BLOCKCHAIN: UNDERSTANDING IT'S POTENTIAL

Charmee Mehta, (Student)
Swathy Dhanesh, (Student)
Radhika Patwardhan, (Sr. Lecturer)
Neeta Kadukar (HOD IT)
Information technology department,
SVKM's Shri Bhagubhai Mafatlal Polytechnic,
Mumbai, India.

Abstract **:** Based on blockchain, the internet is entering a second era. The first era was sparked by a confluence of computing and communications technologies. But this second era will be completely driven by a clever combination of cryptography, software engineering and behavioral economics. The blockchain technology is also called as distributed ledger technology. Like the internet, business models get upended and industries get disrupted by the advent of blockchain technology. But, blockchain has established itself as the world's leading software platform for digital assets.

This paper is an effort to pioneer for presenting the use of Blockchain technology in a broad spectrum. The concepts are interchangeable to a mass scale of industries as finance, healthcare and cloud computing where safety, measurability and efficacy must meet.

Keywords **— Blockchain, cloud computing, healthcare, IoT, e-voting system.**

I. INTRODUCTION

Blockchain technology was actually introduced for the Bitcoin, it facilitates secure online transactions. Basically, blockchain is a decentralized and distributed digital ledger that facilitates recording of data spanning through various computers so that the record cannot be changed later on without the alteration of all subsequent blocks. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. [1]

Blockchain is an emerging technology with a lot of hype being generated around it. It may bring a new era of decentralized although the technology is likewise subject to certain clichés. [2] The word blockchain comes from Satoshi Nakamoto's original Bitcoin white paper from 2008. [3] Although the word Blockchain has not specifically been mentioned, it does describe a technology component. Although most of the components specifies in the paper had existed in the 80's and the 90's the processing power required wasn't available then.

The major reasons for the popularity of the blockchain technology are:

- Decentralized systems
- Distributed ledger
- Secure
- Minting
- No single point of failure

APPLICATIONS

- Cryptocurrency
- Financial instruments and asset registries
- Supply chain records and product-centric data
- Healthcare
- Cloud computing
- Digital identity
- Smart contracts
- Internet of Things
- Voting systems
- Decentralized autonomous organizations

In this paper, we further talk about detail about the application of blockchain in various industries: Finance, IoT, Cloud computing, Healthcare. And then, an e-voting system model is proposed using blockchain.

II. LITERATURE SURVEY

1. The paper "Blockchain: Future of financial and cyber security" written by Sachchidanand Singh and Nirmala Singh[1], explains concept, characteristics, need of Blockchain. It has further explained what is Bitcoin, the Genesis block, the prerequisites of bitcoin such as authenticity, integrity and non-repudiation, and it's advantages. The author has also explained how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking, financial institutions and adoption of Internet of Things(IoT).

2. In the paper "A conceptual secure blockchain- based electronic voting system" written by Ahmed Ben Ayed published in International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017[12], they have described how to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The paper first explains what blockchain is, and then have proposed a system having main requirements as authentication, anonymity, accuracy and verifiability. The proposed e-voting system contains the modules requesting to vote, casting a vote, encrypting votes and adding the vote in the blockchain.

3. The paper "BroncoVote: Secure Voting System using Ethereum's Blockchain" written by Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic and Jordan Mohler[13], has proposed a blockchain-based voting system, named BroncoVote. It preserves voter privacy and increases accessibility, while keeping the voting system transparent, secure, and cost-effective. BroncoVote implements a university-scaled voting framework that utilizes Ethereum's blockchain and smart contracts to achieve voter administration and auditable voting records. In addition, BroncoVote utilizes a few cryptographic techniques, including homomorphic encryption, to promote voter privacy. Their implementation was deployed on Ethereum's Testnet to demonstrate usability, scalability, and efficiency.

