ISSN No:-2456-2165

Blockchain Voting System

W. Ancy Breen[1]
Department of Computer Science
SRM Institute of Science and Technology,
Ramapuram Chennai, India

Anmol Kakkar[2]
Department of Computer Science
SRM Institute of Science and Technology,
Ramapuram Chennai, India

Arnav Kaushik[3]
Department of Computer Science
SRM Institute of Science and Technology,
Ramapuram Chennai, India

Siddhartha Bhattacharjee[4]
Department of Computer Science
SRM Institute of Science and Technology,
Ramapuram Chennai, India

Abstract:- The blockchain voting system provides a revolutionary response to issues with load management, cost, security, and scalability that plague conventional election procedures. Blockchain, in contrast to traditional systems, offers a decentralized, transparent, and unchangeable platform that can manage high voter participation, which makes it perfect for populous nations like India. Voter manipulation is prevented by the system's use of cryptography to secure voter anonymity and data integrity. Because it is decentralized, there are no single points of failure, which improves security. Enabling remote voting lowers the requirement for actual polling places and human involvement while simultaneously boosting voter turnout and cost efficiency. Real-time voter list updates, shared scaling techniques for dependable performance, and wallet-based voting with distinct Vote IDs for fraud prevention are some of the salient features.All transactions are transparent and verifiable, ensuring transparency, security, and confidence. This blockchain-based method improves accessibility and fortifies democratic processes by providing a scalable, secure, and affordable option for contemporary elections.

I. INTRODUCTION

This study proposes a blockchain-based decentralized voting system architecture that offers control, security, validity, and scalability. The system's main feature is wallet-based voter authentication, which employs cryptographic wallets to securely identify and authorize voters while guaranteeing that only qualified voters cast ballots. [1][2]

Important elements include whitelisting to restrict system interaction to certified entities only, strict validation methods including formal verification and in-person testing, and control mechanisms to keep an eye on protocol adherence. By putting forth a dynamic consistency model that adjusts to changing participant loads, the framework also tackles scalability. Blockchain's security features provide immutability and transparency by integrating advanced security methods to guard against risks like double voting, manipulation, and unauthorized access. [3]

II. PROPOSED WORK

India, the largest democracy in the world, has the most convoluted and drawn-out voting process when compared to other nations. Given its intricate structure, our endeavor will be specifically tailored to the Indian voting system, addressing its unique problems and needs. Unlike previous blockchain voting initiatives designed for other countries, this project will take into account the complexity and breadth of India's political structure, ensuring a trustworthy, secure, and efficient electoral process.

This architecture will enable government-issued blockchain identification (private and public key), which will improve authentication. To avoid any influence, the outcome will remain a secret until the election is over. The outcome will be communicated exclusively to approved broadcaster and it can then broadcast the result to wider public.

