IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 6, Ser. II (Nov. –Dec. 2021), PP 53-62
www.iosrjournals.org

Blockchain Elucidating Insurance Claim Stratagem with IoT enabled Telematics system

Preeti Sharma[1], Dr.V.K. Srivastava[2]

1. *Preeti Sharma, Research Scholar, Deptt of Computer Science, Baba Mastnath University, Asthal Bohar, Rohtak, Haryana*
2. *Dr.V.K.Srivastava, Professor & Head, Deptt. of Computer Science &Applications, Baba Mastnath University, Asthal Bohar, Rohtak-124021.*

Date of Submission: 05-12-2021 Date of Acceptance: 19-12-2021

I. Introduction

Blockchain is revolutionizing the digital industry and subsuming multiple sectors including Financial Services, Insurance sector, Healthcare, IT and cyber security [2], etc. Blockchain is a distributed ledger where each member on the network maintains a local copy of the data which is encrypted using public key infrastructure (PKI) security method [30]. In this way, it can establish trust between two different parties without any need of a third-party trust service provider.

Blockchain allows verification of transactions by providing a distributed, secured and immutable ledger[1].

In Blockchain, the decisions or business logic output can be managed and handled by the third party by the use of Smart Contracts which are lines of code that are stored in a blockchain network. Business logics or contracts which are mutually agreed upon by all the members initially can be transformed into smart contracts that govern the future transactions among the participatory members[3].

Utilities of Blockchain enabled system:

Traditional System: In the existing banking system, suppose one person wants to transfer money from his account to another person's account, then there is a subtle need for a third party i.e. Banks. So the person needs to have trust in this third party and has to share critical information in order to use their payment infrastructure. In this scenario, banks are trustworthy mediators between the two parties.

Blockchain-enabled System: For the above scenario, let's suppose we have a blockchain-enabled environment and we want to transact money from one account to another, so the role of the third party for any transaction related activity is not required, as the data is maintained with every peer and, the integrity and consistency is maintained across all the nodes using blockchain, implemented using proper consensus algorithm and peer validations, responsible for the data integrity in blockchain[4].

Various Blockchain platforms for creating distributed applications are Ethereum and Hyperledger. A lot of focus is required in the field of correctness and validation of the contract logic.

BLOCKCHAIN TECHNOLOGY:

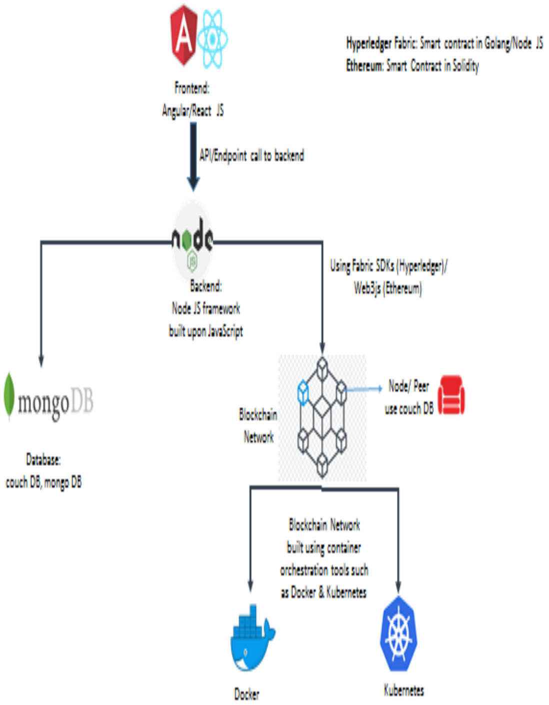


Fig.1: Blockchain Technology

IoT: The vision of IoT is to transform conventional devices into smart and self-governing devices. The idea of IoT is about the formulation of a connected world where things can communicate with each other very efficiently. Various IoT solutions are getting deployed in various sectors which are digitizing the industries.

IOT is a network of interconnected computing devices which have the ability to transmit data over a network without any need of human interaction. It is all about connecting objects to the internet, making the devices smart by enhancing their ability to transmit and receive data to and from internet. In IoT, the daily life objects will be equipped with sensors and devices for communication [5]. The data transmitted by these devices, then can be used for decision making. The analytics and real time insights, gathered from IoT devices can be used to derive various business logics.

IoT can bring transformation by automating the processes which are not feasible to be done manually. An object that can be represented digitally has a great importance and this can only be achieved by use of IoT. IoT focuses on elimination of human intervention and building systems, making various processes autonomous[6].

Blockchain can play a crucial role in the telematics system of IoT devices and how the devices will communicate with each other. Using blockchain for IoT reduces the cost that is associated with the involvement of thirty party individuals and can also prove beneficial by reducing the risk of fraud and unauthorized transactions.

Enhancing the insurance management system in Insurance Industry is one of many suitable use cases of "**Integration of IoT with blockchain**". Smart contracts can help the insurance companies in efficiently managing the claims and the damages done to the vehicle. Information coming from the vehicles can be transmitted to the insurance companies which then can be used to derive the policies that can help in managing the claim process [7]. Whenever a claim request is raised, better paying off strategies can be derived by using the telematics of the vehicle so that only valid claims are paid. Using blockchain and IOT based framework, a solution can be prepared that can start auto-initiation of the claim process.

"Premium Calculation on the basis of drivers meta data collected by IOT devices"

Premium policies can be defined based on the shared customer base. Various factors can be taken into consideration like driving patterns, frequency of raising claim requests, type of vehicle owned by customer and most importantly any fraudulent behavior associated with that customer.

A shared customer base where all the customer details can be stored in blockchain. In case of a new customer, the insurance company can carry out a background verification on that customer, revealing previous insurance records. Shared customer base can help the companies keeping record in a secured way, making investigation process easier. It also reduces the manual efforts in researching each client details and prevents dual claims by the same client. Blockchain, capturing the time –stamped transactions can reduce the probability of frauds. [8] At whole, companies can be linked together in a network that can leverage this shared customer base present in blockchain. Companies can benefit from this as they don't have to put less efforts now on investigating the customers and customers can benefit as they don't have to submit their documents every time they switch to a different Insurance Company. Driver behavior data can also be store in blockchain network [9]. By using an immutable ledger in insurance industry can eliminate the risk of frauds. If the vehicular records are stored in blockchain, it can't be tampered. Better claim management can be done by cross referencing the previous claim details record.

