Visvesvaraya Technological University

Belagavi, Karnataka-590 018

A Seminar Report on

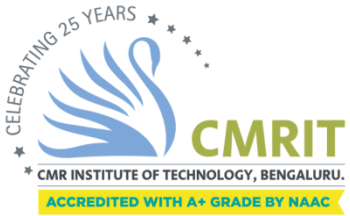
"E-VOTING USING BLOCKCHAIN"

A seminar report submitted in partial fulfillment of the requirement for the VIII semester degree of

Bachelor of Engineering
In
Electrical & Electronics Engineering

Submitted by
Name: AKSHAY RAJEEV
USN: 1CR17EE004

Under the Guidance of
Ms. Lokashree B S
Assistant Professor, Department of Electrical & Electronics Engineering
CMR Institute of Technology



CMR Institute of Technology, Bengaluru-560 037

Department of Electrical & Electronics Engineering

2020-2021

CMR INSTITUTE OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

AECS Layout, Bengaluru-560 037

Certificate

Certified that the Seminar work entitled **"E-VOTING USING BLOCKCHAIN"** has been successfully presented by **Mr. Akshay Rajeev (1CR17EE004)** at CMR Institute of Technology, Bengaluru, in partial fulfillment of the requirements for the VIII Semester degree of Bachelor of Engineering in Electrical & Electronics Engineering of Visvesvaraya Technological University, Belagavi during the academic year 2020-2021. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library.

The Seminar report has been approved as it satisfies the academic requirements in respect of Seminar work as prescribed for the said Degree.

Signature of the Guide	*Signature of the HOD*	*Signature of the Principal*
----------	----------	----------
Ms. Lokashree B S Assistant Professor EEE Department CMRIT. Bengaluru	Dr. K. Chitra Professor & HOD EEE Department CMRIT, Bengaluru	Dr. Sanjay Jain Principal, CMRIT, Bengaluru

CMR INSTITUTE OF TECHNOLOY
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING
AECS Layout, Bengaluru-560 037

DECLARATION

I, Mr. Akshay Rajeev (1CR17EE004), hereby declare that the Seminar report entitled **"E-VOTING USING BLOCKCHAIN"** has been carried out by me under the guidance of **Ms. Lokashree B S,** Assistant Professor, Department of Electrical & Electronics Engineering, CMR Institute of Technology, Bengaluru, in partial fulfillment of the requirements for the VIII Semester degree of **Bachelor of Engineering in Electrical & Electronics Engineering** of Visvesvaraya Technological University, Belagavi during the academic year 2020-2021.

Place: Bengaluru
Date: 26/06/2021

AKSHAY RAJEEV
USN: 1CR17EE004

ABSTRACT

The electronic voting has emerged over time as a replacement to the paper-based voting to reduce the redundancies and inconsistencies. The historical perspective presented in the last two decades suggests that it has not been so successful due to the security and privacy flaws observed over time. This paper suggests a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method. This paper claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process.

Acknowledgement

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people, who are responsible for the completion of the Seminar work and who made it possible, because success is the outcome of hard work and perseverance, but steadfast of all is encouraging guidance. So, with gratitude, I acknowledge all those whose guidance and encouragement served me to motivate towards the success of the Seminar work.

I take great pleasure in expressing my sincere thanks to ***Dr. Sanjay Jain****,* ***Principal, CMR Institute of Technology, Bengaluru*** *for providing an excellent academic environment in the college and for his continuous motivation towards a dynamic career. I would like to profoundly thank* ***Dr. B Narasimha Murthy****, Vice-principal of CMR Institute of Technology and the whole* ***Management*** *for providing such a healthy environment for the successful completion of the Seminar work.*

I would like to convey my sincere gratitude to ***Dr. K Chitra****,* ***Head of Electrical and Electronics Engineering Department, CMR Institute of Technology, Bengaluru*** *for her invaluable guidance and encouragement and for providing good facilities to carry out this Seminar work.*

I would like to express my deep sense of gratitude ***Ms. Lokashree B S, Assistant Professor, Electrical and Electronics Engineering, CMR Institute of Technology, Bengaluru*** *for her exemplary guidance, valuable suggestions, expert advice and encouragement to pursue this Seminar work*

I am thankful to all the faculties and laboratory staffs of ***Electrical and Electronics Engineering Department, CMR Institute of Technology, Bengaluru*** *for helping me in all possible manners during the entire period.*

Finally, I acknowledge the people who mean a lot to me, my parents, for their inspiration, unconditional love, support, and faith for carrying out this work to the finishing line. I want to give special thanks to all my friends who went through hard times together, cheered me on, helped me a lot, and celebrated each accomplishment.