ISSN No:-2456-2165

III. ARCHITECTURE DIAGRAM

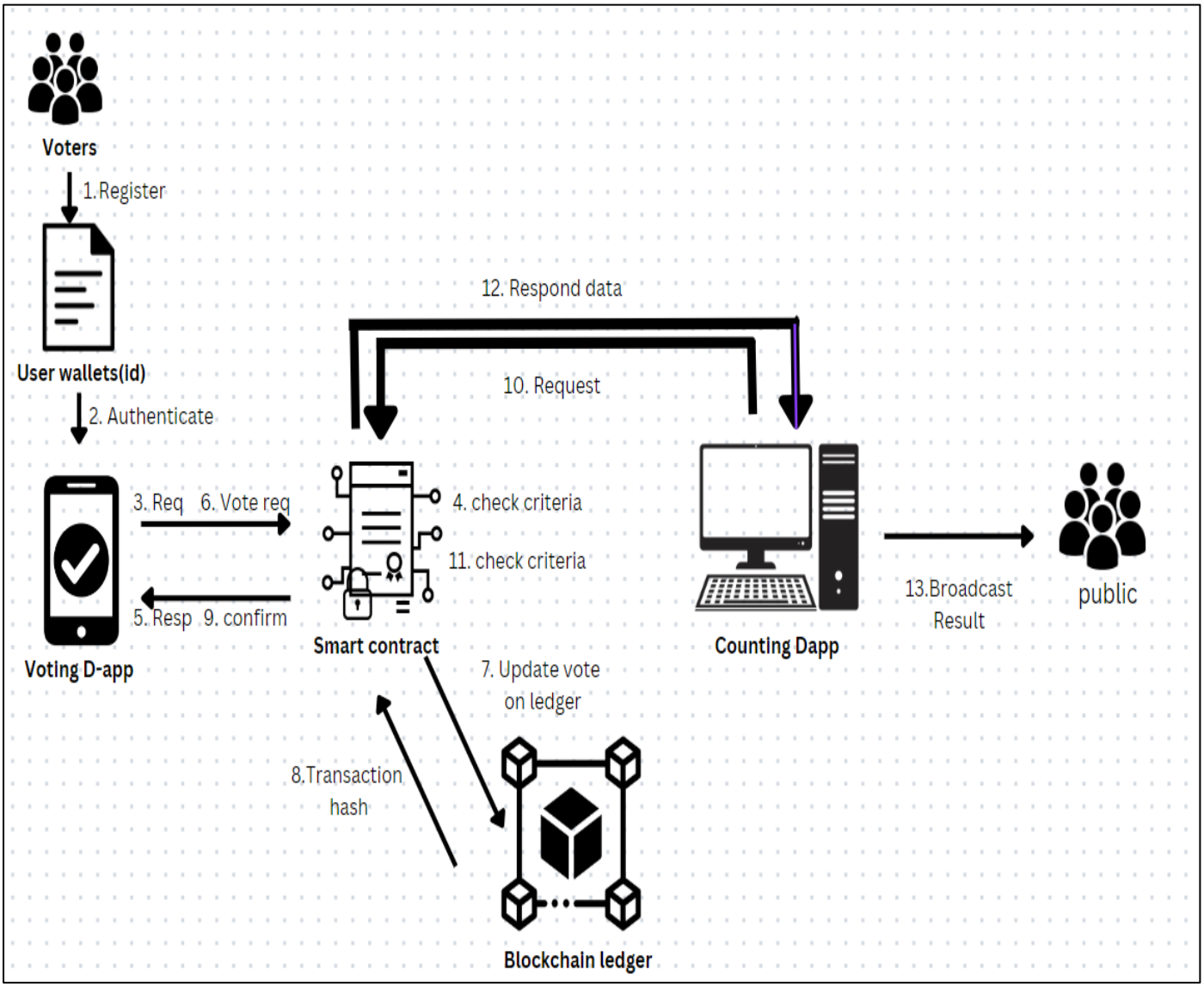

Fig 1 Voting System Architecture

The graphic shows how votes are cast, verified, and counted using decentralized applications (D-apps) and smart contracts in a blockchain-based voting system.

- In order to engage in the electoral process, voters must register their identities.
- Voters authenticate themselves by using user wallets, which are usually connected to a decentralized identification system.
- Voters submit a request to the Voting D-app expressing their desire to cast a ballot.
- The voter's eligibility is verified by the Smart Contract, which makes sure they haven't cast their ballot yet.
- The voter receives a response from the Voting D-app verifying their request.
- Voting D-app receives the Vote Request from the voter and transmits it to the Smart Contract.
- For transparency and immutability, the Smart Contract updates the vote on the Blockchain Ledger.
- As an eternal record of the vote, a Transaction Hash is created and kept on the blockchain.
- Voters receive a confirmation through the Voting D-app confirming that their vote was cast successfully.
- To obtain voting statistics, the Counting D-app makes a request to the smart contract. Prior to transferring any data, the Smart Contract verifies the criteria one more.

The Counting D-app receives data responses from the Smart Contract. After the counting procedure is finished, the outcome is finally announced to the public.