III. APPLICATIONS OF BLOCKCHAIN

A. Financial Services

With blockchain which is basically based on peer-to-peer technology we are entering a new era, which has the capability to change the financial sector which we know currently. [4] The future of financial sector could be in the absence of banks but with transactions approved automatically in seconds or minutes, decreasing the transaction cost significantly and increasing the efficiency and productivity. Many are familiar with Bitcoin and other cryptocurrencies like Ethereum which work with blockchain at its base. So basically, how this system works is, transactions are grouped together in structures known as blocks, which are stored one after another forming a chain of blocks, thus deriving the name 'blockchain'. The links (connections) between the content and blocks are protected by various cryptographic techniques, making hacking nearly impossible, making previous transactions immutable. This creates a system without a central authority.

1) Why blockchain?

Some of the key factors how blockchain impact: [5]

- *Making cross-border payments more efficient:*

Exchange of money has always been a tiresome and slowly process, with high rates, this is particularly true in the case of cross-border transfers. Implementation of blockchain has the potential to speed up this process and simplify it, along with reducing the cost significantly by avoiding the middleman involved.

- *Share trading:*

Blockchain can also be used in share trading. Greater trade accuracy and a shorter settlement process can be achieved by using the blockchain technology in share trading.

- *Smart contracts:*

An emerging application of blockchain is the smart contract. Smart contracts help you in exchanging items like money, property, or anything of value in a conflict-free and transparent manner without the interference of a middleman.

2) Applications and solutions [6]

Exchanges	Merchants	ATMs
Money services	Retail banks	Payments
Brokerage	Payroll and insurance	Capital markets
Corporate banks	Investments	Financial data
Trade finance	Trading platform	Micro transactions

Table 1: Applications and solutions of blockchain in finance

- *Improving online identity management:*

With Blockchain online identity management can be implemented easily, since it is a distributed ledger system with all legible users having access to the information worldwide. Although it is still required for the user to atleast once register their identity on blockchain, after that it can be reused. It also gives the user the capability to authorize users to view their information

B. Internet of things

IoT industry is struggling with issues in privacy and reliability. [7] Blockchain technology is the only way to overcome it. Blockchain is the silver bullet needed by the IoT industry. It allows significant savings for IoT industry manufacturers by keeping tracks of countless linked devices, making the processing of transactions and coordination possible between devices. By creating a more sustainable environment for devices to work on, an approach which is not centralized would remove solitary failure points.

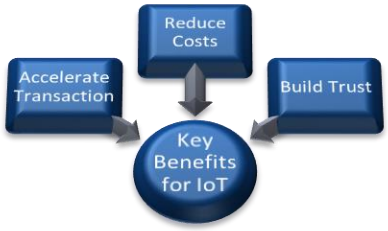


Fig.1 https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

Cryptographic algorithms used by blockchain makes the consumer data more private.

As the ledger is not present in any solitary location, man-in-the-middle attacks cannot be executed. This is because there is not a single thread of communication that can be intercepted making the ledger sustainable to changes which cannot be manipulated by unauthorized user.

The IoT network aids the blockchain in storing an ineradicable data of the history of intelligent equipment. This gives rise to autonomous functioning of ineradicable data without the need for centralized authority. Therefore, the blockchain opens the door to a series of IoT scenarios which were remarkably difficult to implement without it.

Blockchain and IoT can be integrated for secure messaging between devices in an IoT network. As shown in the above model, the message exchanges between devices like financial transactions will get treated by the blockchain.

The ability to maintain a duly decentralized, trusted ledger of all transactions occurring in a network is one of the most exciting capabilities of the blockchain. This ability is essential to drive many compliances and regulatory requirements of industrial IoT (IIoT) applications.

C. Cloud computing

Cloud innovation has been able to create an ecosystem of around trillion dollars. But the fact being, Cloud was just the first accomplishment. The next iteration of computing, for Cloud systems is Blockchain. [8]

The purpose why Cloud was innovated was to bring in decentralization. Nowadays the hardware requirements of companies are very high. This lead to the use of servers. Bu the fact is that, maintaining a server is quite an expensive affair. So moving the servers away from the worksite, to a cloud released it from the shackles of hardware restrictions. The second iteration is to this is the blockchain technology. Blockchain has been able to create networks of computations that are secure as well as democratic and immutable using distributed ledger system. Blockchain thus gives us a combined taste of transparent, un-hackable and reliable services and programs.