Data from data sensor attached to the car can be stored in blockchain which after confirmation and validation can be visible to companies subscribed in the network and can also be stored in cryptic format in case customer does not want to share the information [10].

The sensors which can be used are GPS sensors that can help in asset tracking, Vibration sensor that can detect if vehicle has been hit, and MEMS sensor for detection of signals and accelerometer that can detect a severe accident [11]. Smart Contracts can be triggered if accident occurs, based on that request for claim can be raised, managed by a claiming system that will initiate claim process based on the factors fed to the smart contracts.

Once the on-field data is collected, it can be fed to the smart contract, initially defined and agreed upon and the smart contract can then finalize the deal between the parties again.

The safe and secure Blockchain network, validation and consensus across the network will make sure nothing is tempered and everything is legitimate and appropriate to all.

Payment process can be fastened using Blockchain. Presently, there can be various challenges associated with payment to insurance carriers, like slow processing, potential of fraud, involvement of intermediaries.[12]

IOT TECHNOLOGY

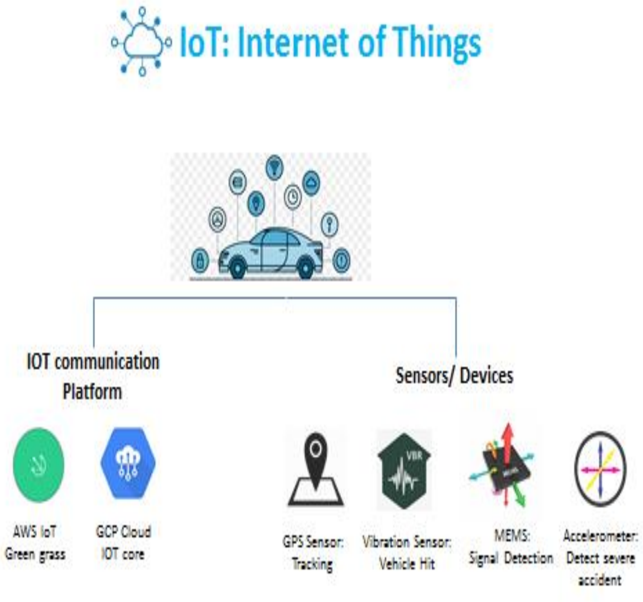


Fig.2: Internet of Things Technology

INTEGRATION OF BLOCKCHAIN AND IoT

Blockchain and IOT Together: Complete anaysis is required when applying blockchain to IOT. One of the main concerns about blockchain, and especially crypto-currencies, resides in its volatility which has also been exploited by people to take unfair advantage of this situation. The integration of the IoT and blockchain will greatly increase the use of blockchain, in such a way as to establish crypto-currencies on the same level as current fiduciary money.[4]

OBJECTIVES

1. Comparison between current Insurance policies and proposed Insurance policies through Blockchain.
2. Smart contracts between Customers and Insurers which ensures transparency in managing claims.

II. Methodology

In this Research, we propose a Blockchain and IOT based framework that will simplify cumbersome process of insurance claim settlement because of opposing interests of insurers and customers.

This framework will have the following features:

1. Smart contracts between Customers and Insurers which ensures transparency in managing claims and calculation of Insurance premium. When a claim request is raised, blockchain will verify the authenticity of the claim for any fraudulent behaviour which leads to faster claim settlement and based on the data stored in blockchain, insurance premium can be calculated in efficient way.
2. A claim handling platform that will streamline the process of raising a claim request using IOT devices which are installed in customer's vehicle that will help in processing vehicle telematics.
3. Blockchain will store all insured vehicles details and in case of crashes and malfunctioning of vehicles, IOT devices will transmit the related details of vehicles to Blockchain which will be immutable and cannot be tampered by anybody. At whole, it will contribute towards creation of "Transparent Insurance ecosystem"
4. Traceability of Automobile using various sensors and detection of each and every move of vehicle can prove be very crucial factor in determining the factors which caused a particular crash or malfunctioning.
5. Blockchain itself can be very vital to Insurance sector but when combined with IOT, it can boost the whole insurance sector and can prove to be very effective in invigorating the insurance ecosystem
6. Elimination of Manual efforts which are required for verification of incidents.
7. As Blockchain is immutable, nobody can tamper the data stored in it, thus preventing any fraudulent incidents.

PROPOSED WORK

Traditional Process of Insurance Management:

In traditional Insurance ecosystem, there is no way to track the complete processing of a particular claim. There is lack of transparency and effective mechanism to derive the premium and insurance claims calculations as there is no capturing of real time data and analytics.

Blockchain Enabled Solution:

Telematics data can be used to determine the factors that may have caused the accident, the data can be captured using various sensors.

Smart contracts can be used for driver rating and premium calculations.

As data and telematics information is stored in blockchain, so insurers, insurance company and auditors can have a clear picture of what has happened during the event of accident and using this information, auditors can help in any conflict resolution.

Real-time data from IOT enabled vehicles, captured using sensors is shared across network and stored in blockchain using consensus algorithm.

Based on the factors defined in smart contract, claim process can be initiated by Insurance company.

As data is shared across driver, Insurance companies and auditors, it becomes very easy to maintain driver past claims and insurance details, based on that premium calculations can be derived. Insurers do not have to upload their documents again and again in case of Insurance company change, as data is stored in a distributed ledger, if allowed by insurer, it can be shared across with other Insurance companies, reducing the efforts to upload documents several time and for insurance companies, to verify the authenticity of the documents. Customer Satisfaction: Customers desire for a fast and transparent processing on where they are in the process flow and what is the next step that needs to be done.

