Designing A Permissioned Blockchain Network for the Insurance Claim Process Using Hyperledger Fabric and Composer

Archana Hombalimath[1*], Neha Mangla[2], Arun Balodi[2]
[1]CMR Institute of Technology, Bangalore, Research Scholar Atria Institute of Technology, Bangalore
[2]Atria Institute of Technology, Bangalore
E-mail: archana.h@cmrit.ac.in, neha.mangla@atria.edu, drbalodi@gmail.com
[*]Corresponding author

Keywords: blockchain (bc), hyperledger fabric, hyperledger composer, vehicle insurance

Received: May 6, 2022

This research aims to examine the benefits of blockchain technology (BCT) in the vehicle insurance process. The article addresses a number of benefits offered by BCT, including automating the identity verification and doing away with the need for numerous parties to manually certify the legitimacy of transactions. India's financial and business networks can be anticipated to change the accounting process to a different extreme with the introduction of BCT. Unfortunately, they are having some difficulties implementing and acclimating to this modern technology. Here is the solution, blockchain technology may help us solve the existing problem. Insurance firms and car owners can benefit from blockchain technology since it can effectively open up communication channels, encourage industry integration, and improve insurance provider's ability to access record. Using BCT, banking operations will be more efficient, quicker, and less expensive because to the removal of middlemen. Decentralization, transparency, and secure transactions will be the main advantages.

Povzetek: Raziskava preučuje prednosti tehnologije blockchain v procesu avtomobilskega zavarovanja: avtomatizacijo, transparentnost in varnost transakcij.

1 Introduction

1.1 Background

According to the IAIS (International Association of Insurance Supervisors), 20 to 30 percent are fraudulent insurance claims. Clients who lack the ethics and legal knowledge are the one who do the insurance fraud. The policyholder's information is not to be shared. Even if an insurance firm blacklists some policyholders, this does not prevent other insurers from doing business with that insurer. Lack of data transparency and asymmetric information between client and insurance company, the policyholder go for contract.

The existing insurance sector, on the other hand, has convoluted underwriting processes, increased price of underwriting time. The insurance business is not well-monitored. As a consequence, analyzing the risks of insurance applicants while avoiding moral hazard is impossible. It's also unable of dealing effectively with the current problem of criminals exploiting blockchain to launder money.

In the field of automobile insurance, there is a cyclical link between insurers, police, repair shops, and insurance providers. Every connection has challenges with low efficiency and complicated services. Insurance expenses are expensive for insurance service providers, particularly administration costs. Contract signing and management, database maintenance, payment and collection of payments, scrutiny of claims, and data analysis, and other tasks consume a significant amount of time and effort.

When a car owner files a claim for vehicle insurance these days, he or she must first contact the insurance company to tell them of the problem, then proceed to the nearest police station to register a FIR and submit the insurance company the relevant application materials. The car owner will not be compensated until the degree of the damage to the vehicle has been certified by the company. According to studies, present automobile insurance claims procedures are often difficult and take an inordinate amount of time to compensate [2, 3].

Insurance reimbursement is time-consuming due to its complexity, and policyholders commonly have unresolved difficulties. Second, insurance companies spend a large amount of time each year, among other things, on the premium payments process, the collecting the records of claim, service providers of insurance, and audits of government. To ensure that all parties fulfil and comply with the contract's agreed-upon requirements, payment of claim and validation is a time-consuming including with huge amount of administrative costs and manually handling all the processes [4].

Blockchain has developed in prominence in recent years is used s technique through decentralization and

trustlessness, for jointly keeping a reliable database, and it is now being used in a range of fields. Decentralization, trustlessness, non-tampering, clarity, and tracking are features of blockchain technology that are well suited for improving the structural adjustment in government, transparency in governance and service, stimulating the growth of intellect and trustworthiness. All over world same time government proposed various "Internet +" technologies with the help of blockchain in variety of government activities. With the help of cryptography and consensus mechanisms blockchain acquires decentralization for data based on peer-to-peer network this kind of decentralized storage system is termed as blockchain. Benefits of BC (Blockchain) technology include confidentiality, data integrity, and tracking of stored data. Insurance, as a risk-based industry, relies on data to stay afloat. A large amount of complete and correct information is required throughout the design of policy, assessment, and claims payout. With the insurance and associated industries, BC has the potential to create information conduits, industry integration can be improved, and increase insurance companies' data access capabilities. With the maturation of blockchain technology, a "blockchain + insurance ecological chain" can be built.

Blockchain has attracted much interest from academics [14], industry, and researchers in recent years, and it's been named one of the top five technology innovations of 2018 [15, 16]. According to [17], the daily output value of Bitcoin is 4.144 million as of September 17, 2020, with an anticipated transaction value of 158.932 million on the blockchain. Blockchain is categorized into three versions. First version of BC got published in 2009 and it was known as blockchain 1.0 which exclusively focused on digital money while nevertheless serving potentially malevolent worldwide participants [3, 18] was dependent on specific protocols. The second version came to existence in 2014 termed as blockchain 2.0 mainly focused on new methods to utilize smart contracts in different cases and domains with Ethereum [19], which offers client digital assets and partially complete capabilities [10], leading the way. Hyperledger projects published Blockchain 3.0 in 2017, with highly adaptable features (Fabric, Composer, and others) as well as user friendly it's a permissioned decentralized application system. Significant systems in logistics, certifications, and finance were established in the second generation of blockchain [20,21,22,23,49,50]. To construct the normality of blockchain technology, all three phases are complementary and assist one another [51]. According to [52,53], insurance is one of the most important forms of help available to communities in the event of an emergency, neutralizing expenses and assisting them. The sector's largest issue is detecting and protecting against counterfeit documents, as well as stopping the goals of phoney participants. Significant insurance companies have seen the impact of Blockchain technology, according to [54], with the majority of them investing in pilot systems. The B3i (Blockchain Insurance Industry Initiative), is one notable example started in 2016 to find out the benefits of blockchain to increase the success rate of data exchange in insurance organizations. As a result of providing a financial source for clients who are in a disastrous position, insurance companies are burdened with inefficiencies and piles of paperwork [56]. Centralized architecture was used by most insurance company in past for system development as shown in Figure 1(a) [53], Figure 1(b) shows the decentralized blockchain by using this architecture insurance company has a unique ability to better its entire value chain, which has always relied on the highest level of good confidence and belief, and define new insurance products for their customers [57] [58].

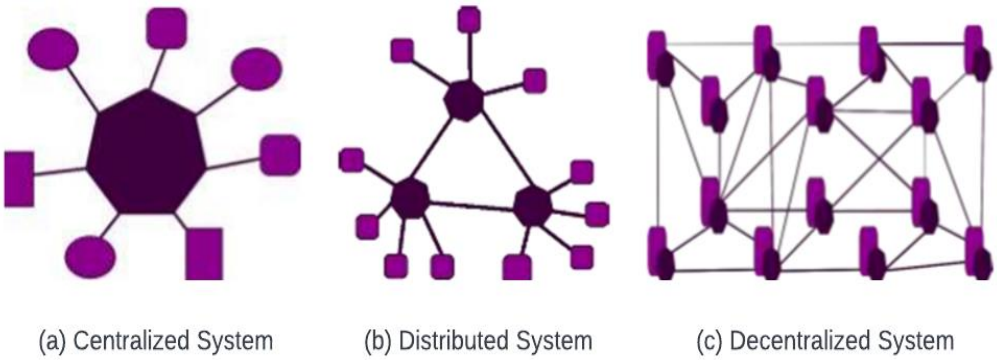

Figure 1: Existing system architecture.

We employed blockchain and smart contract technologies in this research to aid the development of Internet insurance in the following ways:

1.1.1 Mitigate difficulty of insuring effectively

All the insurance data, records of credit and information of individual vehicle will be collected one by one on blockchain which cannot be manipulated or fabricated once the financial sector adopts the BC technology. Adopting BC technology internet insurance can assess health and insurance information of clients online, effectively reducing the time and money for both clients and insurance companies. Reliability of internet insurance businesses' underwriting has considerably enhanced. Simultaneously, mode transfer from offline to online underwriting has been completed for internet insurance. Internet insurance has evolved into a business model rather than a sales channel.

1.1.2 Conducive to improving supervision

Internet crimes are growing increasingly common as a result of a lack of network oversight. On a technical level, blockchain technology has the ability to solve this problem in the future, notably in the operation and control of Internet insurance. Blockchain technology has two features: time tracking and changes that aren't editable. It also essentially verifies the data on the chain's authenticity. Network oversight can significantly reduce with the adoption BC technology in online insurance. On the one hand, the legitimacy of the operation of Internet insurance enterprises may be secured from the perspective of governmental control, thanks to the blockchain's timestamp features and the entire history of information and transaction data from the current block to the genesis block. It has ability to improve insurance industry's existing poor supervision and raise supervisory efficiency.

1.1.3 Suitable for resolving risk management issues

The most important goal is to avoid systemic risk. Moral hazard can be efficiently reduced using blockchain technology. The insured individual's credit history, health condition, asset registration, and use status will be established on the blockchain throughout the online insurance process, from underwriting to claim settlement, because the blockchain establishes a whole trust - free value network. Systemic risk can be avoided by allowing the insurer query all insured's record on blockchain and assess the insured's risk as the information is timestamped.

The second goal is to keep technical hazards under control. Existing computer technology used by internet insurance companies is insufficiently developed, resulting in crash occurs and phishing attacks. Security of internet insurance system is effectively safeguarded by BC technology due to its decentralized structure of ledger and nodes are also decentralized. Through communal maintenance likelihood of technical risks are reduced. The final goal is to keep information security threats under control. Customer information, firm internal information, and other data held by insurers, particularly Internet insurance providers, are extremely valuable. The BC technology assures secrecy of data held by Internet insurance businesses, this system is resistant to attempts to alter or destroy it by unscrupulous actors.

It ensures that Internet insurance companies run smoothly and, to some extent, lowers the cost of system maintenance.

1.1.4 Facilitating effective anti-money laundering

BC technology is used in internet insurance, which efficiently prevents money laundering. Every fund transaction has a unique time stamp, and records deposited into the blockchain must be recognized by the majority of blocks on the blockchain, ensuring the data's dependability and confidentiality to some degree.Simultaneously, transaction data cannot be changed whenever and wherever, and records and information on the blockchain cannot be destroyed whenever and wherever; as a result, time of transaction and the parties involved in transaction of each fund can be traced all the way back, in the context of criminal activities involving online insurance for financial fraud it is found to be really efficient method. It also serves as a more dependable platform for capital chain oversight.

In field of insurance applications, blockchain technology offers the following benefits:

- To some extent, claims settlement can be made more efficient by using blockchain smart contracts.
- To certain extent, the blockchain's security can help policyholders with their privacy and security concerns.
- Blockchain can address the issue of trust between policyholders and insurance companies.
- Blockchain can help to solve the problems related to records tampering in sales transactions.

