CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles

Vehicular announcement can help to avoid traffic jams and allow peoples to know any accident or event occur at any route prior of choosing that route but this announcement contains some flaws as user privacy leakage who involved in announcement as their current location and vehicle ID will be exposed to other peoples and they can misuse this location information to kidnap peoples and other flaw is lack of motivation in user to involved themselves to announce that information to other vehicles which are in their range.

To overcome from above problem author of this paper has introduce concept called Blockchain & incentive based privacy preserving announcement in vehicular network. In propose paper is motivating users to announce their location and event or others received data by providing INCENTIVES and to earn incentive all peoples will get involved in announcement and author adding another concept to avoid incentive lock where user incentives will be expired at the end of the day so they may use this incentive to post their new data to new users.

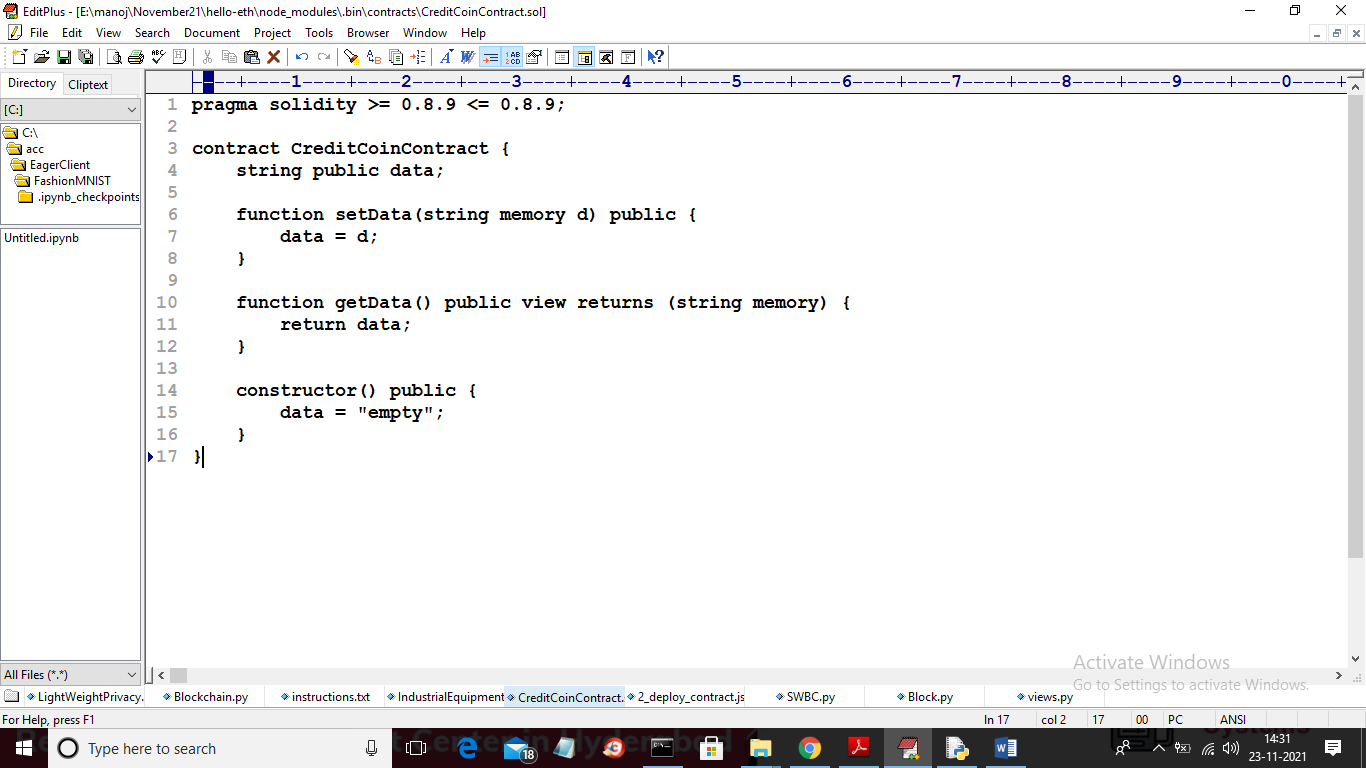
To provide privacy to user author is using symmetric ring signature where all users like INITIATOR who send request and the REPLIERS who reply to initiator requestor will signed to one public, private and secret KEY and then all their ID’s and data will be encrypted using public key and the receiver can decrypt data using their private key.

To prevent attacks author using Blockchain based verification which will store data as Block of chain and each block will be associated with one unique hashcode and before adding any new transaction or Block then Blockchain verify all previous blocks hashcode and if all blocks verification successful then data consider as intact or secured and if not successful then data will be consider as attacked and Blockchain will not allow any block of data to get tamper so Blockchain will provide security to data and by using symmetric encryption user privacy leakage will be avoided.

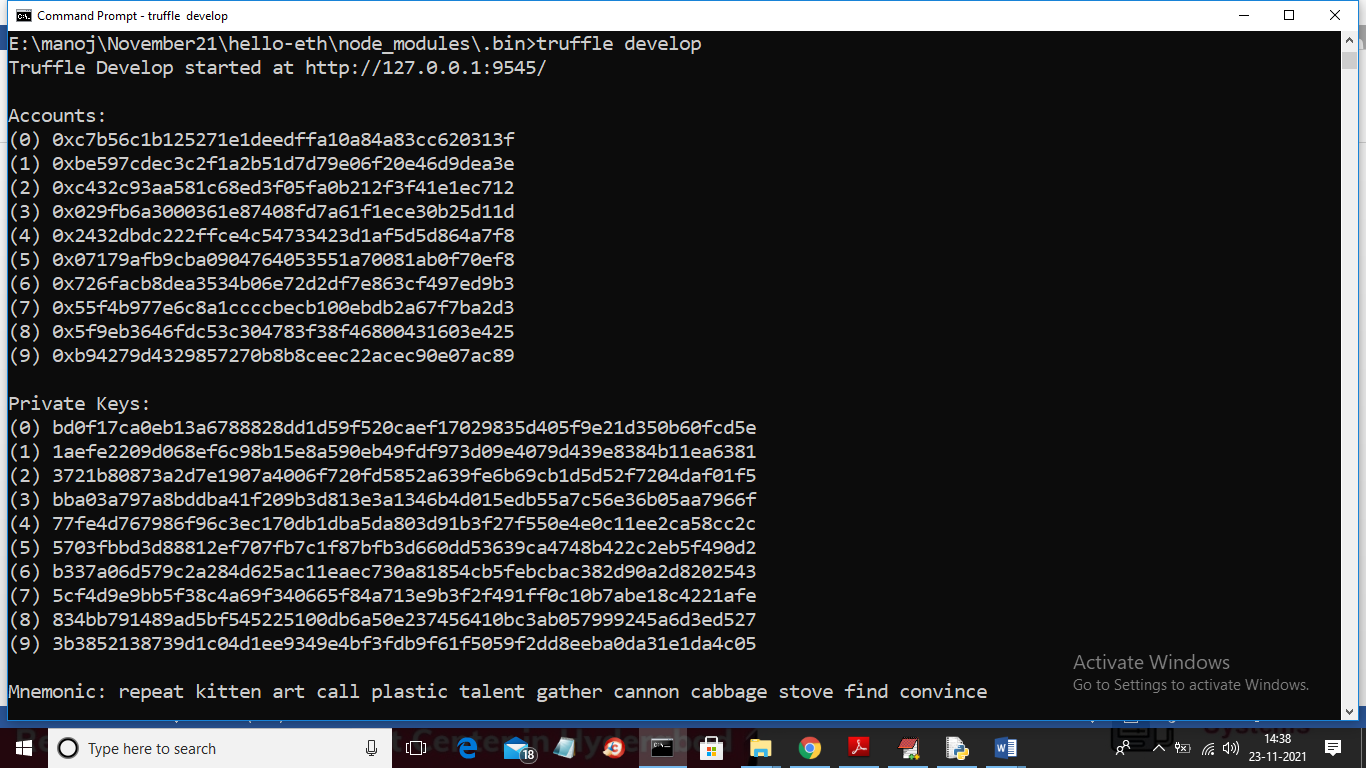
To implement above concept author has designed following modules