ISSN No:-2456-2165

IV. FLOW DIAGRAM

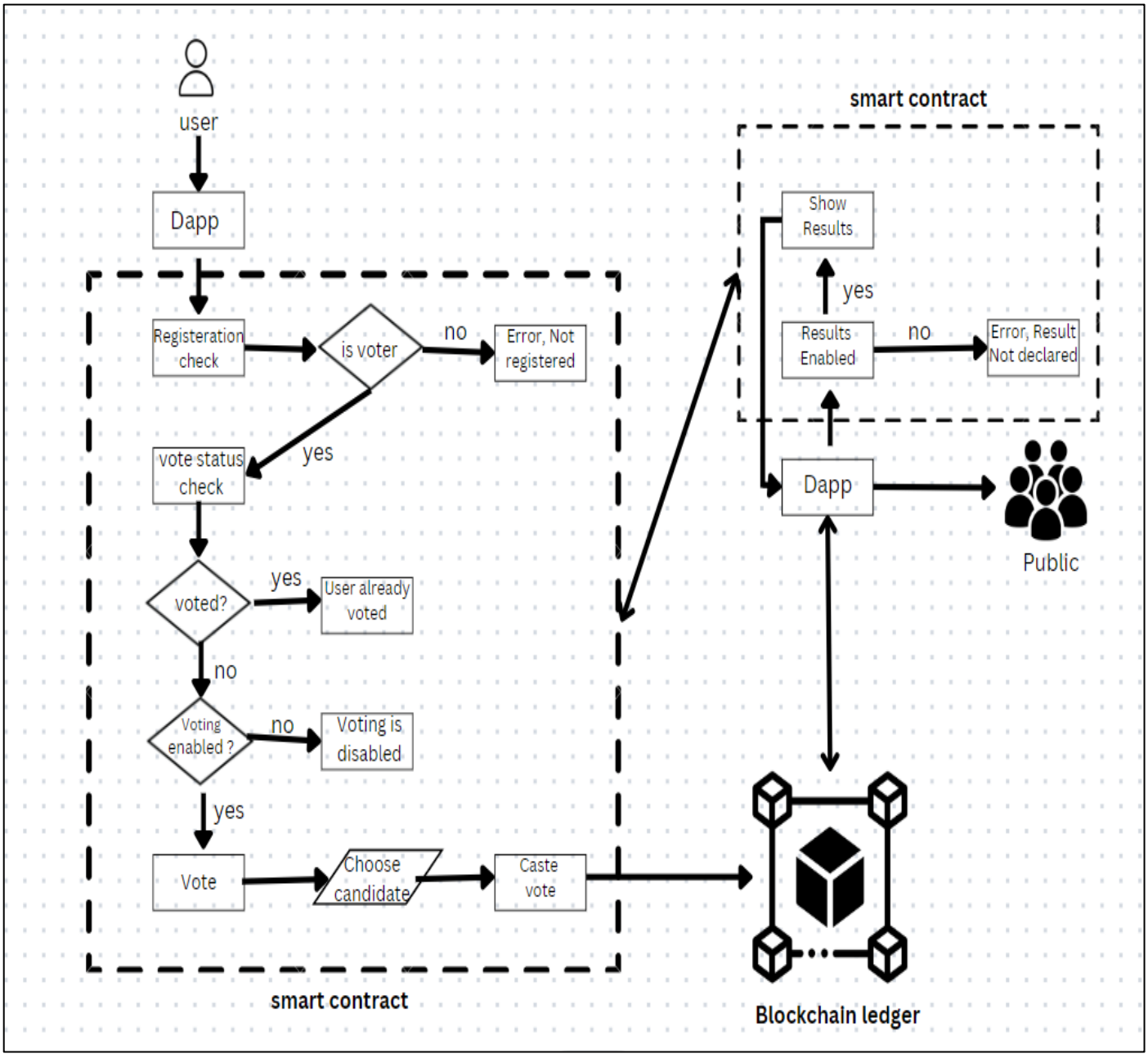

Fig 2 The Voting Process

This graphic shows how a decentralized application (Dapp) and smart contracts are used in a blockchain-based voting process. Here's a condensed explanation:

- User Interaction with Dapp: To cast a ballot, the user communicates with the Dapp. There is a registration check conducted by the system. The user receives an error message if they are not registered.
- Vote Status Check: The system verifies the user's vote status whether they are registered. An error message stating "User already voted" appears if the user has already cast a ballot.
- Voting Enabled Check: The system determines if voting is enabled, if the user hasn't cast a ballot. The user is unable to continue if voting is disabled.
- Voting Procedure: Should voting be activated, the user has the option to select a contender and thencast their ballot.
- Result Declaration: If the results are enabled, the smart contract verifies this. An error message appears if the results are not declared. The Dapp shows the results to the public if they are accessible.