Due to aforementioned characteristics of blockchain, it can aid both the insurers and the policyholder in establishing a long-term relationship. Insurers can use the blockchain mechanism to improve the efficiency of their operations and management, as well as precisely analyze operational risks. Selecting an insurance company that uses a BC claims settlement system can make claim settlement easier for the insured, allowing payment to be collected more fastly and rising the insured's faith in the company. Finally, this study may aid the insurance companies as a whole in improving its sustainability.

And the insured is involved in an accident and files a claim using the smart contract [25], the smart contract's

automatic performance function is activated, and the claim payment is launched, when the system's predetermined requirements are met. To achieve auto settlement of claims, speed up claim settlement efficiency and save costs claim payment will be directly done to beneficiary's account.

The blockchain consensus mechanism presents a feasible solution to the issue of inefficient claim settlement. Smart contracts work on the idea of embedding terms of the contract in software so that the agreement cannot be broken and the cost of doing so is extremely expensive. Smart contracts provide predictability, uniformity, closure, verification, effectiveness, timeliness, and leastprice.

Whenever the information recorded in the blockchain meets the claim contexts, online insurance will initiate the clearing and settlement program immediately. The insurance payout agreement will be immediately terminated once the claim money is electronically given credit to the insured's chosen account. Using blockchain technology to automate claim settlement simplifies the payment process, eliminates several manual review processes, speeds up agreement completion, and lowers the price of agreement validation and completion.

1.2 Research goals

To accomplish the following research objectives, depending on blockchain and smart contract technology, an insurance claims system has been developed [59–89]:

- To design a framework for vehicle insurance claim process.

  Traceable: Allow for greater transparency in the process by allowing the car owner to quickly and easily file an insurance claim, resulting in a faster settlement. BC technology make's sure that all have the equal right to know and select, as all the participants has equal access to data. Regards to the decentralized storage verification mechanism as modifications to the records will be in sync on the chain. In future if a disagreement arises policyholders' rights are protected due the presence of evidence to prove.
- Eliminate multiple claims for one accident.
- Privacy: Using decentralized data access, you can achieve data privacy and security. Information that clients selects to share only will be stored behind the partnership chain. Because of signature secret keys, cryptographic algorithms, and protect multi-party technology, blockchain technology would allow authorized consumers only to connect record, as well asensures that the blockchain alliance member database's basic data and privacy are not leaked. To preserve users' privacy, the insurance contract's content is password-protected. Party can view only personal contract and not the key it is in the party's possession. Smart contracts will be used to effectively integrate the insurance contract, with agreement overview, request, amendment, as well as other details occurring and being stored in the block.
- Non-repudiation: To avoid fraud, provide time stamped transactions. The data will be permanently preserved once it has been verified and uploaded to the blockchain, and the blockchain's inherent time stamp mechanism may note time of transaction. It will very difficult to change the information as it is required to control more than 51% of system nodes.

1.3 Existing vs proposed system

This section highlights the novelty of the proposed system compared to existing system in the insurance domain. Novelty of proposed system is presented by comparing it with existing system as follows

Table 1: Existing system vs proposed system

Existing system	Proposed system
Actual value is transferred between parties by the centralized administration.	Through a cryptographic technique that offers a shared information source on remote nodes, trust is generated.
Contract development, fund transfer, and complex manual information/data review on a physical document.	Real-time access to and analysis of all financial papers enables the immediate start of shipments.
Delays brought on by manual communication and changes made to the contract conditions by all parties	Transaction time is shortened through contract execution on decentralized nodes and real-time status updates.
Due to centralized restrictions, there is no transparency about ownership and location proof.	Transparency brought on by decentralized management.
The transaction charge is increased by the manual process.	Transaction fees were less expensive thanks to automated settlement.
Multiple copies of documentation make it difficult to control modifications that are made.	Multiple parties participating in the transaction process can all examine the document simultaneously in real time without encountering any problems.

The manual procedure produces various platforms for each side, which greatly increases the likelihood of miscommunication and fraud.	With a single platform, there is no room for fraud as everyone receives the same communications.

2 Preliminary

2.1 Blockchain technology

BC technology is a distributed ledger that tracks the history of transactions and is publicly verifiable, distributed, and unchanged. A blockchain, as the name implies, is a collection of blocks that each carry details of transaction and are linked together by a hash of the blocks before and after them to form a chain. The blockchain system is made up of nodes, each of which keeps a replica of the chain's data and connects to other nodes via point-to-point connection. A header, an ID for the past and subsequent blocks, a date, and a set of transactions are all included in each block. Blockchain (BC) is a decentralized technology that allows for the creation of brand-new technological operations and business plans [89]. Blockchain integrates earlier developed technology such as electronic certificates, cryptographic hashes, and decentralized consensus techniques [90]. The underlying digital foundation that underpins apps like bitcoin is known as blockchain. In a cooperative network, the technology improves the process how the transactions are stored and assets are tracked. Practically any other sort of asset that can be exchanged between peers and stored safely and confidentially with no need for third-party authentication can be used as assets. This is because cryptography, network consensus mechanisms, smart coding, and teamwork enforce confidence and provide confirmation without the need for controlling intermediates such as governments and banks [91]. The scientific research of data structure is the foundation for current algorithms, in which nodes are used for datagrams and data warehouses, and they interact with each other via agreed-upon node protocols [92].Blockchain can be discussed alongside other similar techniques because they also can be outlined and reviewed based on empirical data structure studies, with the goal of serving as the core component of existing techniques in which endpoints have been used for datagrams and information repositories, interacting with one another using approved methods. A transaction was indeed demanded in Blockchain, and it is then conveyed to the point-to-point network. When a transaction is authenticated and verified, it is linked to the blockchain's existing blocks, completing it. Figure 2 illustrates this point.

2.2 Features of blockchain

Immutability and security: Blockchain provide a safe and consistent method of storing and retrieving information among nodes in blockchain systems due to its immutability [93]. Unchanging transactions are protected from malicious users' illegal access. Participants can add new transactions but not delete or amend existing ones, making it easier for all nodes to keep records of previous transactions [94]. Information can never be modified after it has been written and kept in the ledger [95]. If a transaction has a mistake, a new transaction must be made, and both transactions arepresent. Because all nodes have complete details for identification, confirmation, and validity, as a result, it reduces reliance on a central integrity entity and the risk of a central entity malfunctioning or manipulating data. [94].

Transparency: The blockchain network imposes confirmation and acceptance testing through a consensus approach, in which any participant can appear and openly begin and append transactions after complying with the blockchain's rules.Since all transactions must be approved by their intended producers, and once a block has been approved, miner nodes send this same block to all of the other nodes within the network, blockchain's consensus, confirmation, and admittance methods ensure network members' confidence [95]. All transactions are made public to all nodes who are part of the networkin this situation, as they are in a public blockchain, but all data in a private blockchain is only accessible to authorized nodes.

Verifiability: Outsiders and insiders can verify transactions conducted and maintained via blockchain technology thanks to cryptography and consensus mechanisms. To be genuine, at least 50 % of participants plus one has to agree on the transaction's validity.

Authenticity: The use of consensus mechanism in blockchain applications ensures the legality of transactions. Furthermore, each block in the blockchain contains past and successive hashed IDs, as well as the producer's and responder's digital signatures.

Ownership and accountability: ownership and accountability can be provided based on the connection between blocks, integrity of transactions, and the approval of the original creators in blockchain-based systems. In addition, participants are aware of a block's or transaction's provenance.

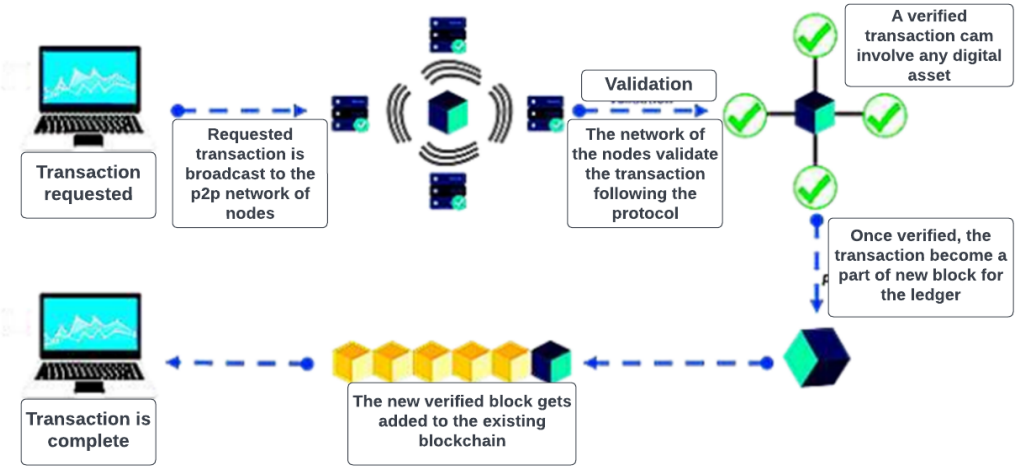

Figure 2: A visual representation of how blockchain works, source: Edureka.

2.3 Blockchain components

Assets:by definition, it's something precious to a company, it enables the transfer of well almost anything of commercial benefit across a blockchain platform. An asset can be intangible: money, stocks, intellectual property rights, certificates, and personal data, or tangible: foodservice at a hotel, real estate investments, depending on the blockchain system. Compared to conventional -assets such as Apple Stock, which have a paper-based right of ownership, a blockchain asset is entirely digital and completely owned by the participant, requiring no third-party agent or agency for transfer or sale.

Transactions: A blockchain transaction is a sequence of time-stamped events that lead to the production of blocks in the ledger. Participants can stay anonymous since transactions are saved using private or public keys; however, third parties can access and verify identities. Most transactions and perhaps other data are publicly reviewed before being put into the ledger using Ralph Markel's tree, as depicted in Figure 3 [96], to ensure system trust and harmonization. The Merkle tree [96] is a huge binary tree data structure which improves in data consistency validation and guarantees, allowing for speedier security authentication in big data applications. The value from each child node is hashed by the parent node.

Algorithm for achieving consensus: A consensus method aids decision-making in decentralized or distributed systems [97]. In a blockchain network, the consensus algorithm is an administrative system in which the majority of untrusted parties agree on the rules to be followed and the best alternative for everyone.Quorum structure, truthfulness, decentralized governance, authentication, nonrepudiation, performance, and byzantine fault tolerance are all characteristics of the blockchain consensus algorithm [97].Whether or not a block is added to the blockchain is determined by this decision.The consensus algorithm plays an important function through enabling collaboration and cooperation, as well as assuring that all members have equal rights and recognition and encouraging constructive participation.For a thorough discussion of consensus algorithms, see [98].

