IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

Blockchain Voting Model

Harshil Tyagi[1], Aryan Srivastava[2], Divyansh Saxena[3]

[1]Senior Data Science Engineer, Dunnhumby, Gurugram, Haryana, India

[2]Data Engineer, Tata consultancy Services, Noida , Uttar Pradesh ,India

[3]System Engineer, Infosys, Banglore, Karnataka, India

Abstract: Voting has been a fundamental part of democracies around the world; it has been the voice to their opinions for individuals in a community. Indian constitution was founded upon the beliefs in individual rights. But in recent years, voter turnout has plummeted while the ever-increasing concerns regarding integrity, security, and accessibility of voting systems haven't been addressed. E-Voting can solve this problem; however, it requires supervision by central authority. In this paper, the available open source Blockchain technology is used to propose a design for a new electronic voting system that could be used in future electronic elections. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments.

Keywords: Voting, Blockchain, Smart contracts, Decentralized application, ledger.

I. INTRODUCTION

The modern internet deals with data, which can be your most valuable entity that you can't touch but want to protect at any cost. This information is saved in an encrypted form on a network which is de-centralised and spread; called the blockchain or ledger. This not only protects your information on a network but also prevents theft, while quickening the process and reducing hefty errors. From time to time computer scientists have claimed that hackers can rig the electronic system to manipulate votes. This has resulted in widespread mistrust and doubt against the current system. The blockchain prevents this as the votes become encrypted and decentralized. In a system build upon blocks and smart contracts private individuals must be assured that their votes were counted and also, they must be able to confirm who they voted for. To implement this, project environment is developed in which a contract (smart contract) will be compiled and migrated on a local Ethereum blockchain. Changes within the blockchain are done with the help of a smart contract through a decentralized application or Dapp. Smart contracts are nothing but set of rules to be followed to give functionality of an election. Finally, users will be able to interact with the contract through a client-side application that will allow users web page to display the vote counts and vote for candidates through the web browser. This application can be hosted on a local server where voting could be done and results could be seen.

II. LITRATURE SURVEY

Current Voting System in India

Electronic Voting Machines ("EVM") are being utilized in Indian General and State Elections to actualize electronic casting partially from 1999 decisions and as of late in 2018 state races held in five states crosswise over India. EVMs have supplanted paper votes in nearly state and general (parliamentary) races in India. There are prior cases in regards to EVMs' tamper ability and security.

Limitations to EVM

Through the current system anyone can know what number of individuals from a surveying station voted in favour of him. This is a critical issue especially if trim sided votes in favour of/against a competitor are thrown in individual surveying stations and the triumphant applicant may demonstrate bias or hold resentment on explicit regions. The Election Commission of India has expressed that the producers of the EVMs have built up a Totalizer unit which can interface a few balloting units and would show just the general outcomes rather than votes from individual surveying stations.

The control units don't electronically transmit their outcomes back to the Election Commission. The Indian EVMs are intentionally structured as remain solitary units to counteract any interruption amid electronic transmission of results. Rather, the EVMs are gathered in checking stalls and counted on the appointed tallying day(s) within the sight of surveying operators of the applicants.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

Decentralized Voting systems

A web application normally interacts with a browser and communicate to a central system server of a network. The whole code of the web-application resides on this center of the server and all of the crucial information resides on a centralized database and whenever it wants to use the application it must communicate with this central server because this is how a web application will work. It's extremely bad to build a voting application based on this model because for one - all of the data stored in the database could change at any time and the vote could change or it can be deleted entirely. Two - all of the code in the application could change at any time and this means that the rules in the election could change so a centralized web application can't be built. Because of these problems we want to build a decentralized blockchain application.

