# CRYPTOGRAPHY (BITS F463)
## Term Project

# DECENTRALIZED DIGITAL VOTING PLATFORM

| | |
|---|---|
| PRAKHAR AGARWAL | 2019A7PS0174H |
| VEDANSH SRIVASTAVA | 2019A7PS0323H |

# Problem Statement

## Traditional Voting Systems:

### 1) Ballot Paper:

A ballot paper is a form which voters fill out in order to exercise their right to vote. Ballot papers list the candidates running for an election and the voter can mark their preferences accordingly. Ballot papers can be considered official documents.

Issues associated with ballot papers

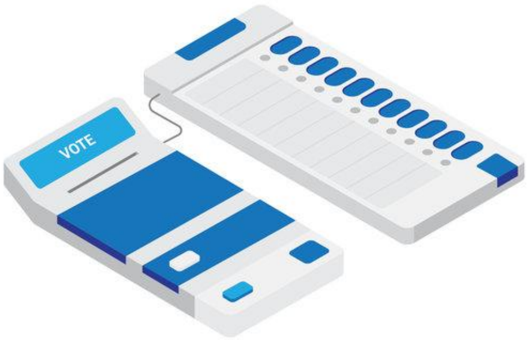
- Unauthorized additional ballots are being introduced into the ballot box;
- Ballots were removed from the voting station for marking outside, then brought back into the voting station by other voters to deposit in the ballot box;
- The ballots being issued by voting station officials are not those officially printed or authorized;
- Ballots are being handled by unauthorized persons during voting;
- Unauthorized assistance is being provided to voters in marking their ballots.

### 2) Electronic Voting Machine (EVM):

Electronic Voting Machine (also known as EVM) is voting using electronic means to either aid or take care of the chores of casting and counting votes.

Issues associated with Electronic Voting Machines

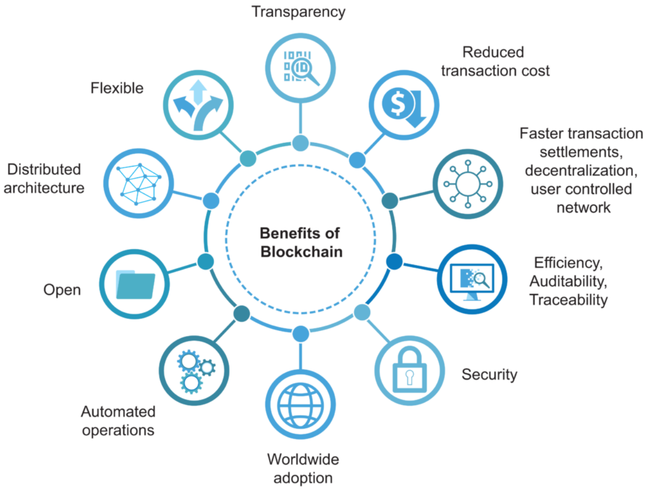
- Vulnerable to malicious programming and can be hacked.
- Most EVMs do not have any mechanism by which the voter can verify their identity before casting the vote due to which fake voters can cast numerous fake votes.
- EVMs can be tampered during manufacturing.
- Susceptible to damage which can result in loss of data.



# BLOCKCHAIN AS A SOLUTION

## Perks of implementing blockchain technology

A blockchain is a distributed ledger that holds information in the form of blocks of varying sizes. The block is closed and linked to the previous block when it is full, producing a chain of data blocks. Without the need of a third party, blockchain ensures that data is accurate and secure. There is no single point of failure in blockchain technology because it is decentralized. Due to encryption and decentralization, each record is verifiable and incorruptible.



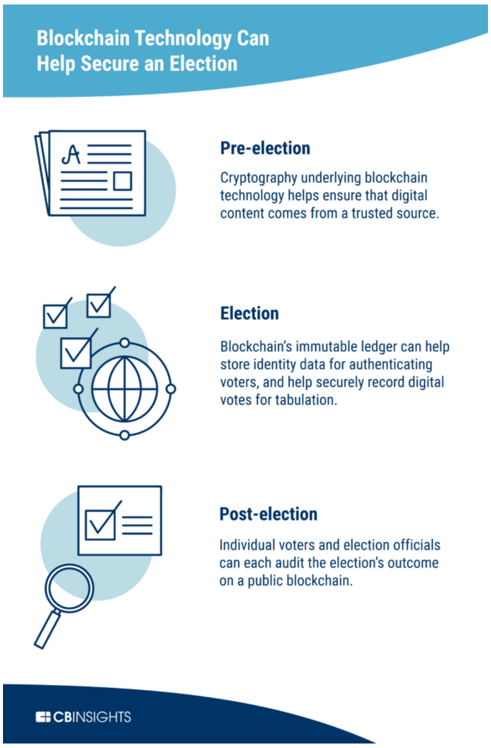
## Using blockchain for developing an e-voting platform

□ Users will login using their phone numbers. On the initial login, they receive a private key for future voting activity.

