Insurance Framework based on Blockchain and Smart Contract

Sahil Shivhare
dept. of Computer Science
Sharda University
Greater Noida, India
shivharesahil0@gmail.com

Abhishek kumar Singh
dept. of Computer Science
Sharda University
Greater Noida, India
lodhiabhishek.in@gmail.com

Nishant Gupta
dept. of Computer Science
Sharda University
Greater Noida, India
nishant.gupta@sharda.ac.in

***Abstract*— Processing insurance claims requires a variety of human-agent interactions, multi-domain entities, and data from several sources. As a result, this procedure is typically time-consuming and labor-intensive. Platforms for intelligent automation built on blockchain technology can greatly increase the speed and scope of claims processing. Insurance policy claiming and settling is a complex process. This settlement process is challenging because of a variety of issues, such as hidden requirements from accusations of fraud by the client or the insurance body. The insurance sector could be completely transformed by the use of blockchain technology and smart contracts. The entire insurance processes, from verification to claim settlement, can be carried out with improved security and increased transparency with the adoption of blockchain technology. This paper gives a framework based on blockchain smart contracts for insurance. If all the requirements are fulfilled at the event of a claim, the transaction takes place; if not, it is rejected. To develop smart contracts, a programming language called Solidity is employed. The system makes use of the consensus algorithm known as Proof of Authority (PoA) for the validation of each transaction.**

Keywords—smart contract, blockchain, Proof of Authority, Consensus Algorithm

I. INTRODUCTION

A policy serves as the representation of an insurance contract, which provides the policyholder with financial security or compensation for losses from an insurance provider. The Insurance Industry has valuation over 500 billion dollar [1]. Health, commercial, and auto insurance contracts come in a variety of forms. These industries are present in many different countries around the world, and governments in places like the EU, Japan, Canada, and the majority of south American nations have created public policies. [2]. Although insurance policies are frequently used, resolving claims is not always a straightforward process. Insurance companies frequently violate the terms and conditions of the contract in order to avoid paying the insured. In Some cases, false calm by the customers is a problem for the Insurance entity. Traditional agreement though legally binding can't solve the above problems. These agreements are not straightforward and have escape clauses. These escape clauses lead to double-dealing generally speaking by the two safety net providers and customer. These issues can be resolved with blockchain-based smart contracts since they reduce the need for trust and financial burden in the present insurance process and offer precise clarity.

This proposed framework smears the technique to make a reasonable building involving smart contract and blockchainto bids. Its main objective is to leverage smart contracts and blockchain technology to assure safe, secure, and fraud-free transactions. By using blockchain to handle client entry, policy issuance, and settlement, this framework strengthens the overall protection framework.

Each block in a blockchain is made up of data. Each block contains the exchange data, timestamp, and cryptographic key for the previous block[3]. This innovation has been widely used for a variety of purposes. Since introduction of Bitcoin in 2009 while highlighting the blockchain architecture[4], Blockchains have distinguished themselves with a variation of applications across a variety of sectors. The widespread use of Bitcoin transactions has been the most well-known implementation of blockchain technology to date [5]. The major financial and banking industry [8] and the public authority's public administrations [6][7] have been identified as two crucial areas where the appropriate implementation of blockchain innovation can lead to enhanced efficiency. A few distinctive qualities of the blockchain technology make it ideal for applications involving money exchange. The decentralised, agreement, provenance, unchanging nature, and irrevocability characteristics of the blockchain are its core characteristics. Decentralized refers to the idea that no single entity with the greatest authority controls the entire blockchain, and it is an important aspect of the blockchain. The foundation of the entire structure is provided by the participants' common knowledge. We refer to this common understanding as agreement. This accord is what we mean when we talk about consensus. Once more, agreement is a vital feature of the blockchain. A blockchain network's participants can only conduct an exchange once they have reached consensus on it.

II. MOTIVATION

The decentralised, secure authentication cycle of blockchain technology is used to store data in blocks. The transactionappeal must pass through a planned agreement computation utilising a consensus mechanism that rolls out any unapprovedrequests before any changes to the blocks may be made. The exchange procedure is secure and immutable since information is encrypted and time stamped in the blocksThe adoption of transparent, highly secure smart contracts boosts the transaction's overall efficiency. Consider that all specifications pass the consensus algorithm and match a transaction process.This block gets appended to the network moving as we move forward to the next process of insurance claim, making the whole system secured, transparent for both client and companies.