Blockchain Voting Model

The objective is to ensure that every vote is counted that all the votes are only one of kind and that the correct candidates with the most votes is actually going to win the election. Smart contracts using blockchain solves these problems and that's why is a better choice for building any voting application. On the blockchain all the data doesn't lie on a central server but instead the data is decentralized and it's distributed across every device connected to the blockchain. A P2P network or blockchain nodes which communicate to one another; so, if a device is connected to the blockchain it is a node and it talks with all the other nodes and will share some of the same responsibilities that a web server might assume. These responsibilities are as follows – it will get a copy of all the data that's shared across the blockchain all this data is contained in bundles of Records that are connected with each other to form the public ledger. All the nodes on the network work together to ensure that all the data on the public ledger remain secure and unchanged and this is important for a voting application because it means that it will always know that the account sent the transaction whenever it vote and that its vote will go to the correct candidate and be recorded forever. Because all of the data is shared across devices on the blockchain, the blockchain fundamentally is a database and because all of the nodes talk to one another on the blockchain, it's also a network so instead of the traditional web model blockchain can be thought of as a network and a database all in one. It's much better to build a voting application on the blockchain in this decentralized way so that we can voters can vote with confidence.

The idea of adapting the digital voting system is to make the whole process of voting simpler, faster and easier. This is more compelling to the modern society. For the public the whole process should be normalized and thus this proposed system will lessen the burden on the Election commission. The blockchain voting model is a unique electronic voting system which is based on Ethereum transactions and utilizes smart contracts to enable a cost efficient and secure elections which ensures public privacy and the result will be generated faster. Key features of blockchain:

- Resilience - Architecture of blockchain is based upon replicated architecture.
- Timestamping - Timestamping is done for securely keeping track of the documents time of creation or modification. It allows interested parties to see, without a doubt, that a document requested exists at a particular date/time. Every block has a timestamp when created in a blockchain transaction.
- Reliability - We can certify or verify the Identities of interested parties, as all the information is present in the Blockchain. This truncates duplicate records, reducing rates and at same time accelerating transactions.
- Unchangeable transactions - If a transaction or data is recorded on the blockchain even once, it cannot be undone. There are no possible ways of going back and modify or edit any data that already has recorded on the blockchain.
- Fraud prevention - The idea of shared information or data prevent practical losses due to fraud or embezzlement. In industries based on logistics, to minimize cost blockchain act as a monitoring mechanism.
- Security- Threat on a normal system is the bringing down of a specific target with the help of DLT, each user that already has a copy of the original blockchain, so the system remains working, even the rest of other nodes fall.
- Transparency - As each transaction is immutable, any changes to public blockchains are viewable to each individual. This provides more transparency.
- Collaboration- The collaboration of parties makes it easier to allow transactions directly with each other without the involvement of mediating third parties.
- Decentralization- There is no service provider or central authority. This process ensures that all transactions are valid and one by one each of the valid transactions are added.

III. TECHNICAL ARCHITECTURE

Block (Ledger)

The ledger/block is open and public so that each user can see and validate transactions. The ledger is decentralized and cronocally exists in all nodes on the network which eliminates the dependency on third party.

Each Block has –

- Data
- Hash
- Hash of the previous block

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

Block Header

Each candidate block has its own block header which consist of metadata such as: Version, Last block address, Transactions, Time and Target. These metadata are used when the block has to be added in an existing blockchain.

