BLOCKCHAIN TECHONOLOGY FOR SECURING INSURANCE DATA AND AUTO-INSURANCE CLAIM

by

HARSHAVARDHANA M	**2015103012**
HARISH S	**2015103593**
JAGAN M	**2015103594**

A project report submitted to the

FACULTY OF COMPUTER SCIENCE

AND ENGINEERING

In partial fulfilment of the requirements for

the award of the degree of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
ANNA UNIVERSITY, CHENNAI – 25
FEBRUARY 2019

Problem Statement

Traditional health insurance system possesses high possible fraudulent or duplicate claims, possible financial loss during digital transactions, complex and high time consuming verification processes. This is the challenge the insurance industry faces and it possess transactional and contractual complexity. The aforementioned problem is an ideal application opportunity for Blockchain implementation. Blockchain can provide significant benefits to the private consortium and all of its participants including the insured customers. Blockchain can address the fundamental challenges of managing and dragging the distributed digital transactions of the problem scenario, as they are extremely secured, manageable and high-speed transactions. A lot of work goes into checking whether a health insurance claim is fraudulent or not. Using the consensus property of Blockchain, we can reduce the work that goes into checking if a claim is fraudulent or not.

Introduction

Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. the linked blocks form a chain. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. Blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. The core technological innovation of blockchain is the consensus which provides a high guarantee that an advisory cannot alter a transaction once this transaction is sufficiently deep in the blockchain, assuming honest nodes control the majority of the nodes in the system. Although blockchain records are not unalterable, blockchain may be considered secure by design and exemplify the distributed computing system with high Byzantine fault tolerance.

Blockchain technology can be utilized in multiple industries including Financial Services, Healthcare, Government, Travel and Hospitality, Retail and CPG. Blockchain can play a key role in the health care sector by increasing the privacy, security and interoperability of the health care data. It holds the potential to address many interoperability challenges in the sector and enable secured sharing of data among the various entities and people involved in the process.

The primary use of blockchain today is a distributed ledger for cryptocurrencies, most notably bitcoin. Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. Major portions of the financial industry are implementing distributed ledgers for using banking and this is occurring faster than expected. Banks are interested in this technology because it has potential to speed up bank office settlement systems. Permissioned blockchain use an access control layer to govern who has access to the network. In contrast to public blockchain networks, validators on private blockchain networks are vetted by the network owner.

Decentralization

By storing data across its peer-to-peer network the blockchain eliminates a number of risks that come with data being held centrally. It has no central point of failure. Blockchain security measures include use of public key cryptography. The shared and distributed ledger is an immutable record of all transactions of the network, a record that all network participants can access. With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.

Data Security

Blockchain technology can be integrated into multiple areas. The primary use of blockchain today is a distributed ledger for cryptocurrencies, most notably bitcoin. Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network are both based on blockchain. Major portions of the financial industry are implementing distributed ledgers for using banking and this is occurring faster than expected. Banks are interested in this technology because it has potential to speed up bank office settlement systems.

Smart Contract

Smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation. It eliminates the hassles and delays inherent in contracts by building the contracts into the transaction.

Consensus

In a business network where participants are known and trusted, transactions can be verified and committed to the ledger through various means of consensus including Proof of Stake, Proof of Work, Multi-Signature and Practical Byzantine Fault Tolerance. It ensures that all transactions are validated before being appended to the blockchain and the blockchain itself is highly tamper-resistant.

Blockchain in Insurance

Insurance providers need an efficient way to process claims, verify that an insurable event (such as an accident) actually occurred, and provide customers with fair and timely pay-outs. With automated insurance claim processing, policy conditions are written into a smart contract stored on the blockchain and connected to publicly available data via the Internet. Whenever an insurable events occurs and is reported by a trusted source, the insurance policy is automatically triggered, the claim is processed according to the terms of the policy specified in the smart contract, and the customer is paid. The benefits for insurance are (i) Eliminates the cost of processing insurance claims (ii) Reduces the opportunity for insurance fraud (iii) Improves customer satisfaction.

Claims are often submitted without all the required supporting detail, so payer(s) need to request additional detail, which adds costs and delays to the settlement process. Further, matching up the claims with the supporting information is challenging for all parties involved. Blockchain can simplify this complicated and time-consuming process and automate the collection and sharing of information.

Blockchain facilitates the development and creation of ‘smart contracts’ and has the potential to reduce costs, to accelerate the underwriting process and also to expedite claims handling processes — again leading to savings in administrative and operational costs. Blockchain may have significant impact upon the efficiency and processes of data collection and sharing, upon the way certain insurance contracts are transacted and how claims in relation to those contracts are managed. The use of ‘smart contracts’ in underwriting and claims management processes is another important innovation in the blockchain environment. It provides excellent experiences to clients receiving their money even before they claim it, since a smart contract could automatically trigger a reimbursement as soon as a given event occurs and reduce human effort.