1. Role settings: Here we have various users such as Initiator (vehicle which send request), Replier (vehicle which reply to initiator), Trusted authority (responsible for key management), Verifier (Trace Manager which perform verification)
2. Packets settings: based on role Echo Announcement packets will be generated as request or reply
3. Request Packet: sent by initiator to get reply from replier so they must agree on announcement
4. Reply Packet: sent by replier willing to join announcement with requester
5. Announcement Aggregate Packet (AGP): packet sent from requester to verifier from verification
6. Generate Key Trusted Authority: generate and manage key by Trusted Authority
7. Run CreditCoin Simulation: using this module initiator vehicle will send request to nearer repliers and then increment incentives of involving replier. Each request and reply packet will be encrypted to avoid privacy leakage
8. Trace Manager Verification: using this module verifier will read all blocks or packets and then verify their hashcode
9. Computation Time Graph: using this module we will plot request, reply and key generation computation time

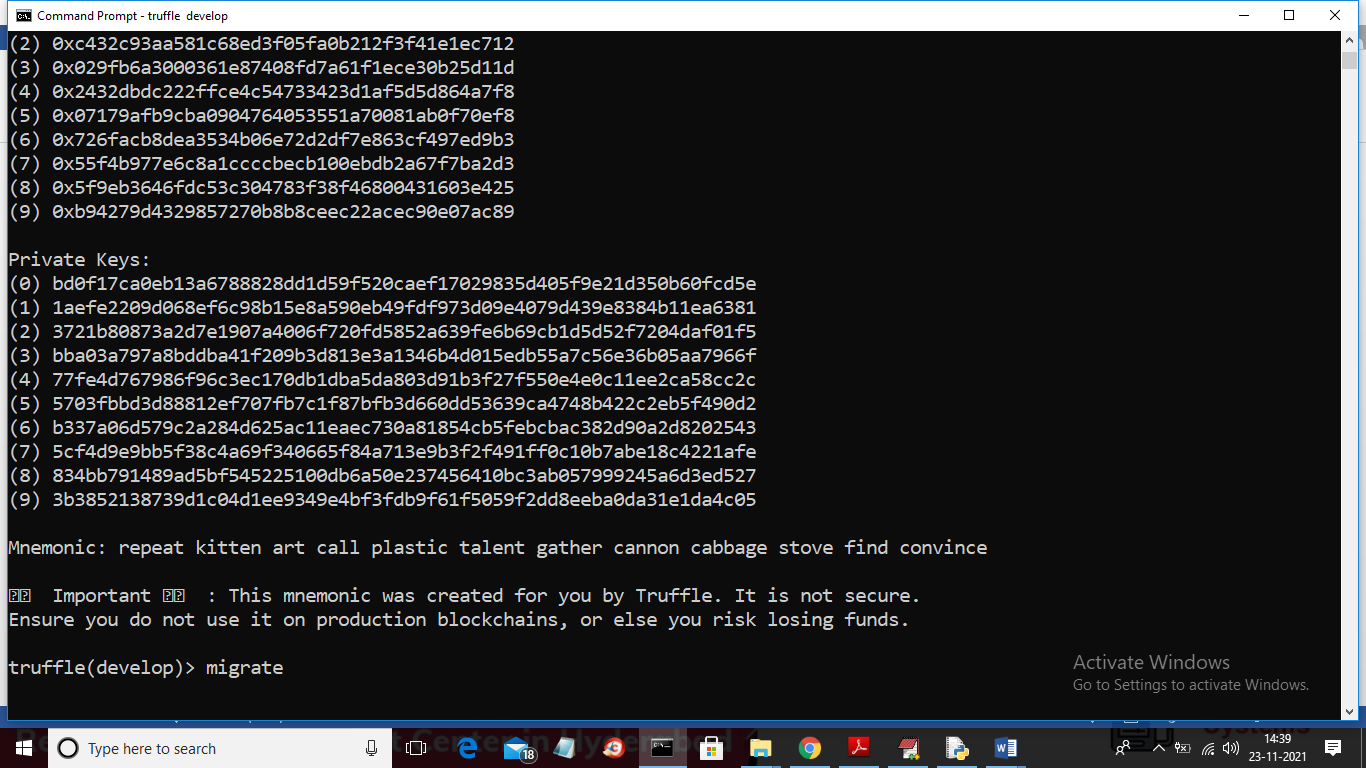
All the packets will be saved in Blockchain using SOLIDITY Contract below code



