RWE grew precisely this pilot plot with Ethereum pioneers slock.it, enabling electric vehicles to charge while holding up at the traffic lights.

7. Supply chain certification

Numerous buyers would want to settle on moral decisions about the items they purchase. Ongoing outrages, for example, the clearance of pony meat as hamburger in the UK, and disclosures about the poor states of article of clothing specialists in creating nations has pushed this issue into the features. Nonetheless, demonstrating the inception of each segment in an item can be unimaginable, and regardless of whether this data is held by a unified expert, it may not be reliable. London startup Provenance offer decentralized production network accreditation.

8. Electricity sharing

It's increasingly proficient to utilize power near where it is created, so as opposed to offering the abundance control back to the framework (which most organized residential sun powered establishments do), if the proprietors of the houses with overabundance power could offer it on the nearby market, it would be a major favorable position. Tragically, this would typically include some significant pitfalls, with the property holders concurring a cost among one another and screen the measure of power being utilized. The MicroGrid venture in New York's Brooklyn unravels this necessity by enabling the family units to purchase and sell vitality by means of shrewd contracts on the Ethereum blockchain. No free estimation or observing required.

9. Identity proof

We effectively live such a large amount of our lives on the web, yet everything goes to a crushing stop when we have to by one way or another associate our advanced character with our quality in the physical world, confirmed by some sort of officially sanctioned desk work or evidence of presence at a specific location. Then, as we battle to keep up our credit records and demonstrate our identity to managers, banks or vehicle rental organizations, private enterprises are profiting from offering our information which has a place with us as people, and which we ought to have the capacity to monetise. Such a large number of associations to make reference to are taking a shot at computerized verification of-character plans, a large number of them blockchain-based. Deloitte's Smart Identity System is likely the best known.

10. Prove ownership of an asset

On the off chance that somebody takes a vehicle in many nations of the world, there's a sensible possibility it will be followed or recuperated. Most government work some sort of enrolment conspire dependent on tag and additionally frame number. However, if there should be an occurrence of a stolen bicycle or something like an extravagance satchel or automaton, such high-esteem compact resources are anything but difficult to take and furthermore to expel from a specific geographic territory where they may have been enrolled. A start-up Mamoru expects to give a worldwide standard to verification of possession.

11. Issue money from a central bank

The possibility of a cashless society is massively engaging governments around the globe. In addition to the fact that it circumvents the need to print notes and mint coins, however it likewise implies a conclusion to the namelessness of money, and gives an approach to follow the spending of people. Different national banks have played with the thought, however the Bank of England has gone similarly as supporting an autonomous investigation at University College London which proposed how cryptographic forms of money may be issued by such a specialist.

12. Shipping process simplification
Delivering crosswise over national fringes produces so much administrative work that it very well may be estimated in entire kg (or pounds, on the off chance that you incline toward magnificent). At the point when shipments are postponed, it can cause an effect all in all inventory network as processing plants sit tight for parts, and at times (for instance, short-lived merchandise), it can influence the feasibility of the entire shipment. Long periods of time and tremendous organization costs are tied up in creating bills of replenishing, so there was a lot of intrigue when shipping monster Maersk as of late reported a blockchain-based bill of filling confirmation of idea.

13. Running a decentralised marketplace
Open Bazar is broadly observed as a successor to Silk Road, however it is unmistakably more than that. Silk Road was a site on a server covered up by the Tor organize. The FBI had the capacity to follow it down, catch the server, and capture those included. Conversely, Open Bazaar is a shared system like BitTorrent. You can download the product and set up your own customer facing facade. It merits referencing that Open Bazaar does not expressly support selling illicit things. From their FAQ: "Venders on the OpenBazaar organize have their own items and are along these lines straightforwardly in charge of consenting to nearby laws (and their own still, small voice) when posting things or administrations. Clients occupied with illegal action can't hole up behind an outsider administration."

14. Music copyright registration
Diverting salary from music to the musician who made it is an enormous worldwide test. Regularly, the managerial expenses of recuperating sovereignties surpass the sum due. Erosion brought about by awkward instalment forms imply that fans who might some way or another be set up to pay to expend music end up unlawfully downloading substance, since it's simpler. Vocalist lyricist Imogen Heap, helped by different Ethereum individuals, reported the dispatch of Mycelia in July to address this issue. Charged as 'reasonable exchange for the music business', it plans to offer additional usefulness, for example, enabling fans to pay for extra substance, and focused on valuing, for example, enabling foundations to utilize tracks at a lower or zero expense. Swedish startup Zeptagram are likewise working here.