Functions in cryptography: Cryptographic Functions employ complicated mathematical computations to transform data into information that is completely useless inside the hands of the wrong people. This blockchain feature enables potentially harmful blockchain network participants to build and append blocks to the chain, as well as conduct secure network operations. Every block of the blockchain contains the immediately preceding block's hash, as well as transaction records and a time and date. Unsymmetrical (public-key) cryptography, in contrast to symmetric key encryption, encrypts with a publicly shared public key and thereafter decrypts with a private key. Blockchain procedures are also secured via hashing. Prior to a transaction, the immediately preceding block's data is hashed and saved. The public key of the transaction creator is hashed and used to establish transaction information about the identity [99, 100, 98].

Distributed ledger: In the marketing world, a ledger is absolutely vital because it stores all records for online and offline activities, as well as clients and their credentials. A ledger is centralized in a typical business IT environment.
The blockchain ledger, on the other hand, is decentralized at its essence, and regardless of the nature of blockchain, it can be accessed by a small number of authorized parties (private) or by all participants (public) (public). Auditability, security, transparency, and accountability are all enforced by the distributed ledger, along with other BC characteristics.

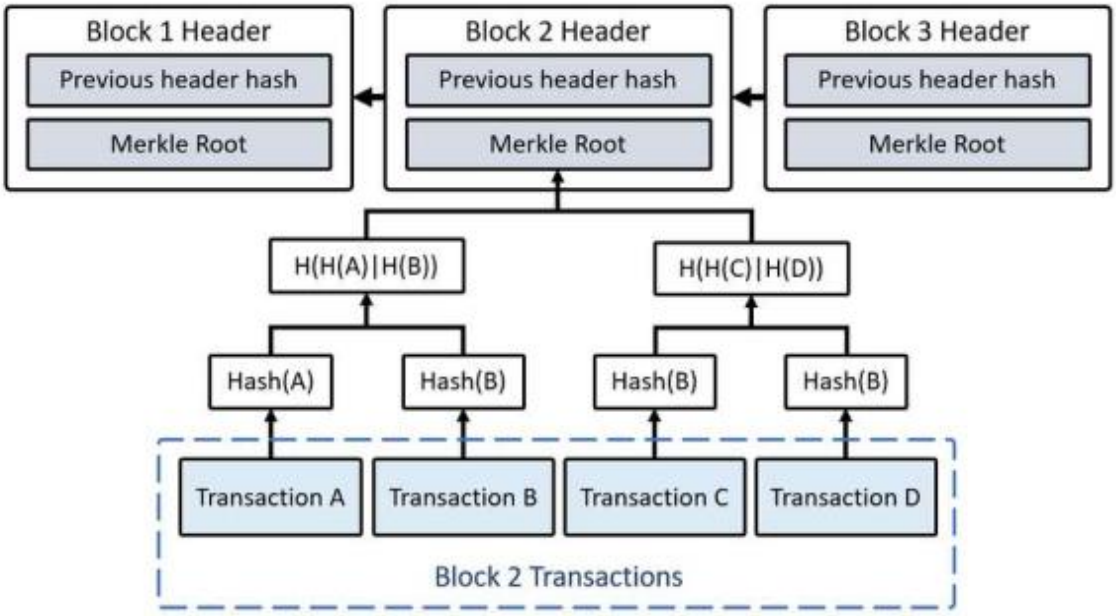

Figure 3: Merkel tree is used to illustrate blocks in blockchain.

2.4 Blockchain types

Public blockchain: This is accomplished without the need for permission on a public blockchain by enabling everybody to participate in the consensus process. Everyone who is a member of a public blockchain can interpret, try writing, and exchange on the network [101,102]. There is no single trustworthy organization in responsible of network supervision and control, hence it is decentralized. This kind of blockchain is safeguarded by encryption, which incentivizes miners to verify it. Miners, who can be anyone on the blockchain, consolidate and propagate transactions [101, 102]. Because no member of the blockchain is trustful, the public blockchain relies on computer systems and brute strength tactics to validate transactions. As a consequence, the miner who achieves all of the right answers at the conclusion of the process rewarded. The most extensively utilized public blockchains are Bitcoin and Ethereum [101, 102].

Private blockchain: this is a permissioned blockchain in which network users are restricted from accessing certain areas of the blockchain. This imposes a centralized control mechanism and allows just a few network participants to modify the network. Because it meets with standards and regulations such as KYC and AML, this sort of blockchain is commonly employed in the banking industry. [102, 101].

Consortium blockchain: this is a quasi-decentralized, permissioned blockchain. Unlike a public blockchain, here it needs permission to enter and only allows a small number of clusters to manage and administer the network. The public clients may indeed be given restricted access to the blockchain through API, with only the most basic of queries possible. This type of blockchain maintains the inherent safety for data of public blockchain while also providing increased network control. Platforms like R3, Quorum, and Corda [102, 100] are examples.

2.5 Blockchain platforms

The sections that follow go over some of the most popular blockchain platforms. Table 2 summarizes this information.

Table 2: The most popular blockchain platforms, source: www.ijacsa.thesai.org 449

Platform	Year Launched	Industry focus	Ledger Type	Consensus Algorithm	Smart Contract	Governance
Hyperledger Composer	2018	Cross-Industry	Permissioned	Pluggable Framework	Yes	Linux Foundation
Ethereum	2013	Cross-Industry	Permissionless	Proof of Work	Yes	Ethereum Developers
Hyperledger Fabric	2015	Cross-Industry	Permissioned	Pluggable Framework	Yes	Linux Foundation
R3 Corda	2016	Financial Services	Permissioned	Pluggable Framework	Yes	R3 Consortium
Quorum	2016	Cross-Industry	Permissioned	Majority Voting	No	Ethereum Developers and JP Morgan Chase
Hyperledger Sawtooth	2019	Cross-Industry	Permissioned	Pluggable Framework	Yes	Linux Foundation
Hyperledger Iroha	2019	Cross-Industry	Permissioned	Chain-based Byzantine Fault Tolerant	Yes	Linux Foundation
OpenChain	2015	Digital Asset Management	Permissioned	Partionned Consensus	Yes	CoinPrism
Stellar	2014	Financial Services	Both Public & Private	Stellar Consensus Protocol	Yes	Stellar Development Foundation
Tezos	2014	Cross-Industry	Permissionless	Delegated Proof of Stake	Yes	Dynamic Ledger Solutions

Ethereum: The blockchain community and developers can use this platform to create and deploy smart contracts applications. The Ethereum Distributed Environment is open-source and allows for the deployment of tokens, cryptocurrency, social apps, wallets, and more. Blockchain technology can be used in a diverse range of companies, not simply banking, thanks to Ethereum's architecture. This platform is made up of a number of different components as follows

- Smart contracts, defined in the Solidity programming language, are used to control all occurrences in Ethereum.
- On the Ethereum network, Ether is the backbone of transactions and cryptocurrency.
- In this platform clients are the people who create and mine the Ethereum blockchain. Geth, Eth, and Pyethapp are some examples.
- The EVM is a blockchain engine which ensures smart contracts for work. EVM's programming language is bytecode, which necessitated the creation of a variety of different smart contract authoring languages, such as Solidity.
- Etherscripter is an user interface that allows you to create Ethereum smart contracts. The drag-and-drop technique enables for the automatic creation of backend codes in LLL, Serpent, and XML in only a few simple steps.

Hyperledger: this is a global partnership led by The Linux Foundation and comprised of industry professionals from financial, accounting, production lines, IoT, technologies, and industries. This platform is an open-source project led by a community dedicated to putting together a set of solid foundations, libraries, and tools for building and implementing organization blockchain systems. Permissioned (private) frameworks exist alongside permissionless (public) frameworks [104].

Corda: This blockchain platform was released by R3 in 2016 as an open-source blockchain technology with widespread support from developers and organizations. This platform has a characteristic that no other blockchain has. It's a restricted blockchain network where only known members can share information. The purpose of Corda was to promote trust, openness, protection, and privacy.

Quorum: This platform of blockchain is a business-oriented blockchain. It's an improved version of the open-source Ethereum client 'geth' that caters to business demands. It is an open-source project that addresses the functionality, security, and access control concerns of businesses. Quorum satisfies the requirements of corporate applications, which include privacy, performance, and permissioning, as well as transaction secrecy, scalability, and speed, as well as authorization.

3 Literature survey

Blockchain technology has risen to prominence as a cutting-edge disruptive technology. As shown in Table 2, several efforts have been made to broaden the scope of blockchain's usefulness. However, there are only a few works in the insurance industry. As a result, we look at the various opportunities and threats that this endeavor

presents. Claims and fraud are the most crucial business processes in the insurance industry that may be improved or re-engineered, according to industry and academic studies. Blockchain's nature, as well as aspects like as cryptography, consensus algorithms, decentralization, and others, make it a perfect remedy for the finance industry. The challenge of data recognition and intelligent data transfer is handled by hashing the identities of members in the blockchain network. The blockchain P2P model has the potential to establish a new range of insurance products while eliminating the need for trusted middlemen. This analysis was carried out in order to find the possibilities that would best position us to begin our future projects. Security and data privacy, scalability, legislation, and taxation are among problems that blockchain technology now faces. Despite the fact that the separate technologies on which blockchain is built are mature, their integration introduces vulnerabilities. Blockchain will become a very strong tool for addressing many of the technical issues that the insurance business is currently facing.

Table 3: Literature survey summary

Authors, Title of Paper, year of publication	**Gaps identified**	**Tools Used**	**Methodology used**	**Major Results**
Anokye Acheampong AMPONSAH *et al. [58] ,2021	• Blockchain 3.0 has yet to be put to good use in the insurance industry. • As previously said, all insurance sector initiatives remain in their infancy. • Because not all data is required by all nodes in private blockchain systems, decentralization of the entire ledger could be theoretically insignificant, but it could worsen storing, scaling, and technical problems.	Hyperled ger fabric	Locating Studies or Data Extraction, Data Screening and Selection, Descriptive Analysis	• The insurance industry, as large as it is now, has realised that blockchain technology may be used to improve essential internal procedures such as submission and processing of claim, detection and prevention of fraud, and so on.
Mayank Raikwar∗ et al. [59], 2018	• Transaction management time, clearing and settlement time, and security are all major concerns in the insurance process.	Hyperled ger fabric, solo consensus algorithm	Implemented an insurance company's operations into smart contracts and stored the outcomes in a blockchain-enabled distributed platform.	The Confirmation time is related to the network size.
Aarti Patkiet al. [63], May 2020	• There is only one point of failure. • Deploying suitable legal framework is a huge task. • Time-consuming and costly KYC (Know Your Customer) process can be completed more quickly and at a lower cost on BCT.	--	Top Indian banks, FinTech organizations, and banking consultants were contacted for primary research. We contacted each of the 25 execs. The information was gathered through organized questionnaires and interviews with senior executives. Secondary data was gathered from Deloitte news bulletins and	Addresses both primary and secondary research aimed at learning more about BCT and how it's used in banking.

			publications, as well as research articles published in research journals.	
D. Popovic et al. [60], 2020	• There are no well-established standards or platforms. • The inability to initiate a claim on more complex insured occurrences due to a lack of trustworthy third-party data.	enterprise risk management (ERM)	**Project mobilisation –** Form a team to carry out the solution you've proposed. Plan more thoroughly. **Delivering capabilities:** Placing processes and mechanisms in position to help the solution to be reality. **Launch -** After testing, deploy the application from a development platform to a real system.	Studying, analysing, and utilising blockchain as a practical reference for insurance sector practitioners.
Vukolic and Marko [61], "Rethinking permissioned blockchains", 2017	• Smart contracts operate progressively, all nodes execute consensus procedures are tricky in all smart contracts, the framework is rigid, and smart-contract execution is non-deterministic, causes major challenges on current blockchain platforms, particularly recent permissioned systems.	Hyperledger fabric	• Design constraints Of Permissioned Blockchains • Using Hyperledger Fabric to Overcome Limitations	A study at the constraints that various permissioned blockchains have.
C. D. Clack, V. et al. [62], 2016	• The duties and responsibilities of those who are able to function under a contract (e.g. designated signatories) • The ability to indicate that if a specific phrase is incorporated or modified, the agreement must be forwarded to a third party for special approval.	Grigg's Ricardian Contract triple	• Presenting the essential requirements for smart legal agreements, • A smart contract's and a smart legal contract's abstract fundamental structure. • The development environment for a structured format for smart legal contracts storage and communication.	• Identification of essential requirements • Description of number of key design options.