Every operation, which is performed with the data such as transportation, processing or storage accounted in the blockchain database. [9] Later on all that happened to the data can be easily tracked and verified by any legible user.

So if some malicious activity is performed with the data, entities who are responsible can be held and appropriate actions can be taken. This promises complete traceability of the data on cloud. The Cloud moved the servers offsite and centralized the processing power to another location. On the other hand, Blockchain distributes the computational power and scatters it across the world.

Varying from the traditional cloud solutions that was centralized, the blockchain based cloud solutions will depend on idle computational power from a pool of providers which will include individual computer users. This results in access to unlimited computational power at a comparatively lower cost since neither the providers nor the users are required to set up any infrastructure. Blockchain has the power to create a more efficient network, an internet/cloud 2.0 (next version of cloud), that further improvises security and computing power.

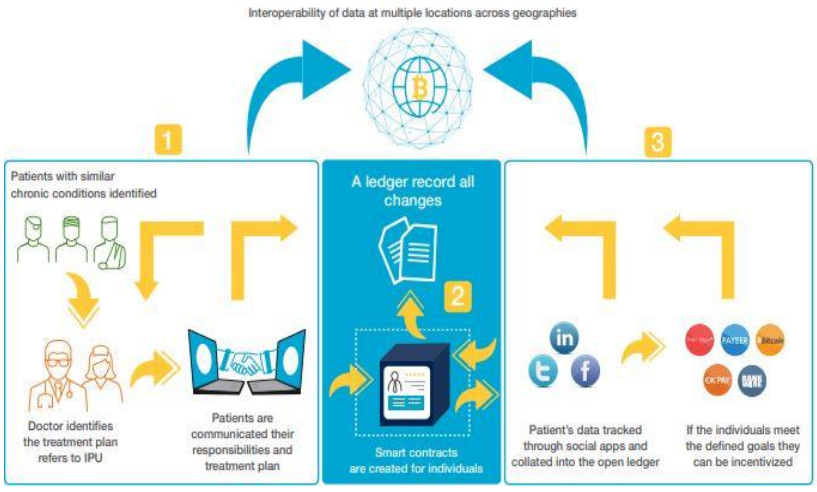


Fig. 2 https://cdn.geekwire.com/wp-content/uploads/2017/11/Screen-Shot-2017-11-20-at-4.04.56-PM-630x448.png

D. Healthcare

The key of any national economy is healthcare. [10] It contributes to 1/5th of the national economy in U.S.A. Obsolete processes, legacy data management systems and outdated infrastructure are hindering the modernization on a large scale.

Patient data is of the utmost importance in the medical industry. Blockchain makes secure storage and data access possible which on the other hand could protect and make efficient diagnosis. The integration of healthcare with tangential services of other industries, such as insurance is feasible. To make this kind of inter-industry collaboration exist, ICON (ICX) is working on ecosystem. The legacy systems still exist in developing nations, which are many steps behind their developed counterparts. Blockchain is helping to the developing nations to get acquainted with developed countries, by rapidly modernizing their healthcare services as it betters patient healthcare and generates revenue.