15. Vote
Electronic voting—whether at nearby or national government level, or with regards to corporations—is legitimately viewed with doubt as the outcomes appear to be available to control without the significant oversights. In light of the straightforwardness offered by open blockchains, for example, Bitcoin or Ethereum, advocates of open government are vocal about the benefits of blockchain-based casting a ballot. Nasdaq has effectively reported plans in Estonia to enable corporate investors to cast a ballot and different new companies are creating e-casting a ballot machines for state and national races that work along these lines.

16. Register land rights
Keeping up a national register of land proprietorship is a costly and work escalated task. Moreover, in nations where there is a background marked by government defilement, they may not generally be reliable. Factom were broadly answered to deal with an answer with Honduras to think of a proof of idea for a blockchain-based land vault. This ended up being less concrete than initially revealed and the task has slowed down, yet somebody, some place will execute this one day.

17. Manage a swarm of robots
This is fact and not theoretical. Expanding automation implies that a wide range of enterprises, from cultivating to assembling, are presently anticipated to depend on extensive quantities of mechanical work.

18. Manage healthcare records
Think about any part where there is a superseding requirement for un-tamperable information and a reasonable review trail, and one of the first to ring a bell is social insurance. Different new businesses are contending in this space, yet one of the all the more fascinating is the Factom/HealthNautica organization in which they "are hoping to verify restorative records and review trails. This is finished by scrambling the information onto the Bitcoin blockchain with a timestamp to check its exactness. The records can't be changed and, in light of the fact that it is hashed to the blockchain, it can't be gotten to without consent. HealthNautica wants to improve proficiency of cases handling and conviction that the records have not been changed."

19. Trade cryptocurrencies
Bitcoin isn't the main digital money. Many other cryptographic money blockchains exist, in spite of the fact that most of these are either outdated or convey basically useless tokens. A large group of trades, some more legitimate than others, have jumped up to provide food for those which merit exchanging: Bittrex, C-Cex and Poloniex are a portion of the famous alternatives.

20. Rent a car
The vehicle rental procedure is regularly more unwieldy than it should be, with protection archives and characters that should be checked, and vehicle mileages and harm reports that are still physically confirmed as a rule. DocuSign depicted their savvy contracts preliminary for vehicle rental, related to Visa's advancement group.

III. FUTURE APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

1. Elimination of Trusted Third Parties:
Blockchain as an innovation can possibly in a general sense influence a wide assortment of procedures and advances. At its centre, the Blockchain is a framework for killing the requirement for trust in exchanges. While that may seem like a straightforward suggestion, a large number of the biggest establishments on the planet exist today to work as confided in outsiders, for instance, SWIFT and the Depository Trust Clearing Company. Corporate open doors proliferate for organizations that can make connected

blockchain technologies targeting explicit exchanges, for instance, the home loan industry.
The ebb and flow scene of home loans requires a complicated snare of title looks, title protection, and incalculable minor exchange charges that are important to keep the framework running. These frameworks exist on the grounds that, generally, the exchange of land has been a procedure that requires an enormous measure of trust in dated records. In any case, the Blockchain would address these worries, and a particular property's record can contain an evident and approved history of exchanges, limiting the requirement for organizations to give chance alleviation and trust administrations, rather the exchange can exist in its very own right. The outcome would close home loans for a small amount of the expense, in a small amount of the time, with generous higher degrees of trust.

2. Protection of Self-Driving Cars:

The genuine capability of Blockchain as an encoded database structure is progressive, energizing, and starting at yet undiscovered. For instance, digital security has been the fly in the balm for broad development in numerous enterprises including driverless vehicles.
Since the beginning of the web, our capacity to push limits has constantly moved a lot quicker than our capacity to shield ourselves from spyware, infections, and programmers – however Blockchain could be the finish of that. Numerous individuals consider the innovation for independent vehicles not exclusively to be consummated in trials yet additionally prepared for the commercial centre. Be that as it may, enactment won't permit driverless autos in any genuine manner at this time, and one integral reason is digital security.
These worries aren't baseless. All things considered, even present day vehicles that are out and about now have been caught remotely by programmers. And keeping in mind that changing your radio station is a certain something, driving your vehicle into a dump is very another. In the past automakers have never had the capacity to ensure full security against digital assaults in their driverless vehicles, yet with Blockchain, they can. This decentralized strategy for dispersion would make each driverless vehicle out and about basically unapproachable. Presently that Blockchain is here, it's difficult to envision an eventual fate of driverless vehicles that doesn't depend on it.