Summary of Related Works

Artificial Intelligence and Automation in Insurance Industry

Automation and AI have transformed almost every sector across the world, and the insurance industry is no exception. According to Accenture’s Technology Vision for Insurance 2017, 94% of “insurance executives agree that adopting a platform-based business model and engaging in ecosystems with digital partners are critical to their business.” In 2016, 35% of insurers reported over 15% in cost savings from automating systems and processes in the last two years. Automation of more complex tasks (other than compliance checks or data entry) such as property assessment and personalized consumer interactions over the years has brought frictionless experiences and cut down redundancy. Employing AI in the claims process has brought better quality and lesser time for handling. AI algorithms can save millions lost to fraudulent claims by scouring data and identify errors and trends. The future is definitely touchless. Machine learning can be useful in evaluating risk and identifying cross-selling opportunities. Online-only insurance technology companies, uses AI, machine learning, and big data to "simplify insurance, price risk more finely and distribute cheaply to a mass market via the internet." For automated claims processing and property assessment, P&C insurance providers are using drones for more accurate information and faster processing.

Internet of Things in Insurance

IoT devices, sensors, and telematics have been fast gaining adoption in the insurance sector. Several data streams and sources (wearables, sensors embedded in vehicles, location-based sensors, GIS) coupled with advanced analytics can help insurers improve risk assessment, price policies based on real data in real time, and proactively encourage customers to buy policies for loss prevention.

More usage-based insurance models for connected vehicles and precise actuarial models are expected with the huge amounts of data (or touchpoints) available thanks to today's amazingly connected world. In the auto insurance sector, for example, the data (speed, time, braking patterns, distance) gives buyers more say in their premiums; risky driving patterns can serve as warning signs. Blockchain can be the "network connecting and ordering data from the multiple devices and apps involved in a multidimensional process." (EY, 2016) It can help manage the huge volumes by ensuring P2P device communication.

Companies such as Aviva and State Farm urge customers to invest in home sensors (others such as FitSense deal with fit tech to help insurers), incentivizing them to help prevent risk to self (e.g. elderly care) and property. For example, Neos Ventures, UK's first connected home insurance specialist, provides preventative smart technology as part of the policy.

Along with the real-time data and advanced digital capabilities, insurers enjoy better customer relationships and risk management, quicker processing of claims, and selling bundled products. Automating and streamlining so many data-driven insurance-related processes such as pricing policies, underwriting, approximating required reserves, and risk profiling help providers come up with valuable, easy-to-use, and affordable products and services.

Blockchain

In the cryptocurrency scenario, the issue between payer and payee is that there has to be a trusted third party to verify the double-spending of money and validate the transactions. It leads to a state where all the participating people has to agree on the trusted authority. The fate of the entire community is given to a single company that run the trusted authority. To make all participants of the network to agree upon transactions that were previously made it is important for all the participants to know all previous transactions. Thus a technology named blockchain is proposed to store all transactions in a public ledger in a tamper-resistant manner. A earlier cryptocurrency called bitcoin used a hard to solve Proof of Work to validate the transactions. Number of transactions bundled in a block is hashed in such a way that the hash contains some leading zeros. The computational complexity increases when number of leading zeros increases. Thus the whole network is given a CPU based voting permission. If the network contains more honest nodes controlling larger CPU power, then the network will have trusted larger chain of blocks.

Financial Applications of Blockchain

Stock Exchanges

The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. It is now theoretically possible for companies to directly issue the shares via the blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain. NASDAQ Private Equity has joined hands with a San Francisco based start-up to implement private equity exchange on top of blockchain.

Asset Management

Assets which can be uniquely identified by one or more identifiers that are difficult to destroy or replicate can be registered in blockchain. This can be used to verify ownership of an asset and also trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone, especially insurers. Everledger is a company which creates permanent ledger of diamond certification and the transaction history of the diamond using blockchain. The verification of diamonds can be done by insurance companies, law enforcement agencies, owners and claimants easily using this blockchain.

Non-Financial Applications of Blockchain

Health Care

Estonia is implementing a blockchain based health care management record to store it in a hacker-proof manner. In that project, logs of access of health care data and audit data is stored in blockchain. All the users can see when the data is accessed but access log cannot be modified.