Lastly, to the ***Almighty****, for showering His Blessings and to many more, whom I didn't mention here.*

CONTENTS

INTRODUCTION

Voting has always been an important part of expressing one's views in a democratic society. Will of the people is a well-respected phenomenon for representation of opinion in formation of electoral bodies. These electoral bodies vary from the college unions to the parliaments. Over the years, `vote' has emerged as a tool for representing the will of the people when a selection is to be made among the available choices. The voting tool has helped improving the trust of people over the selection they make by a vote of majority. This has certainly helped in democratization of the voting process and the value of voting system to elect the parliaments and governments. In 2018, there are 167 counties out of little over 200 who have some kind of democracy; full, flawed, or hybrid etc. Since the trust of people is increasing in democracies it is important that they don't lose their trust on vote and voting system. By virtue of the emerging trust on the democratic institutions, the voting system emerged as a platform to help people to elect their representatives, who consequently form the governments

The power of representation empowers the people with a trust that the government shall take care of the national security, national issues like health and education. policies, international relations, and taxation for the benefit of the people.

In order to make the voting process more effective the institutions like `Election Commission' came into existence in different parliamentary democracies. The institutions, along with setting up the process and legislation for conducting the elections, formed the voting districts, electoral process, and the balloting systems to help in conduct of transparent, free, and fair elections. The concept of secret voting was introduced since the beginning of the voting system. Since the trust on democratic systems is increasing it is important to uphold that the trust on voting should not decrease. In the recent past there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of people was not observed to be effectively quantified and translated in terms of formation of the governments. Such examples can be vastly found in countries like Nigeria, India, Brazil, Pakistan, and Bangladesh.

The disadvantages of such mistrusts are multi-fold and they include but not limited to the following national problems:

- Political instability
- Compromised writ of the government
- Mistrust over the electoral process
- Compromised governance
- Disorder in the state institution
- Chain of command to run state affairs
- Economic instability

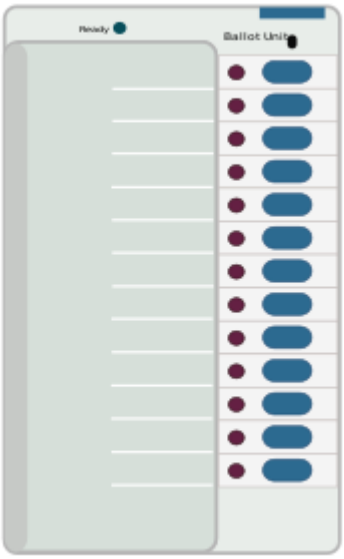


Fig 1: EVM machine

The use of EVMs and electronic voting was developed and tested by the state-owned Electronics Corporation of India and Bharat Electronics in the 1990s. They were introduced in Indian elections between 1998 and 2001, in a phased manner. Prior to the introduction of electronic voting, India used paper ballots and manual counting. The paper ballots method was widely criticized because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots. The printed paper ballots were also more expensive, requiring substantial post-voting resources to count hundreds of millions of individual ballots. Embedded EVM features such as electronically limiting the rate of casting votes to five per minute

LITERATURE REVIEW

In order to improve the trust, the least thing that can be done in this regard is the orientation of the electronic voting based on the biometric authentication. This may help is solving half of the problems being faced by many countries in the electoral process. The e-voting systems have been used by few countries in the past, e.g., Estonia, Ireland, and Norway, while some are not going to use it anymore to eliminate the audit problems.

As a technology, blockchain is quickly becoming unrivalled. Although the Internet has long been familiar with other peer-to-peer applications for file sharing, music streaming, and more, the idea that these types of networks can provide their own security and resources has only been around since 2008. In the decade since its inception, blockchain was mostly tied to the success of the technology that created it, bitcoin.

In recent years, however, it has quickly become a star on its own. With the rise of the world's favourite cryptocurrency, awareness of the mysterious and unique technology behind it also grew. Developers who recognized the value of blockchain are now racing to create new use cases for it and put their ideas into production.