3. Blockchain beyond Bitcoin

The growth of Bitcoin in 2017 advanced the unwavering quality and advantages of the fundamental innovation utilized by this digital cash, the blockchain. In 2017, blockchain turned into the second most prominent hunt word on Gartner's site, and disseminated record innovation will keep on picking up importance crosswise over numerous ventures.
Deloitte predicts that blockchain ventures will surpass distributed computing and IoT in funding speculation. Nations with authority blockchain procedures, similar to Malta, will finish up driving provincial markets and the worldwide business by and large.
Blockchain will address a few advanced security concerns, incorporating issues with contracts, character, and extortion the board. Blockchain-based records will enable online retailers and budgetary associations to helpfully vet their clients and battle against false exercises.
The Blockchain wording will likewise develop after some time. Industry pioneers will underscore on giving utilitarian or building portrayals as opposed to depending on the expression "blockchain." The Australian Securities Exchange, for instance, kept away from the word while declaring its organization of a "conveyed record innovation" for clearing and settlement prior this year, concentrating on its usefulness, instead of searching for ubiquity.
While the publicity around "blockchain" will die down in the coming year, we'll see major blockchain-motivated applications in social insurance, monetary, protection, and web based business parts. Blockchain will turn into the default innovation wherever there is a need to guarantee the uprightness of information.

4. Ensuring a Secure Internet of the Future

The most significant element of blockchain is that it gives top notch security in an unbound Internet where phishing, malware, DDOS, spam and hacks put in risk the manner in which business is done all around.
One of the fundamental advantages that blockchain gives over other record programming is that it depends on cryptography and is customized to be unchanging, one can't return to a specific point on the blockchain and change data. For the 10 years of blockchain's presence, it has never been hacked.
Another significant advantage of blockchain is it's conveyed over various systems, making it incredibly difficult to bring down for a situation of dictator government or unlawful business rehearses. For instance, a land obtained recorded with a blockchain 'keen contract' can't be erased or covered up by any expert, making the proprietor shielded from acts of neglect.
Ultimately, blockchain is an incredible instrument to use to store huge measures of significant documentation in enterprises, for example, social insurance, coordinations, copyright and some more. Blockchain evacuates the requirement for a mediator with regards to legitimizing contracts. Shrewd contract stages are as yet being culminated with regards to ease of use and are required to see wide use in the following 5 years.

5. Blockchain for Digital Advertising

Computerized publicizing faces difficulties, for example, space misrepresentation, bot traffic, absence of straightforwardness and long instalment models. The issue is that motivating forces are not adjusted, making the two sponsors and distributers feel they are on the losing side of the arrangement. The blockchain is the answer for convey straightforwardness to the inventory network since it naturally conveys trust to a trust less situation.
By diminishing the quantity of awful players in the inventory network it empowers the great organizations to flourish. Most significant, distributers can gather a higher level of the complete promotion dollars entering the biological system and will do as such at the season of impression conveyance. The blockchain is still in its early stages, however the fundamental innovation is digging in for the long haul and all advertisement tech organizations ought to take a gander at how it can improve their business.

6. The Effect of Streaming Money on Business:

We have turned out to be so acclimated with the fortnightly or regularly scheduled payroll interval that we accept this as a given in business and as representatives. However 2018 imprints the year when this is never again a required standard. One exceptionally energizing nature of blockchain innovation is miniaturized scale instalments. Another is savvy contracts. These can be joined in fascinating ways, one of which is to make gushing cash. Despite the fact that this was anticipated years prior by Andreas Antonopolis the fact of the matter is simply happening as expected at this point.

Bitcoin initially had charges so low this was about conceivable however arrange stopping up made smaller scale instalments leave. This year we are seeing the lightning system and Raiden organize picking up steam. These both bring back quick small scale instalments.

With a straightforward savvy contract, a worker can be paid progressively while they are working. What's more, this implies really working. Projects can undoubtedly follow keystrokes; see that they are not investing energy in Facebook, and measure efficiency. At that point pay, progressively as they are working. No compensation for smoke breaks. No compensation for that 5 minutes at the water cooler.

This is favourable position both for the business and the worker. Impetuses are adjusted and better workers will be paid better. Need to gain some additional, remain late and fill your record continuously. Numerous organizations as of now use administrations like Upwork. These administrations track remote representatives work progressively. It's anything but a stretch to copy this and simply change the instalment framework.

7. Blockchain and the Future Job Prospects

Numerous specialists have as of late noticed that the interest for the individuals who have down to earth blockchain execution learning has far outpaced supply, viably making it a kind of "blessed vessel" for tech selection representatives.

IV. REVIEW OF LITERATURE

A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman [1] talk about the basic requirement for development, as personalization and data science brief patients to take part in the subtleties of their medicinal services and re-establish organization over their therapeutic information. In this paper, MedRec: a novel, decentralized record the executives framework to deal with EMRs, utilizing blockchain innovation is proposed. This framework will as far as anyone knows give patients an extensive, permanent log and simple access to their restorative data crosswise over suppliers and treatment destinations. Utilizing one of a kind blockchain properties, MedRec oversees verification, privacy, responsibility and information sharing– pivotal contemplations when dealing with delicate data. A secluded plan coordinates with suppliers' current, neighbourhood information stockpiling arrangements, encouraging interoperability and making the framework advantageous and versatile. MedRec will boost medicinal partners (scientists, general wellbeing specialists, and so forth.) to take an interest in the system as blockchain "excavators". This gives them access to total, anonymized information as mining rewards, as a by-product of continuing and verifying the system by means of Proof of Work. MedRec consequently empowers the development of information financial matters, providing huge information to enable analysts while connecting with patients and suppliers in the decision to discharge metadata. The reason for this short paper is to uncover, preceding field tests, a working model through which we dissect and talk about our methodology.