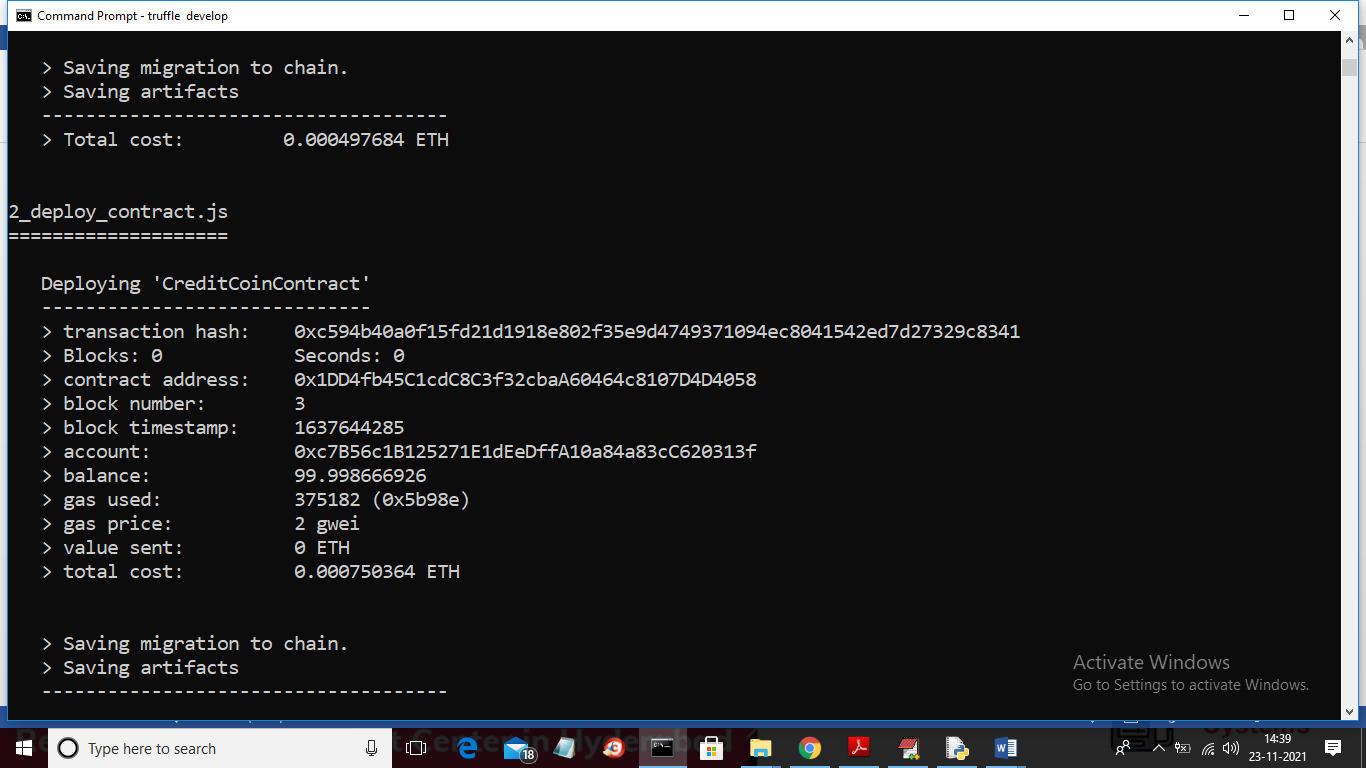
Above solidity function will be deployed and called by Blockchain to store vehicle information. Below are the instructions to deploy and call contract from Blockchain. Now we need to deploy above code to store and access CreditCoin data into Ethereum Tool and to deploy go inside ‘hello-eth\node\_modules\.bin’ folder and in this double click on ‘runBlockchain.bat’ file to get below screen



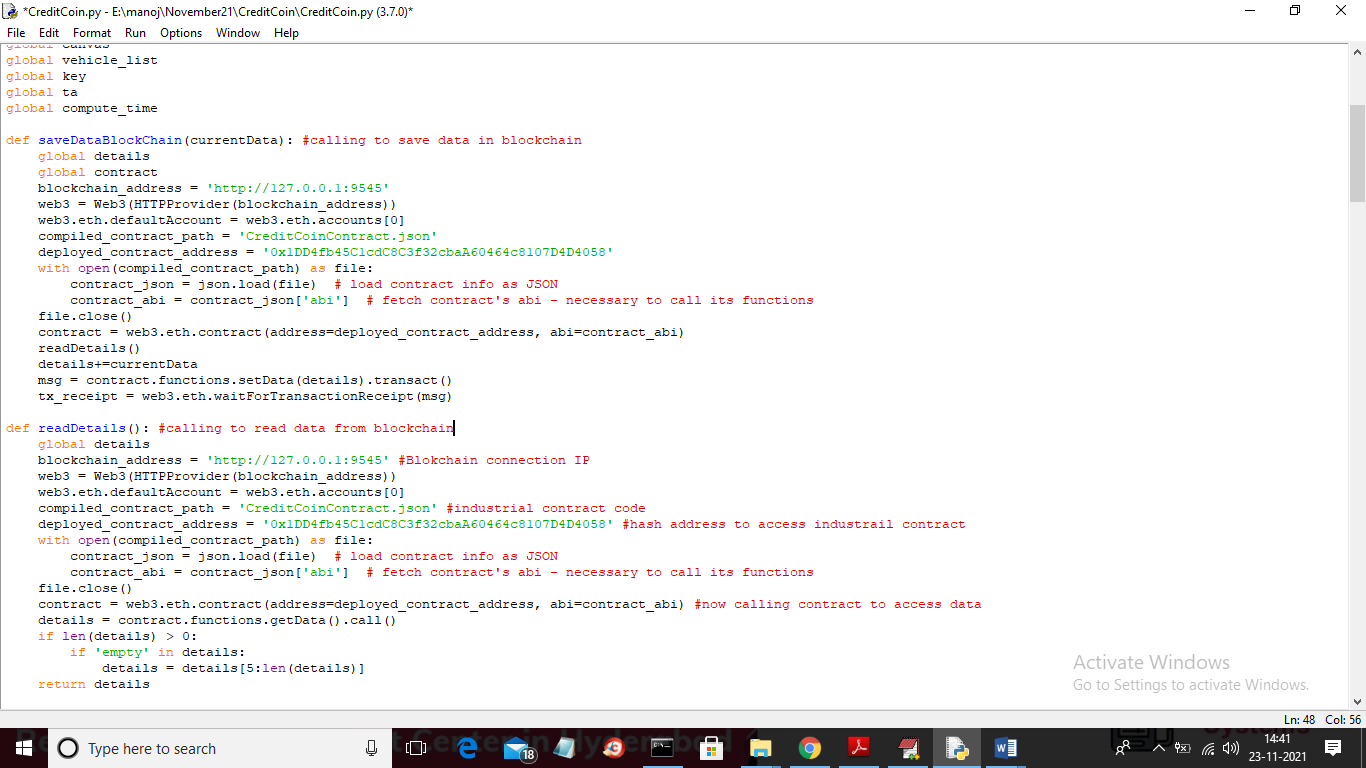
In above screen we can see Blockchain accounts and private keys are generated and now to deploy code type ‘migrate’ and press enter key to deploy code and to get contract access ADDRESS like below screen



