


## Chapter 9

# Understanding Blockchain: Case Studies in Different Domains

**Hemraj Saini**

 <https://orcid.org/0000-0003-2957-1491>

*Jaypee University of Information and Technology, India*

**Geetanjali Rathee**

*Jaypee University of Information Technology, India*

**Dinesh Kumar Saini**

 <https://orcid.org/0000-0002-5140-1731>

*Sohar University, Oman*

### **ABSTRACT**

*In this chapter, the authors have detailed the need of blockchain technology along with its case studies in different domains. The literature survey is described that describes how blockchain technology is rising. Further, a number of domains where blockchain technology can be applied along with its case studies have been discussed. In addition, the authors have considered the various use cases with their recent issues and how these issues can be resolved using the blockchain technology by proposing some new ideas. A proposed security framework in certain applications using blockchain technology is presented. Finally, the chapter is concluded with future directions.*

DOI: 10.4018/978-1-7998-3444-1.ch009

## **INTRODUCTION**

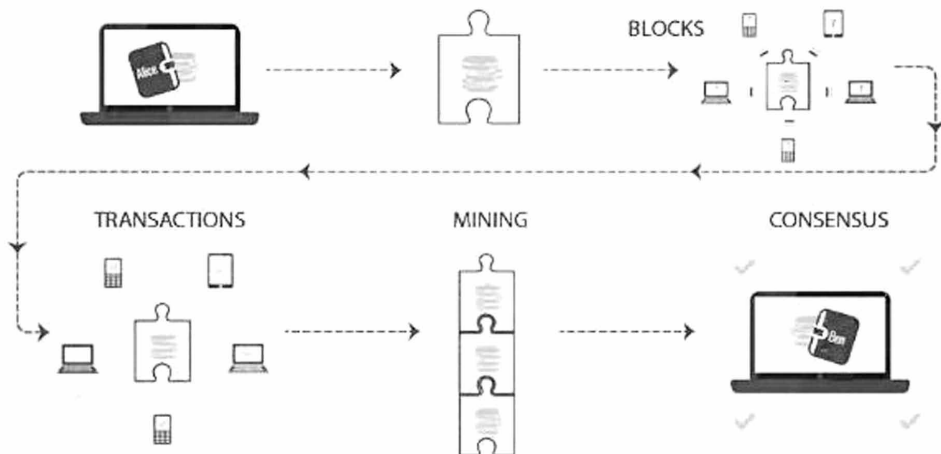
Blockchains have pulled in overall consideration lately and is characterized as an immutable, successive chain of records called blocks. The record contains transactions, documents or some other information, and are fastened together utilizing hashes. It is executed and overseen by a peer-to-peer network (Christin, N., 2011; Iansiti, M., & Lakhani, K. R., 2017; Swan, M., 2015; Cachin, C., 2016) of computers (also called peer nodes) spread everywhere throughout the globe. Blockchain likewise called distributed ledger which utilizes independent PCs (nodes) to record, share and synchronize transactions in their particular electronic ledgers, rather than keeping information incorporated on a server as in a customary record (Nandwani, K., 2018). A Schematic outline of the blockchain is depicted in Figure 1. Blockchains have the potential to disrupt any industry that employs the use of a trusted middleman and gives direct control back to the end-user. In any case, similarly, as with any technological revolution and the paradigm shift that joins it is a procedure of trial and error. What works and what does not and we are as of now in that stage with blockchain advancements. 99% of the business sectors are filled by an unadulterated hypothesis (Peters, M. A., 2017). There are no completely useful blockchain items that can oblige the requests of the majority. Blockchains must be less expensive, snappier, simpler to utilize and similarly as versatile, if not more thus, than the present frameworks set up. The coming of the web drove the technological revolution of the 90's and the industrial upheaval was in the late eighteenth century (Peters, M. A., 2017). These quantum jumps in human capacity and accomplishment change our whole reality and disturb pretty much every settled industry. They change the manner in which we travel, cooperate, communicate, business with one another. All that we once knew is flipped on its head and life gets improved, making things a lot less demanding and progressively productive. The same is the appearance of blockchain technology where the component of trust is the whole sudden put under the control of target numbers and PCs.

Blockchain is the initial step at placing trust into PCs. It sounds kind of terrifying where it would state that however, the seasons of Skynet and eliminators are far away and except if we create methods for keeping self-aware robots from turning into a reality, at that point we ought to be safe. Blockchain technology is still without a doubt so in its earliest stages. Blockchains are moderate, user-unfriendly, unscalable, and costly. For instance, DApps created on ethereum require the end-user to initially buy ethereum and afterward pay a transaction fee each time they accomplish something in the DApp. Then again, EOS expects developers to buy over the top expensive RAM to build up a DApp while the users get transaction fees, simply after the user gets some EOS, downloads an EOS wallet from Github, make a key pair and sends EOS to that key pair. Not to speak to the average consumer who could think less

## Understanding Blockchain

about decentralization. The fact of the matter is that blockchain technology needs to develop before mainstream adoption happens. A blockchain that takes care of enormous real-world problems, finds a harmony among decentralization and administration while giving speed, scalability, cost viability, and overall smooth user experience will be the blockchain that ascends above them all. 2018 was an incredibly dynamic year for blockchain and cryptocurrencies (Houben, R., & Snyers, A., 2018). Numerous jumps in advancement were made and blockchain is entering the worldwide awareness increasingly every day. The subject of mass selection is when, not in the event that it occurs. We unquestionably observe this occurrence very soon, however as things remain at the present minute, the blockchain space still makes them develop agonies to traverse.