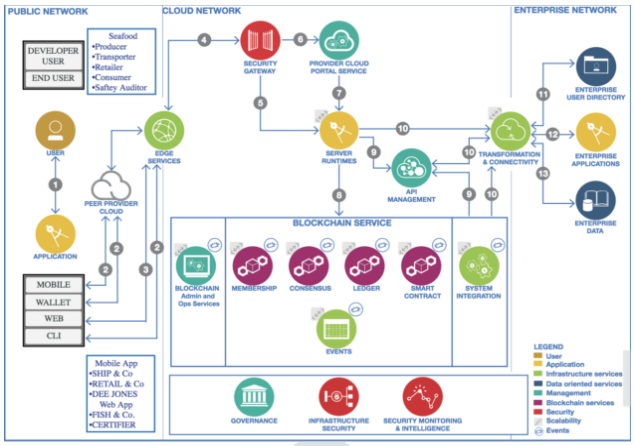


Fig. 3 https://www.capgemini.com/wp-content/uploads/2017/07/blockchain-a_healthcare_industry_view_2017_web.pdf[11]

Patientory, focuses on improving the healthcare by offering a dependable space for stakeholders to load and control data. Their prospective clients are patients, benefactors and medical associations. Patients can get entry to their data feasibly and hand it over to benefactors, who may not have a complete record of the patient's health but will be able to view remarks from previous benefactors and associations. These associations gain from cheaper and effective storage of records. Providing cost efficient solutions to patient data processing is the goal of DokChain. They develop a platform for wide variety of industries including insurance. The two significant blockchain projects working in the healthcare space are Gem and Tierion,

The above diagram illustrates how a chronic-care patient's data can be enhanced on a global network to make medical-history records available. This would enable any hospital, to access this data (once authorized by the patient) regardless of the country in which it is located. Subsequently, the patient's need to carry medical records when traveling internationally to receive treatment becomes inessential.

IV. PROBLEM DEFINITION

In today's scenario, as the transactions are more critical than ever, we need to make them more secure. The pitfalls of the current system of ballot voting are being taken advantage of by people or organizations looking to gain power. Issues like double voting, vote manipulation and identity spoofing are very common in today's voting systems. Frequent travelers and indisposed people are unable to exercise their right to vote. This paper is an effort to counter these problems by using Blockchain technology in an E-voting system. We have decided this system for elections at offices like BMC, colleges and further we can extend the scope of project by including the Election Commission.

V. METHODOLOGY/APPROACH:

The system will be consisting of 3 main use cases:

- Voter
- Candidate
- Election Commission

Election Commission (EC) is the one managing the lifecycle of the election.

Voter is the one for whom the system is made.

Candidate stands for an election created by the Election Commission.

The Election Commission creates a voting process – a ballot in which the candidates and the voters can enroll. All the details pertaining to the election process (registration successful, voting date, winner announcement, etc.) are sent to the respective user on its registered E-mail ID.