Mitt, Sven, [71],"Blockcha in Application - Case Study on Hyperledger Fabric", 2018	• Lack of distributed cross-chain transactions • Support and documentation and inability to support today's fast delivery pace.	open-source Hyperledger Fabric	A network of nodes running Hyperledger Fabric is created and parking spot application is deployed into the network as a smart con- tract.	• On transactions, Hyperledger Fabric supports ACID features (atomicity, consistency, isolation, and durability). • Using validation and business rules in smart contract that provides strong consistency enables strong trust toward the correctness of data and the entire system.
Guy Zyskindet al.[72], 2015	Third-parties collect and control massive amounts of personal data.	mobile software development kit (SDK)	The system is made up of three components. • Users of mobile phones who want to download and use applications; services • Developers of such services who need to process personal data for operational or economic purposes, as well as • In exchange for incentives, nodes are entities methods of managing the blockchain and a distributed private key-value data store.	• Resolved users' privacy concerns during using third-party services. • The emphasis is on mobile platforms. • Applications capture high-resolution personal information on a continuous basis without the user's knowledge or consent.

4 Proposed model

Our approach is based on the concept of implementing insurance provider procedures as consensus mechanism and storing the results in a distributed blockchain platform [59].

4.1 The model's entities

The Agent, who works on behalf of the client and handles the customer's queries to the blockchain network, and the Customer, whom was protected by insurance and requires insurance policies, makes claim demands, and receives reimbursements, are the two main entities in our concept. An agent can work with many clients.

4.2 The model's components

The core elements of our architecture are a decentralized blockchain ledger B which keeps records of all transactions' execution results in (Key, Value) format, a database DB (preferably encrypted) which keeps track

of all clients' insurance contracts and transaction results in (Key, Value) feature, list of endorsers ESC who authenticate the transaction situations of blockchain network, and a set of orderers O who order the transactions sequentially and develop transaction history. Individuals are authenticated and access is controlled using cryptographic procedures.

4.3 Framework for insurance

The insurance structure is made up of assets that allow the network to interchange almost anything with monetary worth. The framework's rules for transactions are governed by smart contracts. In the insurance blockchain network, a block is formed when peer nodes in the validator set V reach consensus on a group of transaction results [105]. Every smart contract has endorsement (or verification) logic that defines the conditions under which it can execute a transaction. The endorsement logic is performed out by a group of endorsers ESC who examine whether contract criteria are met using the blockchain.

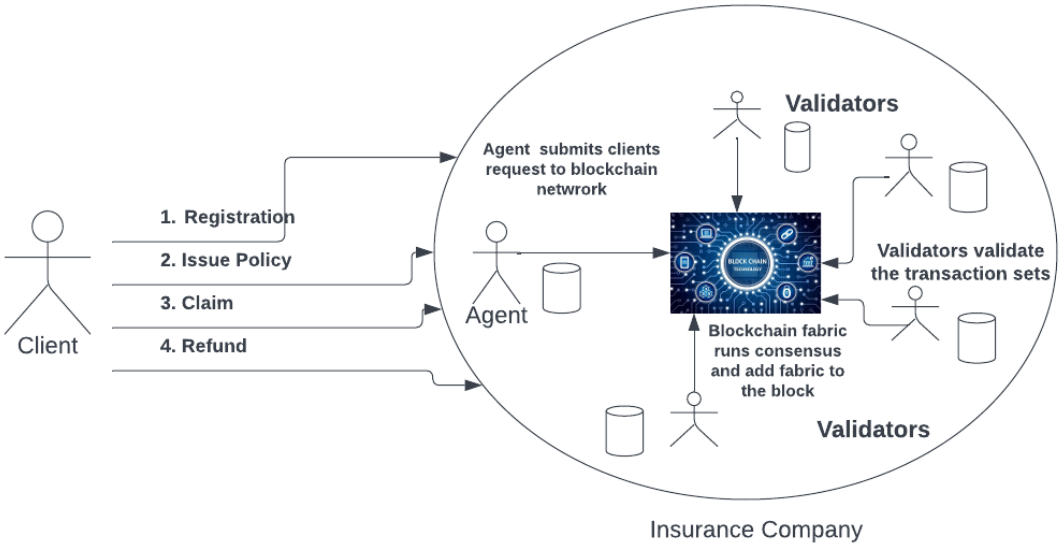

Figure 4: Insurance blockchain framework system model.

4.4 Insurance business model

We'll look at a situation in which the major processes (transactions) are normal insurance operations such as registration of client, assignment of policy, payment of premium, submission of claim, processing refund, and so on. Each transaction is recorded on the blockchain, ensuring that clients do not unfairly accuse the insurer and that the insurer is held responsible for all of its activities. The framework's core workflow is depicted in Figure 5.

Each smart contract is unique. SC_j has a group of endorsers called ESC_j who sign off on the contract's transactions. The word object relates to the client's or policy's attributes. The format of an object is determined during the instantiation of a smart contract. Function f is used to build an object from its properties and function f is used to produce composite keys (primary) from the ID (s). The key's function is to obtain specific object(s) from the database that correspond to the ID(s). We also use partial composite keys (not primary) to get a set of objects from the database in our system. As follows, we go over each contract in depth.

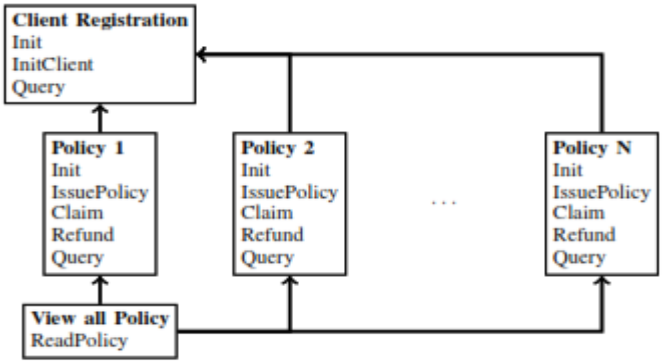

Figure 5: Smart contracts for insurance processes.

Client registration: Clients are registered in the insurance system via smart contracts. During the initialization of the database DB, a structure for the client object (C_o) is created (Algorithm 1). Client attributes such as $C_{id's}$ unique id are utilized as keys, while other client attributes will be used as values.

Algorithm 1: Client Registration: Initialization
Input: Peer Nodes: {$P0, P1, ……., Pi$ }
Endorsement Policy: OR ($P0, ..., Pi$)
1. $C_{OS} \leftarrow (C_{id}, C_{name}, C_{age}, C_{gender}, C_{contact}, C_{history})$;
2. Create the structure C_{OS} in database DB;

An agent creates composite key C_{keyc}, and client object Co is constructed using C_{keyc}used to register a customer (Algorithm 2).

Algorithm 2: Client Registration: InitializationClient
Input: Client structure C_{OS} and agent id A_{id}
1. $C_{keyc} \leftarrow f(A_{id}, C_{id})$;
2. $C_0 \leftarrow \beta\ (S_{Co})$;
3. Store(C_{keyc}, C_o)in DB;

To obtain specific customer information, an agent A of insurance must produce a composite key C_{keyc} (Algorithm 3).

Algorithm 3: Client Registration: Query
Input: Agent id A_{id} and Client unique id C_{id}
Output: Client object C_o
1. $C_{keyc} \leftarrow f(A_{id}, C_{id})$;
2. Search for C_{keyc} in DB;
3. Retrive corresponding C_o if it exits or return Error;

If an agent wishes to access all of his or her customers, he or she can create a partly composite key PCkey with just his or her personal id Aid and use it to scan the database DB.

Policy: Policy issuance, claims, and reimbursements are all part of a smart contract. Structures of policy and policy clients P_S, P_{CS} are created in database DB at startup (Algorithm 4), where amnt, acct, and date on which the amount claimed, indicator of claim acceptance (yes or no), and submission date of claim, respectively.

Algorithm 4: Policy: Initialization
Input: Peer Nodes: {$P0, P1, ……., Pi$ }
Endorsement Policy: OR ($P0, ..., Pi$)
1. $P_S \leftarrow (P_{id}, P_{name}, P_{premium}, P_{reimburse}, P_{term})$;
2. $P_{CS} \leftarrow (P_{id}, C_{id}, amnt, acct, date)$;
3. Create the structure P_S and P_{CS} in database DB;

Client c selects policy P (id P_{id}) from the available policies and pays a premium $C_{premium}$ to the agent A id (A_{id}) in the policy issuing process (Algorithm 5). If the transaction passes all of the regular tests and verifications, the database creates and saves a policy client object called P_{co}.

Algorithm 5: Policy: PolicyIssue
Input: A_{id}, C_{id}, P_{id}, $C_{premium}$
1. Query DB with P_{id} to check if P_{co} already exits;
2. Query smart contract of client C_{sc} to check client C with id C_{id} is registered to agent A with id A_{id};
3. Check if premium of client matches premium in the policy;
4. $C_{keypc} \leftarrow f(P_{id}, C_{id}, A_{id})$;
5. $P_{co} \leftarrow \beta\ (P_{id}, C_{id}, 0, Yes, date)$;
6. Store(C_{keypc}, P_{co}) in database DB;

To handle a claim, client c transmits his credentials to the appropriate agent A (Algorithm 6).The refund process is started if all of the essential conditions are verified. If the claim is accepted, the acct parameter is set to true.