ARCHITECTURE

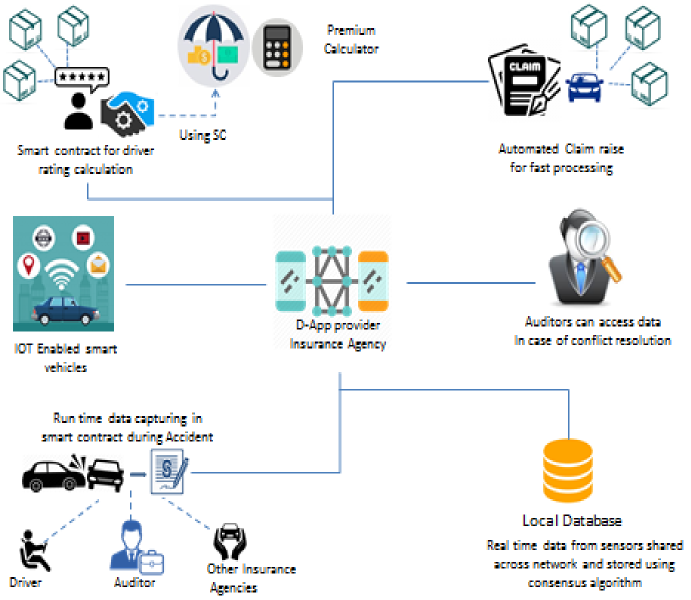

Premium Calculator
Using SC
Smart contract for driver rating calculation
CLAIM
Automated Claim raise for fast processing
IOT Enabled smart vehicles
D-App provider Insurance Agency
Auditors can access data In case of conflict resolution
Run time data capturing in smart contract during Accident
Driver
Auditor
Other Insurance Agencies
Local Database
Real time data from sensors shared across network and stored using consensus algorithm

Fig.3: Architecture of Proposed Work

Benefits of Proposed technology over Current System

Study used blockchain and smart contract technologies to create a traceable online insurance claims system.

(1) Mutual authentication: The suggested technique must be able to check the legitimacy of other people's identities the sender's and receiver's identities. To determine whether the two parties have accomplished mutual authentication, proof must be provided.

(2) Defend against man-in-the-middle attacks: Attackers can intercept messages in the middle of transmission and send illicit messages in the role of users to keep messages safe. As a result, when an attacker uses a man-in-the-middle assault, they are unable to accurately intercept critical information.

(3) Verifiable: The sender's information stream will be signed in the proposed technique. The recipient can then check to see if the signature is valid.

(4) Integrity and unforgery: The suggested technique uses a signature mechanism to assure the message's integrity during the communication process. The message has not been tampered with in any way.

(5) Traceable: Because everyone has access to the same information, blockchain technology ensures that everyone has the same right to know and choose the insurance. The insurance company's track record and the sorts of insurance services it offers are auditable. All transaction information is available to all participants as a result. All change records will be synchronized thanks to the decentralized storage verification mechanism. There will be statistics to prove anything in the future if a dispute arises. Policyholders' rights are safeguarded.

(6) Openness: Both the public and private keys must be set, except that the public key must be set first. The transaction subject's sensitive information is encrypted, and anyone can query it through the public interface, you can access blockchain data and construct related apps. The information in the system is open and transparent, which reduces information asymmetry. As a result, the concerns of moral hazard and adverse selection between the groups are resolved.

(7) Privacy: Only the alliance chain and blockchain technology provide privacy. The policyholder's data will be stored on the blockchain if they opt to disclose it, Blockchain not only does allow authorized users to access data via signature, but it also has the potential to make data more secure. It is not only safe multi-party computing technology, private keys, and encryption technology but also ensuring that the blockchain alliance member's core data and privacy are protected. The database has not been compromised. The content of the insurance is kept private to safeguard the privacy of users. Access to the contract is restricted. The personal contract can only be viewed by the party, and the key is in the party's hands. Contract review, question, modification, and termination other details will emerge and be recorded in the block, and the insurance contract will be signed. Smart contracts are used to automate the entire process.

(8) Information sharing and decentralization: Accounting and storage are decentralized that is, all nodes have the same rights and obligations, and any error or shutdown of one node will result in the shutdown of all others. Any node will have no effect on the network as a whole.

(9) Non-repudiation: After the data has been confirmed and put to the blockchain, it can no longer be changed. The blockchain's built-in time stamp feature can be used to retain data indefinitely. Keep track of the time it

took to create anything. More than 51% of the information changes must be controlled which in an open system will be extremely challenging.[32]

Protocol used in Proposed System:

In our Proposed System we use mTLS for mutual Authentication between parties:

Mutual TLS (or mTLS for short) is a mutual authentication mechanism. By validating that both parties have the correct private key, mTLS assures that the persons at each end of a network connection are who they claim to be. Additional verification is provided by the information contained in their separate TLS certificates. To validate people, devices, and servers within an enterprise, mTLS is frequently used in a Zero Trust security framework. It can also aid in the security of APIs. Zero Trust indicates that by default, no person, device, or network traffic is trusted, which helps to remove numerous security flaws.

TLS stands for Transport Layer Security:

TLS (Transport Layer Security) is a widely used encryption system on the Internet. TLS, formerly known as SSL, authenticates the server in a client-server connection and encrypts communications between the client and the server so that third parties cannot read them.

There are three key points to remember about how TLS works:

1. The differences between a public and a private key.

TLS employs a technique known as public key encryption, which entails the use of two keys: a public key and a private key.

Only the private key can decrypt anything encrypted with the public key.

Only the public key can decrypt anything encrypted with the private key. As a result, if a server decrypts a message encrypted with the public key, it can be assumed that it also has the private key. Anyone can see the public key by looking at the TLS certificate for the domain or server.

TLS certificate No. 2

A TLS certificate is a data file that includes the public key, a declaration of who issued the certificate (TLS certificates are issued by a certificate authority), and the certificate's expiration date for authenticating a server's or device's identification.