This solution ensures that users may only vote if they match the relevant requirements and assures that votes are securely recorded on the blockchain for transparency and immutability.

V. RSA PUBLIC-PRIVATE KEY BASED WALLETS FOR VOTER ID

RSA public-private key cryptography may be used to efficiently manage voter identity and authentication in a blockchain-based voting system.

This approach uses cryptographic wallets to handle voter IDs, guaranteeing a safe, open, and unchangeable voting process.[4][5]

➢ *Private Key Authentication and Public Key Identification*

- **Public Key Identification:** An RSA-based wallet with a distinct set of public and private keys is given to each voter. Voters are uniquely identified by their public key, which is saved and referred to in the voter whitelist that the blockchain network keeps up to date. Only confirmed public keys are included in this whitelist, guaranteeing that only eligible voters may take part in the election.

- **Whitelist-Based Voter Management:** Using the public keys of all registered voters, the system creates a voter whitelist prior to the start of voting. The public keys on this whitelist have been authorized and are qualified to vote. The system verifies a voter's eligibility by comparing their public key with the whitelist when they submit a request to vote.

- **Private Key Authentication:** Voters must use their private key to verify themselves and sign their ballot after their public key has been confirmed. Only the voter can authenticate their identity and validate their voting request since they are the only ones who keep the private key secret.

- **Digital Signatures:** The voter uses their private key to sign the transaction after casting a ballot. The vote has been cast by the legitimate owner of the public-private key combination, as this signature can only be validated with the matching public key.

VI. DESIGN AND IMPLEMENTATION

A. Smart Contract

A smart contract serves as the foundation of the blockchain-based voting mechanism. Decentralized and transparent procedures are made possible by self-executing programs with established rules, or smart contracts. The smart contract in our blockchain voting system makes sure that all voting rules—including casting, validating, and tallying votes—are managed safely and independently. Additionally, it automates the pronouncement of the final result and the counting of votes.

➢ *Control Whitelist*

A whitelist option has been added to limit who may use the system and vote. Participants have to be verified users who have received prior approval. In terms of the Indian voting system, the whitelist is made up of verified voters who registered by providing their voter ID in the form of wallet address and constituency which is provided by the government. The smart contract validates the whitelist before allowing any user to cast a ballot, ensuring that only approved voters may do so.

➢ *Constituencies*

The blockchain system must be connected with the constituency-based voting method used in India. Using their Voter ID, a smart contract will map every voter to the appropriate constituency. Voters are limited to seeing and selecting candidates inside their own constituency. By banning voters from casting ballots in constituencies where they are not registered, this assures localized and fair elections.

➢ *Candidates*

Users will be able to cast ballots for a selection of candidates in each constituency. The candidates' information, including name, party membership, and other details, is stored by the smart contract, which also links each candidate to the appropriate constituency. Only candidates within their constituency may be selected by voters, and efforts to select candidates from beyond their region will be rejected by the system.

➢ *Results*

The results of the vote must be safely saved and made available to the public via the smart contract when it is over. Votes are guaranteed to be transparent and unchangeable thanks to the blockchain. The smart contract counts the votes at the conclusion of the voting time and records the results on the blockchain, where the general public may view them.

B. Dapp (Decentralized Application)

An application developed for a decentralized network, such as a blockchain, that is intended to operate independently of a central authority is known as Decentralized Application. Voting procedures are guaranteed to be safe, transparent, and impenetrable by Dapp.

➢ *Owner/Admin Role:*

To handle high-level features of the voting system, such adding candidates and constituencies or initiating and ending the voting process, an owner or administrator is required. The administrator is also in charge of making sure the smart contracts function as planned and maintaining the system's security.