J. Zhang, N. Xue, and X. Huang [2] talk about current advances of portable figuring and remote detecting inciting the idea of unavoidable interpersonal organization (PSN)-based medicinal services. To understand the idea, the centre issue is the manner by which a PSN hub can safely impart wellbeing information to different hubs in the system. In this paper, a protected framework for PSN-based medicinal services is proposed. Two conventions are intended for the framework. The first is an improved rendition of the IEEE 802.15.6 showcase verified affiliation. It sets up secure connections with unequal computational prerequisites for cell phones and asset constrained sensor hubs. The second convention utilizes blockchain strategy to share wellbeing information among PSN hubs. A convention suite is acknowledged to contemplate convention runtime and different elements. Also, human body channels are proposed for PSN hubs in some utilization cases. The proposed framework shows a potential technique for utilizing blockchain for PSN-based applications.

Minerva Panda, Syed Mohd Ali, Sanjog Kumar Panda [3] talk about the social insurance data kept up in the present Indian situation, where it is freely kept up by medical clinics , establishments and not promptly available in a brought together, educated way. This enormously restrains the wellbeing suppliers' endeavours to improve quality and productivity. This paper tends to this issue on bringing different data from numerous sources into one spot progressively which can be genuinely life sparing. Additionally, low proportion of specialist to tolerant and the low per capita salary in India climbs the medicinal costs consequently expanding the patient's detachment to get appropriate social insurance in their span particularly for individuals in the country zones. A methods by which the extension between the patients and specialists can be gapped and how patients can be treated at a lower cost is the prime concern. This paper centres on the improvement of a versatile/web application, through which patients sends their symptomatic inquiry to the specialists through a server. The versatile application will be furnished with medical aid guidelines, as indicated by the nature and seriousness of the manifestations, either the patients are coordinated to particular divisions or given crisis help for further treatment. Inside the time tremendous measure of information is gathered from clients and specialists, this enormous information will be utilized to prepare machines to mechanize the undertakings somewhat. The data picked up from breaking down huge measures of amassed wellbeing information can give helpful understanding to improve quality and proficiency for suppliers and safety net providers alike. This makes the patients connect for medicinal services arrangements effectively and

economically and makes social insurance a simple reach for the unprivileged too. In this way, this brought together model can fill in as an information gathering, conveyance just as a diagnostic instrument in the medicinal services space.

X. Liang, J. Zhao, S. Shetty, and D. Li [4] talk about the information affirmation and flexibility as vital security issues in cloud-based IoT applications. With the broad reception of automatons in IoT situations, for example, fighting, agribusiness and conveyance, compelling answers for secure information trustworthiness and interchanges among automatons and the control framework have been in dire interest to forestall potential vulnerabilities that may cause substantial misfortunes. To verify ramble correspondence amid information gathering and transmission, just as protect the trustworthiness of gathered information, this paper proposes a dispersed arrangement by using blockchain innovation alongside the conventional cloud server. Rather than enrolling the automaton itself to the blockchain, the paper proposes to stay the hashed information records gathered from automatons to the blockchain arrange and create a blockchain receipt for every datum record put away in the cloud, diminishing the weight of moving automatons with the point of confinement of battery and procedure capacity while increasing improved security certification of the information. This paper displays verifying automaton information accumulation and correspondence in mix with an open blockchain for provisioning information honesty and cloud examining.
Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu and Danyi Li [5] examines the versatile and wearable innovation, individual wellbeing information conveys monstrous and expanding an incentive for human services, profiting both consideration suppliers and therapeutic research. The safe and advantageous sharing of individual wellbeing information is pivotal to the improvement of the communication and coordinated effort of the human services industry. Looked with the potential security issues and vulnerabilities existing in current individual wellbeing information stockpiling and sharing frameworks, just as the idea of self-sovereign information possession, an inventive client driven wellbeing information sharing arrangement is proposed by using a decentralized and permissioned blockchain to ensure protection utilizing channel development plan and upgrade the personality the board utilizing the participation administration bolstered by the blockchain. A portable application is conveyed to gather wellbeing information from individual wearable gadgets, manual info, and restorative gadgets, and synchronize information to the cloud for information offering to human services suppliers and medical coverage organizations. To protect the honesty of wellbeing information, inside each record, a proof of trustworthiness and approval is for all time retrievable from cloud database and is moored to the blockchain organize. Additionally, for adaptable and execution contemplations, a tree-based information preparing and clumping technique is embraced to deal with huge informational collections of individual wellbeing information gathered and transferred by the portable stage.