Many are finding that blockchain's primary value lies in its ability to improve old systems. Enterprising observers saw the technology's potential from the start, as bitcoin offered a more secure and transparent payment processing and banking solution than existing ones. In recent years, the same people have used blockchain to revolutionize industries far and wide, including cloud storage, smart contracts, crowdfunding, and even healthcare. However, one of the biggest problems that blockchain's decentralized muscle can solve is voter fraud.

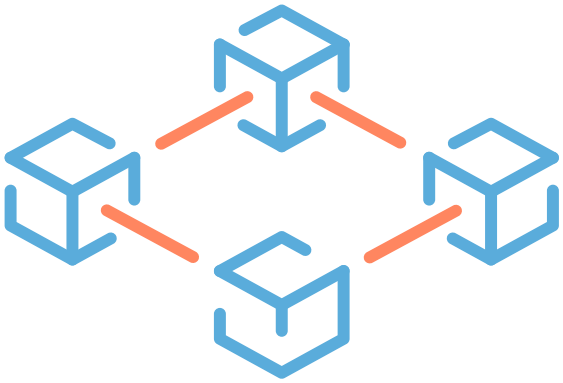


Fig 2: Blockchain Illustration

Blockchain Serves the Voters

In its most basic form, blockchain is a digital ledger. The technology draws its power from the peers—or nodes—on its network to verify, process, and record all transactions across the system. This ledger is never stored, but rather exists on the "chain" supported by millions of nodes simultaneously. Thanks to encryption and decentralization, blockchain's database of transactions is incorruptible, and each record is easily verifiable. The network cannot be taken down or influenced by a single party because it doesn't exist in one place.

It's not only financial transactions that work with blockchain, but any type of data transmission. This kind of system infrastructure is extremely useful for voting because a vote is a small piece of high-value data. Out of necessity, modern voting systems are largely stuck in the last century, and those that want to vote must leave their homes and submit paper ballots to a local authority. Why not bring this process online? Some have tried, but it has proven difficult to put faith in the results due to large gaps in security.

Blockchain can solve the many problems discovered in these early attempts at online voting. A blockchain-based voting application does not concern itself with the security of its Internet connection, because any hacker with access to the terminal will not be able to affect other nodes. Voters can effectively submit their vote without revealing their identity or political preferences to the public. Officials can count votes with absolute certainty, knowing that each ID can be attributed to one vote, no fakes can be created, and that tampering is impossible.

Bringing Elections into the 21st Century

There are already companies working to bring blockchain to the voting populace. One such firm is Horizon State, which has launched a unique solution to answer the question, "If democracy was designed with today's technology, what would it look like?" The company believes its first product is the answer. The company is currently preparing an ICO, planned for October.

Horizon's secure digital ballot box represents a cost-effective and smart solution to the problems inherent in today's voting procedures. Participants will use decision tokens (HST) to cast their votes from a mobile phone or PC, which are then logged into an immutable blockchain and used to reliably verify the outcome of the election. There can be no manipulation, recording errors, or tampering. More than voting, however, this system will be useful simply for making decisions in an environment where

resources and authority are shared. It will also encourage participation.

Voter apathy has seen the number of people show up to cast their votes dwindle in recent years, even as it has become more important to do so. By providing an irrefutable and easy way to vote from one's phone or PC, these numbers would likely rise. Even governments have a reason to change the status quo: a single vote currently costs between $7.00 and $25.00, when all factors are considered. A blockchain product like these costs just $0.50 per vote.

Horizon State co-founder Jamie Skella noted that "Democracy is the opportunity to share in the decision-making processes that relate to the shared matters which affect us. Democracy is about reaching a consensus on how to best use our shared resources to achieve the best outcomes for our partners, children, colleagues, staff, and fellow citizens. Where there are shared resources in any cooperative environment, there remains no question: we need better-shared decision-making tools and processes."

Blockchain-based elections are being trailed in the real world. In November 2018, the Thai Democrat Party, Thailand's oldest political party, held a primary election to elect its new party leader using Z Coin, marking the first large-scale political election carried out using blockchain technology. The vote was concluded with a total of 127,479 votes that came from all over Thailand.1

A True Democracy

Blockchain is paving the way for a direct democracy, where people can decide the course of policy themselves, rather than rely on representatives to do it for them. While the rules of a political election may have to be changed to make way for such a transparent system, blockchain is also ideal for informing business decisions, guiding general meetings, polling, censuses, and more.