3. Handshake with TLS

The TLS handshake is the procedure for confirming the server's ownership of the private key and the TLS certificate. The TLS handshake also specifies how encryption will be carried out once the handshake is complete.

About mTLS and its working.

The server usually has a TLS certificate and a public/private key pair, whereas the client does not. The typical TLS procedure is as follows:

- Client establishes a connection with the server
- The server's TLS certificate is displayed.
- The certificate of the server is verified by the client.
- Over an encrypted TLS connection, the client and server exchange data.

In mTLS, however, both the client and the server have a certificate, and both sides use their public/private key pair to authenticate. There are additional steps in mTLS to validate both parties (additional steps in bold) compared to conventional TLS:

- Client establishes a connection with the server
- The server's TLS certificate is displayed.
- The certificate of the server is verified by the client.
- The client displays his TLS certificate.
- The certificate of the client is verified by the server.
- Access is granted by the server.
- Over an encrypted TLS connection, the client and server exchange data.
- In mTLS, certificate authorities are used.

The mTLS-enabled enterprise functions as its own certificate authority. In standard TLS, the certificate authority is an external institution that verifies that the certificate owner is the legitimate owner of the connected domain (learn about TLS certificate validation).

For mTLS, a "root" TLS certificate is required; this allows an organization to act as its own certificate authority. Authorized clients and servers must use certificates that match this root certificate. The root certificate is self-signed, which means that the company creates it. (This strategy does not work for one-way TLS on the public Internet since certificates must be issued by an external certificate authority.)

Reasons for using the mTLS.

mTLS ensures that traffic between a client and a server is secure and trustworthy in both ways. Users that log in to an organization's network or applications benefit from an extra degree of protection. It also verifies connections with client devices, such as Internet of Things (IoT) devices, that do not require a login process.

mTLS protects against a variety of attacks, including:

On-path attacks occur when an attacker places themselves between a client and a server and intercepts or modifies communications between them. On-path attackers cannot authenticate to either the client or the server when mTLS is utilized, making this attack nearly impossible to carry out.

Attackers can try to "spoof" (imitate) a web server to a user, or the other way around. When both parties must verify with TLS certificates, spoofing attacks become much more difficult.

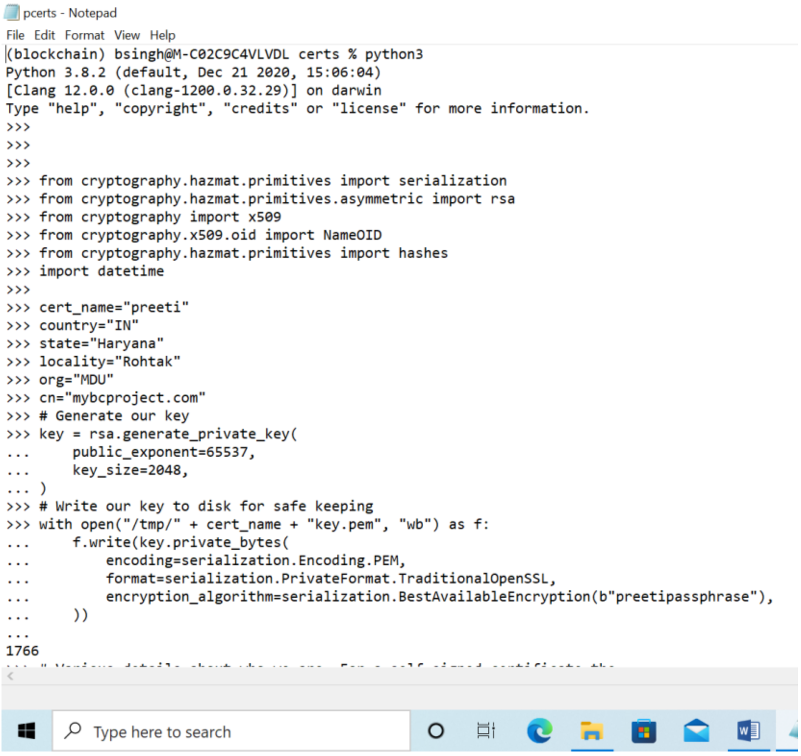
Credential stuffing: Attackers try to get in as a legitimate user using leaked credentials from a data breach. Credential stuffing attacks against businesses that employ mTLS cannot succeed without a validly issued TLS certificate.

Brute force assaults: A brute force attack is when an attacker employs fast trial and error to guess a user's password. Brute force attacks are typically carried out via bots. mTLS ensures that gaining access to an organization's network requires more than just a password. (Rate restriction is another option for dealing with bot attacks.)

Phishing attacks: The purpose of a phishing attack is often to collect user credentials, which are subsequently used to breach a network or application. Even if a user falls victim to such an attack, the attacker will still need a TLS certificate and a private key to use those credentials.

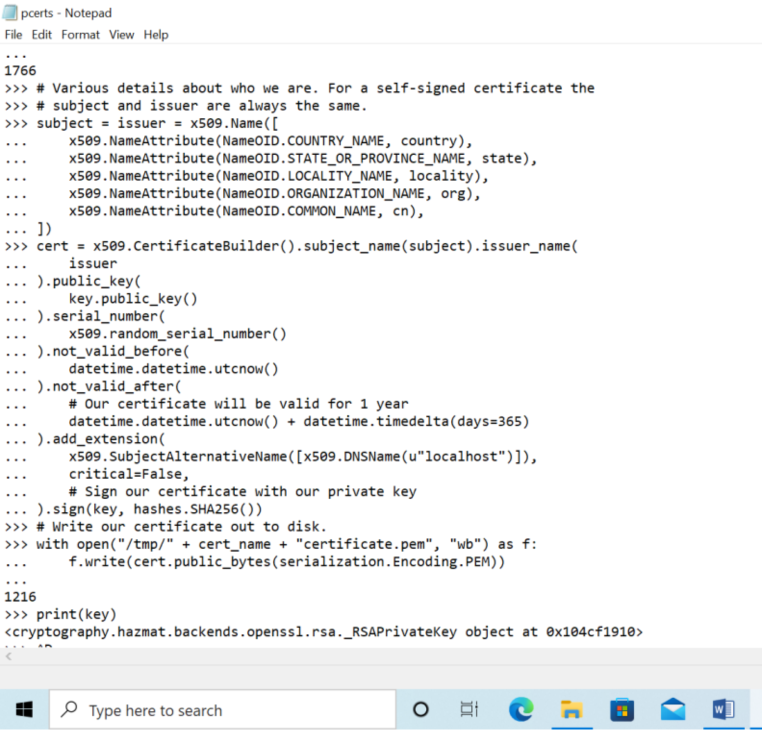
Malicious API requests: mTLS ensures that API requests only originate from valid, authenticated users when it is used for API security. This prevents attackers from sending malicious API calls with the intent of exploiting a vulnerability or subverting the API's intended functionality.[33]