V. PROPOSED WORK

Increasing usage of technology that can be worn on the human body and the Internet-of-Things has led to opportunities and blockers to the healthcare domain. With the use of cloud and big data analytics, the data individual devices leads to considerable data related to health and insights can be drawn. Medical professionals can use this data to link with other Electronic Health Record data, to enable health monitoring, sickness detection and cure. Insurance companies can make thorough and planned procedures according to individual cases, profiting patients to select flexible insurance plans as per requirements. However, for health data sharing between institutions, issues such as security and interoperability come into play. Health data are privacy-sensitive, more so considering amount of health data being stored in cloud, increasing the hazards of exposure of data. Existing systems use centralized architecture, which requires centralized trust. Blockchain depends on replacing names with identifiers and public key infrastructure (PKI), keeping the privacy of the users. The subsequent sections below give a broader understanding of the proposed system.

VI. SYSTEM ARCHITECTURE

Below figure outlines the system architecture of this application:

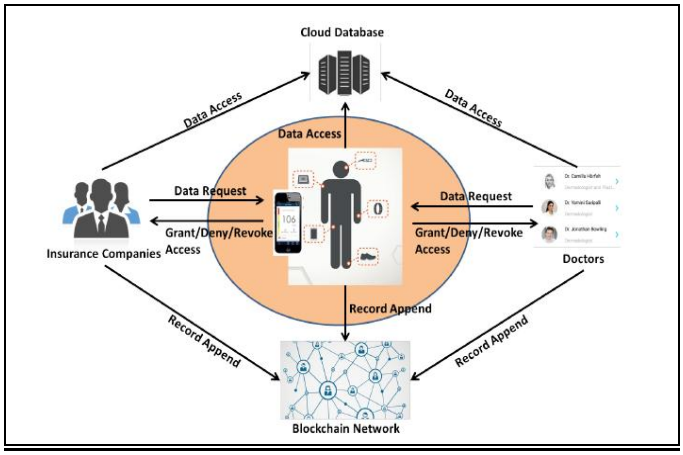


Figure 1

1. User: User is the personal health data owner who is responsible for grant/deny/revoke of access to data from other parties like healthcare providers and insurance companies. If user wishes to get a treatment, he/she will share the relevant medical data with the doctors of choice. Once treatment is done, data access is revoked so that future access is not permitted. This also applies to user-insurance company tie-ups. User can also keep track of daily activities according as per prescribed treatment which includes medicine consumption schedules to share with the provider of treatment. The data is uploaded to cloud.

2. Wearable Device: Wearable Devices does the job of converting health info into readable format. This data is then made in sync to user's online account. A set of wearable devices are associated with each account. Once health data

is created, it will be uploaded to blockchain network for integrity protection and for storage.

3. Healthcare Provider: Doctors or hospitals are selected by a certain user for medical test, who in turn prescribe treatment. With user's permission, this treatment data can be shared with other healthcare providers after uploading in blockchain network. Also, the existing healthcare provider can seek access to old health data of user. All these requests and accesses given by user are recorded the blockchain.

4. Health Insurance Company: User may request a health insurance provider or an insurance agent for an insurance quote for the user's treatment. To be able to provide an appropriate insurance policy, the insurance companies may seek access to blockchain data of medical treatment and previous medical history. Considering the blockchain blocks are immutable, user cannot alter previous medical data already recorded in the blockchain, which ensures accurate information is provided to insurance companies as well. The insurance claims can also be logged on the blockchain.

5. Blockchain Network: Blockchain network is used for following purposes: a) Health data collected from both devices and healthcare providers are uploaded to blockchain network for integrity. b) For access to health data from healthcare provider and insurance company, each data access request should be processed to get a permission from the data owner. c) All access requests and access granted/revoked etc activities should be recorded in blockchain network.

6. Cloud Database: The cloud DB stores user health data, data requests from the healthcare provider and insurance companies, data access record and data access control policy. Data access is accountable and traceable. Once data leakage is detected, the malicious entity can be identified.

VII. IMPLEMENTATION

A. Personal Health Data Collection:

Information and data for personal health originates from wearable gadgets, for example, action trackers or keen watches, and restorative gadgets, for example, pacemakers, just as manual user input for treatment following, for example, prescription use and imparting training. To synchronize the individual information to the cloud for easier access and further usage, the client initially can enrol to the cloud specialist organization for an online record with enough storage. Figure 2 demonstrates the information accumulation and synchronization engineering.