Figure 1. Schematic outline of Blockchain



## Key Advantages of Blockchain

### A. Distributed

Blockchain enables a wide assortment of PCs to partake in a network, circulating the processing power. For instance, Amazon purchases and keeps up a private arrangement of computing power for AWS, nobody, however, Amazon can contribute this. Interestingly the blockchain association Ethereum permits nearly anybody to contribute their PC to their system, just by introducing their product. Distribution decreases the chance of altering, extortion, and tampering. With more hubs ready

to partake, frameworks are difficult to “takedown” by means of customary brute force network attacks.

## **B. Trustless**

Blockchain enables advanced exchanges to occur between gatherings who don't confide in one another. Envision a digital coin stored in a document on your PC. You may read the document an endless number of times. The estimation of this digital currency would near zero. Previously, focal experts (banks) have gone about as records, tracking the number of coins every one of us has access as a bought together to evade the issue of duplication. By distributing the Ledger to numerous nodes, and synchronizing the ledger through Consensus, blockchain permits parties who don't confide in one another, to trust that the exchange is genuine and not useless. After some time, trust can be expanded further, by means of shared procedures and permanent records of exchanges. This encourages a monstrous scope of potential digital transactions that couldn't have occurred before without a focal specialist overseeing them.

## **C. Immutable**

When a transaction is concurred and shared over the distributed system it turns out to be near difficult to fix. Indeed, after some time, it ends up increasingly hard to fix. In an open record, like Bitcoin, this implies you can investigate the blockchain and find the number of Bitcoins in anyone's record, or follow where reserves were distributed. In different situations, this could be utilized to follow supply chains, or check who got to specific documents on a system.

## **D. Decentralized**

Blockchain likewise underpins the decrease in centralized monopolies infrastructures or “middlemen” and expels costs. By distributing systems, blockchain can discover economies of scale, without single incorporated speculation. This builds rivalry in the market, by bringing down the hindrances to the passage, putting pressure on all members to turn out to be progressively effective. In addition, enabling peers to transact with no prerequisite for trust upsets the present business practices of associations who encourage trust for example Banks. Transactions straightforwardly between peers may prompt a decrease in “middle man” steps, further expanding business sector effectiveness.

## **Challenges of Blockchain**

### **Wasteful**

Each node runs the blockchain so as to keep up Consensus over the blockchain. This gives outrageous dimensions of adaptation to non-critical failure, guarantees zero downtime, and makes the information stored on the blockchain perpetually unchangeable and restriction safe. Yet, this is inefficient, as every node rehashes a task to achieve consensus consuming electricity and time in transit. This makes calculation far slower and more costly than on a customary single PC. There are numerous activities that look to diminish this cost concentrating on elective methods for looking after Consensus, for example, Proof-of-Stake.

### **Network speed/cost**

Blockchain systems expect nodes to run. However, the same numbers of the systems are new, they do not have the number of nodes to encourage broad utilization. This absence of resource shows as:

- Higher costs—as hubs look for higher prizes for finishing transactions in a supply and demand situation
- Slower transactions—as hubs organize transactions with higher prizes, backlogs of transactions develop.

After some time, effective public blockchain networks should incentivize nodes, while making ideal expenses for clients, with transactions finished in a significant time allotment. This balance is key to the financial matters of each blockchain.

### **The size of the block**

Every transaction or “block” added to the chain builds the span of the database. As each hub needs to keep up the chain to run, the computing necessities increase with utilization. For substantial public usage of blockchain this has one of two effects:

- Smaller ledger—Only one out of every odd node can convey a full copy of the blockchain, conceivably influencing immutability, consensus, etc.
- More centralized— There is a high obstruction to a passage to turn into a node, empowering a bigger measure of centralization in the network, with greater players ready to take more control.

Neither of these situations is alluring, without thinking about the full ramifications, as it will probably influence the utilization cases for blockchain variations.

## Speculative markets

Numerous blockchains are run utilizing token/currency models to support advancement or deal with the financial matters of nodes. For instance, Ether (ETH) is the currency used to pay for computing power (or Gas) on the Ethereum organizes. In this manner, ETH is a cash for computing power.

Customary currencies like USD, GBP, EUR (additionally called Fiat currencies) are commonly connected to the estimation of their particular economies for example GBP to the UK. These economies are very much created, directed and stable. In any case, because of the possibly troublesome nature of Blockchains, individuals have taken to guessing on the estimation of the digital economies they create.