Algorithm 6: Policy: Claim
Input: A_{id}, C_{id}, P_{id}, $C_{reimburse}$
1. $C_{keypc} \leftarrow f(P_{id}, C_{id}, A_{id})$;
2. Query DB using C_{keypc} to check if P_{co} exits;
3. If object P_{co} exist, check acct in P_{co}.
4. if acct=Yes then
   if amt + $C_{reimburse} \leq P_{reimburse}$ then
      Refund(A_{id}, C_{id}, P_{id}, $C_{reimburse}$);
   end
   else
      Refund(A_{id}, C_{id}, P_{id}, $P_{reimburse}$ -amt);
      acct ← No, update acct in P_{co};
   end
end

The claim process starts off the refund process. During the reimbursement process, the total amount claimed amnt in the P_{CO} is changed in DB.

Algorithm 7: Policy: Refund
Input: A_{id}, C_{id}, P_{id}, $K_{reimburse}$ from claim
1. $C_{keypc} \leftarrow f(P_{id}, C_{id}, A_{id})$;
2. Query DB using C_{keypc} to check if P_{co} exits;
3. Update amnt = amnt + $K_{reimburse}$ in P_{co};

Agent A can acquire information about his or her clients who have purchased a specific insurance P_{id} by searching the DB with a key P_{Ckey} created by A_{id} and P_{id}. This basically retrieves $\{P_{coi}\}i\in\{0,...,N\}$through the database.An agent can indeed retrieve information about each particular policy issued by the insurance company by using the Search queries method in the policy smart contract.

Algorithm 8: Policy: Query
Input: P_{id}
Output: P_o
1. Search for P_{id} in DB;
2. Retrive corresponding P_o if it exits or return Error;

4.5 Notations

The notation of the proposed scheme as follows

C_o	client object
DB	database
C_{id}	client unique id
C_{Keyc}	Composite key c
I_A	Insurance Agent A
A_{id}	Agent id
PC_{key}	Partial composite key
P_S	Policy structure
P_{CS}	Policy client structure
amt_c	claimed amount
C_{AI}	Acceptance Indicator of Claim
C_{SD}	Submission Date of Claim
P_{id}	Policy id
C	client
P_{CO}	Policy client object
C_{os}	Client Structure
C_{SC}	Client smart contract
P_o	Policy Object
AML	Anti-Money Laundering
EVM	Ethereum Virtual Machine

4.6 Transactions in the framework

Client c sends a transaction request to agent A on the proposed blockchain network. The request includes the smart contract technique and client attributes required for the function to operate. Agent A signs the transaction, which is then approved by the smart contract's endorsers. After the transaction has been validated, Agent A presents it to the ordering nodes O in order to arrange the transactions chronologically. With all of the transactions they have received, the peer nodes run the core consensus function, attaching the new records to the blockchain.

4.7 Potentail of blockchain in financial services

While many insurance businesses still rely on a conventional setup and have little knowledge of their clients, they are unable to provide the services that customers expect. The biggest drawback from the perspective of an insurance provider is the enormous gap between this method of service supply for clients and the real service provision. However, a lot of people are unaware of blockchain technology can improve the security and efficiency of the insurance process.

The process of filing insurance claims can be streamlined using blockchain technology. It is possible to rapidly and securely verify claims and process them. Additionally, blockchain is impervious to corruption and tampering because it is a distributed system.

The financial industry has a larger range of applications for blockchain [106], including:

- Smart contracts are used for real-time trade settlement at decreased cost, the issue of commercial paper, and the settling of delivery and payment.
- Eliminating errors caused by manual auditing and shortening the trade finance process with minimal middlemen in international trade
- Online application and claim settlement for insurance.

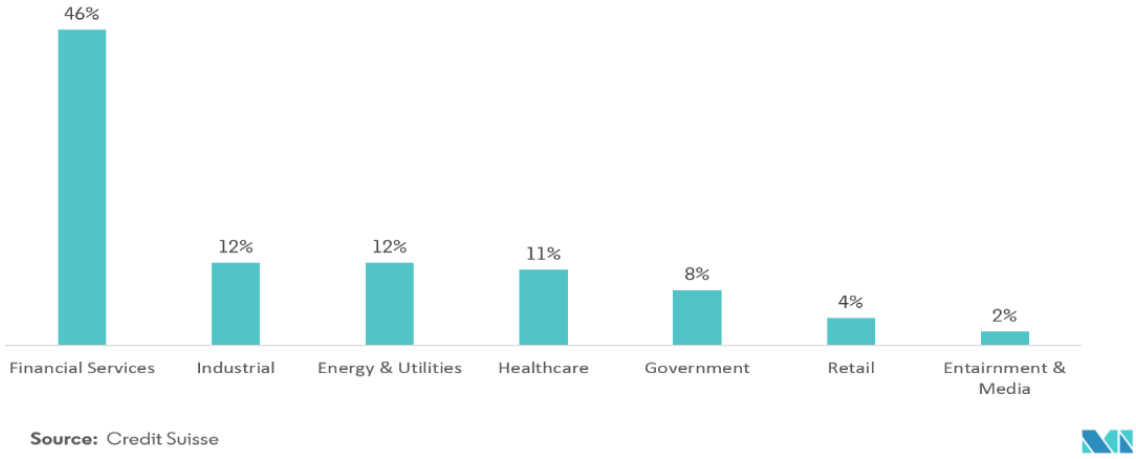

Figure 6: Potential of Blockchain among various industries, in %, 2018, source: Credit Suisse

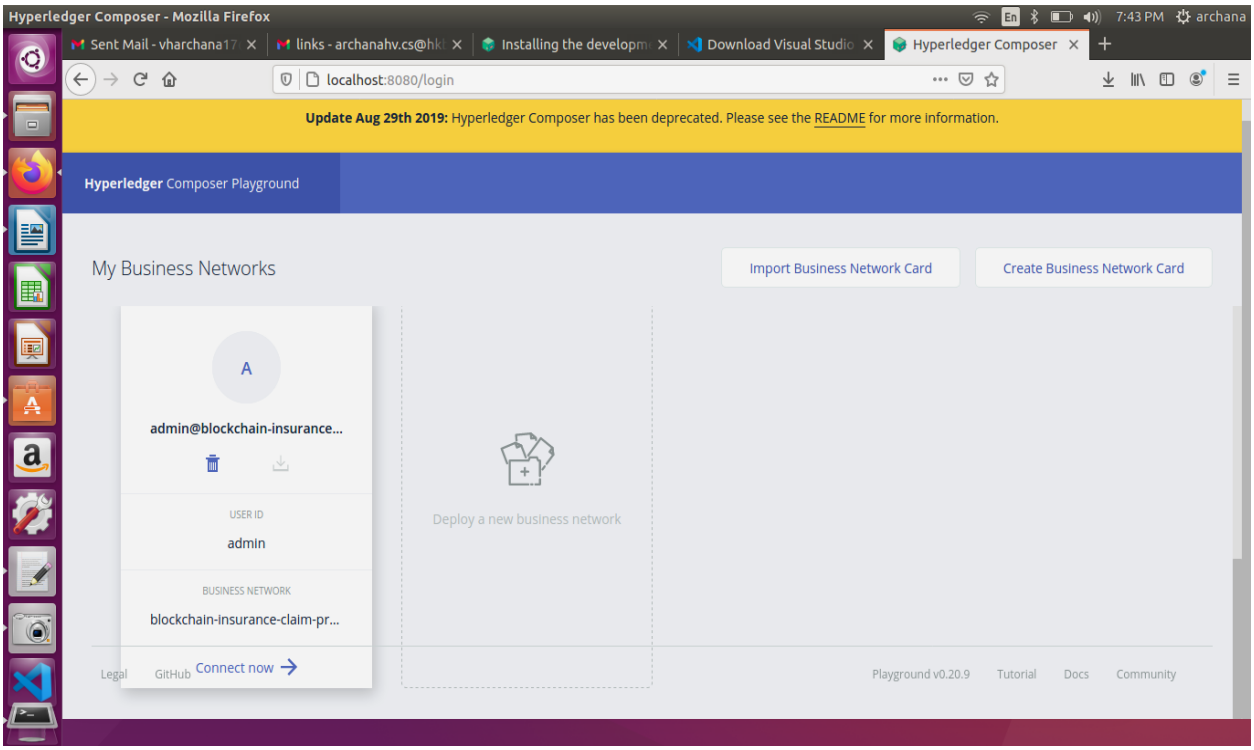

Figure 7: My business network page.

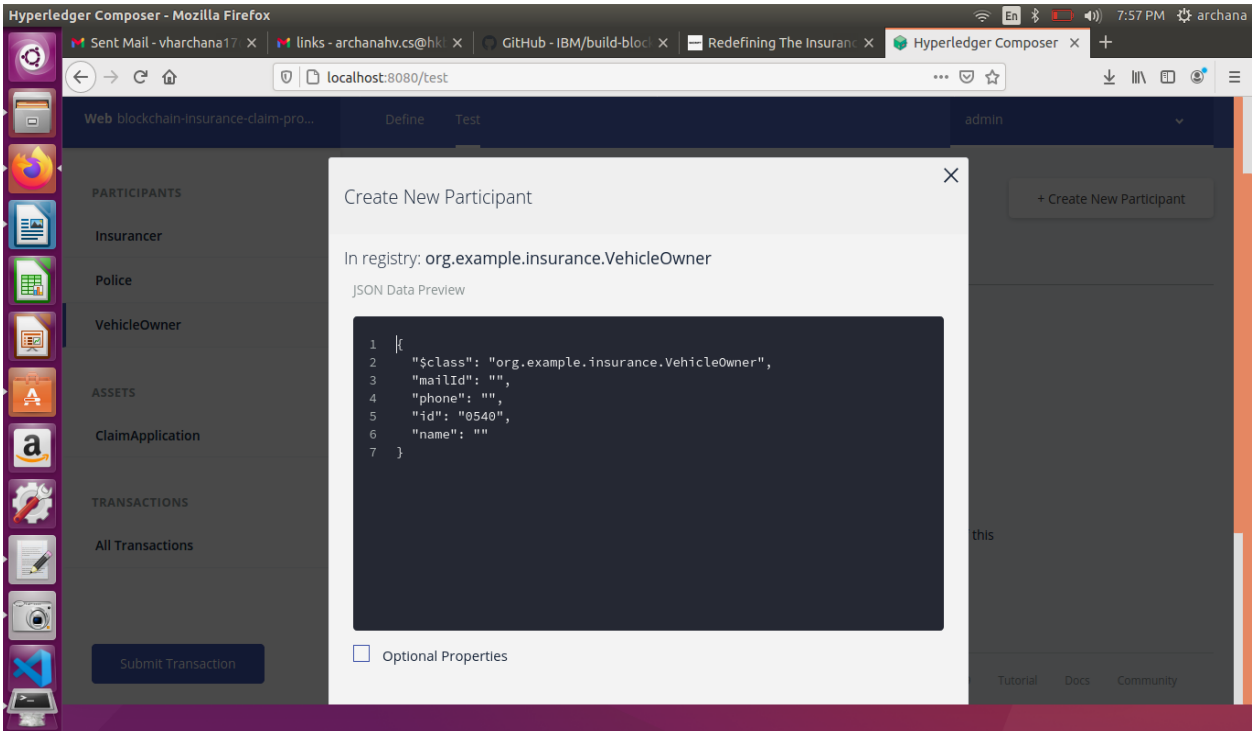

Figure 8: Screenshot of create vehicle owner participant.