□ On a successful login, users will be redirected to a dashboard where they can access the voting zone i.e. a list of all candidates to whom a user can vote.

□ While casting a vote, users authenticate themselves using the private key which they received in their initial login activity.

□ Their vote is logged into an immutable blockchain and used to reliably verify the outcome of the election. There is no possibility of any sort of manipulation, recording errors or tampering taking place.



Blockchain Technology Can Help Secure an Election

**Pre-election**

Cryptography underlying blockchain technology helps ensure that digital content comes from a trusted source.

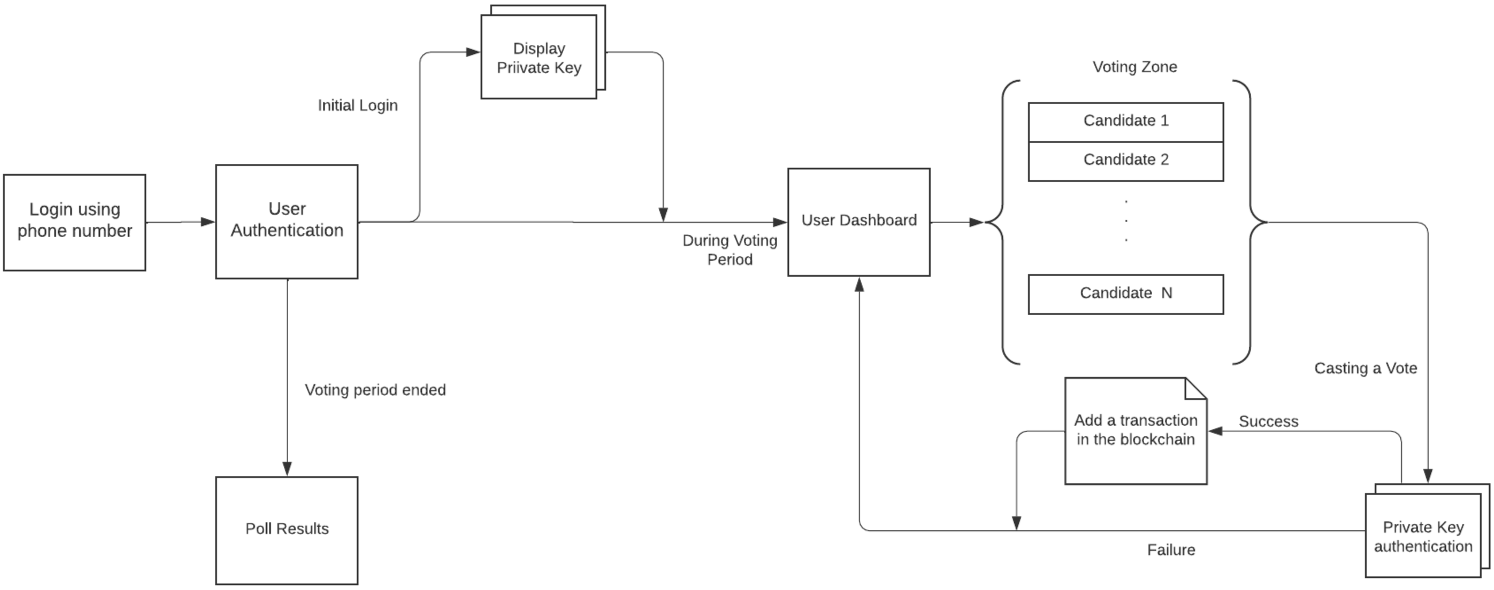
**Election**

Blockchain's immutable ledger can help store identity data for authenticating voters, and help securely record digital votes for tabulation.

**Post-election**

Individual voters and election officials can each audit the election's outcome on a public blockchain.