Certificate generation for Mutual Authentication:



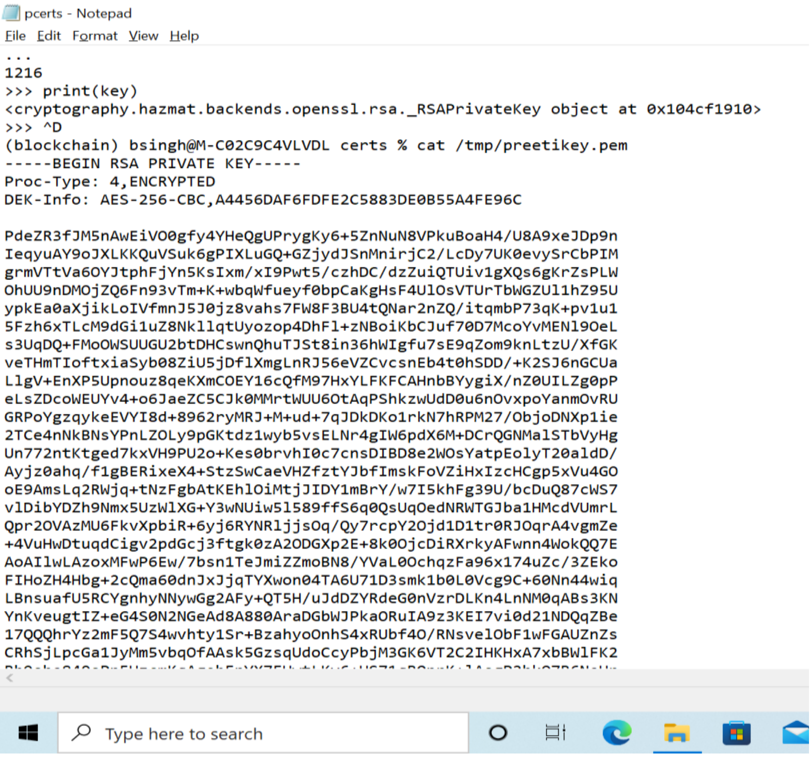
```
(blockchain) bsingh@M-C02C9C4VLVDL certs % python3
Python 3.8.2 (default, Dec 21 2020, 15:06:04)
[Clang 12.0.0 (clang-1200.0.32.29)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>>
>>>
>>> from cryptography.hazmat.primitives import serialization
>>> from cryptography.hazmat.primitives.asymmetric import rsa
>>> from cryptography import x509
>>> from cryptography.x509.oid import NameOID
>>> from cryptography.hazmat.primitives import hashes
>>> import datetime
>>>
>>> cert_name="preeti"
>>> country="IN"
>>> state="Haryana"
>>> locality="Rohtak"
>>> org="MDU"
>>> cn="mybcproject.com"
>>> # Generate our key
>>> key = rsa.generate_private_key(
...     public_exponent=65537,
...     key_size=2048,
... )
>>> # Write our key to disk for safe keeping
>>> with open("/tmp/" + cert_name + "key.pem", "wb") as f:
...     f.write(key.private_bytes(
...         encoding=serialization.Encoding.PEM,
...         format=serialization.PrivateFormat.TraditionalOpenSSL,
...         encryption_algorithm=serialization.BestAvailableEncryption(b"preetipassphrase"),
...     ))
...
1766
... # Various details about who we are. For a self-signed certificate the
```

Fig.4: Certificate generation(Part 1)



```
...
1766
>>> # Various details about who we are. For a self-signed certificate the
>>> # subject and issuer are always the same.
>>> subject = issuer = x509.Name([
...     x509.NameAttribute(NameOID.COUNTRY_NAME, country),
...     x509.NameAttribute(NameOID.STATE_OR_PROVINCE_NAME, state),
...     x509.NameAttribute(NameOID.LOCALITY_NAME, locality),
...     x509.NameAttribute(NameOID.ORGANIZATION_NAME, org),
...     x509.NameAttribute(NameOID.COMMON_NAME, cn),
... ])
>>> cert = x509.CertificateBuilder().subject_name(subject).issuer_name(
...     issuer
... ).public_key(
...     key.public_key()
... ).serial_number(
...     x509.random_serial_number()
... ).not_valid_before(
...     datetime.datetime.utcnow()
... ).not_valid_after(
...     # Our certificate will be valid for 1 year
...     datetime.datetime.utcnow() + datetime.timedelta(days=365)
... ).add_extension(
...     x509.SubjectAlternativeName([x509.DNSName(u"localhost")]),
...     critical=False,
...     # Sign our certificate with our private key
... ).sign(key, hashes.SHA256())
>>> # Write our certificate out to disk.
>>> with open("/tmp/" + cert_name + "certificate.pem", "wb") as f:
...     f.write(cert.public_bytes(serialization.Encoding.PEM))
...
1216
>>> print(key)
<cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x104cf1910>
```