The use cases for blockchain voting software are many and diverse. Its ability to engage and manage a constituency is crucial to the future of society, not just to produce a transparent outcome but to encourage all people to participate in their communities. Currently, the technology is still in its infancy, but it matures alongside the young voters it will one day help, and looks to be a key part of our collective future

METHODOLOGY

1. MODELING OF ENTIRE E-VOTING PROCESS

The system modeling helps in drawing the entire system on paper to develop a deep understanding of the system and to identify errors and flaws that can be observed before the system can be implemented.

2. DETERMINATION OF THE SUITABLE TECHNOLOGY PLATFORM TO ENSURE ANONYMITY, PRIVACY, AND SECURITY

The e-voting process requires the features like privacy, security, anonymity, and verifiability as the core function of this solution, it is important that the choice of the underlying technology is consistent to meet these challenges. It has been identified that the Blockchain technology sufficiently deals with all such challenges.

3. DEVELOPMENT & TECHNOLOGY INTEGRATION WITH THE PERCEIVED E-VOTING MODEL

Based on the system model, the system will be developed and will be integrated with the baseline technology.

Blockchain consists of three important concepts: blocks, nodes and miners.

Blocks

Every chain consists of multiple blocks and each block has three basic elements:

The data in the block.

A 32-bit whole number called a nonce. The nonce is randomly generated when a block is created, which then generates a block header hash.

The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be

extremely small).
When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

Miners

Miners create new blocks on the chain through a process called mining.
In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens, miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it is as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially

Nodes

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning.

Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions.

Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scalability of trust via technology.

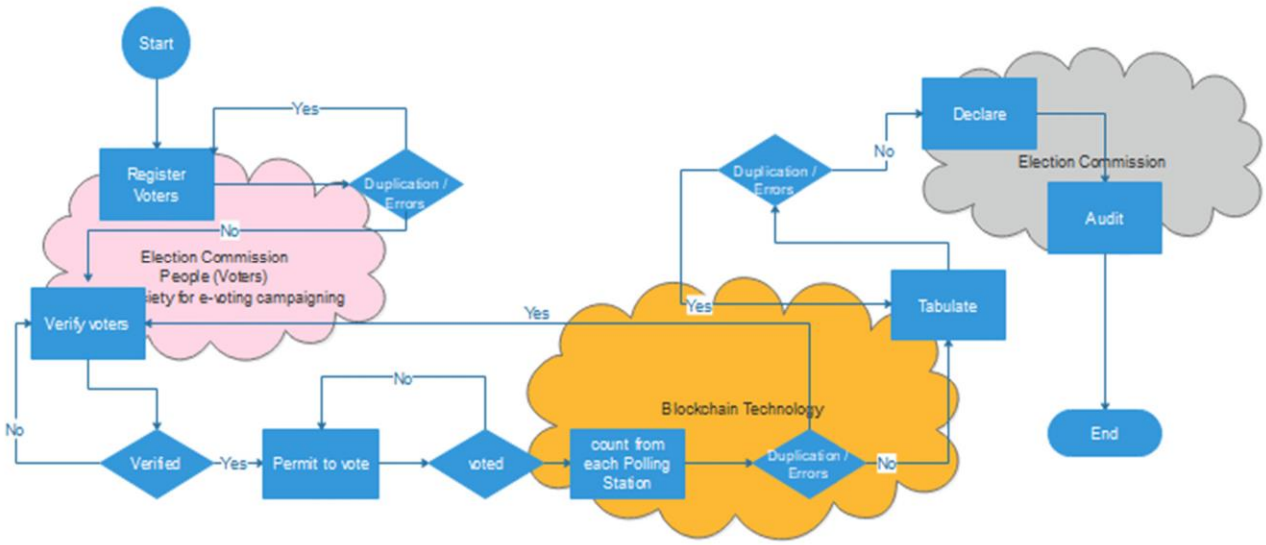


Fig 3: Voting process

Blockchain has three different types, i.e., public blockchain, private blockchain, and consortium blockchain. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public
blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively [38]. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country.

RESULTS AND DISCUSSION

The paper presents a perspective in the electronic voting process. That includes but not limited to identifying the polling process, the selection of the suitable hash algorithm, the selection of adjustments in the blockchain, the process of voting data management, and the security and authentication of the voting process in particular are discussed.