As these business sectors are liable to restricted guidelines and are exceedingly theoretical they are inclined to quick variance and control, spiking transaction value. This presents specific dangers while transacting from Fiat currencies into blockchain currencies. For instance, 1 ETH may cost ~\$200 today, yet ~\$180 tomorrow, a 10% price fluctuation (Ametrano, F. M., 2016). While this can make vast rewards, it likewise introduces high degrees of vulnerability for undertakings created on public blockchain innovation.

## Hard and Soft Forks

Numerous blockchains and currencies decentralize their basic leadership. For instance, Bitcoin enables nodes to “signal” support for upgrades deeply software that runs the system. This permits the blockchain to stay away from bringing together basic decision making, yet in addition, it presents challenges when communities are partitioned about the best course.

At the point when nodes change their software, there is potential for a “Fork” in the chain. Nodes working the new software won’t acknowledge indistinguishable transactions from nodes working the former one. This makes another blockchain, with a similar history as the one it is based on.

Forks make noteworthy uncertainty, as they can possibly piece the intensity of the blockchain arrange into loads of variations. They are additionally prone to be essential, as, without the ability to refresh the software, the blockchain is probably not going to be future proof.

## Immutable Smart Contracts

When the smart contract is added to the blockchain, it ends up permanent, in that it can't be changed. In the event that there are imperfections in the code that might be misused by hackers, they are there until the end of time. This isn't a worry when a smart contract isn't being utilized, however as smart contracts carry on like records, they can be utilized to store a lot of significant worth.

This can make situations where hackers can abuse code defects to send the substance of smart contracts to their very own records. As the blockchain is permanent, these transactions are extremely difficult to fix, which means a lot of significant worth might be lost until the end of time.

## Solutions of Weaknesses of Blockchain

All the weaknesses of the blockchain can be removed using three different consensus protocols named proof-of-work, proof-of-stake and proof-of-useful-work (Vukolić, M., 2015; Yu, B., Liu, J., Nepal, S., Yu, J., & Rimba, P., 2019; Baldominos, A., & Saez, Y., 2019; Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H., 2017). A brief summary of these three protocols is given below.

### Proof-of-work

A self-explanatory pictorial representation of proof-of-work is shown in Figure 2.

### Proof-of-stake (virtual mining)

A self-explanatory pictorial representation of proof-of-stake is shown in Figure 3.

### Proof-of-useful-work

A self-explanatory pictorial representation of proof-of-useful-work is shown in Figure 4.

Table 1 represents the comparison of proof-of-stake and proof-of-work and proof-of-useful-work.

## CASE STUDIES

Beyond the simple applications, bitcoin has transcended the environment in the cloud, ensuring data privacy and other major issues. For the future of blockchain, it

has great potential in empowering the citizens of developing countries in different sectors like healthcare, identity management, and other commercial uses. Some of the following case studies represent the strength of blockchain.

Figure 2. Proof-of-work

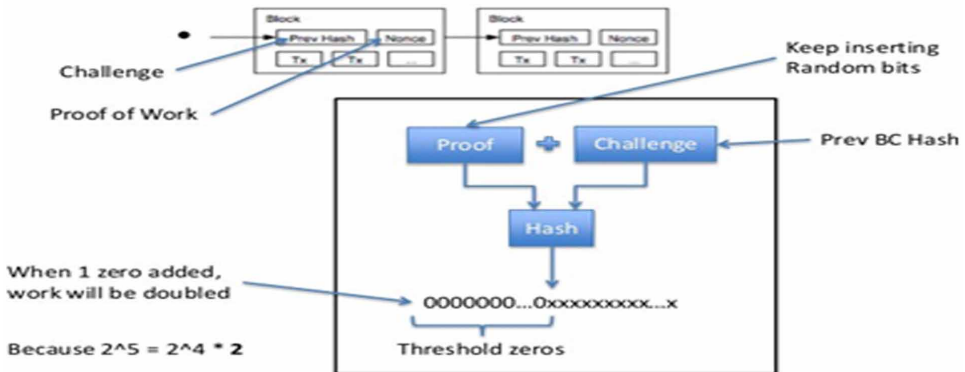
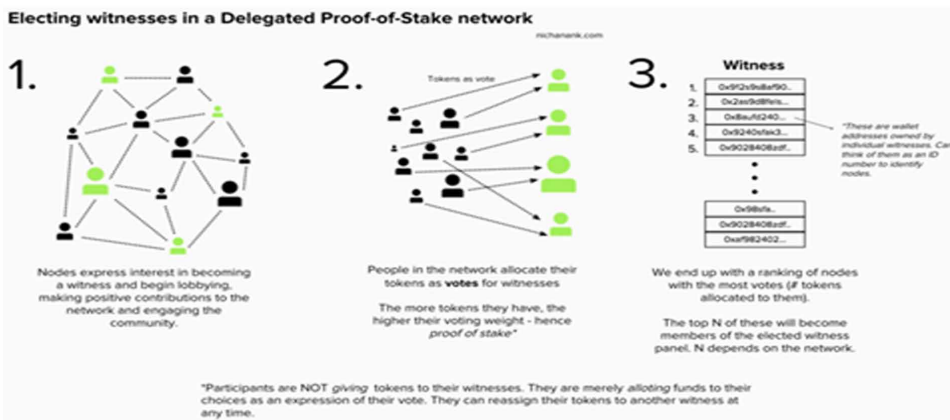