## Web-application Flowchart



## Implementation of Zero-Knowledge Proofs

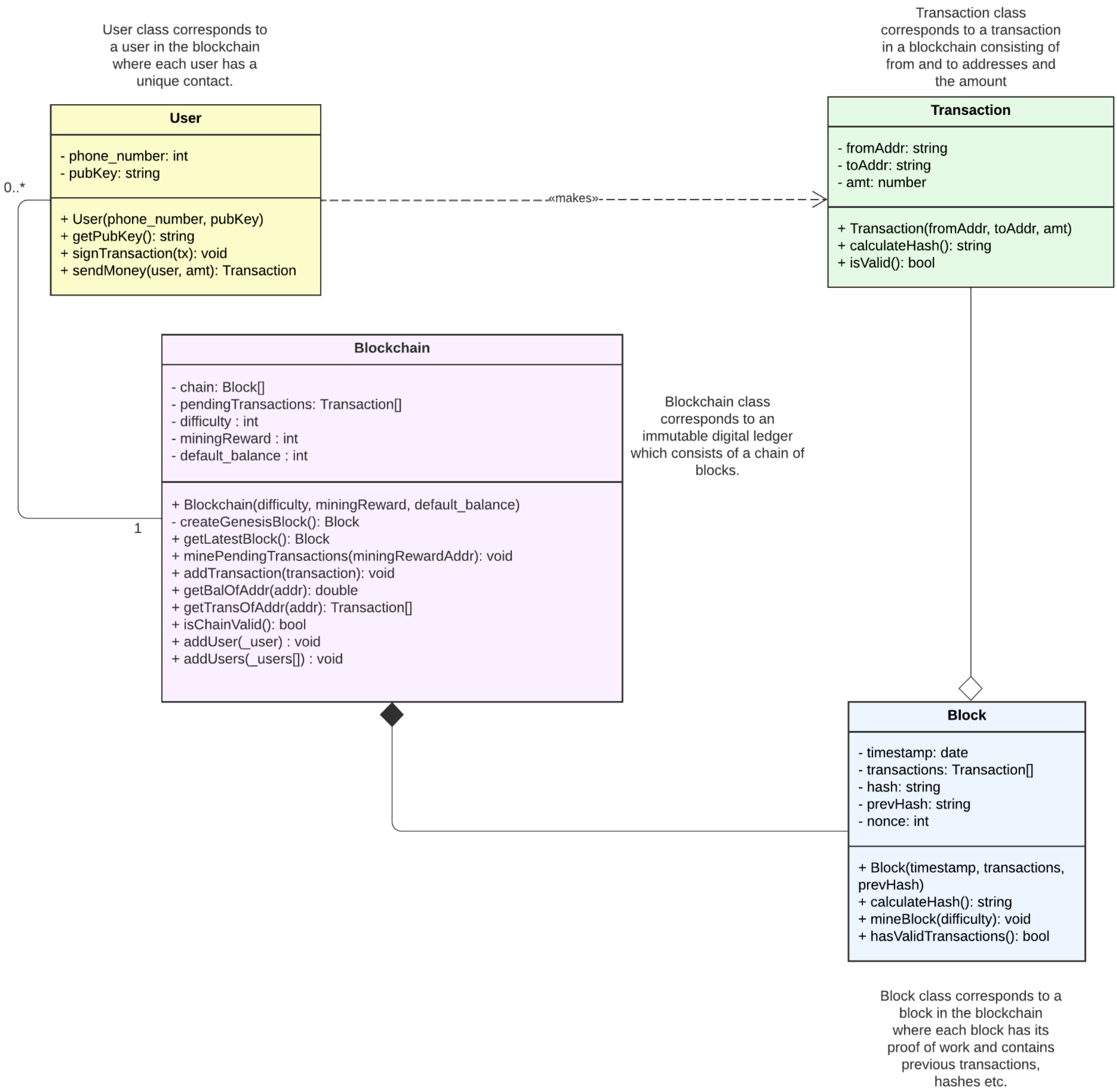
A cryptographic procedure that allows a party to confirm ownership of information without exposing it is known as zero knowledge proof.

B
Bob does not know what path Alice took inside the cave, but randomly chooses a path to ask Alice to take back to the entrance. This process repeats multiple times.
B
A
Alice selected a path randomly within the cave to get to the passcode locked door

In our scenario, each user has a private key that is confidential and that he does not wish to share. However, the private key is required for signing the transaction.

As a result, we may utilize ZKPs to validate the user's private key without requiring the user to reveal it.

# UML DIAGRAM FOR OUR APPLICATION



User class corresponds to a user in the blockchain where each user has a unique contact.