➢ *Dapp Owner Panel:*

The system administrator is the intended user of a Dapp (Decentralized Application) owner panel. Using this panel, the administrator may oversee every facet of the election procedure, such as monitoring voter turnout percentages and guaranteeing the system's general integrity.

➢ *Vote Page:*

Registered voters may log in, browse the candidates running for office in their district, and cast their ballots on the vote page, which is the user-facing portion of the Dapp. Votes are immediately stored on the blockchain and real-time voting is ensured by the vote page's connection to the smart contract.

➢ *Basic Structure:*

The blockchain voting system will have a layered structure, providing safe and smooth functionality:

➢ *Login Via Wallet:*

Voters access the system with a cryptocurrency wallet (like MetaMask). By acting as a decentralized identity provider and doing away with conventional usernames and passwords, the wallet improves security.

VII. INDIAN DEMOGRAPHICS

India now consists of 28 states. Currently, the nation is home to 1.21 billion people. With 19.96 crore people living there, Uttar Pradesh is the most populous state in India, according to the State Census 2011. With 60, 7688 people, Sikkim is the state with the fewest population in the nation. [6]

Table 1 List of state and UT's by population (According to 2011 Census) [6]

State/UT	Population
Uttar Pradesh	199812341
Maharashtra	112374333
Bihar	104099452
West Bengal	91276115
Madhya Pradesh	72626809
Tamil Nadu	72147030
Rajasthan	68548437
Karnataka	61095297
Gujarat	60439692
Andhra Pradesh	49386799
Odisha	41974218
Telangana	35193978
Kerala	33406061
Jharkhand	32988134
Assam	31205576
Punjab	27743338
Chhattisgarh	25545198
Haryana	25351462
Delhi (UT)	16787941
Jammu and Kashmir	12541302
Uttarakhand	10086292
Himachal Pradesh	6864602
Tripura	3673917
Meghalaya	2966889
Manipur	2855794
Nagaland	1978502
Goa	1458545
Arunachal Pradesh	1383727
Puducherry (UT)	1247953
Mizoram	1097206
Chandigarh (UT)	1055450
Sikkim	610577
Andaman and Nicobar Islands (UT)	380581
Dadra and Nagar Haveli (UT)	343709
Daman and Diu (UT)	243247
Lakshadweep (UT)	64473
Total (India)	1210854977

Table 2 List of state and UT's by Constituency [7]

State/Union Territory	Seats
Andaman and Nicobar Islands	1
Andhra Pradesh	25
Arunachal Pradesh	2
Assam	14
Bihar	40
Chandigarh	1
Chhattisgarh	11

Dadra and Nagar Haveli and Daman and Diu	2
Delhi	7
Goa	2
Gujarat	26
Haryana	10
Himachal Pradesh	4
Jammu and Kashmir	5
Jharkhand	14
Karnataka	28
Kerala	20
Ladakh	1
Lakshadweep	1
Madhya Pradesh	29
Maharashtra	48
Manipur	2
Meghalaya	2
Mizoram	1
Nagaland	1
Odisha	21
Puducherry	1
Punjab	13
Rajasthan	25
Sikkim	1
Tamil Nadu	39
Telangana	17
Tripura	2
Uttar Pradesh	80
Uttarakhand	5
West Bengal	42
Total	543

Table 3 States divided into groups based on constituency and Population

State	**Seats**	**Population**
Group 1		
Uttar Pradesh	80	19,98,12,341
Uttarakhand	5	1,00,86,292
Himachal Pradesh	4	68,64,602
Total	**89**	**21,67,63,235**
Group 2		
Maharashtra	48	11,23,74,333
Madhya Pradesh	29	7,26,26,809
Goa	2	14,58,545
Dadra &Nagar Haveli & Daman and Diu	2	5,86,956
Total	**81**	**18,70,46,643**
Group 3		
West Bengal	42	9,12,76,115
Odisha	21	4,19,74,218
Bihar	40	10,40,99,452
Total	**103**	**23,73,49,785**
Group 4		
Tamil Nadu	39	7,21,47,030
Telangana	17	3,51,93,978
Chhattisgarh	11	25545198
Kerala	20	3,34,06,061
Lakshadweep	1	64473
Sikkim	1	610577