Figure 3. Proof-of-stake



### A. Proposed Decentralized Voting Application

Our application determines the vote count of the voter for certain people who are to be selected. Firstly, in this application, we determine the illegibility of the voters



## Understanding Blockchain

using blind signatures. For high availability and result immutability of privacy using double private blockchain and using bitcoin logic to redesign transactions and new protocols to cast a vote. The proposed system contains:

Figure 4. Proof-of-useful-work

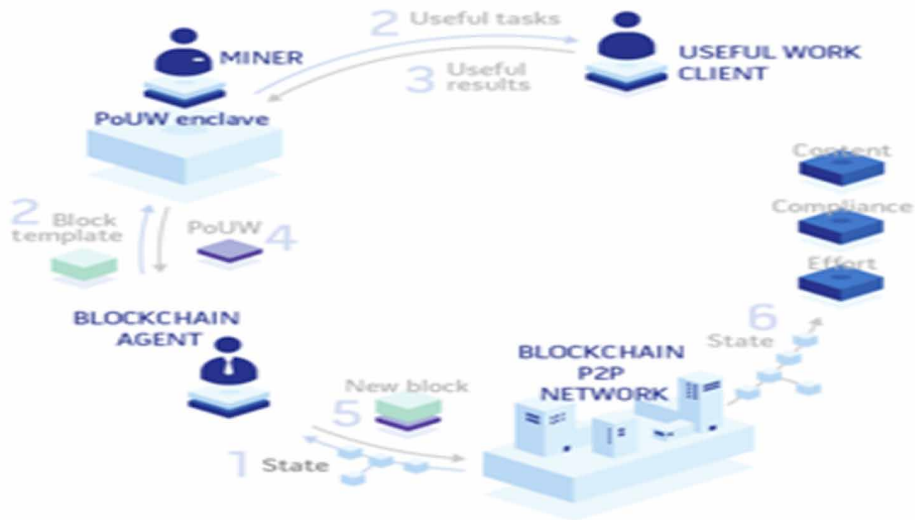


Table 1. Proof-of-stake, Proof-of-work, and proof-of-useful-work

Proof-of-work (PoW)	Proof-of-stake (PoS)	Proof-of-useful-work (PoUW)
Power-hungry, enough energy to power a small country is required to secure the blockchain.	ECO-friendly, minimum recourses required to secure the blockchain	Very much power-hungry
Incentivizes centralized mining farms.	Truly decentralized mining.	Truly decentralized mining.
Advanced technical knowledge required.	Very little technical knowledge required.	Very little technical knowledge required, mining scheme requires training deep learning models
It requires constant tweaking and monitoring.	Set it and forget it.	Set it and forget it.

- Anonymity
- Check flag for voter's illegibility
- Voting integrity with the system.

- Vote Verification

## **Different Phases in the System**

### **Publishing phase**

It's a dummy approach to publicize the system and generating candidate ballots. The Authority has eligible bling signature which is communicated securely to prevent any attacks like DOS, Men-in-the-middle Attack

### **Login phase**

After the publishing phase, the voter's will login and then verification will be done for eligibility. This phase also deals with the impersonation and EIDs establishment.

### **EID generation phase**

This phase will be used to generate the public-private key for electronic identity. For every identity made, an EID password will be established in order to prevent tampering and impersonation. The generation of OTP can also be done.

### **Voting phase**

For the generation of Blockchain transactions, our Voting phase ensures data consistency and isolation as depicted in Figure 5.

### **Blind signatures**

These digital signatures (Seo, J. H., 2019) are heavily used in our application for transactions working for eligible voters sign and extract public and private keys and encrypt them in Ballot. The Ballot is sent to Electoral Authority (admin) and verifies the source of the ballot, removes the outer envelope and Encrypts the keys and sends back to the eligible voter.

## **System Protocol**

This phase depicts the working of the voting application using different phases as per the sequence provided in Figure 6.