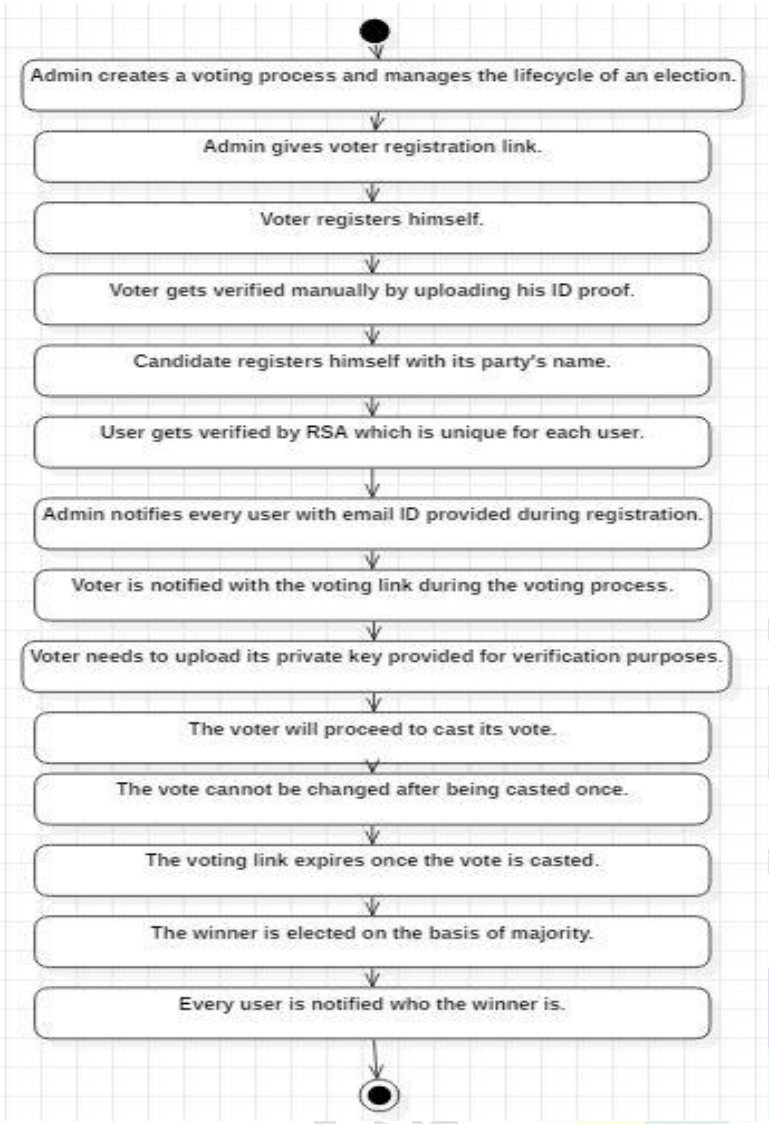
Voter creates an account, registering itself for the election. Do note that the voter needs to verify itself by uploading the Voter ID generated manually before the election process gets started. Meanwhile, Candidate gets registered for the ballot in which it needs to stand for the election. The verification of each user in the system is done by allocating a RSA private key to each user (voter/candidate).

The voter is given a unique link by the EC when the election time arrives. The voter will be able to cast its vote only once, and cannot be changed. Voter needs to verify itself by entering the RSA private key given to it. The voting link expires as soon as the ballot time is completed.

EC counts the votes, and the election results are sent to each registered user for that ballot.

An intuitive interface will be used to portray the vote share of each candidate.

Flow of system:



VI. CONCLUSION & FUTURE SCOPE

Blockchain has the potential to act as a foundation of an entirely new Internet - from one that is information based, to one that is value based.

"Blockchain's ability to generate unprecedented opportunities to create and trade value in society will lead to a generational shift in the Internet's evolution, from an Internet of Information to a new generation Internet of Value", as said by Goldman Sachs.

So, at its core, by discontinuing the intermediaries from the service and ingeniously obliterating how they operate a blockchain injects trust into the network. Analogously, blockchains are the absolute iterative computers. Once propelled, they never drop and offer an inconceivable volume of resiliency. These qualities make them steadfast and appealing in order to make a new generation of decentralized services and software applications functional.

VII. REFERENCES

1. Sachchidanand Singh, Nirmala Singh, "Blockchain: Future of financial and cyber security"
2. Barclays Bank's Simon Taylor , "Blockchain: understanding the potential" , July 2015
3. Kaye Scholer , "An Introduction to Bitcoin and Blockchain Technology" , February 2016 .
4. https://www.rolandberger.com/en/Point-of-View/Blockchain-The-future-of-the-finance-industry.html
5. https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-blockchain-use-cases-in-financial-services.html 4
6. https://www.infosys.com/industries/financial-services/white-papers/Documents/blockchain-adoption-financial-services.pdf
7. https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html
8. https://cointelegraph.com/news/why-blockchain-is-cloud-20-expert-take 6
9. https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains
10. https://www.investinblockchain.com/blockchain-transform-industries/
11. https://www.capgemini.com/wp-content/uploads/2017/07/blockchain-a_healthcare_industry_view_2017_web.pdf
12. "A conceptual secure blockchain- based electronic voting system" written by Ahmed Ben Ayed published in International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017
13. "BroncoVote: Secure Voting System using Ethereum's Blockchain" written by Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic and Jordan Mohler