**User**

- phone_number: int
- pubKey: string

+ User(phone_number, pubKey)
+ getPubKey(): string
+ signTransaction(tx): void
+ sendMoney(user, amt): Transaction

Transaction class corresponds to a transaction in a blockchain consisting of from and to addresses and the amount

**Transaction**

- fromAddr: string
- toAddr: string
- amt: number

+ Transaction(fromAddr, toAddr, amt)
+ calculateHash(): string
+ isValid(): bool

**Blockchain**

- chain: Block[]
- pendingTransactions: Transaction[]
- difficulty : int
- miningReward : int
- default_balance : int

+ Blockchain(difficulty, miningReward, default_balance)
- createGenesisBlock(): Block
+ getLatestBlock(): Block
+ minePendingTransactions(miningRewardAddr): void
+ addTransaction(transaction): void
+ getBalOfAddr(addr): double
+ getTransOfAddr(addr): Transaction[]
+ isChainValid(): bool
+ addUser(_user) : void
+ addUsers(_users[]) : void

Blockchain class corresponds to an immutable digital ledger which consists of a chain of blocks.

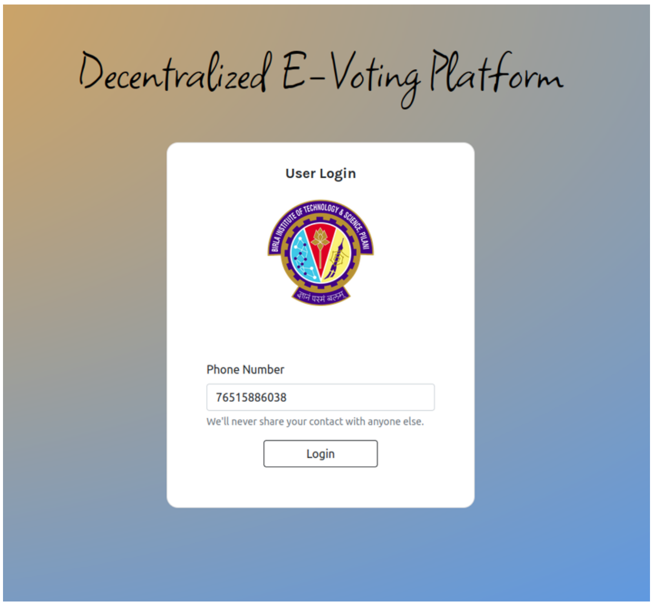
**Block**

- timestamp: date
- transactions: Transaction[]
- hash: string
- prevHash: string
- nonce: int

+ Block(timestamp, transactions, prevHash)
+ calculateHash(): string
+ mineBlock(difficulty): void
+ hasValidTransactions(): bool

Block class corresponds to a block in the blockchain where each block has its proof of work and contains previous transactions, hashes etc.

## Screenshots of Working Application



Decentralized E-Voting Platform

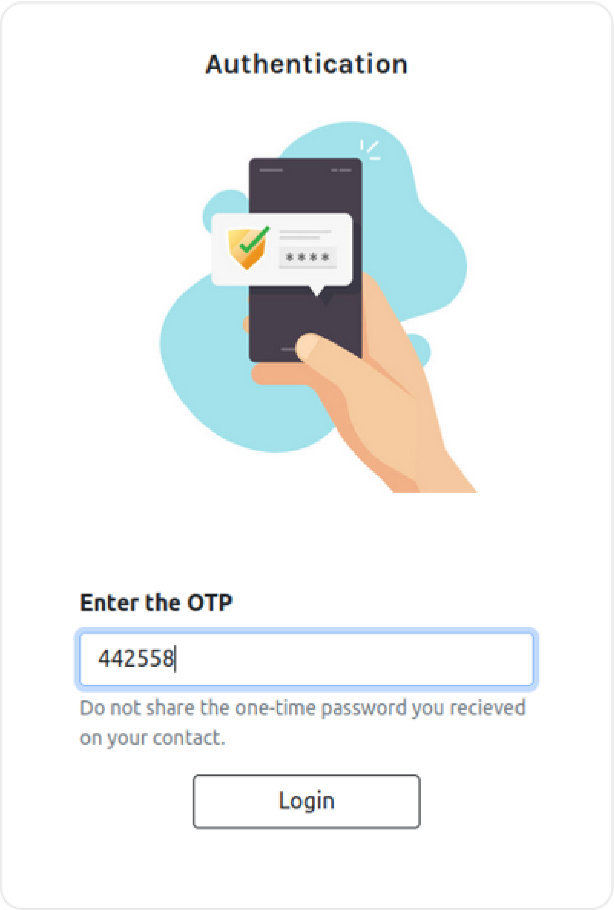
User Login

Phone Number

76515886038

We'll never share your contact with anyone else.