The polling process discussed in this paper is inspired from the actual voting process used on the polling day, which includes the physical and logical verification of the voter and the voter's data but only by using the voters lists etc. The electronic voting process ensure that the voters is verifiable by its physical record, e.g., the national identity card and also verifiable by using the biometric authentication. The availability of the verification system on the polling time is extremely essential and the process can't be completed without the completely available system. The threats to the verification process can be extremely high if either the system is not available or the system is not in a state to be used effectively for the purpose of the voter's verification. It is the responsibility of the election commission and allied institutions to ensure that the equipment, tools, and technologies are available to make / keep the proceedings on track. The process can only be successfully completed if all the stakeholders perform their duties with extreme coherency and consistency.

ADVANTAGES

- ENHANCED SECURITY

  Your data is sensitive and crucial, and blockchain can significantly change how your critical information is viewed. By creating a record that can't be altered and is encrypted end-to-end, blockchain helps prevent fraud and unauthorized activity. Privacy issues can also be addressed on blockchain by anonymizing personal data and using permissions to prevent access. Information is stored across a network of computers rather than a single server, making it difficult for hackers to view data.

- GREATER TRANSPERANCY

  Without blockchain, each organization has to keep a separate database. Because blockchain uses a distributed ledger, transactions and data are recorded identically in multiple locations. All network participants with permissioned access see the same information at the same time, providing full transparency. All transactions are immutability recorded, and are time- and date-stamped. This enables members to view the entire history of a transaction and virtually eliminates any opportunity for fraud.

- INSTANT TRACEBILITY

  Blockchain creates an audit trail that documents the provenance of an asset at every step on its journey. In industries where consumers are concerned about environmental or human rights issues surrounding a product — or an industry troubled by counterfeiting and fraud — this helps provide the proof. With blockchain, it is possible to share data about provenance directly with customers. Traceability data can also expose weaknesses in any supply chain — where goods might sit on a loading dock awaiting transit.

- INCREASED EFFICIENCY AND SPEED

  Traditional paper-heavy processes are time-consuming, prone to human error, and often requires third-party mediation. By streamlining these processes with blockchain, transactions can be completed faster and more efficiently. Documentation can be stored on the blockchain along with transaction details, eliminating the need to exchange paper. There's no need to

reconcile multiple ledgers, so clearing and settlement can be much faster.

- AUTOMATION

  Transactions can even be automated with “smart contracts,” which increase your efficiency and speed the process even further. Once pre-specified conditions are met, the next step in transaction or process is automatically triggered. Smart contracts reduce human intervention as well as reliance on third parties to verify that terms of a contract have been met. In insurance, for example, once a customer has provided all necessary documentation to file a claim, the claim can automatically be settled and paid.

APPLICATIONS

- Cryptocurrency exchange
- Voting mechanism
- Secure sharing of medical data
- NFT marketplaces
- Music royalties tracking
- Cross-border payments
- Real-time IoT operating systems
- Personal identity security
- Anti-money laundering tracking system
- Supply chain and logistics monitoring
- Advertising insights
- Original content creation
- Real estate processing platform

CONCLUSION

Mistrust in the voting is not an uncommon phenomenon even in the developed countries. The electronic voting, however, has emerged as an alternative but still not being practiced at a large scale. The electronic voting is anticipated to have a great future yet the past is not that glorious. In some countries e-voting is not an option while few are in a process to eliminate the security, verifiability, and anonymity concerns. There are issues that require immensely deep consideration by the legislatures, technologist, civil society, and the people. This research has proposed a framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm, selection of adjustments in the blockchain, process of voting data management, and the security and authentication of the voting process. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process.

FUTURE WORK

1. Blockchain is not a Distributed Computing System

Blockchain is a network that relies on nodes to function properly. The quality of the nodes determines the quality of the blockchain. For example, Bitcoin's blockchain is strong and incentivizes the nodes to participate in the network. However, the same cannot be true for a blockchain network that does not incentivize the nodes.

2. Scalability Is An Issue

Blockchains are not scalable as their counterpart centralized system. If you have used the Bitcoin network, then you would know that the transactions are completed depending on the network congestion. This problem is related to scalability issues with blockchain networks. In simple words, the more people or nodes join the network, the chances of slowing down is more!

3. Some Blockchain Solutions Consume Too Much Energy

Blockchain technology got introduced with Bitcoin. It uses the Proof-of-Work consensus algorithm that relied on the miners to do the hard work. The miners are incentivized to solve complex mathematical problems. The high energy consumption is what makes these complex mathematical problems not so ideal for the real-world.