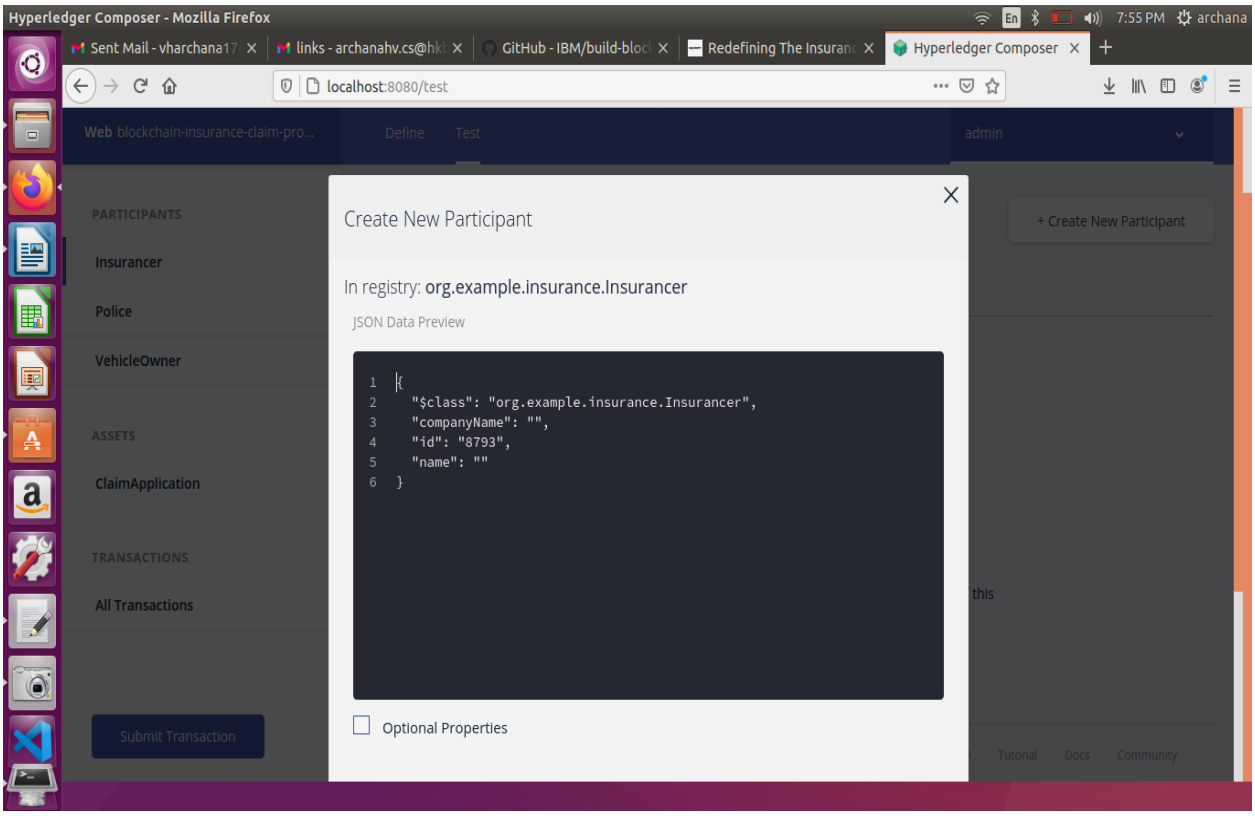

Figure 9: Screenshot of create insurance provider participant.

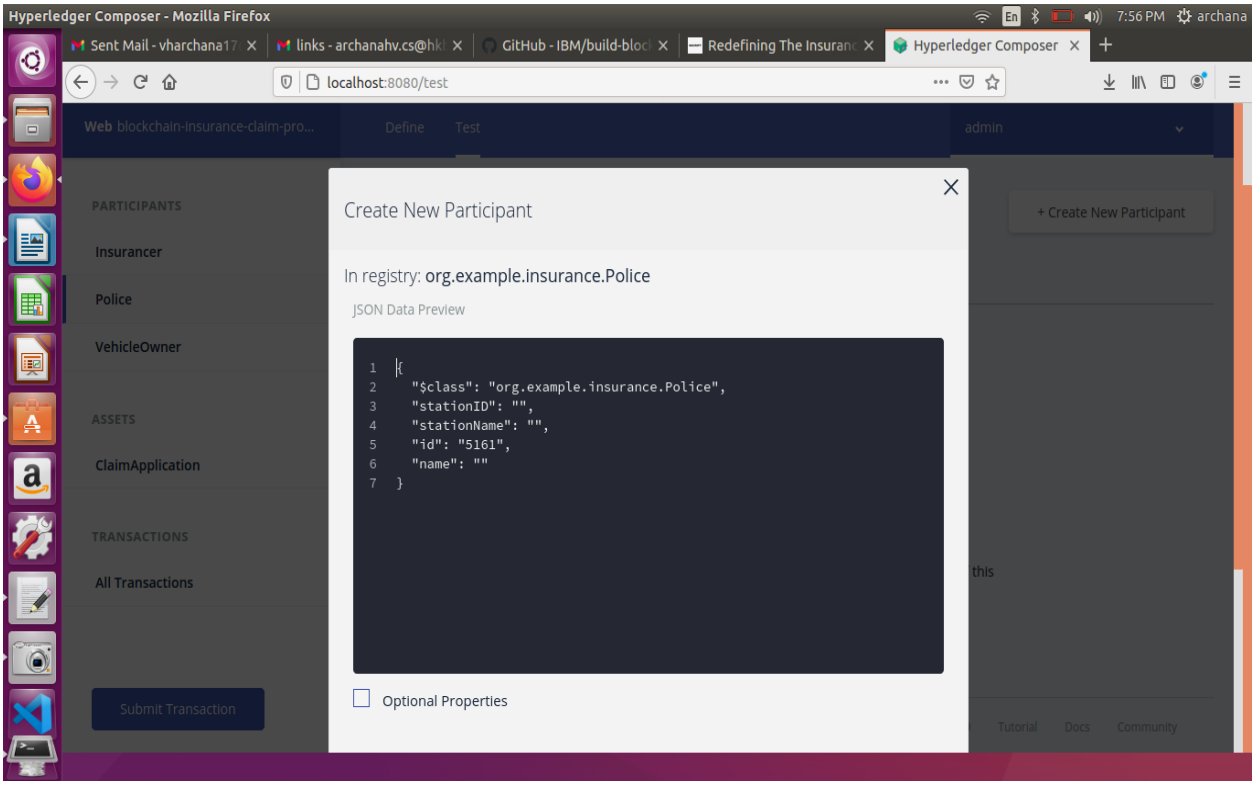

Figure 10: Screenshot of create police participant.

5 Results

Using hyperledger composer tools such as hyperledegr composer playground created business network page for insurance claim application processing.

6 Discussion

People's perceptions of blockchain technology have altered, and it has sparked a flurry of new business concepts. Plenty of insurance businesses have understood the importance of blockchain technology at this point. In the future, "blockchain + insurance" will be used at a higher level and in a bigger scope in the insurance industry. As more than just a finding of the research, the aforementioned goals were achieved:

- Smart contracts can be used to provide automatic claim settlement: From the occurrence of an insurance event through the reimbursement of payouts, all information and data will be created automatically across smart contracts, eliminating necessity investigation, hazard assessment, and evaluation.If a vehicle has insurance, for example, the record can be auto-generated and given to the insurance company, which will receive orders to pay the indemnity right away, which is better than prior insurance claims and reduces operational costs while improving customer service.
- By sharing information, you may verify a customer's identity security: Currently, the insurance sector faces the issue of workers or agents pressuring clients to accept surrender or

  survivor benefits. The main cause is that insurance companies do not have a system in place to control consumer identification. When a client receives a blockchain identity, the customer's identification information is no longer determined by the citizen ID but must be validated by all parties involved, minimizing the risk of numerous legal conflicts in the sector.
- Through entering data, you can develop a blacklist for the industry: Due to the insurance industry's low bar, a big percentage of agents breach the principle of good faith, and a large proportion of clients break laws and regulations. Practitioners and clients cannot be identified, and effective feedback cannot be delivered, because the industry lacks a blacklist platform. Blockchain data storage technology will be utilized to construct an industry blacklist as well as an open and transparent blacklist database to combat insurance fraud.
- Enhance the mutual insurance system by utilizing traceability technology. The inability of members to understand the flow of every fund is a major barrier restricting mutual insurance's expansion. Participants will have a clear awareness of each fund's spending and whereabouts thanks to the blockchain's information traceability technology,

allowing them to fully trust the mutual insurance organization. Mutual insurance groups will prosper over time if they operate in an atmosphere of complete trust.

- Defending against bogus claims by using the chain's subject information. Insurers typically lose authority of the true conditions of the insurance subject after establishing a property insurance contract. The complete process of tracking and managing the underlying assets of insurance is realized using blockchain technology to link the underlying assets to the chain, protecting the true contractual advantages and eliminating risks of repetitive insurance, target out of control, and false claims.

  In general, blockchain technology has shown a lot of promise in the insurance business. This will be especially essential in the ideological conflict and technological integration between blockchain technology and the insurance industry, as well as in "helping the real economy and avoiding financial risks."

7 Future study

The various ways in which the blockchain can transform the insurance industry:

- In FY2019, insurance crime in India was estimated to be around $45 billion. Insurer fraud, including data breaches, claim fraud, and qualifying fraud, is currently at an all-time level. The use of software created using smart contracts on the blockchain can minimize such fraudulent operations. This action will result in two things. With the use of blockchain technology, everyone will have access to information that cannot be changed.
- The decentralized technology that enables insurance firms to reduce costs and boost profits is strongly supported by the industry. The use of blockchain technology could assist save far more nearly $hundreds of millions of dollars annually in costs. Blockchain will eliminate data replication, enhancing design and validity while lowering loss or false claims. A further way that distributed ledger will cut expenses is by doing away with middlemen.
- Since then, everybody would be able to see information about the blockchain, service providers will find it simpler to communicate with one another, reducing mistake and fostering more trust between all parties. Because 3rd parties' validation is usually inadequate, the acquisition of new insurance contracts by various parties may result in misunderstanding and inconsistencies. However, access to information through a searchable, public digital network reduces waiting time and fosters trust amongst all parties. Both insurers and clients gain from open access to the real-time database since any modifications that result can be viewed and validated by all. It will be much less necessary for the insurer to rely on consultants for data, which will instantly streamline the insurance procedure.
- The peer-to-peer insurance system is a newer insurance model which is still in its early stages of development. It was created with the goal of enhancing transparency, minimizing threats, and decreasing malpractice. As a result of such a model's intricate structure, expansion concerns, and claim handling, insurance firms still encounter difficulties. Several researchers think that blockchain technology will soon help P2P insurance by minimizing fraud and enhancing scalability in order to address these problems.
- A blockchain transaction can assist insurance businesses in tracking meaningful results and, if needed, adjusting price, scheduling, or terminating. Launching innovative insurance policies, expanding their coverage, and locating customer groups in developing world and rural areas may all be done using the confirmed and confirmed data on the blockchain.