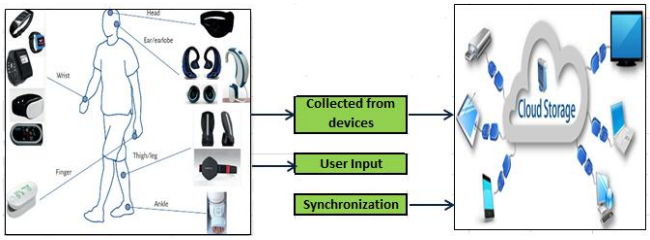


Figure 2

B. Personal Health Data Integrity Protection and Validation

Figure 3 demonstrates the fundamental information stream from the client gadget to the cloud server, at long last tied down on the record with verification of uprightness and approval. The wellbeing information originates from an assortment of gadgets throughout the day, bringing about countless records. To encourage adaptable and proficient information preparing and respectability insurance, we build up a tree-based strategy for the honesty the board of wellbeing information record. A few information records are bunched to frame a tree-based information structure and handle dynamic information enrolment. The appropriation of Merkle tree understands the versatility prerequisite, and in particular improves the productivity to approve the information respectability. Merkle tree is a double tree structure where the information is a rundown of hashed information records. These records are requested when they are produced. Each two records are gathered and the hashes of the two information records become two leaf hubs of the Merkle tree and thusly comprise an abnormal state bunch hub with the gathering hash created by linking two hashes. Two gathering hubs will pursue a similar method to produce another larger amount bunch hub with another hash. This progression is rehashed until there is a solitary hash which will end up being the tree root, that is, the Merkle root.

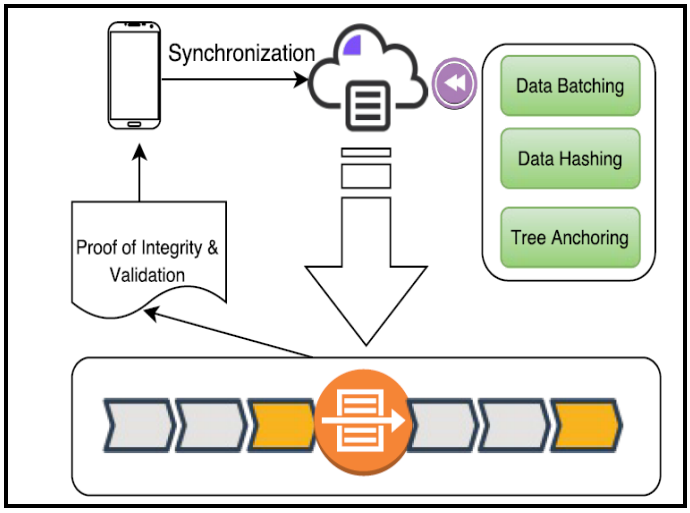


Figure 3

Chainpoint is an open standard for making a timestamped evidence of any information, document, or arrangement of occasions, which proposes an adaptable convention for distributing information records on the blockchain and creating a Merkle confirmation for every datum record. In our usage, we stay a rundown of information records to different Fabric channels by restricting the Merkle root to a blockchain exchange and confirm the uprightness and presence of information without depending on a confided in outsider. The hash of information records brings two points of interest. For a certain something, each Merkle tree can have a substantial number of records since just the hash of the information record is put away. For another, the hash is a viable measure to distinguish changes so that once a bit of information is altered, the activity can be recognized effectively by navigating the tree.

C. Data Sharing and Healthcare Collaboration

The client can impart information to human services suppliers to look for medicinal services administrations, and with insurance agencies to get a statement for the protection approach and to be guaranteed. At the point when information sharing is recognized in the framework, there will be an occasion produced to record the information get to ask for. The occasion record can be portrayed utilizing a tuple as frecordhash, proprietor, beneficiary, time, area, expiry date, and mark. There are distinctive sorts of tasks from various gatherings, as recorded in Table 4.1.

TABLE 1: Types of Operations in the Healthcare Collaboration System

Health Data	Operator	Operation
Personal Health Data	User	Update, Query
	Healthcare Provider	Query
	Insurance Company	Query
Medical History	Healthcare Provider	Update, Query
	User	Query
	Insurance Company	Query
Insurance Information	Insurance Company	Update, Query
	User	Query
	Healthcare Provider	Query

