SURVEY ON MEDICINE SUPPLY CHAIN USING BLOCKCHAIN TECHNOLOGY

Kuntal Chaudhari[1], Poonam Ghadage[2], Dhanashree Ghodvinde[3], Shivani kedar[4], Prof. Kanchan Doke[5]
Department of Computer Engineering
[1,2,3,4,5] Mumbai University

Abstract- *Evolved from the Merkle Tree, Blockchain Technology is a fully decentralized digital register which keeps a secure history of data exchanges. The decentralization aspect of Blockchain Technology does away the need of any central authority for managing it. In this paper we present a comprehensive overview on blockchain technology. We first begin by shedding light on the fundamentals of Blockchain Technology then we analyse some typical algorithms used in various blockchains. Blockchain, the foundation of Bitcoin, has received extensive attention recently. Being an ineradicable data storing technology, Blockchain can be used not only in financial assets but anything which has some value. However, being a human invention, downsides are even here in the blockchain technology such as scalability issues, security problems, and not-so-user-friendly for non-technical people. Next, with common technical issues we have talked about the recent advances. We lastly conclude this paper by laying out possible future developments of blockchain technology.*

I. EXISTING SYSTEM

In todays world it is very necessary to secure our systems as the output that we get after performing every action is same regarding both the system so the question is how the existing system different from the current system. Our day-to-day operations generate constant data flow. When you use your credit card to transfer some money for your dear nephew or send a contract to your partner to sign, you send them a copy, not an original. What's more, if, on account of a Word report, it's conceivable to have two models of a document (the unique rendition and the one you sent), some different resources (like cash) can't be copied. In this way, everybody must make certain that after you made an installment, you don't have another form of a similar money that can be exchanged to somebody else. Traditionally, we rely on some mediators, like banks, that hold all the data in one database or data center. It has the only copy of data, and, in theory, everyone involved has access to it. Reality is a little bit different and more complex, however. Apart from the fact that we must trust those intermediaries when submitting our info, there are problems that appear over time. The actuality that everything is put away in one spot (which means it's brought together), makes it powerless against assault. Additionally, as on account of the previously mentioned contracts, opposite sides can't take a shot at a similar report at the same time, which makes issues of renditions that may be lost, documents moving all over between the beneficiaries, and other burdens, for example, time delays. As the output which we are getting is same but it is very important to consider many factors such as transparency, security and shared trust. When we are performing any transaction it is important to secure it, as nowadays people are facing enumerous problems but in this system there is no shared trust. For example, if we are performing any transaction between the entities which do not trust each other then the intermediary entities between them such as VISA,SWIFT etc. there can be many failures from single point. Sometimes there may be latency problem between the transactions, so it is very important to maintain the trust between each other so this system does not provide that much of shared trust between them.

The second main factor making difference is reconciliation occur while storing records of every entity which delays the settlement so reconciliation is needed in this system. Reconciliation is an accounting process that uses two sets of records to ensure figures are correct and in agreement. It confirms whether the money leaving an account matches the amount that's been spent, and ensures the two are balanced at the end of the recording period. Reconciliation provides consistency and accuracy in financial accounts. But time delays occur in the system due to this so this is second most factor.
The third main factor is that in this system there is no distributed databases so manual efforts are more in the system. There must be copy of every activity happening in the processes and so it is essential to maintain a copy of every entity participating in the system. So there is manual exception handling in this system so this factor should be eliminated from the system as it disturbs the consistency in the system. There will be high impact on the system mainly in the health sector if due to manually any errors occurred in this system while maintaining the records, then its consequences may result badly. As the data in this sector is quite sensitive so it is important to make sure that their data should be secure.

In this system, there are many intermediary entities participating in this system and controlling the system such as there is a central authority in this system looking every small to small things who is responsible for every modification done. There is access to the third parties so that they can make or perform any changes needed in the system. So here security issue arises and most probably that due to the entities working between the system so it does not have peer to peer network which may results in increased transaction costs and may increase the real time execution of the system.

For example, If you want to deal with your family related financial issue regarding your property and investment so you will first contact the lawyer which will act like the central authority taking control over your issue, so this can take time as well as increase the transaction cost due to that lawyer so if there is no such central authority only one system where you can interact and solve your problem by sharing your identity only with those people with whom you want to share and where your time is consumed.

1.1 ADVANTAGES:

- ***Transparency:***

The existing system provides transparency throughout the system, as transparency means good communication, better fluency in the system. There is better interaction in the system as there are many entities working throughout the system. Any modification in the system does not affect the user level, which indeed means that the transparency in the system is maintained.

- ***Consistency:***

Data integrity implies data consistency, Multiple users access a database. Some read values while some others update these same values. Consistency assures that this data is same across all its present copies in the databases. Any user can update, modify, or even read the data which ensures that the consistency is maintained.