8 Conclusion

Distributed ledger technology is a potentially advanced technique for reliable online transactions, thus businesses whose operations are based on its use have a great potential. With the use of this platform, businesses engaging in multi-party companies can build responsibility based on dependable real-time information transmission. Which can provide useful and effective technologies that can be utilized in the development of systems, giving firms a competitive edge in terms of technology and operational efficiency. In this paper following contributions are made for the progress of vehicle insurance using blockchain technology. To begin with, problems related to online underwriting are solved successfully using blockchain technology. Secondly, this technology facilitates better oversight. Third, it is practical to avoid several claims for a single accident. Fourth, decentralized data access makes it easier to achieve data privacy and security. Fifth, providing time stamped transactions is beneficial in preventing fraud.

References

[1] International Association of Insurance Supervisors (IAIS). Available online: https://www.iaisweb.org/home (accessed on 20 August 2021).

[2] Raikwar, M.; Mazumdar, S.; Ruj, S.; Gupta, S.S.; Chattopadhyay, A.; Lam, K.Y. A Blockchain Framework for Insurance Processes. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018. https://doi.org/10.1109/ntms.2018.8328731

[3] Limin, H.; Jianmin, Y. Application Research of Blockchain in the Field of Medical Insurance. In Proceedings of the 2019 3rd International Conference on Economics, Management Engineering and Education Technology (ICEMEET 2019), Suzhou, China, 18–19 May 2019.

[4] Zhang, X. Design and Implementation of Medical Insurance System Based on Blockchain Smart Contract Technology. Master's Thesis, Huazhong University of Science & Technology, Wuhan, China, May 2019.

[5] Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 2018, 5, 31–37. https://doi.org/10.1109/mcc.2018.011791712

[6] Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. 2018, 5, 1184–1195. https://doi.org/10.1109/jiot.2018.2812239

[7] Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access 2018, 6, 17545–17556. https://doi.org/10.1109/access.2018.2805837

[8] Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. IEEE Commun. Mag. 2017, 55, 119–125. https://doi.org/10.1109/mcom.2017.1700879

[9] Xia, Q.; Sifah, E.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based data sharing for electronic medical records in cloud environments. Information 2017, 8, 44. https://doi.org/10.3390/info8020044

[10] Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. 2019, 6, 8770–8781. https://doi.org/10.1109/jiot.2019.2923525

[11] Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A Blockchain-based medical data sharing and protection scheme. IEEE Access 2019, 7,118943–118953. https://doi.org/10.1109/access.2019.2937685

[12] Kumar, S. (2020). Relevance of Buddhist Philosophy in Modern Management Theory. Psychology and Education, Vol. 58, no.2, pp. 2104–2111.

[13] Johari, R.; Kumar, V.; Gupta, K.; Vidyarthi, D.P. BLOSOM: BLOckchain technology for Security of Medical records. ICT Express 2021, in press. https://doi.org/10.1016/j.icte.2021.06.002

[14] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang, Y. Zhang, ―Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks, ‖ 2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc., 2018. https://doi.org/10.1109/glocom.2018.8648141

[15] Kumar, S. (2020). Relevance of Buddhist Philosophy in Modern Management Theory. Psychology and Education, Vol. 58, no.2, pp. 2104–2111.

[16] K. Panetta, ―5 trends emerge in the Gartner Hype Cycle for emerging technologies, ‖ Gartner. accessed December 8, 2020 unpublished.

[17] Blockchain.inf, ―Blockchain Charts‖ https://www. blockchain.com/ charts/, accessed September 17, 2020 unpublished.

[18] E. Kapsammer, B. Pröll, W. Retschitzegger, W. Schwinger, M. Weißenbek, & J. Schönböck, ―The Blockchain Muddle: A Bird's-Eye View on Blockchain Surveys‖, In Proc of the 20th Int Conf on Infor Integ and Web-based App & Ser (pp. 370-374). https://doi.org/10.1145/3282373.3282396

[19] K. Wang, & A. Safavi, ―Blockchain is empowering the future of insurance‖. Available at https://techcrunch.com/2016/10/29/blockchainis-empowering -the-future-of-insurance unpublished.

[20] F. Casino, T. K. Dasaklis, & C. Patsakis, ―A systematic literature review of blockchain-based applications: Current status, classification and open issues‖. Telemat Informatics 2019. https://doi.org/10.1016/j.tele.2018.11.006

[21] J. Mendling, I. Weber, W. V. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar, A. Gal, ―Blockchains for business process management-challenges and opportunities, ‖ ACM Trans. on Mgt Inf. Sys (TMIS). 2018 Feb 26;9(1):1-6. https://doi.org/10.1145/3183367

[22] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. Choo, A. Y. Zomaya, ―Blockchain for smart communities: Applications, challenges and opportunities, ‖ J of Net & Comp App. 2019 Oct 15;144:13-48. https://doi.org/10.1016/j.jnca.2019.06.018

[23] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, K. Ko, ―Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. IEEE Access. 2017 Dec 6; 6:1513-24. https://doi.org/10.1109/access.2017.2779263

[24] Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J. Med. Syst. 2018, 42,152. https://doi.org/10.1007/s10916-018-0994-6

[25] Buterin, V. A next-generation smart contract and decentralized application platform. Ethereum White Paper 2014, 3, 36.

[26] Roy, S.; Das, A.K.; Chatterjee, S.; Kumar, N.; Chattopadhyay, S.; Rodrigues, J.J. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing-based healthcare applications. IEEE Trans. Ind. Inform. 2018, 15, 457–468. https://doi.org/10.1109/tii.2018.2824815

[27] Wazid, M.; Das, A.K.; Kumari, S.; Li, X.; Wu, F. Provably secure biometric-based user authentication and key agreement scheme in cloud computing. Secur. Commun. Netw. 2016, 9, 4103–4119. https://doi.org/10.1002/sec.1591

[28] Sureshkumar, V.; Amin, R.; Vijaykumar, V.R.; Sekar, S.R. Robust secure communication protocol for smart healthcare system with FPGA implementation. Future Gener. Comput. Syst. 2019, 100, 938–951. https://doi.org/10.1016/j.future.2019.05.058

[29] Roy, S.; Chatterjee, S.; Das, A.K.; Chattopadhyay, S.; Kumari, S.; Jo, M. Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things. IEEE Internet Things J. 2017, 5, 2884–2895. https://doi.org/10.1109/jiot.2017.2714179

[30] Banerjee, S.; Odelu, V.; Das, A.K.; Srinivas, J.; Kumar, N.; Chattopadhyay, S.; Choo, K.K.R. A provably secure and lightweight anonymous user authenticated session key exchange scheme for the Internet of Things deployment. IEEE Internet Things J. 2019,6, 8739–8752. https://doi.org/10.1109/jiot.2019.2923373

[31] Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. Comput. Secur. 2019, 86, 132–146. https://doi.org/10.1016/j.cose.2019.06.002

[32] Sehgal.P, Kumar.B, Sharma.M, Salameh A.A, Kumar.S, Asha.P (2022), Role of IoT In Transformation Of Marketing: A Quantitative Study Of Opportunities and Challenges, Webology, Vol. 18, no.3, pp 1-11.

[33] Yang, J.; Li, J.; Niu, Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener.Comput. Syst. 2015, 43–44, 74–86. https://doi.org/10.1016/j.future.2014.06.004

[34] Soni, P.; Pal, A.K.; Islam, S.H. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput. Methods Programs Biomed. 2019, 182, 105054. https://doi.org/10.1016/j.cmpb.2019.105054

[35] Masdari, M.; Ahmadzadeh, S. A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems.J. Netw. Comput. Appl. 2017, 87, 1–19. https://doi.org/10.1016/j.jnca.2017.03.003

[36] Amin, R.; Islam, S.H.; Biswas, G.P.; Khan, M.K.; Kumar, N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Gener. Comput. Syst. 2018, 80, 483–495. https://doi.org/10.1016/j.future.2016.05.032

[37] Chen, L.; Lee, W.K.; Chang, C.C.; Choo, K.K.R.; Zhang, N. Blockchain based searchable encryption for electronic health recordsharing. Future Gener. Comput. Syst. 2019, 95, 420–429. https://doi.org/10.1016/j.future.2019.01.018

[38] Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inf. Secur.Appl. 2020, 50, 102407. https://doi.org/10.1016/j.jisa.2019.102407

[39] Szabo, N. Smart contracts: Building blocks for digital markets. EXTROPY J. Transhum. Thought 1996, 18, 16.

[40] Szabo, N. The Idea of Smart Contracts. 1997. Available online: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html(accessed on 20 August 2021).

[41] Vanstone, S. Responses to NIST's proposal. Commun. ACM 1992, 35, 50–52.

[42] Johnson, D.; Menezes, A.; Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inf. Secur. 2001, 1, 36–63. https://doi.org/10.1007/s102070100002

[43] Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. ACM Trans. Comput. Syst. 1990, 8, 18–36. https://doi.org/10.1145/77648.77649

[44] Sierra, J.M.; Hernández, J.C.; Alcaide, A.; Torres, J. Validating the Use of BAN LOGIC;

Springer: Berlin/Heidelberg, Germany, 2004; pp. 851–858. https://doi.org/10.1007/978-3-540-24707-4_98

[45] Hyperledger Fabric Docs. Available online: https://hyperledger-fabric.readthedocs.io/_/downloads/en/release-2.2/pdf/ (accessed on 20 August 2021).

[46] Foschini, L.; Gavagna, A.; Martuscelli, G.; Montanari, R. Hyperledger Fabric Blockchain: Chaincode Performance Analysis. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. https://doi.org/10.1109/icc40277.2020.9149080

[47] Uddin, M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. Int. J. Pharm. 2021, 597, 120235. https://doi.org/10.1016/j.ijpharm.2021.120235

[48] Marcus, M.J. 5G and IMT for 2020 and beyond. IEEE Wirel. Commun. 2015, 22, 2–3.