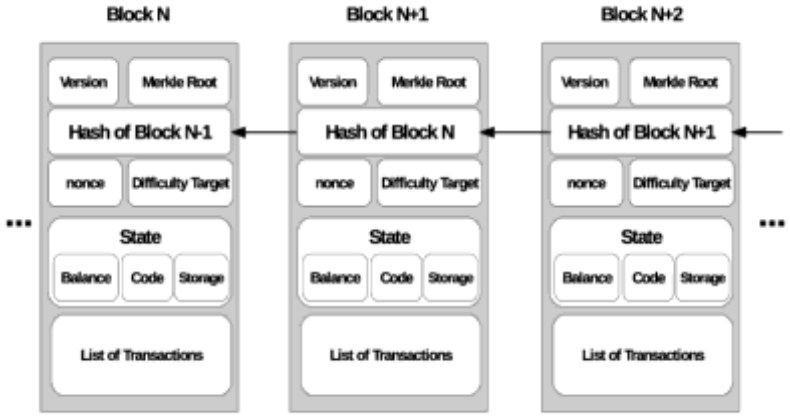

Fig. 01: A simple blockchain structure

To identify a block in a block chain a cryptographic hash or a digital signature is used. This is obtained by a method called hashing. Generally the hashing is done twice with SHA 256 Algorithm. Each and every block uses the hash from the previous blocks to create its own hash such that the hash generated is always unique. These blocks are chained together and after the chaining the data becomes immutable which is the core concept for the block chaining.

Smart Contracts

A smart Contract is a self-executing contract which consist of terms and agreements between a buyer or seller, these contracts are written into lines of codes. It permits only those transactions which are trusted and it permits the agreements that has to be carried out between the desperate and third parties without any need of a governing party.
Smart contract is a piece of code which is deployed on the blockchain and is uniquely identify identified by an address. The smart contract implementation includes user defined methods, state defined variables, and events. Smart contracts are implemented through a high-level language such as python and solidity.

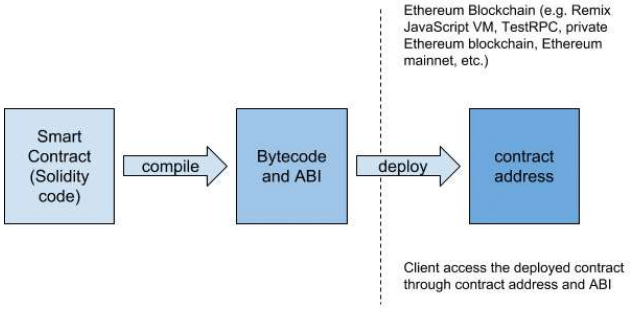

Fig. 02: Stages of Smart contract development

Decentralized Application or DAPP

The smart contracts can directly be used by end-users who can send the calls or transaction to the smart contracts through Ethereum clients however to provide a more lucid and easier to use interface to smart contracts Decentralized applications can be created and applied over these smart contracts a DAPP includes a front-end user interface which is implemented by utilizing HTML, CSS and back-end (typically implemented in JavaScript).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

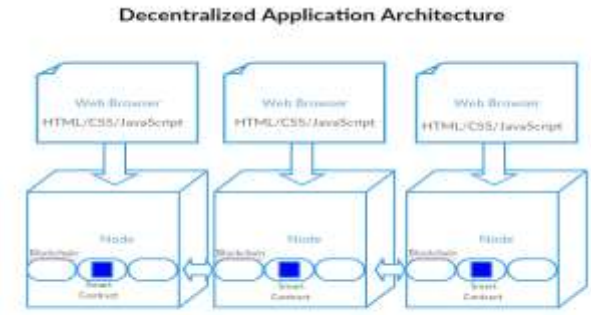

Fig. 03: Architecture of DAPP

Ethereum Blockchain

The structure of the Ethereum blockchain is fundamentally the same as bitcoin's, in that it is a common record of the whole exchange history. Each hub on the system stores a duplicate of this history. The major distinction with Ethereum is that its hubs store the latest condition of each shrewd contract, notwithstanding the majority of the ether exchanges. For each Ethereum application, the system needs to monitor the 'state', or the present data of these applications, including every client's parity, all the contract code and where it's everything put away. Bitcoin utilizes unspent exchange yields to follow who has how much bitcoin. While it sounds progressively intricate, the thought is genuinely straightforward. Each time a bitcoin exchange is made, the system 'breaks' the aggregate sum as though it was paper cash, issuing back bitcoins such that influences the information to carry on likewise to physical coins or change.