After running above command will get below screen



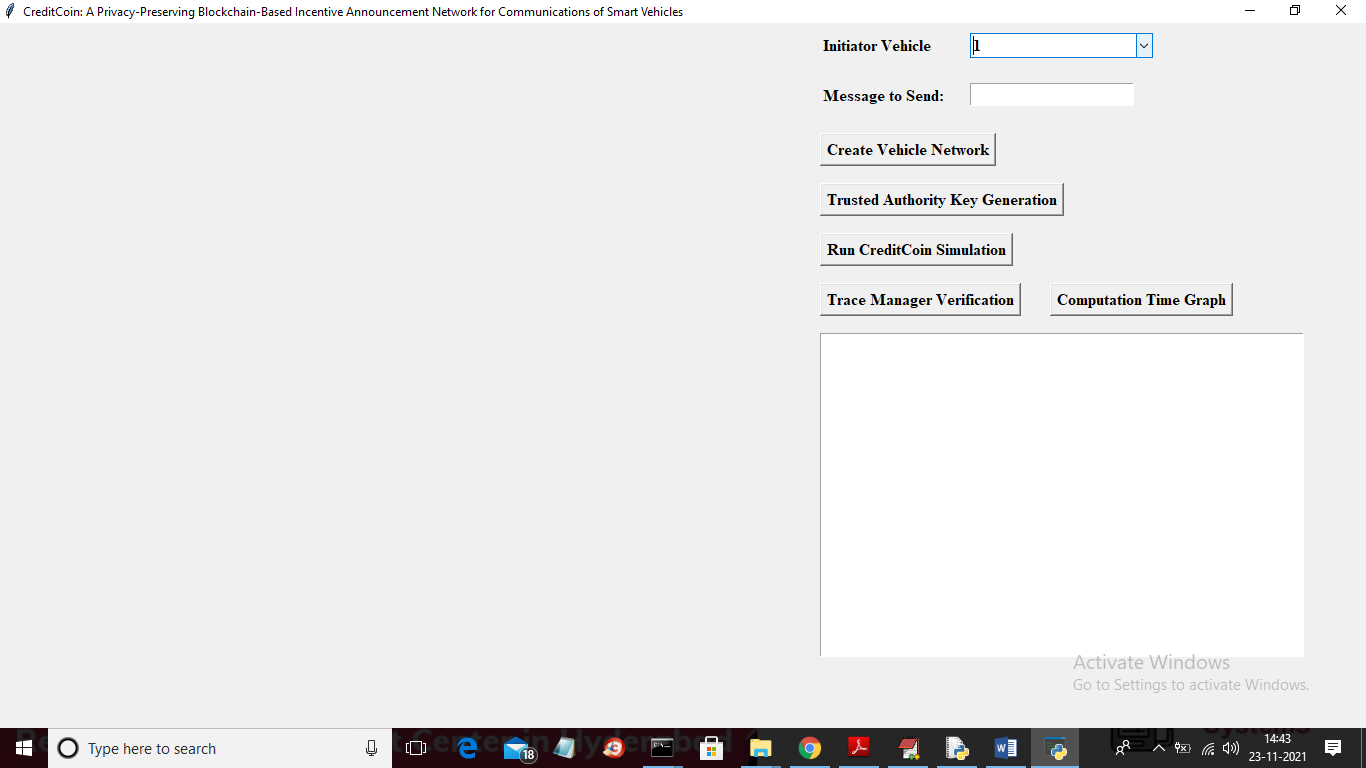
In above screen we can see Credit Coin contract deployed to Blockchain and we can call above code to store all vehicle communication details. In below code will specify above contract address to acess Blockchain



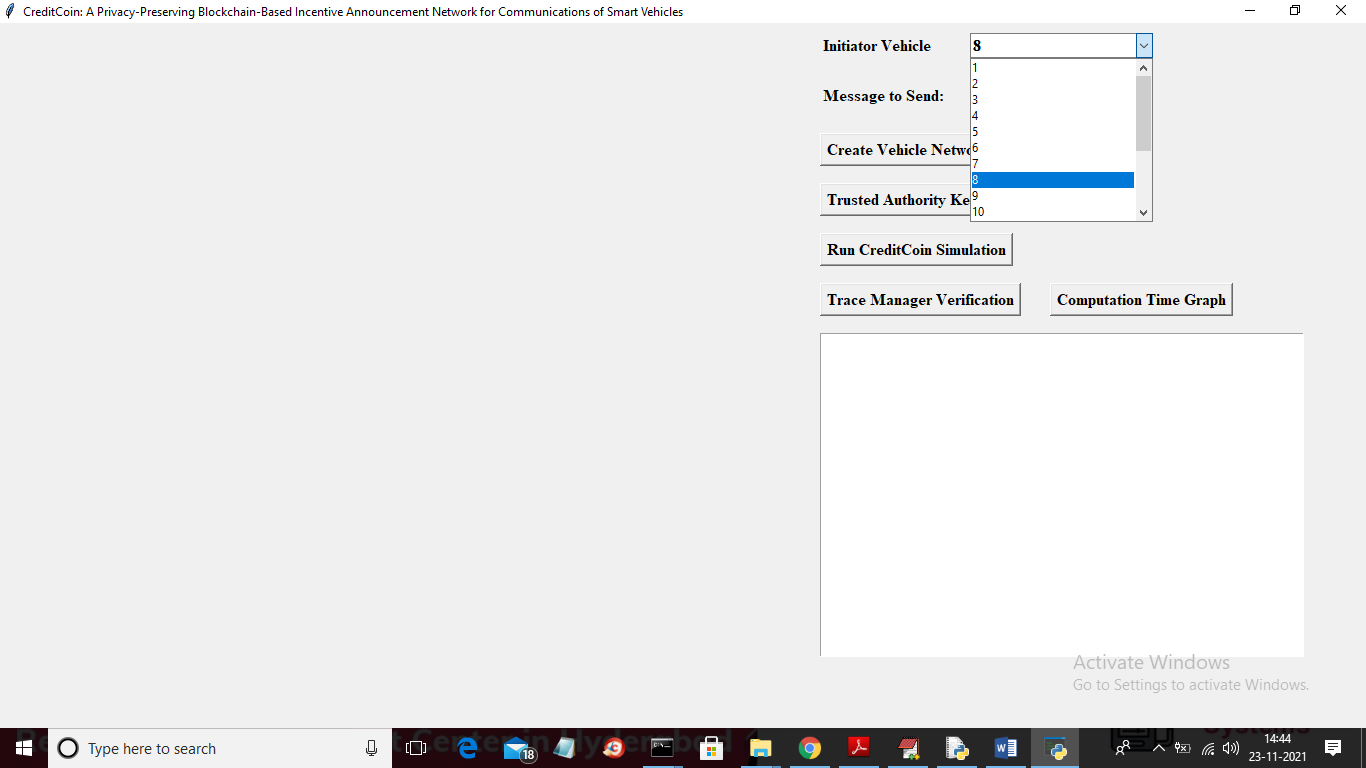
In above screen you can read red colour comments to know how Blockchain is calling to store and read data.