## Understanding Blockchain

Figure 5. Implementing blind signatures

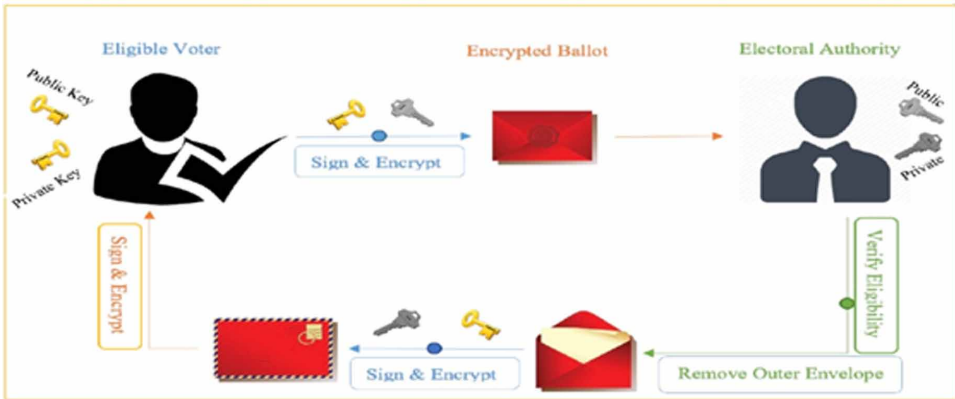
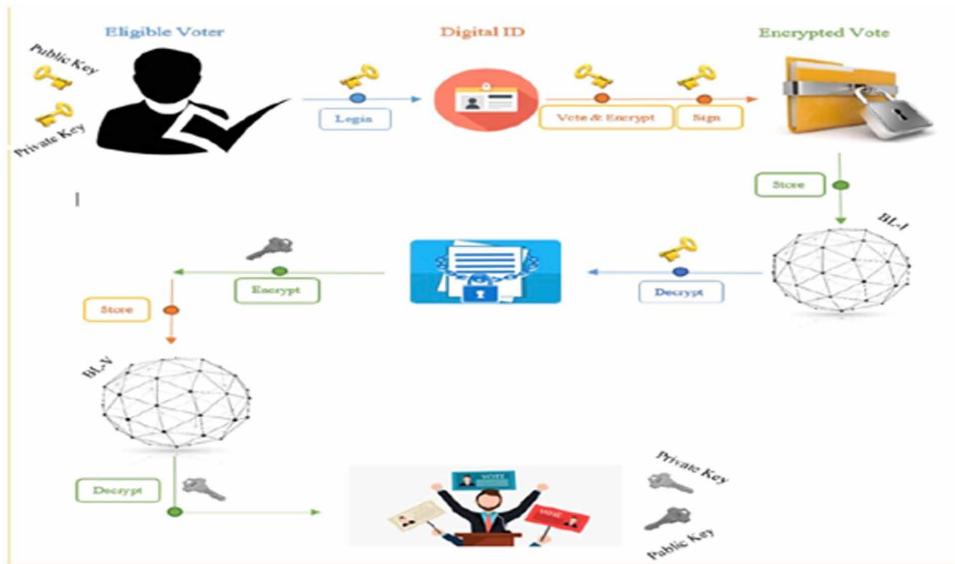


Figure 6. Proposed complete Solution



## Threat Model

Various models have been taken in care for the full functionality of the Blockchain without any foreboding of threat initiation. As Blockchain helps with decentralization, and impenetrable security level, various threats are seldom to be seen. Some of the most common threats (Saini, H. Rao, Y.S., Panda, T. C., 2012; Rathee, G., Saini,

H., 2016) are DDoS Attack, Sybil Attack, Freak Attack, Malwares, Cross-Site Scripting (XSS), etc.

## **Evaluation**

After the completion of the project, we will study all the sufficient properties of the proposed system design and these are the availability of the project, integrity with the OS and web page, uniqueness, accuracy, and election secrecy.

## **SOME OTHER SECURITY ANALYSIS AND LEGAL ISSUES**

### **Security Analysis**

#### **DDoS**

For the application to fail under DDOS Attack, the attacker must perform it on every node in the network. But tampering with the boot nodes will eventually inform the institution and the location could be found out. For locating failed blocks, we can use a fault-tolerance algorithm

#### **Authentication Vulnerability**

As the value of the hash will be unique to each and every individual or eligible voter, there is seldom a chance of multiple voting process by the voters. This will not only help with the ease to finalize the output result with incrementing by +1 but also eradicates out the total chances of the system malfunctioning.

#### **Sybil Attacks**

The consensus algorithms implemented in the project are prone to these attacks. Furthermore, with the incoming of the strong cryptography features and limited access to the ledger, Blockchain solves today's most often security problems

## **Legal Issues**

### Transparency

No method of transparency can be offered to the voters in today's electoral scheme. Without some other tech involvement, transparency in the system is a very tedious task with the formulation of a new law by government officials.

### Voter Privacy

Voter privacy in pen and paper scheme is meandering which may involve leakage of voter credentials and vote to the party or the candidate. To satisfy the privacy, initiation of the non-traceable vote will be prominent to implement.

### Remote Voting

To prevent coercion resistance in the election, remote voting could be of good use. If the results can be used in websites or mobile applications, there is no chance of misconfigured results, but on the negative side, people with good hacking skills can take down the host website and different threats can be introduced. We can use Blockchain features to subdue these effects.

## **Comparison**

### Traditional Blockchain Solution

In the traditional Blockchain solution, we can observe the common implementation of litecoin, dash, ripple and many other programming languages based bitcoin implementation. There is less privacy needed even though implemented in a suitable domain of programming languages.