4. Blockchain Cannot Go Back — Data is Immutable

Data immutability has always been one of the biggest disadvantages of the blockchain. It is clear that multiple systems benefit from it including supply chain, financial systems, and so on. However, if you take how networks work, you should understand that this immutability can only be present if the network nodes are distributed fairly.

5. Blockchains are Sometimes Inefficient

Right now, there are multiple blockchain technologies out there. If you pick up the most popular ones including the blockchain technology used by Bitcoin, you will find a lot of inefficiencies within the system. This is one of the big disadvantages of blockchain.

REFERENCES

[1] EIU Democracy Index 2017. Accessed: Aug. 3, 2018. [Online]. Available: https://infographics.economist.com/2018/DemocracyIndex/

[2] ScienceDirect. Democracy Online: An Assessment of New Zealand Government Web Sites. Accessed:Aug.1,2018.[Online].Available:https://www.sciencedirect.com/science/article/pii/S0740624X00000332

[3] M. Volkamer, O. Spycher, and E. Dubuis, ``Measures to establish trust in Internet voting," in Proc. 5th Int. Conf. Theory Pract. Electron. Governance, 2011, pp. 1 6.

[4] É. Bélanger and R. Nadeau, ``Political trust and the vote in multiparty elections: The Canadian case," Eur. J. Political Res., vol. 44, no. 1, pp. 121 146, 2005.

[5] T. Kunioka and G. M. Woller, ``In (a) democracy we trust: Social and economic determinants of support for democratic procedures in Central and Eastern Europe," J. Socio-Econ., vol. 28, no. 5, pp. 577 596, 1999.

[6] T. van der Meer, ``In what we trust? A multi-level study into trust in parliament as an evaluation of state characteristics," Int. Rev. Administ. Sci., vol. 76, no. 3, pp. 517 536, 2010.

[7] D. Basin, H. Gersbach, A. Mamageishvili, L. Schmid, and O. Tejada, ``Election security and economics: It's all about eve," in Proc. Int. Joint Conf. Electron. Voting, 2017, pp. 1 28.

[8] P. Bevelander and R. Pendakur, ``Electoral participation as a measure of social inclusion for natives, immigrants and descendants in Sweden," Tech. Rep., 2008, p. 33.

[9] S. Wolchok et al., ``Security analysis of India's electronic voting machines," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 1 14.

[10] R. L. Rivest, ``The threeballot voting system," Tech. Rep., 2006, p. 15.