Contact Verification

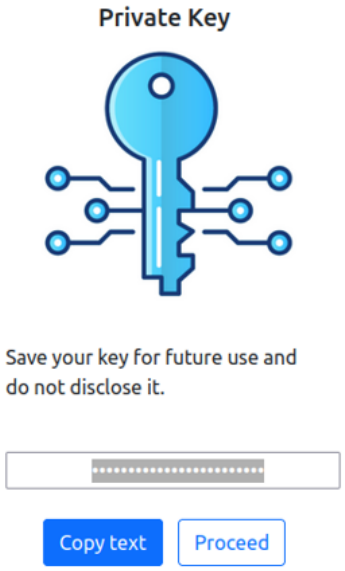


Authentication

Enter the OTP

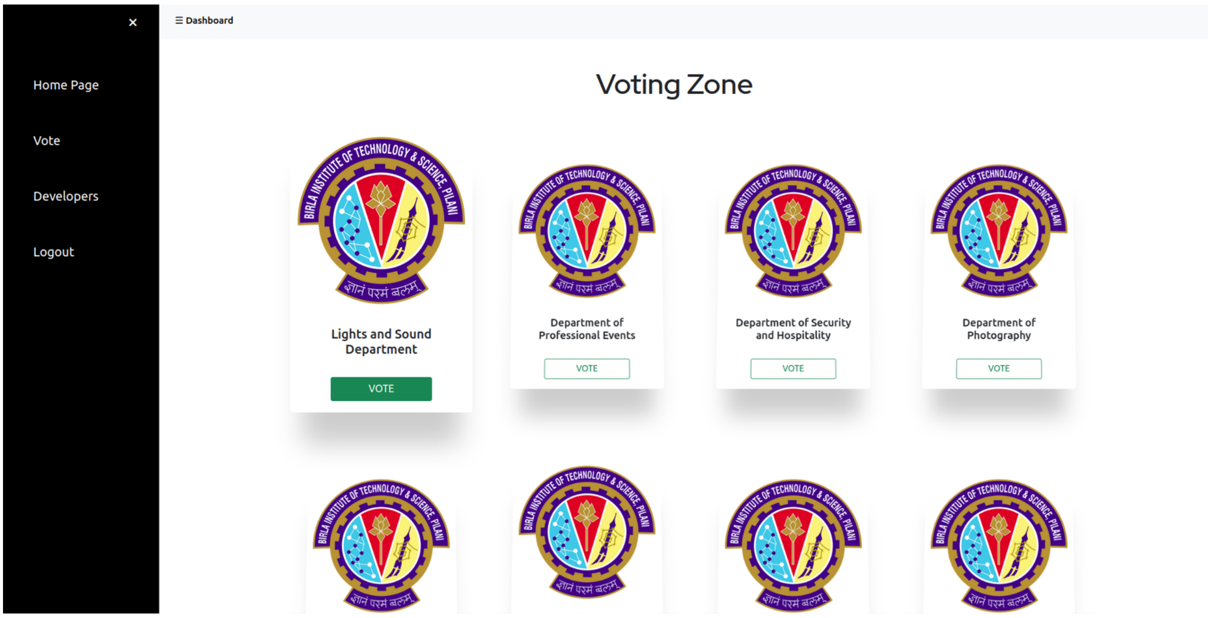
442558

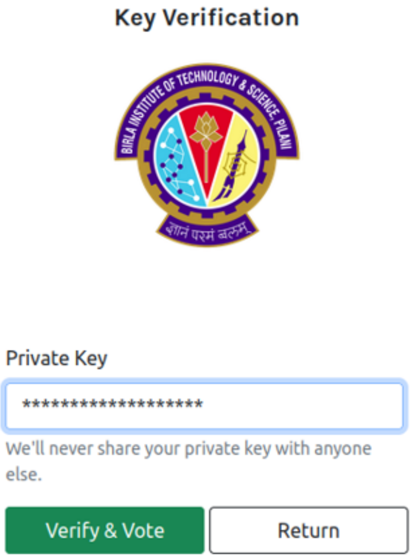
Do not share the one-time password you recieved on your contact.



Private Key

Save your key for future use and do not disclose it.


×
☰ Dashboard
Home Page
Vote
Developers
Logout
Voting Zone
Lights and Sound Department
VOTE
Department of Professional Events
VOTE
Department of Security and Hospitality
VOTE
Department of Photography
VOTE



We'll never share your private key with anyone else.

Thankyou for Voting !