- ***Mutability:***

Mutability means that the data can be changed as per user satisfaction, where in other system the data cannot be changed so this is the one major drawback in the system. Mutability means the quality of being changeable.

1.2 DISADVANTAGES:

- ***Time consuming:***

This system takes a lot of time for processing the data, as it provides good output but the time taken is greater then the usual. Due to which sometimes it becomes quite difficult for the others to complete their desired task on time. So the accuracy decreases throughout the system.

- ***Insecurity:***

The system acquires a major risk of insecurity. Insecurity within the system can later on turn into a huge big issue or a problem so it is very important to assure that the system is secure. As nowadays there is a great necessity of security within the entire system.

- ***No traceability:***

If the system does not provide traceability then the supply chain also disturbs, the same affects the security also. Traceability mainly refers to track the needs of every user within the system. While performing the transactions, traceability should be maintained.

- ***High transaction cost:***

As there are many intermediary entities in the system so dependency increases. Transaction cost increases due to this entities, while performing any big deals, so it was the basic necessity that this entities should be eliminated.

- ***Need manual efforts:***

This system needs manual efforts throughout that means to maintain records in the system or to modify or to update the data in the system manual efforts are needed. This is increases the timestamp within the system. As this system does not have distributed databases.

- ***No shared trust:***

Entities who do not trust each other transact so there should be shared trust between the system. so this is a major problem in this system as there are many entities in the system playing their respective roles in the system.

- ***Third party access:***

This system have central authority controlling the entire system. So the third parties can access the system which increases the cost and also affects the real time execution of the system. Due to this insecurity also increases in the system.

II. BLOCKCHAIN SYSTEM

To tackle the issues referenced above, look into researcher Stuart Haber and W. Scott Stornetta in 1991 began taking a shot at a cryptographically-verified framework where timestamps of the docs couldn't be balanced or then again antedated. The main huge outcomes on the field of the blockchain were, be that as it may, accomplished more than 10 years after the fact by Satoshi Nakamoto when he utilized Haber and Stornetta's plans to build up Bitcoin's framework. Somehow or another, blockchain presents another technique for things to be done: each hub can see all exchanges that are occurring in the framework what's more, ought to get a duplicate of every one of them to refresh its information and, basically, favour it. Essentially, it is only another method for putting away information. The main thing that isolates it from the officially existing advancements for information stockpiling is the means by which the entire procedure is finished. The blockchain is based on the rule that all data ought to be dispersed over various areas rather than only one, utilizing the most abnormal amount of cryptography. It implies that all members are associated with each other and have a similar duplicate of given information.

On the off chance that you have utilized downpours before, you most likely seen a few similitudes. Subsequently, innovation gives us a decentralized variant of the database or a computerized record of exchanges that are accessible to anybody in the system. It enables clients to use distributed correspondence with each other by bypassing outsiders (information stockpiles) in practically any task. I won't make a plunge the procedure, yet essentially, it includes understanding a computational issue (see infographics underneath for a progressively point by point clarification). These squares are at that point added to effectively existing ones making a chain (consequently, the name) where all data is maintained in sequential control and can be effectively gotten to (which makes it really open). When you become a piece of the framework, you are given two keys: open (your location or, for effortlessness, your username) and private (your secret phrase). As such, a programmer can't submit any offense since the individual should discover and adjust a particular hinder in addition to all the previous ones, yet as you definitely know, every one of the squares are found over all the current PCs, all the while. In addition, they are encoded with extraordinary scientific capacities (client's private keys). With such a rich and, at first sight, a subtle strategy, the powerlessness issue turns out to be practically insignificant. Presently, in 2018, it turned into a type of an resource that can be put resources into for individuals who are looking for circumstances and not hesitant to go for broke .Even though the market is highly volatile, the demand is huge. Cryptocurrency is a form of digital currency that uses encryption techniques to regulate its amount and validate funds transfer, operating independently of a central bank. Blockchain seems to be particularly useful for monitoring the movement of goods. Because every transaction goes onto the ledger, and because every node in the system4)keeps a duplicate of each exchange, it takes into account moment access to data about a item's wellspring of beginning and who took care of it at each port. The blockchain in other words, is the inverse of the web. It has a fat convention layer and a meager application layer. frameworks have obviously existed for quite a long time, however what's happening about blockchains is that they enable it to occur at a mass, web level scale, without the requirement for a concentrated administration instrument, and notwithstanding the resistance of amazing foes.

ADVANTAGES:

health records:

Additionally, as a disseminated record based innovation, where all members keep up a duplicate of the record, it dispenses with manual endeavors and deferrals because of compromise needs since information consistency is a key quality of the disseminated record, Blockchain can help by using the cryptographically-secured consensus protocols that assure validation and agreement by all relevant parties, as well as real-time replication of data to each participant's copy of the ledger.