LIST OF FIGURES

LIST OF ABBREVIATIONS AND SYMBOLS

EVM: Electronic Voting Machine

SEMINAR REPORT

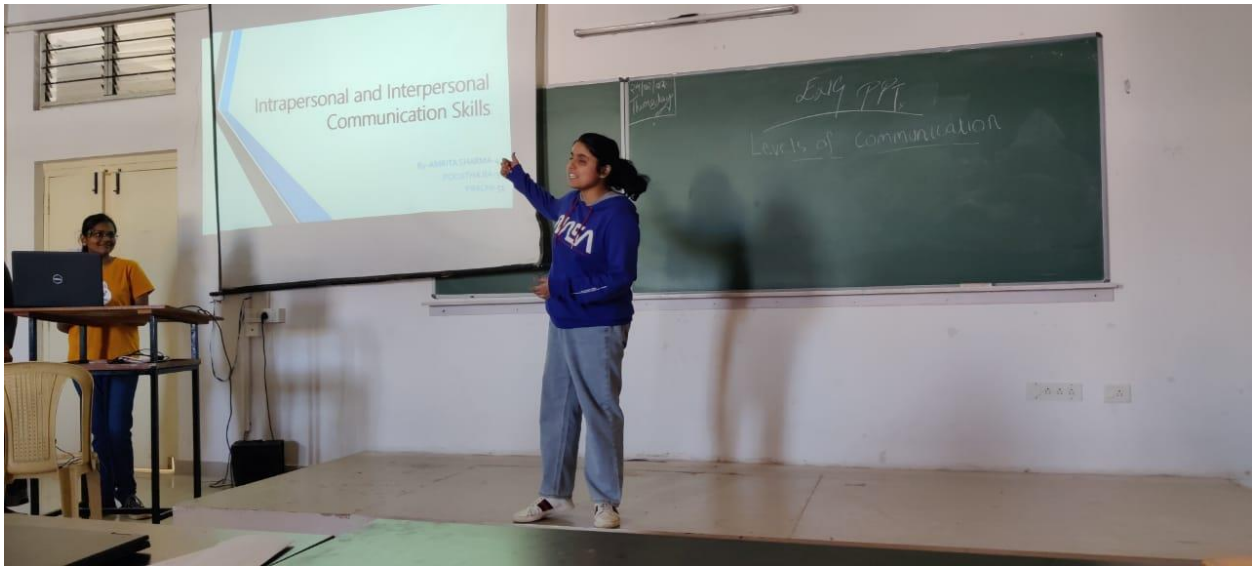
Odd Semester 2020-21

Paper: 18EGH18 Communicative English

Topics Assigned:

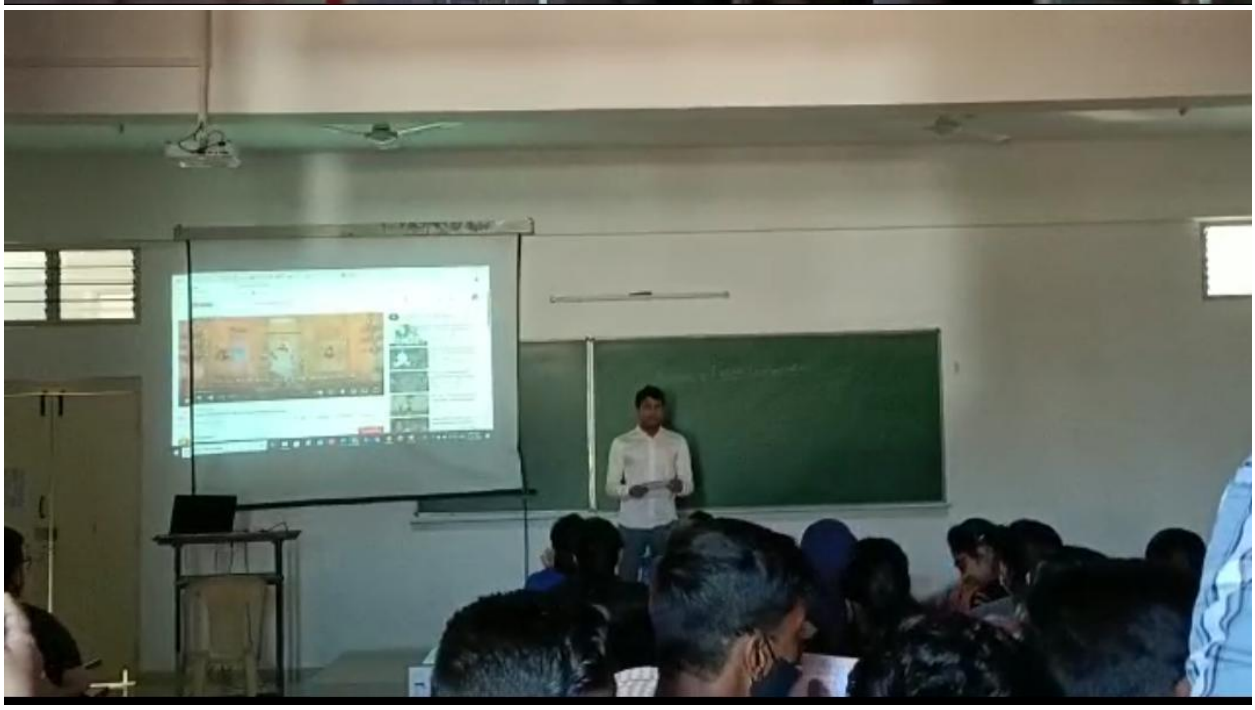
1. Fundamentals of communication
   Members: Vachana Vageesh
   Rohan Rajendra
   Jayajeeva N
   Abhishek Kundagol

2. Interpersonal and Intrapersonal communication
   Members: Kumkum Kumari
   Manik Ranjan
   Akanksha



3. Barriers of Communication
   Members: Soorya Charan Madisetty

Bala Seetha Rami Reddy Chaikam
Sanisetty Satwik
Y Narasimha



Feedback:

Students found the seminars helpful and productive to learn the topics as well and communicative skills in a cognitive manner. They used different methods including traditional chalk and board method, PowerPoint presentation, live quizzes, role plays, etc. to present the

topics effectively. Active participation from the students encouraged the presenters to present confidently and they took feedback from the audience about their seminars.