Main application output screens

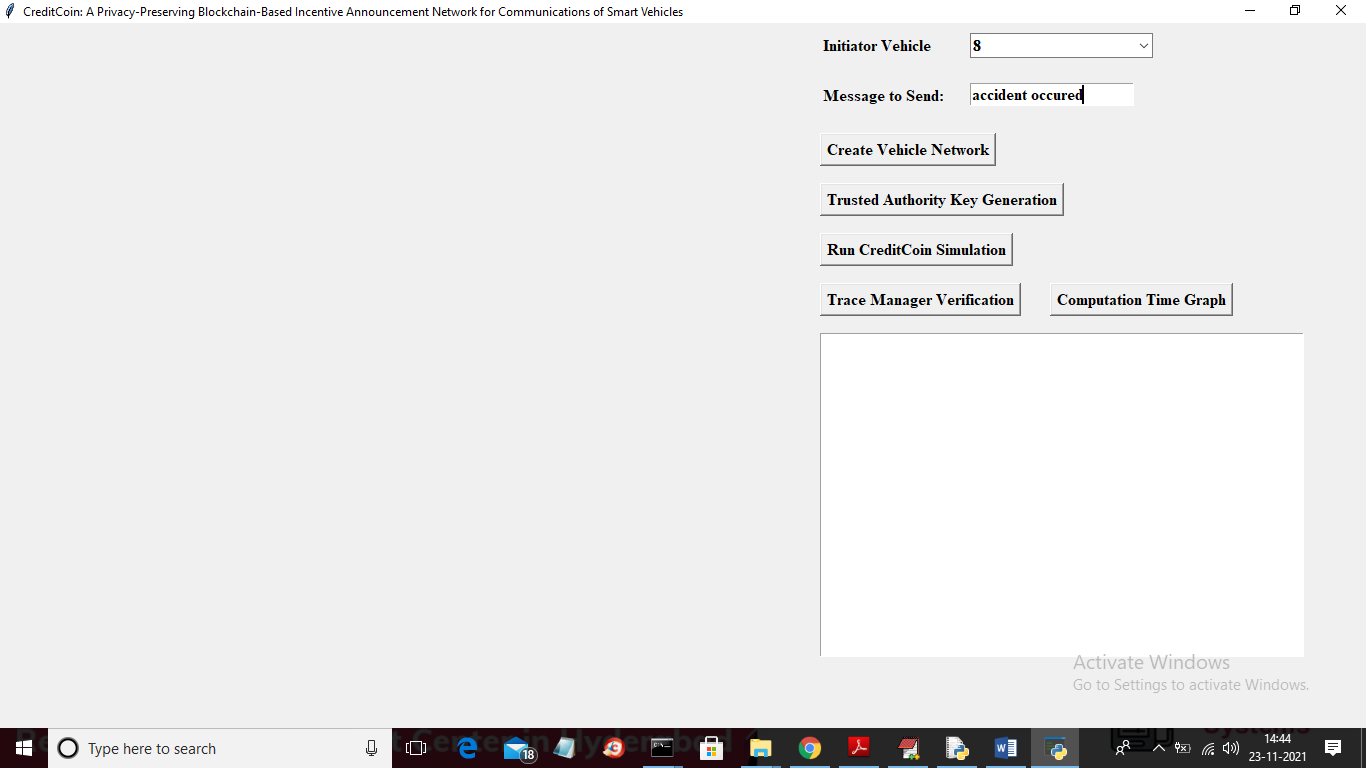
To run project double click on ‘run.bat’ file to get below screen



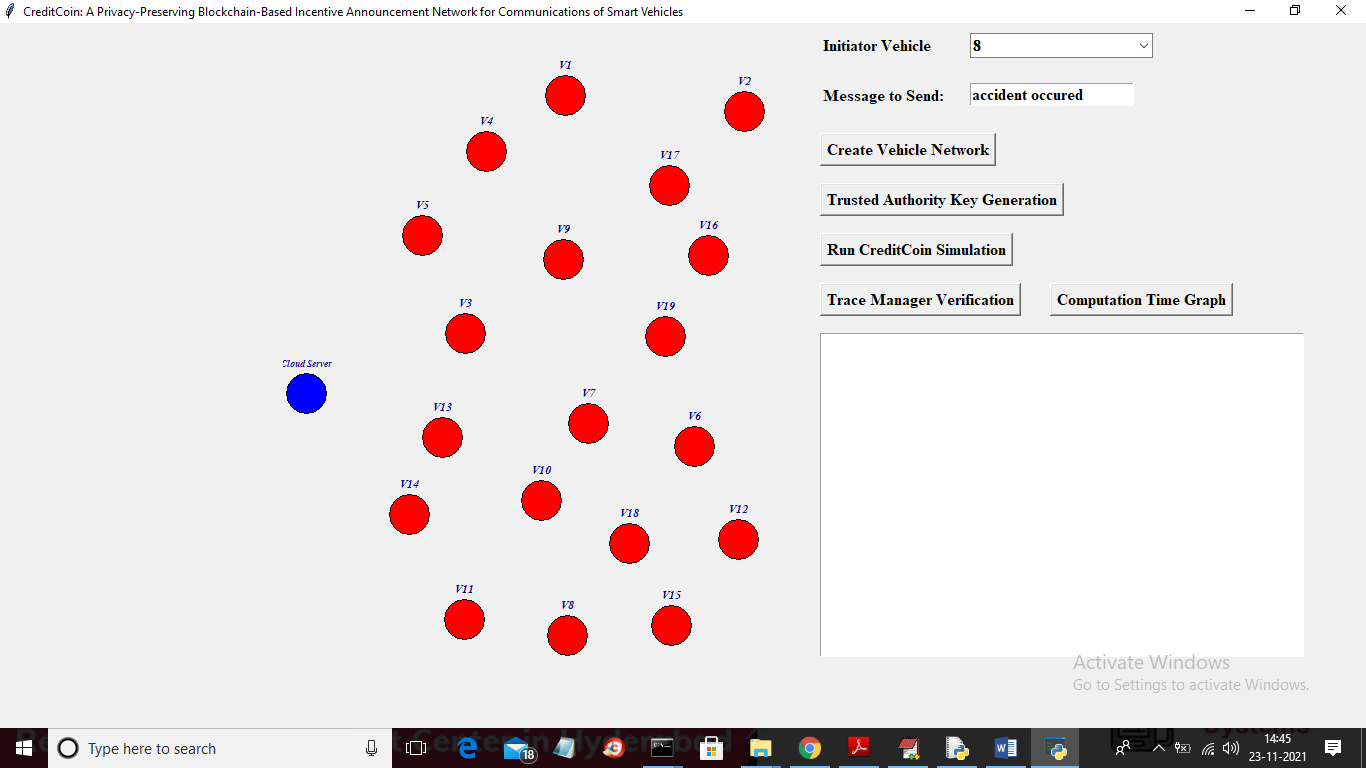
In above screen first drop down box contains all vehicles ID’s and then you can enter message to send to other vehicle