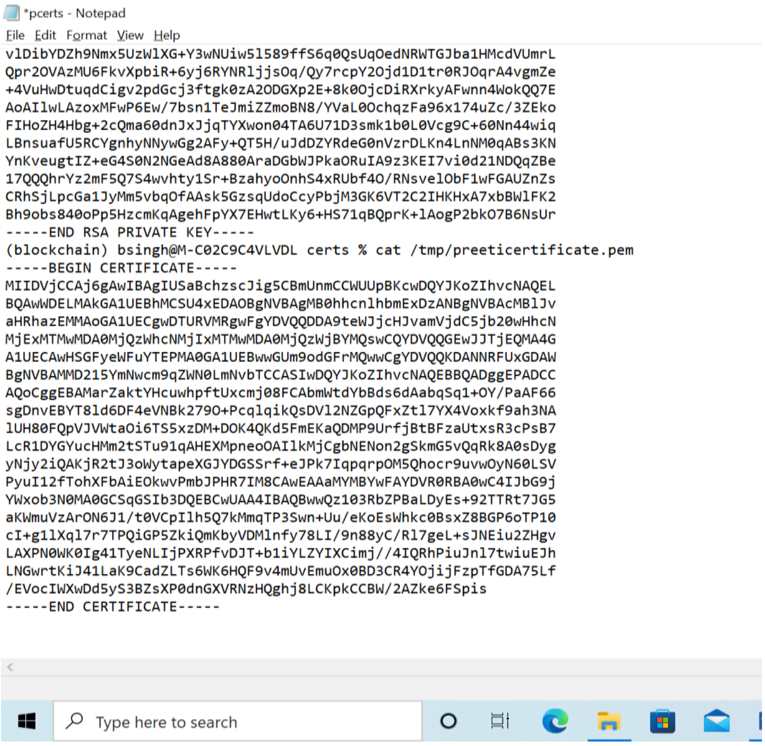
Fig.5: Certificate generation(Part 2)



```
...
1216
>>> print(key)
<cryptography.hazmat.backends.openssl.rsa._RSAPrivateKey object at 0x104cf1910>
>>> ^D
(blockchain) bsingh@M-C02C9C4VLVDL certs % cat /tmp/preetikey.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,A4456DAF6FDFE2C5883DE0B55A4FE96C

PdeZR3fJM5nAwEiVO0gfy4YHeQgUPrygKy6+5ZnNuN8VPkuBoaH4/U8A9xeJDp9n
IeqyuAY9oJXLKKQuVSuk6gPIXLuGQ+GZjydJSnMnirjC2/LcDy7UK0evySrCbPIM
grmVTtVa6OYJtphFjYn5KsIxm/xI9Pwt5/czhDC/dzZuiQTUiv1gXQs6gKrZsPLW
OhUU9nDMOjZQ6Fn93vTm+K+wbqWfueyf0bpCaKgHsF4UlOsVTUrTbWGZUl1hZ95U
ypkEa0aXjikLoIVfmnJ5J0jz8vahs7FW8F3BU4tQNar2nZQ/itqmbP73qK+pv1u1
5Fzh6xTLcM9dGi1uZ8NkllqtUyozop4DhFl+zNBoiKbCJuf70D7McoYvMENl9OeL
s3UqDQ+FMoOWSUUGU2btDHCswnQhuTJSt8in36hWIgfu7sE9qZom9knLtzU/XfGK
veTHmTIoftxiaSyb08ZiU5jDflXmgLnRJ56eVZCvcsnEb4t0hSDD/+K2SJ6nGCUa
LlgV+EnXP5Upnouz8qeKXmCOEY16cQfM97HxYLFKFCAHnbBYygiX/nZ0UILZg0pP
eLsZDcoWEUYv4+o6JaeZC5CJk0MMrtWUU6OtAqPShkzwUdD0u6nOvxpoYanmOvRU
GRPoYgzqykeEVYI8d+8962ryMRJ+M+ud+7qJDkDKo1rkN7hRPM27/ObjoDNXp1ie
2TCe4nNkBNsYPnLZOLy9pGKtdz1wyb5vsELNr4gIW6pdX6M+DCrQGNMalSTbVyHg
Un772ntKtged7kxVH9PU2o+Kes0brvhI0c7cnsDIBD8e2WOsYatpEolyT20aldD/
Ayjz0ahq/f1gBERixeX4+StzSwCaeVHZfztYJbfImskFoVZiHxIzcHCgp5xVu4GO
oE9AmsLq2RWjq+tNzFgbAtKEhlOiMtjJIDY1mBrY/w7I5khFg39U/bcDuQ87cWS7
vlDibYDZh9Nmx5UzWlXG+Y3wNUiw5l589ffS6q0QsUqOedNRWTGJba1HMcdVUmrL
Qpr2OVAzMU6FkvXpbiR+6yj6RYNRljjsOq/Qy7rcpY2Ojd1D1tr0RJOqrA4vgmZe
+4VuHwDtuqdCigv2pdGcj3ftgk0zA2ODGXp2E+8k0OjcDiRXrkyAFwnn4WokQQ7E
AoAIlwLAzoxMFwP6Ew/7bsn1TeJmiZZmoBN8/YVaL0OchqzFa96x174uZc/3ZEko
FIHoZH4Hbg+2cQma60dnJxJjqTYXwon04TA6U71D3smk1b0L0Vcg9C+60Nn44wiq
LBnsuafU5RCYgnhyNNywGg2AFy+QT5H/uJdDZYRdeG0nVzrDLKn4LnNM0qABs3KN
YnKveugtIZ+eG4S0N2NGeAd8A880AraDGbWJPkaORuIA9z3KEI7vi0d21NDQqZBe
17QQQhrYz2mF5Q7S4wvhty1Sr+BzahyoOnhS4xRUbf4O/RNsvelObF1wFGAUZnZs
CRhSjLpcGa1JyMm5vbqOfAAsk5GzsqUdoCcyPbjM3GK6VT2C2IHKHxA7xbBWlFK2
```