Jammu and Kashmir	5	12541302
Puducherry	1	12,47,953
Total	**95**	**18,07,56,572**
Group 5		
Karnataka	28	6,10,95,297
Gujarat	26	6,04,39,692
Delhi	7	1,67,87,941
Ladakh	1	0
Rajasthan	25	6,85,48,437
Total	**87**	**20,68,71,367**
Group 6		
Punjab	13	2,77,43,338
Haryana	10	2,53,51,462
Assam	14	3,12,05,576
Jharkhand	14	3,29,88,134
Manipur	2	28,55,794
Tripura	2	36,73,917
Meghalaya	2	29,66,889
Nagaland	1	19,78,502
Arunachal Pradesh	2	13,83,727
Mizoram	1	10,97,206
Andaman & Nicobar	1	3,80,581
Andhra Pradesh	25	49386799
Chandigarh	1	10,55,450
Total	**88**	**18,20,67,375**

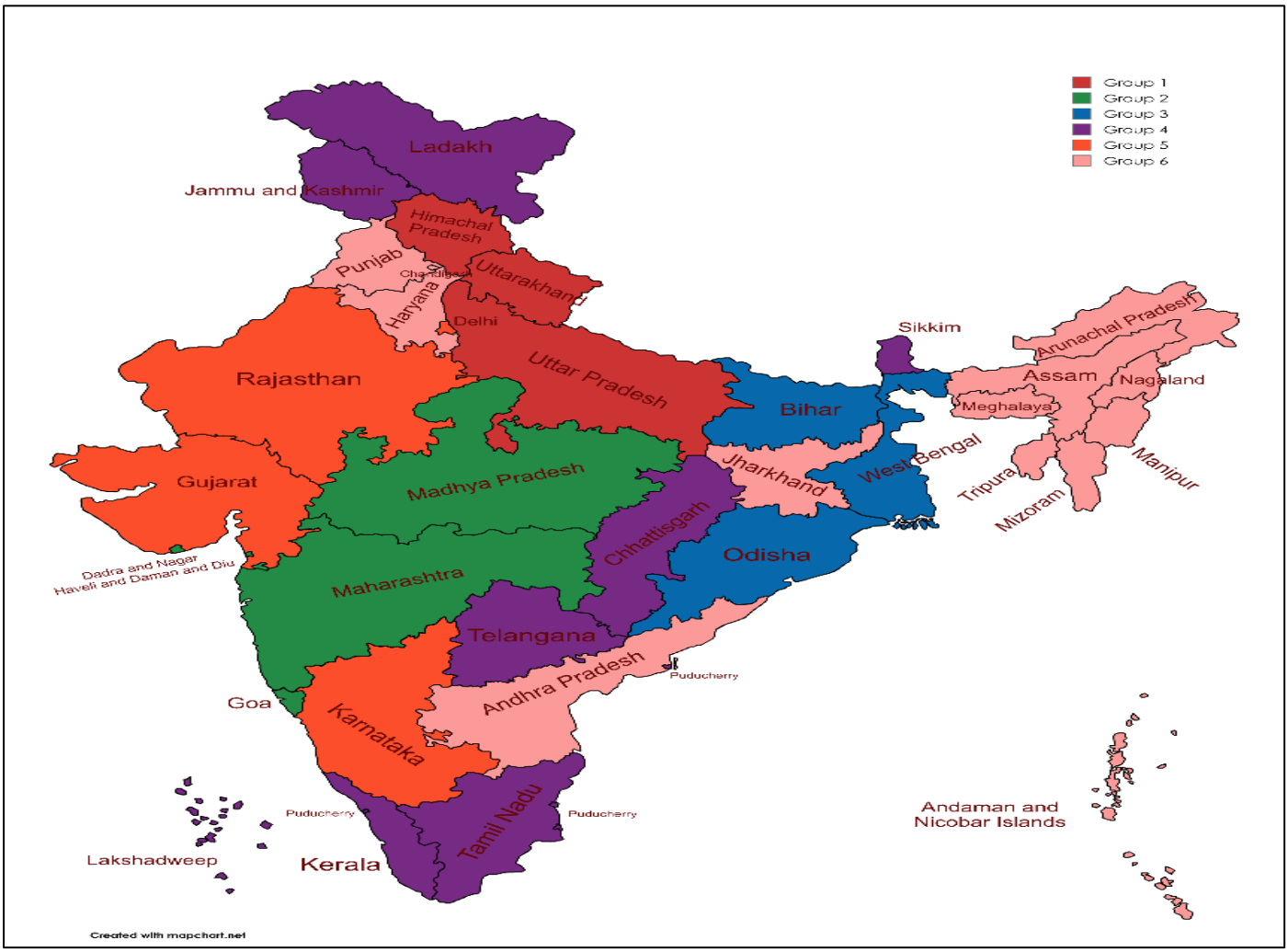

Fig 3 Indian Map based on our Voting System

Elections will be held in six groups, each with a 12-hour voting session, in order to facilitate smooth and well-organized electoral procedures. The following explains how this arrangement helps the election:

➢ *Similar Seats and Population-Balanced Groups:*
The groups have been organized in a way that makes each group's population and number of seats comparable. This makes it easier to handle logistics by guaranteeing that each group has a controllable voting population.

➢ *Effective Administration:*
Election officials may more efficiently distribute resources, including polling places and staff, across the groupings if they have comparable seat counts and demographics.

➢ *12-Hour Voting Period*

- *Time Management:*
The election process is concentrated and well-organized since each group has a 12-hour window in which to cast a ballot. This reduces the possibility of misunderstanding and promotes order.

- *Voter Convenience:*
Voters may organize their participation within a certain time range, which makes it simpler to meet varying schedules and obligations.

➢ *Overall Advantages*

- *Streamlined Procedure:*
The election process is made more efficient by assigning distinct voting periods and combining states with comparable populations. This lowers the likelihood of logistical problems.

- *Fair Representation:*
This technique promotes a fair election environment by ensuring that all organizations receive equal attention and resources.

All things considered, this systematic method makes the election run more smoothly while guaranteeing that every voter gets the chance to take part in a meaningful way.