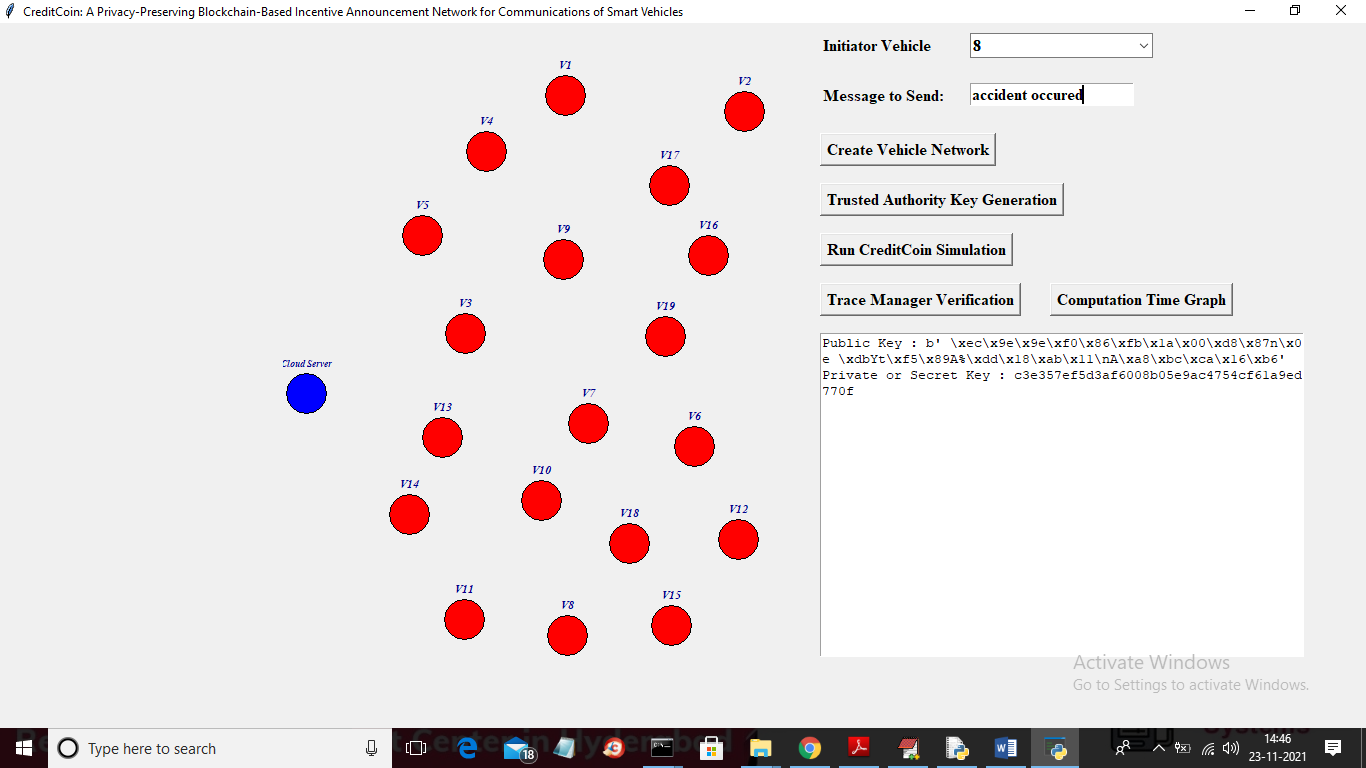
In above screen from drop down list I selected INITIATOR vehicle id as 8 and then enter some message to send to other vehicle



