IBM Block Chain – Vote now App

Concept and Setup

Concept:

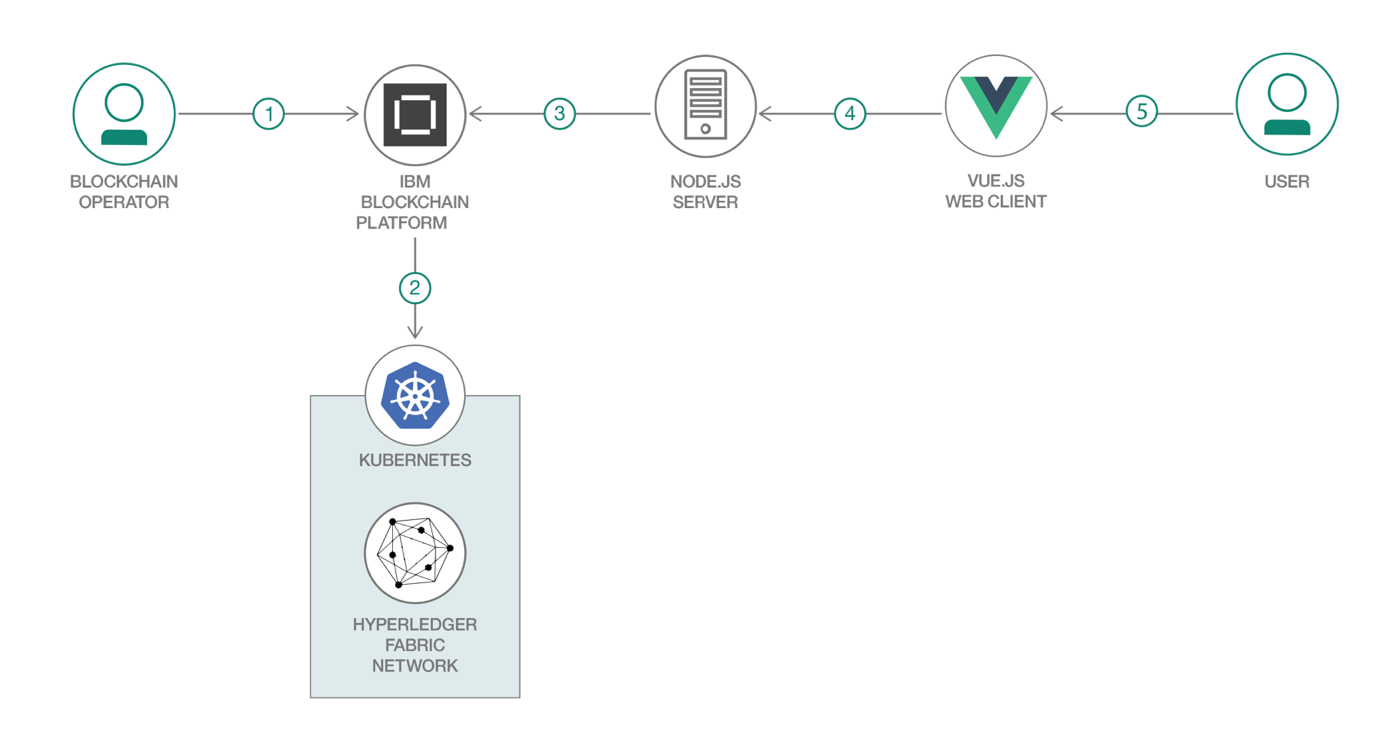
* IBM Block chain will be used to register a user when a user is successfully authenticated with Aadhaar API authentication.
* During above transaction we create a private and public key for the voter with our Block chain certificate authority that is running on the IBM cloud, and add those keys to the wallet.
* Block chain will be used to then record each casting of vote from user as a transaction on Block record.
* If the same user is tried to vote a cast again then an error will be thrown based on the transaction which has the key details. A block record transaction is immutable. Each transaction that is submitted to the ordering service must have a signature from a valid public-private key pair, we can trace back each transaction to a registered voter of the application, in the case of an audit.
* A dynamic report can be shown showing the results of Voting for various parties by setting up query on couch DB.
* IBM Block chain Hyperledger Fabric network provides confidentiality, resiliency, flexibility, and scalability.

Overall Architecture

Diagram

Description automatically generated

Flow diagram:



1. The blockchain operator sets up the IBM Blockchain Platform 2.5 service.
2. The IBM Blockchain Platform 2.5 creates a Hyperledger Fabric network on an IBM Kubernetes Service, and the operator installs and instantiates the smart contract on the network.
3. The Node.js application server uses the Fabric SDK to interact with the deployed network on IBM Blockchain Platform 2.5 and creates APIs for a web client.
4. The Vue.js client uses the Node.js application API to interact with the network.
5. The user interacts with the Vue.js web interface to cast their ballot and query the CouchDB to see current poll standings.