[49] D. E. Kouicem, A, Bouabdallah, H. Lakhlef, ―Internet of things security: A top-down survey, ‖ Computer Networks. 2018 Aug 4; 141:199-221. https://doi.org/10.1016/j.comnet.2018.03.012

[50] Q. E. Abbas, J. Sung-Bong, ―A survey of blockchain and its applications, ‖. In 2019 Int Conf on Art Intel in Inf and Comm (ICAIIC) 2019 Feb 11 (pp. 001-003). IEEE. https://doi.org/10.1109/icaiic.2019.8669067

[51] W. Liu, Q. Yu, , Li, Z., Li, Z., Su, Y. and Zhou, J., ―A BlockchainBased System for Anti-Fraud of Healthcare Insurance,‖ In 2019 IEEE 5th Int. Conf. on Compu. Commun. (ICCC) (pp. 1264-1268). IEEE. https://doi.org/10.1109/iccc47050.2019.9064274

[52] Ms. Elena Rosemaro. (2014). An Experimental Analysis of Dependency on Automation and Management Skills. International Journal of New Practices in Management and Engineering, 3(01), 01 - 06. https://doi.org/10.1109/iccc47050.2019.9064274

[53] H. Kim, M. Mehar, ―Blockchain in Commercial Insurance: Achieving and Learning Towards Insurance That Keeps Pace in a Digitally Transformed Business Landscape, ‖ SSRN Electron J 2019. https://doi.org/10.2139/ssrn.3423382

[54] M. Mainelli, B. Manson ―Chain reaction: How blockchain technology might transform wholesale insurance, ‖ How Blockchain Technology Might Transform Wholesale Insurance-Long Finance. 2016 Aug 1. Available at SSRN: https://ssrn.com/abstract=3676290.

[55] L. S. Howard, ―Blockchain insurance industry initiative B3i grows to 15 members, ‖ Insurance Journal. 2017; 6:2017.

[56] T. Q. Nguyen, A. K. Das, L. T. Tran, ―NEO Smart Contract for Drought-Based Insurance, ‖ 2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019, 2019. https://doi.org/10.2139/ssrn.3423382

[57] Y. Guo, Z. Qi, X. Xian, H. Wu, Z. Yang, J. Zhang, L. Wenyin, ―WISChain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security, ‖ Proc. 2018 1st IEEE Int. Conf. Hot Information-Centric Networking, HotICN 2018, 2019. https://doi.org/10.1109/hoticn.2018.8606011

[58] Anokye Acheampong AMPONSAH1 *, Professor Adebayo Felix ADEKOYA2m, Benjamin Asubam WEYORI3Blockchain in Insurance: Exploratory Analysis of Prospects and Threats, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 1, 2021. https://doi.org/10.14569/ijacsa.2021.0120153

[59] Mayank Raikwar∗, Subhra Mazumdar†, Sushmita Ruj†, Sourav Sen Gupta†, Anupam Chattopadhyay∗, and Kwok-Yan Lam∗ "A Blockchain Framework for Insurance Processes", 978-1-5386-3662-6/18/$31.00 ©2018 IEEE. https://doi.org/10.1109/ntms.2018.8328731

[60] D. Popovic, C. Avis, M. Byrne, C. Cheung, M. Donovan, Y. Flynn, C. Fothergill, Z. Hosseinzadeh, Z. Lim*, J. Shah, Understanding blockchain for insurance use cases A practical guide for the insurance industry. Presented at the Sessional Meeting of the Institute and Faculty of Actuaries [Staple Inn], 03 February 2020. https://doi.org/10.1109/ntms.2018.8328731

[61] Vukolic and Marko, "Rethinking permissioned blockchains" in ´ Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ser. BCC '17. New York, NY, USA: ACM, 2017. https://doi.org/10.1145/3055518.3055526

[62] C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: essential requirements and design options", arXiv preprint arXiv:1612.04496, 2016.

[63] Ms. Nora ZilamRunera. (2014). Performance Analysis on Knowledge Management System on Project Management. International Journal

of New Practices in Management and Engineering, 3(02), 08 - 13. https://doi.org/10.17762/ijnpme.v3i02.28

[64] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016. https://doi.org/10.1109/access.2016.2566339

[65] I. Nath, "Data exchange platform to fight insurance fraud on blockchain," in 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), Dec 2016, pp. 821–825. https://doi.org/10.1109/access.2016.2566339

[66] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017, pp. 9–14. https://doi.org/10.1145/3055518.3055531

[67] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in Consumer Electronics (ICCE), 2016 IEEE International Conference on. IEEE, 2016, pp. 467–468. https://doi.org/10.1109/icce.2016.7430693

[68] Baliga, A. (2017). Understanding Blockchain Consensus Models. Retrieved October 2019, from https://www.persistent.com/wp-content/uploads/2018/02/wp-understanding-blockchainconsensus-models.

[69] Buterin, V. (2013, December). A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved December 2019, from https://github.com/ethereum/wiki/wiki/WhitePaper.

[70] Aarti Patki1 · Vinod Sople2, "Indian banking sector: blockchain implementation, challenges and way forward", Journal of Banking and Financial Technology, 11 May 2020. https://doi.org/10.1007/s42786-020-00019-w

[71] Mitt, Sven, "Blockchain Application - Case Study on Hyperledger Fabric", 2018.

[72] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland "Decentralizing Privacy: Using Blockchain to Protect Personal Data", 2015. https://doi.org/10.1109/spw.2015.27

[73] H. Sukhwani, J. M. Martnez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)," in 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Sept 2017, pp. 253–255. https://doi.org/10.1109/srds.2017.36

[74] https://www.policybazaar.com/motor-insurance/general-info/articles/car-insurance-claim-process-guide/

[75] Blog written by Ashwin SoorajKudwa, Blockchain: Life and Vehicle Insurance, 08/23/18

[76] https://www.marutitech.com/artificial-intelligence-in-insurance/

[77] P. K. Sharma et al, "Software Defined Fog Node Based Distributed Blockchain Cloud Architecture", IEEE Access, volume 6, February 1, 2018. https://doi.org/10.1109/access.2017.2757955

[78] Mrs. Monika Soni. (2015). Design and Analysis of Single Ended Low Noise Amplifier. International Journal of New Practices in Management and Engineering, 4(01), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/33. https://doi.org/10.17762/ijnpme.v4i01.33

[79] L.Wang and R. Ranjan, ``Processing distributed Internet of Things data inclouds," IEEE Cloud Comput., vol. 2, no. 1, pp. 76_80, Jan. 2015. https://doi.org/10.17762/ijnpme.v4i01.33.

[80] M. Chiang and T. Zhang, ``Fog and IoT: An overview of research opportunities," IEEE Internet Things J., vol. 3, no. 6, pp. 854_864, Dec. 2016. https://doi.org/10.1109/jiot.2016.2584538

[81] Valentina Gatteschi et al., "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?", Future Internet 2018, 10, 20. https://doi.org/10.3390/fi10020020

[82] Fran Casino et. al., "A systematic literature review of blockchain-based applications: Current status, classification and open issues", 22 November 2018, 0736-5853/ © 2018 The Authors. Published by Elsevier Ltd. https://doi.org/10.1016/j.tele.2018.11.006

[83] Pradip kumarsharma et. al., "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT", VOLUME 6, 2018. https://doi.org/10.1109/access.2017.2757955

[84] Jin Ho Park et. al, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", 2017, 9, 164; doi:10.3390/sym9080164.

[85] Min Xu, Xingtong Chen and Gang Kou, "A systematic review of blockchain", Xu et al. Financial Innovation (2019).

[86] Hany F. Atlam et.al., "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues", 2017 IEEE International Conference on Internet of Things. 2017 IEEE. https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2017.105

[87] Ms. Pooja Sahu. (2015). Automatic Speech Recognition in Mobile Customer Care Service. International Journal of New Practices in Management and Engineering, 4(01), 07 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/34. https://doi.org/10.17762/ijnpme.v4i01.34

[88] X. Sun, N. Ansari, and R. Wang, ``Optimizing resource utilization of a data center," IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2822_2846,4th Quart., 2016. https://doi.org/10.1109/comst.2016.2558203

[89] K. Valtanen, J. Backman, S. Yrjola, ―Blockchain-Powered Value Creation in the 5G and Smart Grid Use Cases, ‖ IEEE Access 2019. https://doi.org/10.1109/access.2019.2900514

[90] F. Z. Meskini, R. Aboulaich, ―A New Cooperative Insurance Based on Blockchain Technology: Six Simulations to Evaluate the Model, ‖ 2020 Int. Conf. Intell. Syst. Comput. Vision, ISCV 2020, 2020. https://doi.org/10.1109/iscv49265.2020.9204170

[91] A, Tapscott, D. Tapscott, ―How Blockchain Is Changing Finance, ‖ Harv Bus Rev 2017.

[92] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, K. A. Ogudo, ―A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications, ‖ Int J e-Collaboration 2020. https://doi.org/10.4018/ijec.2020010102

[93] Mr. Dharmesh Dhabliya, Ms. Ritika Dhabalia. (2014). Object Detection and Sorting using IoT. International Journal of New Practices in Management and Engineering, 3(04), 01 - 04. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/31. https://doi.org/10.17762/ijnpme.v3i04.31

[94] S. Olnes, J. Ubacht, M. Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov Inf Q 2017. https://doi.org/10.1016/j.giq.2017.09.007

[95] P. K. Singh, R. Singh, G. Muchahary, M. Lahon, S. Nandi, ―A Blockchain-Based Approach for Usage Based Insurance and Incentive in ITS, ‖ IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, 2019. https://doi.org/10.1109/tencon.2019.8929322

[96] Y. C. Chen, Y. P. Chou, Y. C. Chou, ―An image authentication scheme using Merkle tree mechanisms, ‖Futur Internet 2019. https://doi.org/10.3390/fi11070149

[97] L. S. Sankar, M. Sindhu, M. Sethumadhavan, ―Survey of consensus protocols on blockchain applications, ‖ 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017, 2017. https://doi.org/10.1109/icaccs.2017.8014672

[98] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. Choo, A. Y. Zomaya, ―Blockchain for smart communities: Applications, challenges and opportunities, ‖ J of Net & Comp App. 2019 Oct 15;144:13-48. https://doi.org/10.1016/j.jnca.2019.06.018

[99] J. Lake, Understanding cryptography 's role in blockchains 2019. Unpublished.

[100] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, G. Das, ―Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems, ‖ IEEE Consum Electron Mag 2018. https://doi.org/10.1109/mce.2018.2816299

[101] J. J. Bambara, P. R. Allen, K. Iyer, R. Madsen, S. Lederer, M. Wuehler, Blockchain: A practical guide to developing business, law, and technology solutions. McGraw Hill Professional; 2018 Feb 16.

[102] T. K. Sharma, Public Vs. Private Blockchain: A Comprehensive Comparison 2019 unpublised.

[103] Mycryptopedia, 2018, Consortium Blockchain Explained, unpublished.

[104] C. Saraf, S. Sabadra, ―Blockchain platforms: A compendium, ‖ IEEE Int. Conf. Innov. Res. Dev. ICIRD 2018, 2018. https://doi.org/10.1109/icird.2018.8376323

[105] C. Christian, "Blockchain, cryptography, and consensus," 2017.