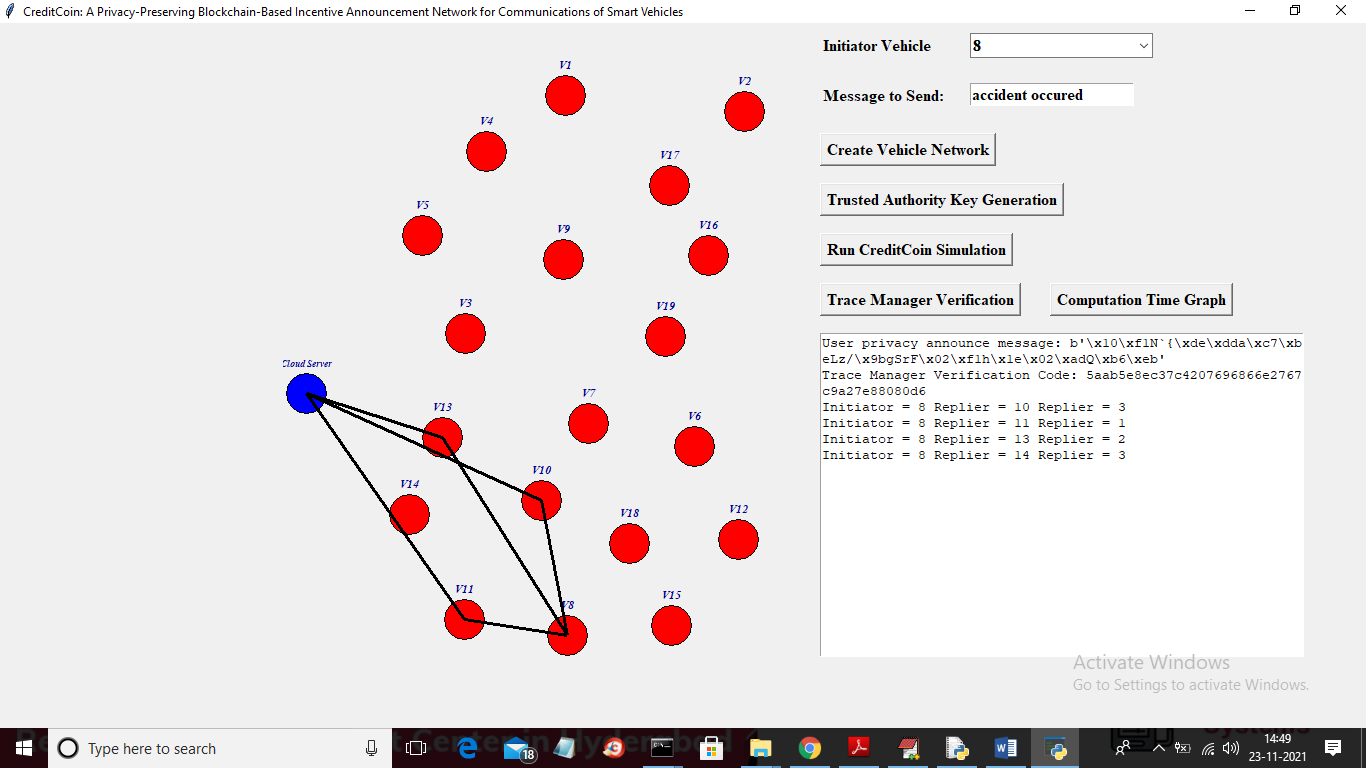
In above screen I entered some message and now click on ‘Create Vehicle Network’ button to create simulation screen



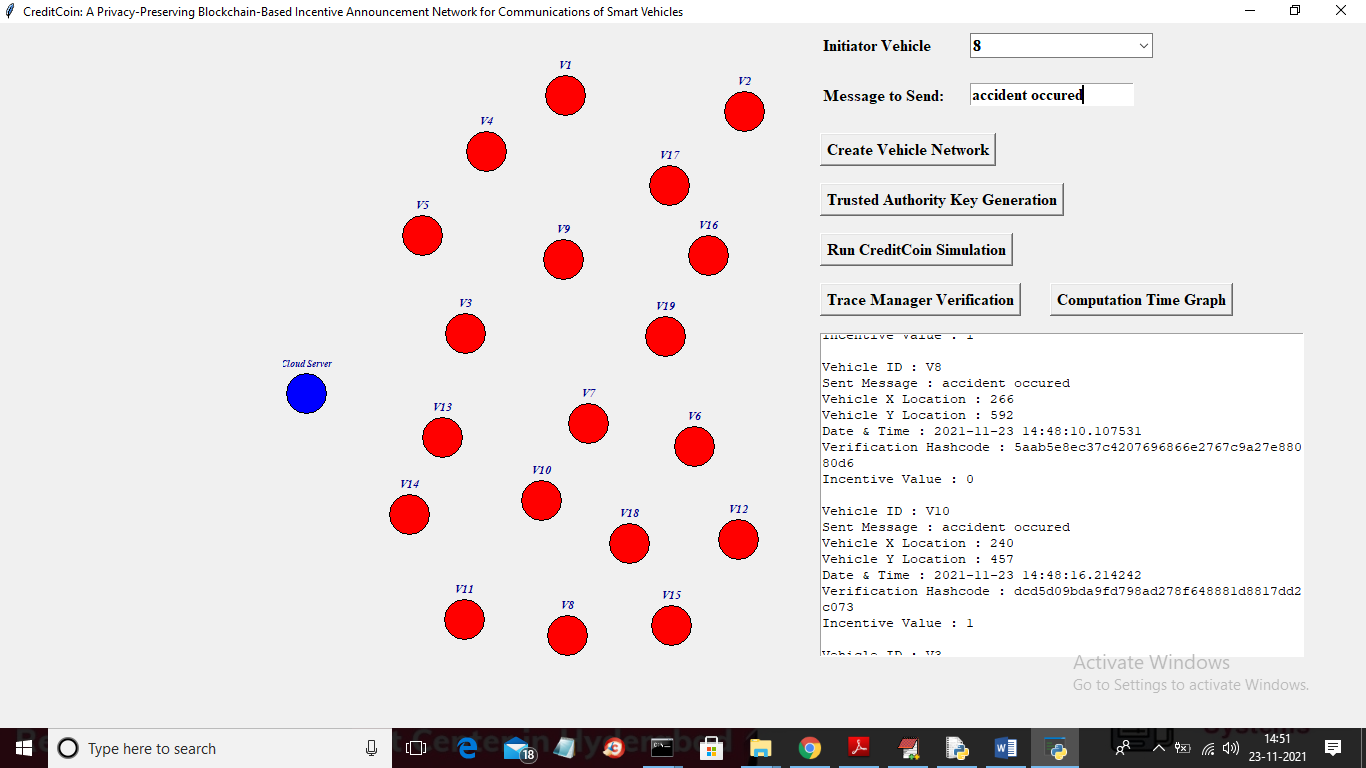
In above simulation screen all red colour circles are VEHICLES and blue colour circle is the Cloud Server and now click on ‘Trusted Authority Key Generation’ button to generate keys for encryption