VIII. CONLCUSION

By addressing major issues with conventional election procedures, the suggested blockchain-based voting system offers notable advancements in terms of security, transparency, scalability, and affordability. The system makes sure that only qualified voters may cast ballots, eliminating fraud and manipulation, by using cryptographic wallets for voter authentication, smart contracts for vote management, and decentralized applications (D-apps) for safe and immutable vote recording. Voter identification is secured by the use of public-private key encryption, and transparency is ensured by the decentralized architecture of the system, which also removes single points of failure.

Specifically designed for the intricate and densely populated Indian electoral system, the architecture enables effective remote voting, decreasing the requirement for actual polling places and increasing voter participation.

Election procedures are made more efficient and well-organized by include elements like real-time updates, dynamic scalability, and a phased voting process by state groupings. This system, which makes use of blockchain technology, aims to improve democratic processes by offering a scalable, safe, and reasonably priced option for contemporary elections.

REFERENCES

[1]. B. Shahzad and J. Crowcroft, ‘‘Trustworthy electronic voting using adjusted blockchain technology,’’ IEEE Access, vol. 7, pp. 24477–24488, 2019
[2]. F. P. Hjálmarsson, G. K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson, ‘‘Blockchain-based E-Voting system,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 983–986.
[3]. U. Can Cabuk, E. Adiguzel, and E. Karaarslan, ‘‘A survey on feasibility and suitability of blockchain techniques for the E-voting systems,’’ 2020
[4]. I. Abraham, G. Gueta, D. Malkhi, L. Alvisi, R. Kotla, and J.-P. Martin, ‘‘Revisiting fast practical byzantine fault tolerance,’’ 2017
[5]. C. Cachin and M. Vukolić, ‘‘Blockchain consensus protocols in the wild,’’ 2017
[6]. "List of states with Population, Sex Ratio and Literacy Census 2011". *www.census2011.co.in*
[7]. ”https://www.mea.gov.in/Uploads/PublicationDocs/19167_State_wise_seats_in_Lok_Sabha_18-03-2009.pd"