Music Industry

The process by which music royalties are determined has always been a convoluted one, but the emergence of the internet has made it even more complex giving rise to the demand of transparency in the royalty payments by both artists and song writers. This is where the blockchain can play a role. The technology can help maintain a comprehensive and accurate distributed database of music rights ownership information in a public ledger. In addition to rights ownership information, the royalty split for each work can be determined by smart contracts.

Keyless Security Infrastructure

Namecoin is an alternative blockchain technology that is used to implement a decentralized version of Domain Name Server. Current DNS servers are controlled by governments and large corporations, and could abuse their power to censor, hijack, or spy on a consumer's internet usage. With blockchain technology internet's DNS is maintained in a decentralized manner. Public Key Infrastructure technology is widely used for centralized distribution and management of digital certificates. Every device needs to have root certificate of the Certificate Authority to verify digital signature. While PKI has been widely deployed and incredibly successful, dependence on a CA makes scalability an issue. The characteristics of the blockchain can help address some of the limitations of the PKI by using Keyless Security Infrastructure.

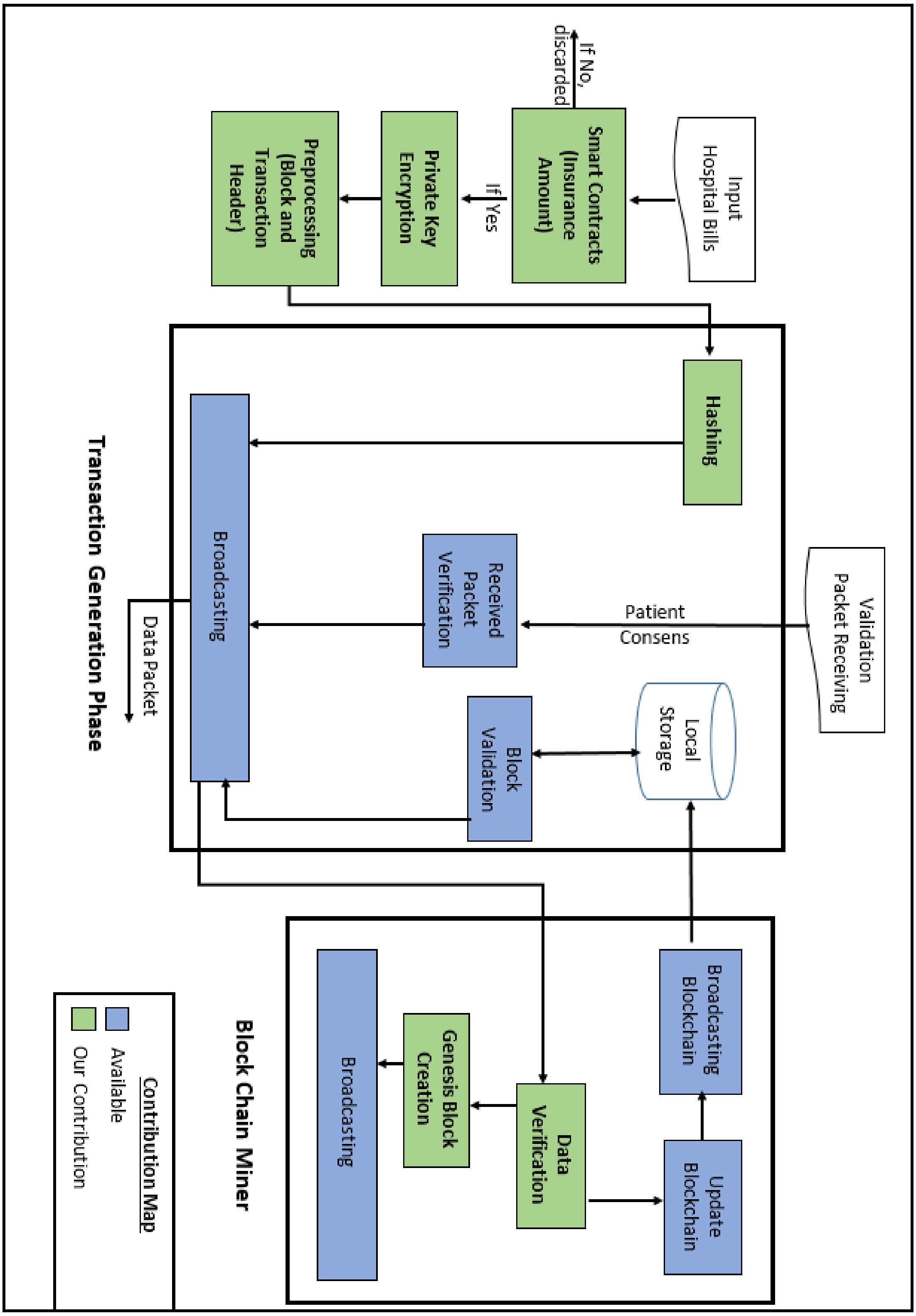
Blockchain in IoT

Blockchain-IoT combination can work perfectly. For once us cases can be derived as follows.

1. Facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices.
2. Allows us to automate in a cryptographically verifiable manner several existing, time-consuming workflows.

There are some practical deployment difficulties in deploying IoT blockchain. These difficulties range from transactional privacy to the expected value of the digitized assets traded on the network. Blockchain-IoT combination can be powerful and can cause significant transformations across several industries, paving the way for new business models, novel and distributed application, yet this blockchain model has some restrictions like scalability. The authors have talked about minimizing the data copied in a blockchain. They claim that security is not compromised using 51% attack yet minimizing the total data copied among the nodes. A new model of blockchain is proposed for limited memory availability using B language.

Architecture Diagram



Flow Diagram

Modules Description

Our module has three phases.

- Pre-processing Phase
    1. Smart Contracts
    2. Private Key Encryption
    3. Preprocessing

- Transaction Generation Phase
    1. Hashing
    2. Received Packet Verification
    3. Block Validation
    4. Broadcasting

- Blockchain Miner
    1. Data Verification
    2. Genesis Block Creation
    3. Broadcasting Blockchain

PREPROCESSING PHASE

In this phase we have implemented smart contracts to decide whether to initiate the transaction or not. We have also encrypted the data using RSA algorithm to restrict the access.

- **Smart Contracts** – it takes the Bill ID and Bill amount as input. Smart Contracts automatically claims the patient bill amount whose insurance amount must be less than the insurance limit. And if the insurance amount is less than or equal to the insurance limit the data is sent to the encrypted phase if not it is discarded.

```
Begin
    For each transaction do
        let input:= getbillamount();
        if ( input <= insurance limit)
            encrypt the input data
        else
            discard
   done
End
```

- **Private Key Encryption** – It takes the patient treatment details as the input and encrypts the data using RSA Algorithms and produces the encrypted data.

   1. *Choose two different large random prime numbers p and q*
   2. *Calculate n where* $n=p*q$

      n is the modulus for the public key and the private keys
   3. *Calculate the totient* $\Phi(n)$ *where* $\Phi(n)=(p-1)*(q-1)$
   4. *Choose an integer e such that* $1<e<phi(n)$ *and e is co-prime and e and* $\Phi(n)$ *share no factors other than 1*

      $gcd(e, \Phi(n))=1$
   5. *Calculate d to satisfy the congruence relation* $de\Xi 1(\mathrm{mod}\ \Phi(n))$ *i.e.,* $de=1+k*\Phi(n)$ *for some integer k where d is kept as the private key exponent*

- **Preprocessing** – It takes the encrypted data as input and checks all the necessary data to instantiate a claim that has been uploaded or not and produces the block containing the block header and transaction header

```
if (values not equal NULL)
    append previous block's hash value to the current block
    append date and time of occurrence of transactions
else
    upload bills
```

TRANSACTION GENERATION PHASE

Once the treatment has been made then patient's details should be stored in blockchain. This phase contains hashing the patient details, treatment details and verification processes. Every transaction begins in this phase.

- **Hashing –** It takes the block containing the block header and transaction header as the input and hashes the data in the block using SHA-256 algorithm.

```
Begin
   Det := Givedata(Did)
   Hval := ComputeHash(Det)
   Kbpub := Public key of the peer;
   TxData := encrypt ( Det, Kbpub);
   TxData := append (TxData,Hval);
End
```

- **Received Packet Verification** - In blockchain every transaction has to be verified by other peers in a network to take appropriate decision. The following steps has to be done in this module

  - *The receiving peer obtains the public key of the peer generating transaction.*
  - *The peer decrypts the received packet using the public key obtained.*
  - *The peer computes the hash of the message.*
  - *If H = Hash, broadcast the transaction to the other peers else discard the transaction.*

- **Block Validation** - This module is available in every peer of the blockchain network. The peers in the network obtains the newly mined block from the miner. They check the validity of the block. If valid they update their blockchain else discards the new block. Procedure for the block validation is given below

  - *The peer checks whether the block contains valid transactions by checking each transaction's validity.*
  - *If any invalid transactions it discards the block.*
  - *Else It checks whether the block header contains the same number of leading zeros as mentioned in the consensus algorithm.*
  - *If lesser or greater number of zeros it discards the block.*

- *Else It checks whether the new block correctly references the hash of the peer’s last block.*
- *If it correctly references updates blockchain and then it broadcasts this new updated blockchain else discards this new block.*

BLOCKCHAIN MINER

In this phase new block will be generated by the miner by solving proof of work and updates the blockchain. This module contains genesis block creation, data Verification, broadcasting blockchain.