Fig.6: Certificate generation(Part 3)



```
vlDibYDZh9Nmx5UzWlXG+Y3wNUiw5l589ffS6q0QsUqOedNRWTGJba1HMcdVUmrL
Qpr2OVAzMU6FkvXpbiR+6yj6RYNRljjsOq/Qy7rcpY2Ojd1D1tr0RJOqrA4vgmZe
+4VuHwDtuqdCigv2pdGcj3ftgk0zA2ODGXp2E+8k0OjcDiRXrkyAFwnn4WokQQ7E
AoAIlwLAzoxMFwP6Ew/7bsn1TeJmiZZmoBN8/YVaL0OchqzFa96x174uZc/3ZEko
FIHoZH4Hbg+2cQma60dnJxJjqTYXwon04TA6U71D3smk1b0L0Vcg9C+60Nn44wiq
LBnsuafU5RCYgnhyNNywGg2AFy+QT5H/uJdDZYRdeG0nVzrDLKn4LnNM0qABs3KN
YnKveugtIZ+eG4S0N2NGeAd8A880AraDGbWJPkaORuIA9z3KEI7vi0d21NDQqZBe
17QQQhrYz2mF5Q7S4wvhty1Sr+BzahyoOnhS4xRUbf4O/RNsvelObF1wFGAUZnZs
CRhSjLpcGa1JyMm5vbqOfAAsk5GzsqUdoCcyPbjM3GK6VT2C2IHKHxA7xbBWlFK2
Bh9obs840oPp5HzcmKqAgehFpYX7EHwtLKy6+HS71qBQprK+lAogP2bkO7B6NsUr
-----END RSA PRIVATE KEY-----
(blockchain) bsingh@M-C02C9C4VLVDL certs % cat /tmp/preeticertificate.pem
-----BEGIN CERTIFICATE-----
MIIDVjCCAj6gAwIBAgIUSaBchzscJig5CBmUnmCCWUUpBKcwDQYJKoZIhvcNAQEL
BQAwWDELMAkGA1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExDzANBgNVBAcMBlJv
aHRhazEMMAoGA1UECgwDTURVMRgwFgYDVQQDDA9teWJjcHJvamVjdC5jb20wHhcN
MjExMTMwMDA0MjQzWhcNMjIxMTMwMDA0MjQzWjBYMQswCQYDVQQGEwJJTjEQMA4G
A1UECAwHSGFyeWFuYTEPMA0GA1UEBwwGUm9odGFrMQwwCgYDVQQKDANNRFUxGDAW
BgNVBAMMD215YmNwcm9qZWN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMarZaktYHcuwhpftUxcmj08FCAbmWtdYbBds6dAabqSq1+OY/PaAF66
sgDnvEBYT8ld6DF4eVNBk279O+PcqlqikQsDVl2NZGpQFxZtl7YX4Voxkf9ah3NA
lUH80FQpVJVWtaOi6TS5xzDM+DOK4QKd5FmEKaQDMP9UrfjBtBFzaUtxsR3cPsB7
LcR1DYGYucHMm2tSTu91qAHEXMpneoOAIlkMjCgbNENon2gSkmG5vQqRk8A0sDyg
yNjy2iQAKjR2tJ3oWytapeXGJYDGSSrf+eJPk7IqpqrpOM5Qhocr9uvwOyN60LSV
PyuI12fTohXFbAiEOkwvPmbJPHR7IM8CAwEAAaMYMBYwFAYDVR0RBA0wC4IJbG9j
YWxob3N0MA0GCSqGSIb3DQEBCwUAA4IBAQBwwQz103RbZPBaLDyEs+92TTRt7JG5
aKWmuVzArON6J1/t0VCpIlh5Q7kMmqTP3Swn+Uu/eKoEsWhkc0BsxZ8BGP6oTP10
cI+g1lXql7r7TPQiGP5ZkiQmKbyVDMlnfy78LI/9n88yC/Rl7geL+sJNEiu2ZHgv
LAXPN0WK0Ig41TyeNLIjPXRPfvDJT+b1iYLZYIXCimj//4IQRhPiuJnl7twiuEJh
LNGwrtKiJ41LaK9CadZLTs6WK6HQF9v4mUvEmuOx0BD3CR4YOjijFzpTfGDA75Lf
/EVocIWXwDd5yS3BZsXP0dnGXVRNzHQghj8LCKpkCCBW/2AZke6FSpis
-----END CERTIFICATE-----
```

Fig.7: Certificate generation(Part 4)

Conclusion and Future Scope:

Blockchain technology has shifted people's perspectives, and it has spawned a slew of new business ideas. Many insurance firms are still involved at this point and have grasped the significance of blockchain technology "Blockchain +" will be used in the future.

In the insurance industry, the term "insurance" will be employed at a higher level and in a broader context.
The following objectives were met as a result of this study:

(1) Use smart contracts to automate the payment of claims.
Smart contracts will generate information and data automatically, removing the need for human intervention, investigation, damage assessment, and assessment are all necessary.
For instance, if a car is involved in an accident, if you have an insurance accident, you can collect your insurance information and upload it to your account.
The insurance company is notified, and the insurance company is instructed to automatically
pay the indemnity, which is more efficient than current insurance claims and saves time.Also it
reduces costs and enhances the customer service experience

(2) Make consumer identity security verification a reality through sharing information.
Currently, the insurance sector is plagued by personnel or agent shortages.
Customers are being forced to accept surrender or survival benefits.
The reason for this is that insurance companies do not have a system in place to control customer identification.
When a customer receives a blockchain identity, his or her personal information is no longer accessible.
The citizen ID is used to assess eligibility, but it must be validated by all parties involved.
Almost completely remove the dangers of numerous court cases in the industry.