Table 1

This record is then submitted to the blockchain arrange which is trailed by a few stages to change a rundown of records into an exchange. A rundown of exchanges will be utilized to frame a square, and the square will be approved by hubs in the blockchain arrange. After a progression of procedures, the honesty of the record can be safeguarded, and future approval on the square and the exchange identified with this record is accessible. Each time there is a task on the individual wellbeing information, a record will be reflected to the blockchain. This guarantees each activity on close to home wellbeing information is responsible. We execute an entrance control conspire by using the Hyperledger Fabric participation administration segment and the channel plot, as is appeared in Figure 4.4. The CA, otherwise called the enrolment specialist co-op, is in charge of participation enrolment by issuing enrolment testaments and exchange declarations for taking an interest hubs in the Hyperledger Fabric blockchain organize and taking an interest Fabric customer, and creating the entrance control list amid channel foundation as indicated by client settings and activities. Distinctive access type can be determined in the authentication, for example, inquiry and update tasks for chaincode execution in the channel. Chaincode is a bit of code that is sent to Hyperledger Fabric for empowering connections among companions and the mutual record. There are three activities on the chaincode, including send, summon and inquiry. A chaincode can be introduced on a blockchain by executing a convey exchange while a chaincode execution is propelled by summon exchanges. Channel is shaped to detach singular exercises among approved gatherings.

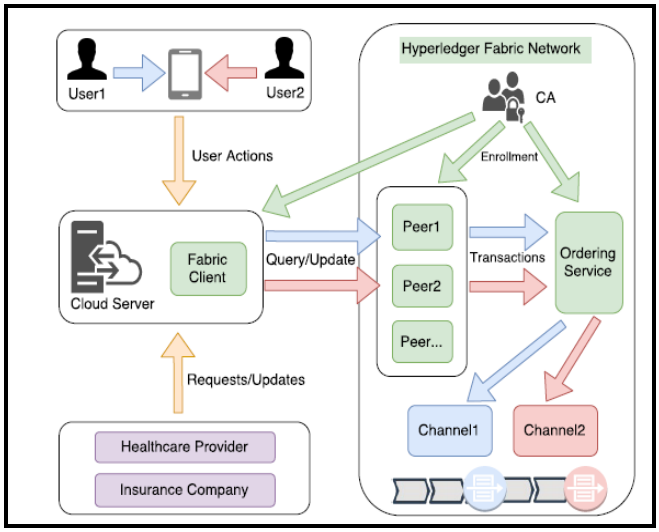


Figure 3

To give detachment between various information sharing space, the CA issues declaration to the Fabric customer on the cloud server, blockchain organize peers for exchange approval, and the orders (for requesting administration). We have two channels set up for two clients, individually. In Figure 3, both user1 and user2 may perform information gathering and synchronization on their individual portable stages, and the social insurance versatile application will send web solicitations to the cloud server to for information synchronization or inquiry. Social insurance suppliers and insurance agencies additionally speak with the server to ask for or update wellbeing information and medical coverage data. With the authorization from clients, these solicitations will be permitted to take an interest in a specific channel. The cloud server is arranged with a Fabric customer to speak with the Fabric blockchain organize peer. For various client exercises, the information will be marked with various channel ID to recognize disconnected area. The inquiry or update demands from the server will be sent to the Fabric arrange through Fabric customer for exchange affirmation. Conveyed companions will approve the approaching solicitations and propose exchanges by executing chaincode. The requesting administration is in charge of checking exchange marks and request them with channel IDs. For each channel, there is a subledger, as a component of the framework record, to record all exchanges as squares. For security concerns, the client can specifically impart wellbeing information to information requester, in view of the need of how close to home wellbeing information is required to help the human services administration. For instance, a client's protection history may not be significant when the client is conversing with a dental specialist. Thus, the client's dental treatment isn't fundamental for skin testing or other treatment. To issue a particular declaration, the client can state unmistakably in the authentication what classification of individual information is permitted get to, regardless of whether read-just or read-compose get to is permitted. In addition, in various channels, diverse grained data is shared. In this sense, our framework gives a client characterized, fine-grained security assurance and access control approach, upgrading the information responsibility for.

VIII. MATHEMATICAL MODEL

ECDSA (elliptic curve digital signature algorithm) is the base by means of which a blockchain leads to transaction acceptance. ECDSA is an equation like y2 = x3 + a x + b. These values are generally a=0 and b=7 for most blockchain implementations (for e.g. bitcoin). The corresponding graph for this is y2 = x3 + 7 (Figure 4).

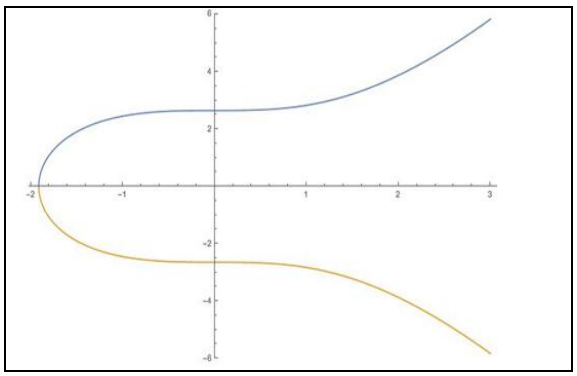


Figure 4

One property of elliptic curves is that a non-vertical line intersects two points (non-tangent), leading to the line intersecting the curve at a third point always. In reality, one can characterize "expansion" on the bend as finding that third direct comparing toward two given focuses. This is essentially what is done in ECDSA, then again, actually the tasks are performed modulo some expansive prime number M.