- **Data Verification -** This module finds a hash below a targeted hash value (PoW). We have four types of algorithms for consensus in blockchain. Consensus is the only algorithm we can use. Four types of algorithms are:

  1. Practical Byzantine Fault Tolerance Algorithm
  2. Proof-of-work
  3. Proof-of-Stake
  4. Delegated Proof-of-Stake

  We have done block diagram with Proof of Work.

  Consensus Algorithm - The proof of work is a computational client puzzle where computation power is needed to solve the puzzle and the nodes who solve the puzzle first will add the block to blockchain and will get a reward in mining network. Once a block is completed, it will be broadcasted to all the mining nodes and all of them start to mine. The miner node who solves that first will add that block to block chain.

```
set target to currenttarget
broadcast target
Set nonce to 0
While hash  target AND NoPoWCompleteSignal; do
    nonce = nonce + 1
    hash = Hash( block + nonce )
```

```
Done
Send NoPoWCompleteSignal
Update block to BlockChain
```

- **Genesis Block Creation -** In this module, the genesis block for bootstrapping the blockchain application is created using configtxgen tool which is an inbuilt tool with Hyper ledger. This tool takes an input file configtx.yaml and outputs the binary file which should be used when creating initial setup for blockchain.

- **Broadcasting Blockchain -** This module broadcasts the newly created block to other peers in the network.

```
Trans := GenerateTrans()
   For each peer in the network; do
      Kbpub = Public key of the peer;
      TxData := encrypt ( Trans, Kbpub);
      TxData := encrypt ( TxData, Kapri);
      Broadcast to every neighbour node
   done
```

Note: Here, Kaprimeans the Private key of the sender and Kbpub means the public key of the receiver.

PERFORMANCE MEASURES

The output statistics of running a workload with different configurations can be used to evaluate the Blockchain against three performance metrics.

- **Throughput:** measured as the number of successful transactions per second. A workload can be configured with multiple clients and threads per clients to saturate the Blockchain throughput.

- **Consensus delay:** Take the consensus delay based on block generation times. A user who requires high confidence (e.g., 99%)

must wait for several key blocks to accept a transaction as completed. This guarantees the importance of consensus delay.

- **Fairness:** Calculate the proportion of the ratio of blocks in the main chain not generated by the largest miner with respect to all blocks in the main chain, and the ratio of blocks not generated by the largest miner with respect to all generated blocks.

- **Mining power utilization:** Calculate the proportion between the aggregate work of the main chain blocks and all blocks.

- **Time to prune:** For each node and for each branch, measure the time it took for the node to prune this branch. This is the time between the receipt of the first branch block and the receipt of the main chain block that is longer than this branch.

- **Latency:** measured as the response time per transaction. Driver implements blocking transaction, i.e. it waits for one transaction to finish before starting another.

- **Scalability:** measured as the changes in throughput and latency when increasing number of nodes and number of concurrent workloads.

REFERENCES

[1] Lijing Zhou, Licheng Wang, Yiru Sun, "**Blockchain-Based Medical Insurance Storage System**," in *Springer J Med Syst*, 2018.

[2] Craig Wright, Antoaneta Serguivea, "**Sustainable Blockchain-Enabled Services: Smart Contracts**," in *2017 IEEE International Conference on Big Data,* IEEE, 2017, pp. 4255-4264.

[3] Gabriela Ciocarlie, Karim Eldefrawy, and Tancrede Lepoint, "**BlockCIS – A Blockchain-based Cyber Insurance System**," in *2018 IEEE International Conference on Cloud Computing,* IEEE, 2018, pp. 378-384.

[4] Mayank Raikwar, Subhra Mazumdar, Sushmita Ruj, Sourav Sen Gupta, Anupam Chattopadhyay, Kwok-Yan Lam, “**A Blockchain Framework for Insurance Processes**,” in *9th IFIP International Conference on New Technologies, Mobility and Security,* IEEE, 2018.

[5] Chuka Oham, Raja Jurdak, Salil S Kanhere, Ali Dorri, Sanjay Jha, “**B-FICA Blockchain based Framework for Auto-insurance Claim and Adjudication**,” in *2018 IEEE International Conference on Cloud Computing,* IEEE, 2018.

[6] Tarr, Julie-Anne, “**Distributed Ledger Technology, Blockchain and Insurance: Opportunities, risk and Challenges**,” in *Insurance Law Journal, 2018, Vol.* 29, pp. 254-268.