III. Related works

A. Processing Insurances Claims with Blockchain.

Blockchain enables shared confidence amongst the participating peers by providing auditability and visibility. Blockchain's smart contracts can also speed up processing while lowering operational and maintenance costs. The authors of suggest using a blockchain platform to process insurance claims by exchanging documents as part of a group knowledge sharing entity across the several relevant sectors, thereby enhancing accessibility and reducing inequities. In a similar vein, the authors investigated the potential for Blockchain integration inthe insurance sector from a regulatory perspective. They displayed How auditability promotes compliance and visibility with regulation. A Blockchain framework is introduced by WISChain. for claimants and insurance companies. Briefly, they discuss the creation of a browser plugin that addresses security concerns password protection for online identity protection.

B. Modeling of Attack in Blockchain Solutions

Although it has many advantages, using blockchain introduces potential attack points. Blockchain-based systems are vulnerable to a multitude of assaults that could jeopardise the integrity of data, notwithstanding conventional databases' greater security. Consequently, determining attack scenarios and carrying out relevant threat modeling is crucial. Cyber-physical system security concerns have been thoroughly examined in earlier publications. However, there are not many studies on how to classify Blockchain attack types. /Blockchain technology is a cutting-edge innovation with a lot of promise. Exploring the security of this novel technology is necessary given its potential. Although a lot of work has been done in this area, no complete threat model that categorizes all potential dangersand attack vectors within the blockchain ecosystem is now available. It is quite helpful to have a framework to utilize in identifying known attacks and pointing out ones that may have been overlooked when talking about potential security threats to a system and trying to determine whether a system is secure by design. In order to establish a useful threat model for the blockchain, the security risks associated with it are mapped to STRIDE, a well-known threat model created by Microsoft.

IV. Methods and Materials

The techniques and materials used to accomplish the objectiveare talked about in this segment. The objective is to make a protection biological system utilizing blockchain innovation. The main idea is to demonstrate the agreement's full capacity and execution. Its circumstances and justification for execution will be written using the Solidity programming language and organised as magnificent agreements. On an Ethereum-based distributed stage using blockchain technology, these negotiations will be managed. The main part of this section offers a simple framework model for the structure. The auxiliary resources present the pertinent features, the insurance structure's system, the network stage, agreement calculations, blockchain blocks, dazzling policies, and the structure's components and calculations. The findings and structure investigation are presented in segment three. In Fig 4, the entire building is finally completed.

The execution of blockchain innovation in the sphere of numerous protection processes is the important commitment of this proposed framework. Additionally, it makes use of a specific agreement computation(for this situation: Proof of Authority) in the framework and the point by point calculation and the clarification of the entire cycle.

V. Details of the Framework

The whole System Diagram is show in figure below. It suggests that, in conjunction with the appropriate agent, the consumer may register, issue a policy, submit a claim, and receive a reimbursement. The information is uploaded to the Ethereum private network with the aid of the proper agent. All client requests must be submitted inside the network by the agent. The validators must validate the transactions at the time of the transaction.

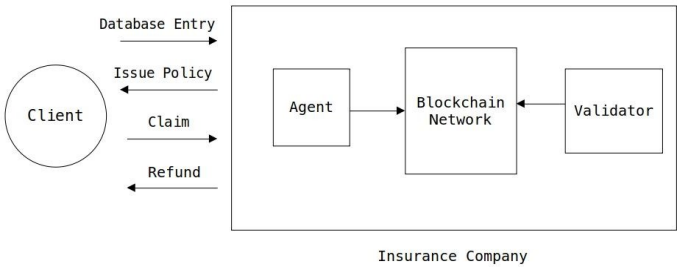

Fig 1: Diagram of Full System

It needs to be made clear that its purpose is to act as a foundation for an insurance company.. As a result, the diagrammed model solely includes the company's customers and members. In this instance, the private Ethereum network serves as the blockchain network. The validators have already been chosen, and they will validate transactions in accordance with the Proof of Authority algorithm's guidelines.

A. AUTHENTICATION

The system provides a basic frontend that incorporates the authentication procedure for the system's stakeholders even if its core component is a proposed algorithmic architecture. TheGoogle Firebase system is in charge of maintaining the authentication. Both the client and the authority share the same login. A hard coded filter is activated after login in to filter the client and the authority. Because it needs to be confidential and discreet within the agency, the authority members are manually registered. Therefore, the sign-up is only useful for the clients.

B. USER AGENT

It doesn't matter if it's a desktop, console, or web application; they control key components including policy issuing, policy initialising, and other client inquiries. The agent and the validator share the same portal since the agency may occasionally select one for both duties. The agent panel interface, allows user to operate every feature, including seeing client lists, agency policy lists, transaction histories, etc.

C. ENTITES INVOVLED IN THE MODELS

The main entity who is directly involved in the model is the client. He has the option to sign up for the contracts, get insurance, file claims, obtain refunds, and more. A middleman, or agent, processes all client paperwork and

requests before uploading them to the blockchain network. The system involves the following parties, who are in charge of validating contract terms and transactions as well as entering contracts into the record. Customer, insurance company authority, agents, and validators are the parties involved.