### Proposed Blockchain Solution

The platform implements all the solutions in ethereum, solidity and other bitcoin consensus protocols using of RSA algorithm implemented with the generation of private keys. The main idea of proposing this blockchain solution for the voting system is to make the electoral system cheaper and quicker. By doing this, the barrier between voters and officials to be elected will be an endgame. Furthermore, with ease in operation, we can assure a direct form of democracy as people will be in more ease to use it and give a better result in return without any involvement of a central

agency. We also implemented a simple voting application using smart contracts (solidity, ethereum) for the proper conduct of system execution while maintaining security features like privacy and authentication verification. By comparing with the current process of the electoral system, we can observe that blockchain technology has a new future for democratic countries where most of it is pen and paper-based. Using the ethereum private blockchain, we can transmit hundreds of transactions in one second, for countries with bigger democracy, this system can provide a well-executed result with seldom chances of result tampering. The use of modern hash algorithms makes the data fetching impenetrable and isolated within each and every block. Decentralization has made the platform much more secret and private than that of centralized systems. Our proposed system will ensure that all the blockchain concepts will be executed properly resulting in a better approach to implement the platform practically in the provinces or the region. The pros and cons of our solution are represented in Table 2.

*Table 2. Traditional Blockchain Solution Vs Proposed Blockchain Solution*

<b>Traditional blockchain solution</b>	<b>Proposed blockchain solution</b>
Operated with decentralized property	Operated with decentralized property
Programming tools: Native Programming Languages (Java, Python, C++, ASP.NET, C#)	Programming tools: Ethereum, Solidity, web3.js
Time of Transaction: Minutes	Time of Transaction: Seconds
Implementing client-server architecture and RDBMS	Facilitates P2P architecture and smart contracts; no RDBMS required

## **B. Proposed e-Waste Management System**

India is the fifth-biggest maker of the e-waste on the planet amazingly has not many arrangements with regards to reusing and appropriately arranging e-waste (Terazono, A., et al., 2006). Therefore, e-waste is an inevitable problem, but this problem can be stopped before it turns into a disaster. The current solutions are not enough to properly dispose of e-waste, the present scenario can be changed very easily if the proposed solution is applied to it.

The proposed e-waste Management system depends upon resourceful contracts made by utilizing blockchain progression. Bringing government work environments, clients and assistants on the corresponding blockchain stage will incite improved checking and higher transparency at the same time. Blockchain will empower the appropriate maintenance of records of the electrical and electronic supplies launched

### **Understanding Blockchain**

in the technical market by various makers and retailers (Gupta, N., & Bedi, P., 2018). This will empower smart contracts to verifiably choose collectors and disapprove of inappropriate collectors at whatever point required. In a similar manner, we provide the inclusion of clients as individuals from this blockchain. Offering motivations to lure clients to channelize their e-garbage to the formal part can fill in as the hidden stage in lessening the nature of the tangled division in e-waste management. Also, collection centers, as well as recycling units, are being included in our proposed system. These bright contracts will help control the initial point and extent of e-waste collected, delivered and reused all over in the framework.

*Table 3. List of all the nodes*

<b>S.No</b>	<b>Node</b>	<b>Description</b>
1.	Producer(PR)	A node association with Ethereum arranges a producer/provider/ merchant of EEE in India.
2.	Retailer(RT)	A node associated with the Ethereum arranges the largescale purchaser of the EEE from PR and pitches to the clients.
3.	Collection Centre(CC)	Spot where the E-waste is briefly put away by the PR, which is gathered by RT from clients. Proprietors of CC are associated with Ethereum organize as nodes.
4.	Recycling Unit(RU)	A Government Certified Unit where E-waste from CC is reused in a situation well-disposed way. The proprietors of RU are additionally associated with Ethereum organize.

*Table 4. List of other participants in e-waste management*

<b>S. No.</b>	<b>Participant</b>	<b>Description</b>
1.	Government's Agency(GA)	An initial point on the Ethereum organizes as in-charge of composing and keeps up savvy contracts for the EWM framework.
2.	Consumer(CS)	A hub on the Ethereum arranges that utilizes the EEEs for their very own advantage.

In our proposal, we use Ethereum blockchain to approve Electronic Waste Management in India. Table 3 and Table 4 represent the list of all types of nodes used in the solution and list of other participants in e-waste management respectively. The center addressing GAs manages the smart contract for coordinating the surge of e-garbage across over multiple accomplices and CSs. GAs endorse only those PRs and RTs who will join this e-waste administrator blockchain. Owners of CCs and RUs, who wish to set up their associations in our country, ought to similarly transform into a bit of this EWMB. CSs will benefit from this project by getting

pre-portrayed spurring powers for channelizing their e-squander to real accomplices present on the blockchain. The splendid contract made by GAs will contain the following components that will track the activities of every part. The complete flow diagram of our e-waste management system is depicted in Figure 7.