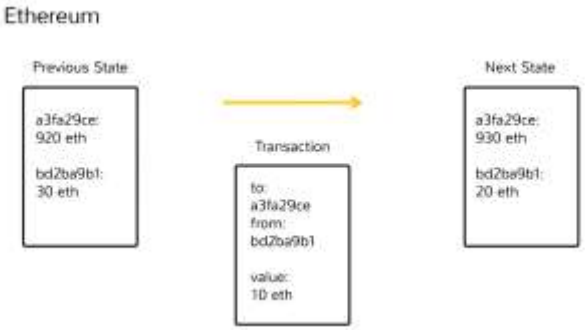

Fig. 04: Ethereum Blockchain

IV. SYSTEM ANALYSIS AND DESIGN

The main objectives of the Project is to build an application (client-side) that will communicate to the smart-contracts on the given blockchains. This DAPP will have a table of individual candidates that will list all the mentioned names, ids, and counts of votes. It will have a form or a survey where individuals can caste vote for desired candidates.

There are substantial social and personal benefits to using this blockchain system as well such an easier and faster voting procedure which will lead to maximum voter turnout. This system can be implemented for a greater number of countries/cities as the penetration of internet in the universe increases. We might definitely see a future where each party will create an application-system that is related to our ideas.

Requirement Analysis

Fig. 05: Requirement Analysis of Blockchain

IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

Proposed System

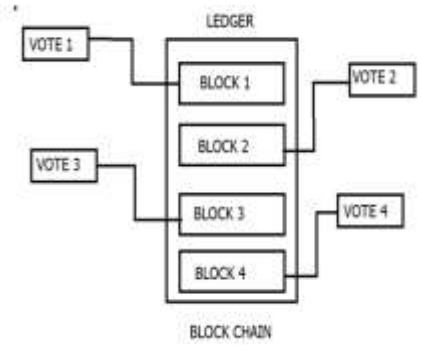

Fig. 06: Block Diagram of a ledger in blockchain

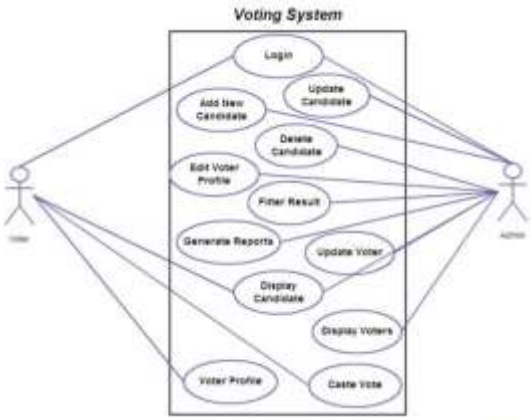

Fig. 07: Use Case Diagram

The model is accomplished by creating a decentralized application where individuals submit their transactions to the smart contract linked to the Decentralized application form and Dapp's web interface as well. The Dapp's web UI which indicates the transaction to the blockchain platform and gives the output of the transfer. State information is received via transactions in the smart contracts in the web interface. A Decentralized application is deployed on an ethereal node which serves the Decentralized application's web-based user interface. The Decentralized application logic is controlled by the associated smart contracts which are deployed on the blockchain platform. Decentralized applications which have special storage requirements can make use of decentralized storage platforms like a swarm.

Roles in Process

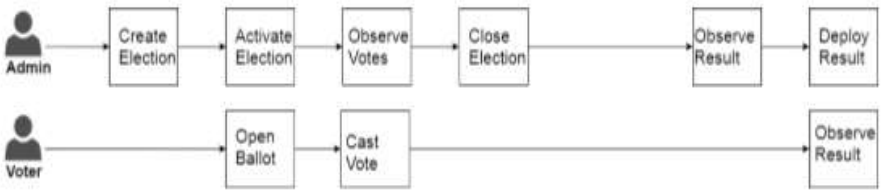

Fig 08: Roles of Admin and Voter

Administrators: Election administrators manages the complete process of an election. Many trusted organizations and companies are enrolled with this role. The election administrators specify type of election and create a fore mentioned election, ballots configuration, register voters in the system, deciding the lifetime of the election and giving commissioned nodes.