(3) Create a blacklist for the industry by submitting data.
Because the insurance market has a low entry barrier, there are a lot of agents.
There are many people in the profession who break the rule of good faith, and there are also many clients who do.Laws and regulations have been broken. However, because there isn't a blacklist platform in the country,
The identification of practitioners and customers in the industry does not allow for appropriate feedback.
The use of blockchain data storage technology to create a blacklist for the industry

In addition, the creation of an open and transparent blacklist database will be beneficial defending against insurance fraud

(4) Using traceability technology, improve the mutual insurance mechanism.
The key factor limiting the growth of mutual insurance is that participants are unable to comprehend the flow of each fund. The information tracing technology used by the Blockchain can ensure that participants have a clear understanding of each fund's expenditures and whereabouts, allowing them to fully trust the mutual insurance organization.
Mutual insurance organizations will achieve long-term success in an environment of complete trust development.

(5) Defending against bogus claims by using the chain's subject information.
Overall, blockchain technology has shown a lot of promise in the field of insurance .This will play a bigger role in the ideological and technological clashes.
The insurance business will benefit from the inclusion of blockchain technology ,more responsibility for "supporting the actual economy and avoiding financial hazards".

References/Bibliography

[1]. A.Akande, Disruptive power of Blockchain on the insurance Industry, University of Tartu.
[2]. T.D.A.D.R.M.K.-K.R.C. Paul J. Taylor, A systematic literature review of blockchain cyber security, Chngquing University of Posts and Telecommunications., 2019.
[3]. B.R. Abhinav Choudhary, Blockchain A potential Game-changer for Insurance Claim, ITC Infotech.
[4]. C.M.J.C.E.S.M.D. Ana Reyna, “On Blockchain and its integration with IoT-Challenges and Opportunities”,2018.
[5]. IoT in the Insurance industry-what it is , why it matters and how we can help- Lead Cloud.
[6]. B.M.t.S.C.M.S.B.Markus Loffler, Insurers need to plug into the Internet of Things- or risk falling behind, Mckinsey & Company,2016.
[7]. V.S.Sriram Natarajan, Demystifying Blockchain for insurance, NIIT technologies, 2017.
[8]. Blockchain in Insurance: Guranteed Coverage and Benefits, WNS Global Services, 2018.
[9]. P. A. F. C. Leticial Rubinstein Cavalcanti, A Business Model for Vehicle Insurance based on Blockchain Smart contracts, 2018.
[10]. S. E. M. Pauline Adam- Kalfon, Blockchain, a catalyst for new approaches in Insurance-PWC, 2017.
[11]. R. R. C.Prbha, Automatic Vehicle Accident Detective and Messaging System using GSM and GPS Modem.
[12]. Blochain in Insurance: Risk Not, Reap Not, 2017.
[13]. T. C. J. C. J.-T. L. a. S. P. Pia Brüggemann, Claims in the digital age:How insurers can get started-Mckinsey & Company, 2018.
[14]. H. S. M. R. G. António Brandão1(&), Systematic Review of the Literature, Research on Blockchain Technology as Support to the Trust Model Proposed Applied to Smart Places.
[15]. M. I. H. G. S. M. I. W. M. W. M. I. Y. G. A. V. B. G. Q. H. K. S. M. a. X. C. Zhi Li, A Blockchain and AutoML Approach for Open and Automated Customer Service, 2019.
[16]. M. Mylrea, AI Enabled Blockchain Smart Contracts:, 2018.
[17]. K. X. (. M. I. a. N. G. MOHAMED RAHOUTI1, Bitcoin Concepts, Threats, and Machine-Learning Security Solutions, 2017.
[18]. S. M. I. M. M. R. M. I. M. S. H. S. M. I. E. H. M. I. M. F. A. S. M. I. M. G. F. I. Md. Abdur Rahman1, Blockchain and IoT-based Cognitive Edge Framework for Sharing Economy Services in a Smart City, 2019.
[19]. Y. W. J. W. M. S. a. R. R. Gihan J. Mendis, Blockchain as a Service: A Decentralized and Secure Computing Paradigm, 2019.
[20]. Ahsan Manzoor, Madhsanka Liyanage, An Braeken, Salil S. Kanhere, Mika Ylianttila , Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing.
[21]. H.-L. P. T.-H. T. H.-T. H. Y. N. Van-Cam NGUYEN§, Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract.
[22]. A. K. J. M. D. K. Nelson Bore, On Using Blockchain Based Workflows.
[23]. S. X. Chen, Blockchain Based Professional Networking and Recruiting Platform.
[24]. Xuhui Chen, Jinlong Ji, Changqing Luoy, Weixian Liaoz and Pan Li , When Machine Learning Meets Blockchain:A Decentralized, Privacy-preserving and Secure Design, 2018.
[25]. M. H. M. C.-S. K. Md Mehedi Hassan Onik1, A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0, 2018.
[26]. M. S. S. S. K. a. R. J. Ali Dorri, BlockChain: A Distributed Solution to Automotive Security and Privacy.
[27]. J. C. B. R. M. K. W. Lennart Bader⋆, Smart Contract-based Car Insurance Policies.
[28]. H. O. a. S. K. *. Younsun Kim, Proof of Concept of Home IoT Connected Vehicles, 2017.
[29]. 2. R. J. S. S. K. A. D. S. J. Chuka Oham1, B-FICA: BlockChain based Framework for Auto-insurance Claim and Adjudication, 2018.
[30]. T. D. A. D. R. M. K.-K. R. Paul J.Taylor, "A systematic literature review of blockchain cyber security," in Chongquing University of Posts and Telecommunications, 2019.
[31]. B. L. a. W. Vorobev, Enabling the Vehicle Economy Using a Blockchain-Based Value Transaction Layer Protocol for Vehicular Ad-Hoc Networks, 2018.
[32]. Chen, C.-L.; Deng, Y.-Y.; Tsaur, W.-J.; Li, C.-T.; Lee, C.-C.; Wu, C.-M. A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology. Sustainability 2021, 13, 9386
[33]. https://www.cloudflare.com/en-gb/learning/access-management/what-is-mutual-tls/

Preeti Sharma, et. al. “Blockchain Elucidating Insurance Claim Stratagem with IoT enabled Telematics system.” *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(6), 2021, pp. 38-62.