Figure 7. e-waste Management System



Table 5. Traditional Blockchain Solution Vs Proposed Blockchain Solution

Current Solution	Proposed Solution
Local market using ends up in black market recycling units use toxic chemicals, and use child labor.	E-waste recycling unit is trackable, easy to manage the operations, and easy for the administration to use.
The capital generated from this solution is often miscalculated and is often very less from what it should be. Most of the capital earned from this process ends up in the hands of illegal recycling unit owners.	The capital generated through this system Will be properly calculable and this would Help the government generate more capital from E-waste.
User is mostly in dark and not aware where their E-waste ends and unfortunately, most of them don't even care about what happens to their E-waste. At least the user should be aware of how much their E-waste is worth.	Through our proposed Solution users and manufacturers of the E-waste would have an insight where their E-waste ends up. It would be a more responsible and manageable operation for the manufacturing side.
The current situation of E-waste recycling exposes a lot of workers to toxic chemicals Like lead, mercury, etc. And these units also don't have proper equipment and techniques to deal with generated this E-waste.	Although the use of Hazardous chemicals cannot be stopped, it can be reduced. Recycling E-waste is Manageable through our solution. If proper recycling units are set up properly. This solution will bring proper standards in the E-waste recycling industry.

Utilizing of blockchain, all the participating parties can be easily connected to each other and will be able to track and use this proposed solution to efficiently manage E-waste management and the government to generate appropriate capital from this recycling of the E-waste through our proposed solution. Clients and makers of the E-waste would have a knowledge where their E-waste winds up. It would be a progressively mindful and reasonable activity for the assembling side.



## ***Understanding Blockchain***

In order to fulfill this goal, the government needs to associate with the cooperative authorities who are supposed to handle the process. Also, the awareness also plays a very important role in order to get the people on the track of the recycling process. For this to happen, the government needs to take it seriously (Nandwani, K., 2018).

Despite the fact that the utilization of Hazardous synthetic can't be halted yet can be diminished. At last, as Blockchain is public to everyone and is able to access where the E-waste went and who handled this information would be very useful for government and manufacturing companies to plan and efficiently manage E-waste and also be responsible for proper recycling E-waste. A comparative analysis is given in Table 5.

### **C. Decentralized Kickstarter Crowdfunding**

Kickstarter is an application as depicted in Figure 8 that allows investors, no matter big or small to invest in projects they see on the application, again, the projects can also be of varying sizes and require a varying amount of investments. This is a very useful and unique application as the investors are paying the project owner some amount of money in return for the stocks, or profits or whatever their agreement is and the owner gets the required funding to start his business.

A very important feature of kickstarter is that it only allows money to be transferred from an investor to an owner when a certain threshold limit is touched that has been set by the owner in order to start his project. This is something that needs to be taken special care of. Now, like all applications and especially the applications that involve money kickstarter hits certain road bumps and problems. The biggest issue with kickstarter is the fact that money is not tracked. Once the investor gives his money to the owner, he can do whatsoever he wishes with that money, he can use it for his personal use or he can be honest and use it for the project as he mentioned before. Another problem with it is that as the project owner can also work with fiat money in the physical world, it is nearly impossible to know how much money did he actually make and what share of it is to be given to the investor.

The proposed kickstarter clone will be hosted on the RinkebyTestnet which is a free Ethereumtestchain, the same code can then be shifted to the real Ethereum Blockchain with minimal effort. This would allow us to test the application as if it was hosted live and not spend any Ether doing it either. The application we tend to build will be nearly the same as kickstarter when it comes to features and procedures to be followed to host your project on it or be an investor on the application. The frontend will be nearly identical to the real kickstarter application in terms of general usage. Where the difference lie is in the use of smart contracts to restrict the usage of money invested and in the participation of the investors every time the owner wants to spend money. If the owner wants to spend money, he will issue a request in

the application and the smart contract will make sure that 51% of voters have voted favorably for the spending of money and only then that money will be moved from the project account to the account destined for. This will nullify the possibility of the project owner using project money for personal usage and benefits. Also, the investors will be able to track and know where there invested money is being used.

*Figure 8. A generic model for Kickstarter*



In order to be an investor in the first place, a certain amount of money have to be donated by the investor. Once that is done, that money will be submitted to the project account and that investor will be added to a list of investors for that project and will get his voting rights for any spending in the future.

The project owner is the only one who can make spending requests on the application and can need to make genuine requests as otherwise the investors will vote NO and that transaction will be canceled. As the money will be in the account of the project account (that is possible using a contract account instead of externally owned account), the owner cannot spend money on his own and has to abide by the rules.

Once the request is approved, that money will be transferred to whatever destination address was. This will solve both the major problems –money tracking and proper usage of money. Table 6 represents the comparison of the traditional and proposed blockchain solution.