Electoral Voters:Voters can authenticate themselves for elections they are eligible for, load election ballots, cast their vote and validate their votes after an election is over through result window.

IJARCCE
ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 9, September 2021
DOI: 10.17148/IJARCCE.2021.10920

Election as Smart Contract

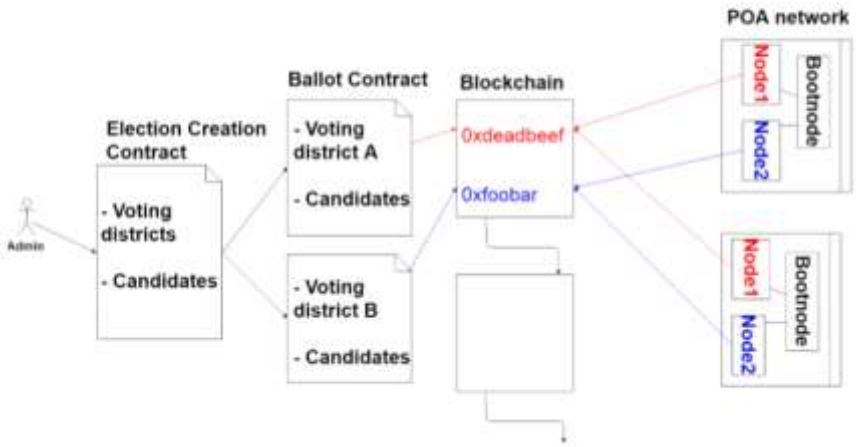

Fig 09: Election as a smart Contract

Transactions in Ethereum

The interaction in the Ethereum network is done in the form of Transactions. Ethereum network is a form of database which provides us the facility of storing data in distributed and secure network. Transactions enables the users to modify or update the data/state stored in the Ethereum network like a query would do in a usual RDBMS system. A usual Ethereum network circulates its own native currency which is called as ether. Apart from this normal transaction system, ether is used as the transaction fee or service charge which is often referred as gas in Ethereum network when the network is processing the transaction. This can be seen in the following table:

TxHash	Block	Age	From	To	Value	[TxFee]
0xdead...	1337	33 sec ago	0xbeef...	Token	10 Ether	0.087
0xface...	1337	33 sec ago	0x4242...	0x1234...	1 Ether	0.056