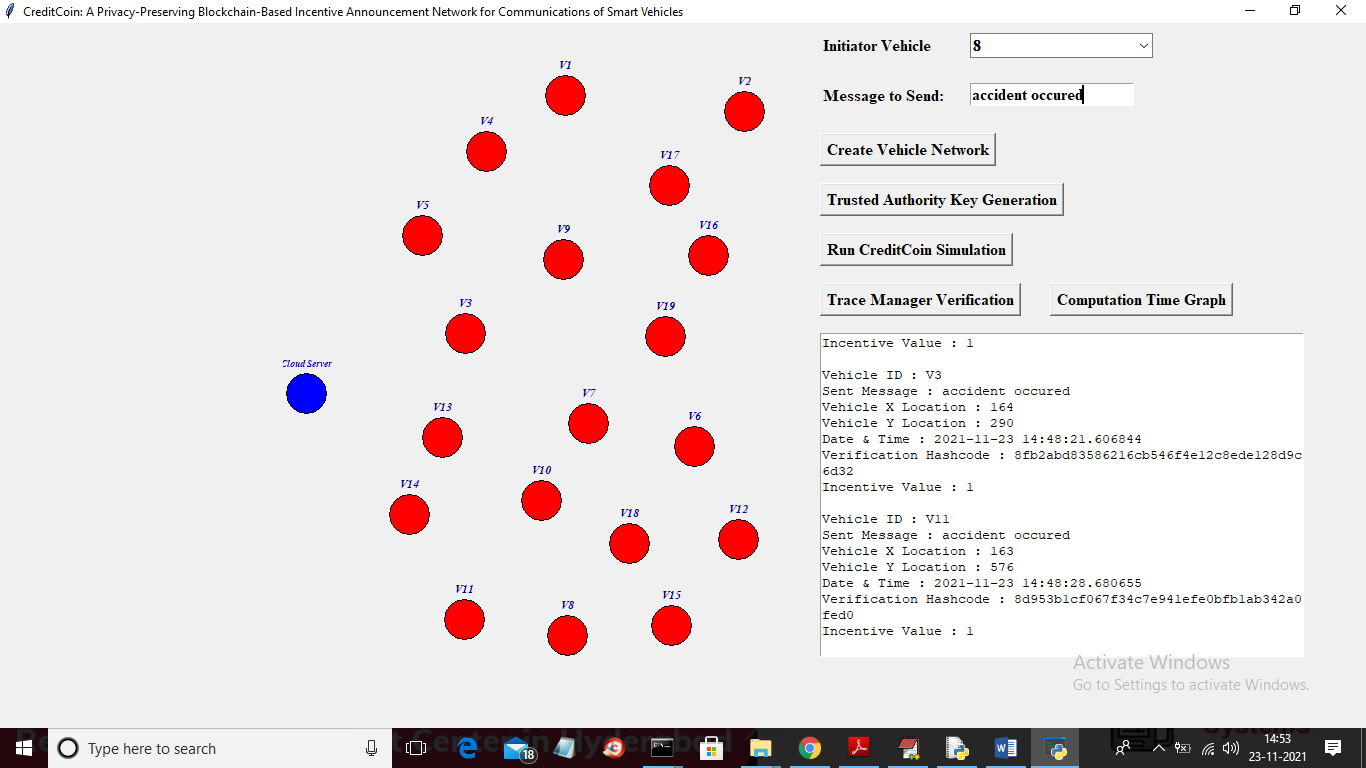
In above screen in text area we can see keys are generated and now click on ‘Run Credit Coin Simulation’ button to allow selected Initiator to send request to nearer vehicle and get reply. All this data will be stored in Blockchain so it may take few seconds time to show below output



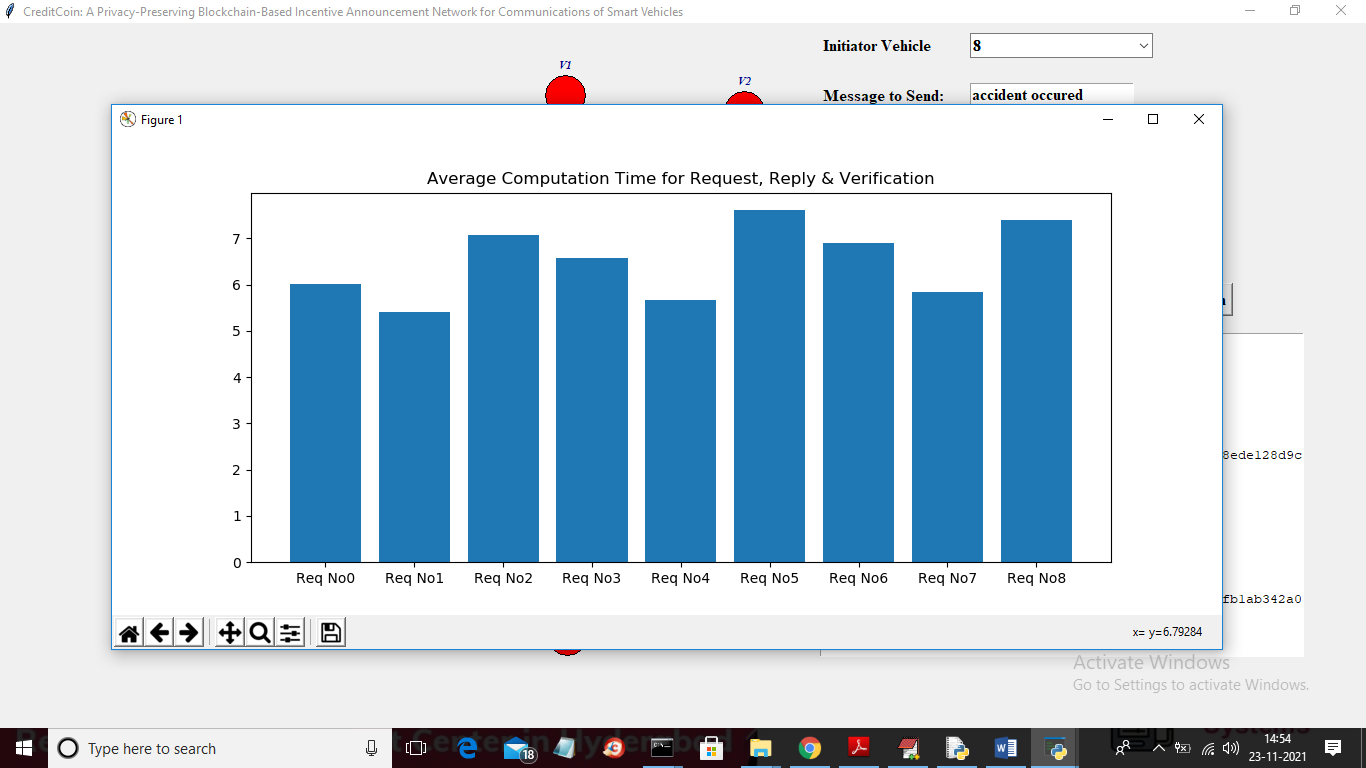
In above screen we can see INITIATOR and repliers are exchanging announcement between each other and cloud server and in text area we can see which initiator sending request to which replier and all this data will saved in Blockchain and to read or verify data click on ‘Trace Manager Verification’ button to get below output



In above screen in text area we can see decrypted vehicle ID involved in announcement with their X and Y location, Date time and verification hashcode and incentive values and if hashcode mismatch then verification will be failed. You can scroll down above textarea to view all vehicles details like below screen



In above screen click on ‘Computation Time Graph’ button to get below graph for each vehicle request, reply sending and verification time



In above screen x-axis represents request no and y-axis represents computation time require for sending request, reply and verification.