In particular, in ECDSA, addition of two points (p1,p2) and (q1,q2), and the doubling of (p1,p2), are performed as follows:

Addition of (p1,p2) and (q1,q2):
c = (q2 – p2) / (q1 – p1) mod M
r1 = c2 – p1 – q1 mod M
r2 = c (p1 – r1) – p2 mod M

Doubling of (p1,p2):
c = (3 p12) / (2 p2) mod M
r1 = c2 – 2p1
r2 = c (p1 – r1) – p2

"Division" is shown in the primary line of every calculation. This means the item, modulo M, of the articulation to one side of the cut by the multiplicative inverse (MI) of the articulation to one side of the cut. Since M is a prime, each nonzero whole number from 1 to M-1 has a MI. For instance, the MI of 5 mod 17 is 7, in light of the fact that 5*7 = 35 = 1 mod 17; at the end of the day, 5-1 mod 17 = 7. By and by, these inverses are quickly determined by methods for the Euclidean algorithm, where one gathers the divisors with a specific goal in mind.

One other primer detail is the means by which to "multiply" in this mathematical structure, specifically to ascertain an articulation, for example, *m * (p1,p2)* for some whole number m. This should be possible by first multiplying the info (p1,p2), and after that utilizing the addition over and over until m duplicates of (p1,p2) have been included, however this obviously isn't functional when m and M are huge, as they are in genuine blockchain applications. Rather, such "multiply" tasks are normally done utilizing the binary algorithm for multiplication, which we will outline here for standard whole numbers however which can be effectively adjusted to ECDSA:

To calculate *r = n * b mod M*: First set t to be the biggest power of two with the end goal that t < =n, and set r = 1. At that point perform:

A: If n >= t, set r = b + r mod M, and set n = n – t; else set t = t/2.

B: If t >= 1 set r = 2 * r mod M, and go to A (if t < 1, we can conclude).

IX. CONCLUSION

The paper [2] addresses the adoption of blockchain in social network domain but not fully explores the benefits of the blockchain.
[4] addresses the blockchain adoption in Internet of Things environment. [1] proposes a record management system focusing on EMRs using smart contract, but raises privacy concerns.
In the paper [5] that has been taken as base for this seminar, the authors have suggested design and implementation of a mobile healthcare system for personal health data collection, sharing and collaboration between individuals and healthcare providers, as well as insurance companies. The system can also be extended to accommodate the usage of health data for research purposes. By adopting blockchain technology, the system is implemented in a distributed and trust-less way. The algorithm to handle data records can preserve both integrity and privacy at the same time. Meanwhile, the paper adopts the concept of channel supported by Hyperledger Fabric to deal with the isolated communication required by specific scenarios. In the future, the authors will explore how to combine both personal health data and medical data together and cover a broader scenario. From the paper, it can be concluded that the system can handle a large dataset at low latency, which indicates the scalability and efficiency of the data process. By adopting Merkle tree method to batch data, we implement an algorithm with the computation complexity of O(log2n). This is an important advantage when the data records are collected at high frequencies.

X. ACKNOWLEDGMENT

With immense pleasure, we are publishing this paper as a part of the curriculum of M.E. Computer Engineering. It gives us proud privilege to complete this paper work under the valuable guidance of Principal for providing all facilities and help for smooth progress of paper work. We would also like to thank all the Staff Members of Computer Engineering Department, Management, friends and family members, who have directly or indirectly guided and helped us for the preparation of this paper and gave us support right from the stage when the idea was conceived.

REFERENCES

[1] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using Blockchain For Medical Data Access And Permission Management," in Open and Big Data (OBD), International Conference on. IEEE, 2016.

[2] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," IEEE Access, 2016

[3] Minerva Panda, Syed Mohd Ali, Sanjog Kumar Panda, "Big data in health care: A mobile based solution," in International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). IEEE, 2017.

[4] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using Blockchain" in Military Communications Conference, MILCOM 2017. IEEE, 2017.

[5] Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu and Danyi Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications", IEEE, 2017

Few other sources referred:
https://www.newgenapps.com/blog/future-of-blockchain-technology-applications
https://medium.com/yope-chain/30-things-you-can-do-with-a-blockchain-b23b2ab39664
https://medium.com/yope-chain/five-blockchain-development-challenges-for-legacy-organisations-e0f57e6b808c