Key Steps to setup IBM Block chain and its Integration with client app – Vote now app.

1. Login into IBM cloud account and spin up Kubernetes cluster service.
2. Deploy IBM Blockchain platform service on cluster.

Graphical user interface, application, Teams

Description automatically generated

Diagram

Description automatically generated

* Nodes
* Channel
* Organizations
* Smart contracts

Building network in IBM Blockchain platform service:

1. Create Voter CA (Certificate Authority - Node) and below are its users
   1. Add certificate authority with credentials and admin type client and associate it to Voter CA.
   2. Create Voter admin type admin and associate/register the user to Voter CA.
   3. Create peerVote type peer and associate/register the user to Voter CA.
2. Create Organization – Voter MSP
   1. Create MSP definition Voter MSP and specify Voter CA as Root certificate authority.
   2. Register Voter admin user as admin of the Voter MSP organization.
   3. Create and register Voter peer for Voter MSP organization which uses user peerVote.
3. Create Orderer CA (Certificate Authority - Node) which orders transactions and below are its users
   1. Add certificate authority with credentials admin type client and associate it to Orderer CA.
   2. Register admin for Orderer CA - Create Ordereradmin type admin and associate/register the user to Orderer CA.
   3. Repeat above step to Create OrdererVote type orderer and associate it to Orderer CA. Use root affiliation.
4. Create Organization – Orderer MSP
   1. Create MSP definition Orderer MSP and specify Orderer CA as Root certificate authority.
   2. Associate Ordereradmin as admin for organization - Orderer MSP.
5. For Ordering service add a node.
   1. Add Orderer select Orderer CA as certificate authority and ordering service enroll user ordererVote and MSP organization is Orderer MS with Fabrix version as 1.4.7-0.
6. Add Consortium member – Voter MSP (org)
   1. Under Nodes – Voter MSP – Consortium members select Voter MSP as peer organizations “Voter”.
   2. The consortium member is the orderer to transact.
7. Create Channel:
   1. Create VoteNow channel with orderer as Ordering service , organization is Voter MSP as member of this channel.
   2. Policy default to 1 out of 1. Select Channel creator as Voter MSP and identity as Voter Admin.
8. For VoteNow channel go ahead add one of the peers – Voter Peer and make it as anchor peer. There were be 2 block transactions on Block chain service.
9. Add Smart contract –
   * Upload voterContract.cds created through Visual studio with IBM Block chain extension.
   * Under **Installed smart contracts**, find the **voterContract** smart contract from the list installed on our peer and click **Instantiate** from the overflow menu on the right side of the row.
   * On the side panel that opens, select the channel Votenow on which to instantiate the smart contract. Click **Next**.
   * Select Voter MSP as the organization member to be included in the endorsement policy. Click **Next**.
   * Skip the **Setup private data collection** step and simply click **Next**.
   * Give the **Function name** as init and leave the **Arguments** blank. **Note: init is the method in the voterContract.js file that initiates the smart contracts on the peer.**
   * Click **Instantiate smart contract**.
10. Establish connection between app and network- Create connections in Voter msp (Organization) peer. Click on download to get Voter MSP connection profile json which establish a connection between the Node.js web application and the Blockchain Network. Below is the content of the json.

Text

Description automatically generated

It has organization, peers and certificates.

1. Register an app user under Voter CA.
   1. Add app admin type client.
   2. Add attribute
      1. hf.Registrar.Roles - \*.
2. In web app server application, under the server folder have ibpConnection.json. Then in config file have below details

Text

Description automatically generated

Under Wallet folder – *app-admin.id* gets created/registered. This has public-private key.

User getting added from web app when Aadhaar authentication is successful -

Register the Voter on Block chain network from app, which will get added to users under Voter CA node as shown below:

A screenshot of a cell phone

Description automatically generated

Web server structure-

Graphical user interface, application, table

Description automatically generated

Casting of Vote-

Cast a Vote after voter authentication and once he votes. The transaction on the channel will get inserted as one block and one transaction on that block record from the web app received by ordering service. Each voter id had a public and private key associated which got recorded in a transaction. Each transaction is immutable.

A screenshot of a video game

Description automatically generated

Results of Voting-

All casting of vote transaction will be in recorded in transactions on Blockchain and its unique for every voter. A report can be generated by querying the CouchDB to show the results for each party. Recounting and tracing back each votes is very easy due to the nature of Block chain.