Traceability:

The main advantage of using this application is medicine supply chains merely track and store orders and deliveries, with providing features as transparency, traceability and auditability . In the medicine supply, in order to maintain trust and reliability along the whole supply chain, it is essential for the stored records to be tamper-proof, while the best case would be if each actor issuing transactions could do that without relying on any centralized third-party intermediary.

Shared trust:

In numerous ways, you can do with concentrated frameworks what Blockchain guarantees to do? with one center contrast; trust. That is the enormous favorable position for Blockchain, anyway as expressed, blockchain is certifiably not a silver projectile to settle all utilization cases, at that point there are a couple of helpful inquiries that one ought to be requesting to decide blockchain materialness.

Secure:

The security component is that the hashes likewise fill in as the connections in the blockchain. Each square incorporates the past block unique hash. Checking whether hash matches is block, anyway is simple, and once the hubs have done as such they update their separate duplicates of the blockchain with the new square. This is the consensus protocol.

Peer-to-peer network:

an advanced Record of exchanges that are accessible to anybody in the system. It enables clients to use distributed correspondence with each other by bypassing outsiders (information stockpiles) in nearly any operation.

Authorized participants access data:

The third feature is authentication. Each action that takes place on the blockchain is associated with a private key that belongs only to individual actors. Unlike traditional enterprise systems, there’s no such thing as administrator privileges. This gives blockchains much better security, something that everybody appears to ignore as a result of the innovation's initial relationship with the clearance of unlawful merchandise. During a time of enormous information ruptures and wild worldwide cybercrime, the planning of another innovation touching base to take care of this issue is especially helpful.

Reduced transaction cost:
Blockchain as a decentralized, distributed system with no focal or controlling expert, implies taking out delegates that outcomes in diminished exchange costs and close ongoing exchange execution, which is a route not the same as what has been finished by monetary establishments, exceptionally while exchanging cash abroad.

Immutability:
Once an exchange or a bit of code is affirmed, the data is permanent?— ?its absolutely impossible an individual or gathering of people can fudge it without assuming control more than a huge number of PCs all the while. Furthermore, each new advance going ahead can possibly be substantial in the event that it expands upon the unchangeable group of past action.

2.2 DISADVANTAGES:

Slow transaction:
Because of their complex, encoded nature, blockchain exchanges can be moderate, particularly contrasted with current Mastercard ones. Only for correlation, a Bitcoin exchange can take as long as 5 hours to complete, which makes the likelihood to pay for your supper utilizing cryptographic money profoundly far-fetched. Besides, as they develop in size, these blockchains become increasingly perplexing and fantastically cumbersome, which will in the long run make them much slower.

Complex: As the chain of blocks grows, the algorithms becomes more complicated. As here we use SHA algorithm where it is very difficult to predict the input by the given output. There are data in the form of different blocks so the work has to be done by individual block itself due to which work load increases.

Lack of regulation:
lack of regulation creates a risky environment. Because of inadequate administrative oversight, blockchain is a rearing ground for con artists what's more, showcase controllers. For instance, a viewpoint (at first sight) cryptographic money Oncecoin, which guaranteed its financial specialists to turn into "the following Bitcoin," ended up being a cunning Ponzi conspire that denied a large number of individuals of their cash.

ACKNOWLEDGMENT

Having endured the experience, there were many who helped us in our project and we very much like to thank everyone. We are profoundly obliged to our HOD Dr. D. R. Ingle, for giving us this significant chance to do this task and we express our generous gratitude.

We also thank our project guide Prof. Kanchan Doke and our coordinator Prof. Rahul Patil for kindly helping and advising during the work and also who gave this opportunity to work on this paper on “SURVEY ON MEDICINE SUPPLY CHAIN USING BLOCKCHAIN TECHNOLOGY” through which we came to know about so many new things.

It is incredible joy to recognize the assistance and recommendation, which we got from the Dept. of Computer Engineering. We thank everyone who helped us in finding information about report. Much good help and support has given on various events by our entire family.

CONCLUSION

Blockchain is a revolutionary technology which has changed the way people interact with the Internet. In this cyber world, where nothing is private, and no data is safe, Blockchain has shown promising potentials of being the best bet of people dealing with the value-sensitive commodities. In this paper we have discussed about the basics of blockchain technology which can be used as a reference for people new in this field. We have also outlined its possible application and the challenges it faces. The aim of this paper is to provide a comprehensive readymade idea of the working of blockchain technology which can be used by students or whoever interested in getting familiar with this revolutionary technology.

REFERENCES

[1] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective,” 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618

[2] V. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, 2014.

[3] P. Vasin, “Blackcoins proof-of-stake protocol v2,” 2014. [Online]. Available:https://blackcoin.co/blackcoin-posprotocol-v2-whitepaper.pdf

[4] NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015. [Online]. Available http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[5] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc: eee:monogr:9780128021170