## Understanding Blockchain

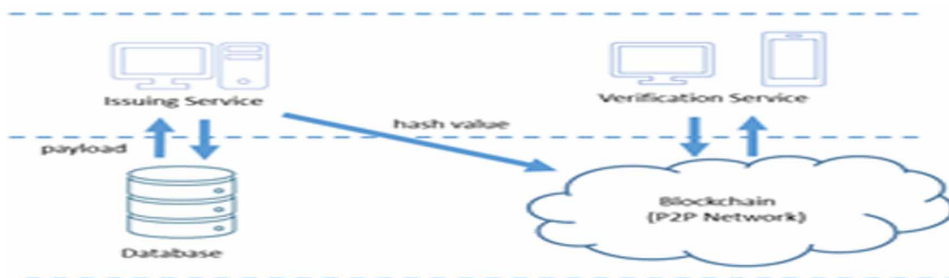
Table 6. Comparison of a traditional and proposed blockchain solution

Traditional solution	Proposed block-chain solution
Centralized controlled	Decentralized controlled
Integrity: Not always possible	Integrity: every user can be sure that the data they are retrieving is uncorrupted and unaltered since the moment it was recorded
Transparency: same as Integrity	Transparency: every user can verify how the blockchain has been appended over time
The traditional application uses a traditional database, on which a client can perform four functions on data: Create, Read, Update, and Delete.	The blockchain is designed to be an append-only structure. A user can only add more data, in the form of additional blocks. All previous data is permanently stored and cannot be altered.
Traditional application incurs transaction cost.	A blockchain carries no transaction cost. (An infrastructure cost yes, but no transaction cost.)
Selected users can see the data.	All participants see consistent data.
Scalability is a major issue	Blockchain simplifies the processes and thus scalability is not an issue.

## Issuing and Verifying College Degree using Blockchain

It is easy to use, yet the secure application of issuing and verifying college degrees. Authorized personal can issue the degrees in blockchain, and anyone can verify its existence or validity.

Figure 9. Generic Architecture



The goal is to create a De-centralised application for issuing and verifying college degrees using blockchain. Following are the goals for the setup process for building the application which is also depicted in Figure 9:

- Setup the development environment.
- Learn how to write a contract, push degree data (pdf) into the block, compiling it and deploying it to our development environment.
- Interact with the smart-contract on the blockchain.
- Propose a simple and easy to use applications to deploy degrees on the blockchain.

Advantages of the proposed approach can be as follows-

- No central authority or a third party required. All the functionality and working will be taken by the peer to peer networks.
- There is no way of tampering of college degree's as concepts of "PROOF OF WORK" and "PROOF OF STAKE" are highly maintained.
- No individual can try and change the data in the degrees present in the block.

For the basic idea, we will go with the smart contracts and object-oriented programming in Solidity.

## **CONCLUSION**

In this manuscript, we have reviewed the state-of-art of the blockchain technique along with its case studies in various fields. Further, we have described various blockchain uses cases and explored the different applications in the blockchain with a significant proposed scenario. The aim of this paper is to point out the significance of blockchain in various fields. Further, we have defined how blockchain technology could be helpful in various fields having a decentralized network. In our future work, we will propose a solution corresponding to the above IIoT blockchain discussion with some analyzed and evaluated parameters.

## **REFERENCES**

- Ametrano, F. M. (2016). *Hayek money: The cryptocurrency price stability solution*. Available at SSRN 2425270
- Baldominos, A., & Saez, Y. (2019). *Coin. AI: A Proof-of-Useful-Work Scheme for Blockchain-based Distributed Deep Learning*. arXiv preprint arXiv:1903.09800

## **Understanding Blockchain**

Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, p. 4)*. Academic Press.

Christin, N. (2011). Peer-to-peer networks: Interdisciplinary challenges for interconnected systems. In *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives* (pp. 81–103). IGI Global. doi:10.4018/978-1-61692-245-0.ch005

Gupta, N., & Bedi, P. (2018, September). E-waste Management Using Blockchain based Smart Contracts. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 915-921). IEEE. 10.1109/ICACCI.2018.8554912

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. Academic Press.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 118–127.

Nandwani, K. (2018). *Squaring the Blockchain Circle*. Available at: <https://kunalnandwani.com/books/>

Peters, M. A. (2017). Technological unemployment: Educating for the fourth industrial revolution. *Journal of Self-Governance and Management Economics*, 5(1), 25–33. doi:10.22381/JSME5120172

Rathee, G., & Saini, H. (2016). Security Concerns with Open Research Issues of Present Computer Network. *International Journal of Computer Science and Information Security*, 14(4), 406–432.

Saini, H. Rao, Y.S., Panda, T. C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications*, 2(2), 202-209.

Seo, J. H. (2019). Efficient Digital Signatures from RSA without Random Oracles. *Information Sciences*.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Terazono, A., Murakami, S., Abe, N., Inanc, B., Moriguchi, Y., Sakai, S. I., ... Wong, M. H. (2006). Current status and research on E-waste issues in Asia. *Journal of Material Cycles and Waste Management*, 8(1), 1–12. doi:10.1007/10163-005-0147-0

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer.

Yu, B., Liu, J., Nepal, S., Yu, J., & Rimba, P. (2019). Proof-of-QoS: QoS Based Blockchain Consensus Protocol. *Computers & Security*, 87, 101580. doi:10.1016/j.cose.2019.101580

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557-564). IEEE.