Table1: Example of public transaction

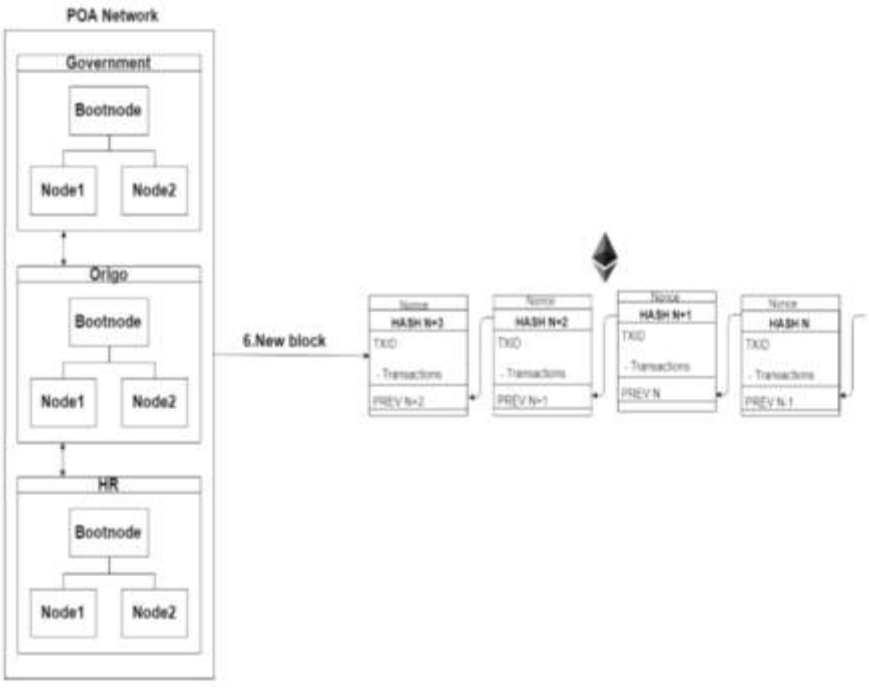

Figure 10: Block added to blockchain

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10920

V. CONCLUSION

The EVMs and ballot systems have already showed that larger number of issues could lead to widespread political unrest in our country. It is crucial for any democratic system to have a trustable voting system that gives the least number of obstacles for a voter who wants to vote. The proposed system not only handles voter data confidentially and integrity but also provides a transparent system for validation of the electoral campaign. Keeping all these features in mind the proposed model is a comprehensive solution that satisfies all the requirements required to solve this problem.

Blockchain has a great future and part in transforming today's technology. It has scope not only in electoral systems but also in different sectors such as supply chain management, digital advertising, forecasting, cyber security, Internet of things, networking, etc. Custom electoral purposes based blockchain networks could be revolutionary for the democratic systems. An e-wallet for voting using blockchain technology can be proved very useful once introduced in the market. This wallet not only prohibit the interference of any third party but also has an open ledger which makes it trustworthy. The current project only shows the transaction of votes between 10 clients in a Ethereum blockchain for two representatives. In the nearby future, it is also possible to introduce various new types of hybrid blockchain networks equipped with better encryption algorithms and it can also help in reshaping the way we use various devices in our daily life. This technology will make the process transparent and easy to avoid any type of fraud activity.

ACKNOWLEDGMENT

Dr. R.P. Mahapatra (Prof., HOD CSE, SRM-IST), **Analp Pathak** (Assistant Professor, SRM-IST), **Govind Verma** (Assistant Professor, SRM-IST) are gratefully acknowledged for their inputs and discussions during this study.

REFERENCES

[1]. Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized Oracle Network Available at: https://link.smartcontract.com/ whitepaper
[2]. TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain/
[3]. N. Uribe, "10 Benefits of Electronic Voting," 01 August 2016.
[4]. National Institute of Standards and Technology, "Federal Information Processing Standards Publication", (2012). [18] S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).
[5]. Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today.
[6]. X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, "Distributed bitcoin account management," in 2016 IEEE Trustcom/BigDataSE/ISPA, Aug 2016, pp.
[7]. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, —A survey on the security of blockchain systems.
[8]. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy - Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom
[9]. A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM - Ahmed Ben Ayed, Department of Engineering and Computer Science, Colorado Technical University, Colorado Springs, Colorado, USA.
[10]. J. Jan and Y. Chen and Y. Lin, "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England, (2001) October 16-19.
[11]. D. L. Dill and A.D. Rubin, "E-Voting Security", Security and Privacy Magazine, Vol. 2(1). (2004), pp. 22-23.
[12]. D. Evans and N. Paul, "Election Security: Perception and Reality". IEEE Privacy Magazine, vol. 2(1). (2004), pp. 2-9.

BIOGRAPHY

Harshil Tyagi, B. Tech in Computer Science and Engineering (2015-2019) from SRM Institute of Science and Technology, Chennai, India. Currently working as Senior Data Science Engineer, Dunnhumby, Gurugram, Haryana, India.

Aryan Srivastava, B. Tech in Computer Science and Engineering (2015-2019) from SRM Institute of Science and Technology, Chennai, India.Currently working as System Engineer at Tata Consultancy Services, Noida, Uttar Pradesh, India.

Divyansh Saxena, B. Tech in Computer Science and Engineering (2015-2019) from SRM Institute of Science and Technology, Chennai, India.Currently working as System Engineer at Infosys, Banglore, Karnataka, India.