D. THE INSURANCES FRAMEWORKS MACHANISM

The client must register with the values for all other necessary attributes as well as a unique id. A database must be maintained with these IDs. Previously, all rules and legislation would be drafted using smart contracts. The transactions are meant to be activated once all of the requirements or logics have been met. Each transaction's execution logs and record logs are saved in a ledger on the blockchain network. Between each transaction, endorsers and validators review the transaction, approve it, and then deposit the transaction block in the blockchain ledger.

E. ETHEREUM PLATFORM

The distribution of the entire network will be implemented on a private Ethereum platform. The access to this blockchain is restricted. The insurance company authorities extend invitations to participants to join this network. This specialized network will restrict who can use the network based on restrictions on access. In this scenario, the network will allow the ledger to be distributed to a specific participant subset without making the transaction data broadly accessible.

CONSENSUS ALGORITHM

The Proof of Authority method is used by the framework to validate and generate transaction blocks prior from adding them to the Ethereum network. The validators will be preselected by the insurance company. Only those who have proven their trustworthiness in that capacity are allowed to generate new blocks and transaction logs over the network. The validators are permitted to create transaction logs and other monitoring tools once they have been chosen.

The Proof of Authority algorithm's flow diagram for the particular use case of this research issue is shown in Figure 2. The insurance authority is fundamentally represented by the authority's members. The period's configuration option must be passed through by the algorithm. Using the issuing authority of the insurance agent, After being verified, the transaction blocks are subsequently added to the organization's personal Ethereum network. If not, the block is thrown away.

In order for the algorithm to function with the applicable system network, configuration settings will be required, to put it in a broader context. The configuration will include, among other things, the chain-data, the gas cap, and other pertinent information. In order to approve a new block, the authority members—in this example, the validators—will now have to work through difficult mathematical puzzles. A validator's mined block would be chosen to incorporate into the foremost blockchain network after certification is successfully accomplished. The validator or other necessary agents must add the block to the mainframe. The block will be preserved if not.

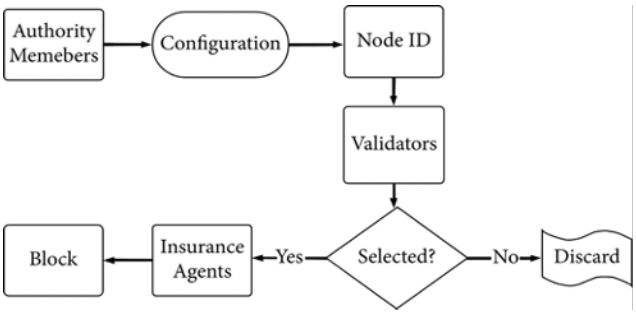

FIGURE 2: FLOW CHART OF THE PROOF OF AUTHORITY (POA)

BLOCKCHAIN IN INSURANCE

A blockchain is composed of a number of blocks that each include many transactions. The blockchain grows longer with each new block that is uploaded. Figure 3 displays the structure of block. Each block is confirmed by a certain validator before being added to the blockchain or executed. Because of its timestamps and hashes, each block can be distinguished from the other blockchains in a certain way. Thereis data kept in blocks in addition to the hash and time stamp. Depending on what the application requires, this information changes. We've included a sample blockchain block for an insurance application below. Examples of crucial insurance data include Amount, Customer_ID, Agent_ID, and critical insurance data.

The Ethereum smart contract platform will be used to contractualize the blockchain containing the insurance data, and Access control will be implemented for each peer or validator of the system's resources. Electronic contracts known as "smart contracts" are made between a customer and a service benefactor. Given how specifically stated and transparent the contracts are, there is very little potential of manipulating the processing is done in accordance with the terms of the contract because validators who have a complete understanding of the contract are in charge.

When a customer demands a refund in accordance with the insurance smart contract depicted in Fig 4, it transmits account information to the validator. The contract details are examined by the validators, who then submit a confirmation of their choice. Following that, it completes the execution process and makes crucial modifications to the blockchain

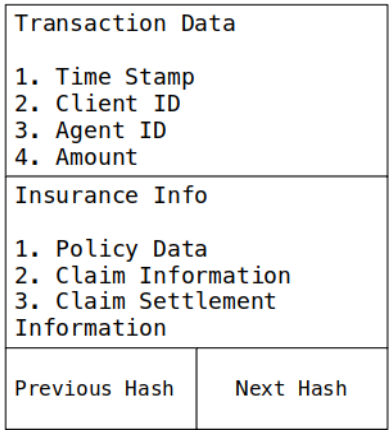

FIGURE 3: STRUCTURE FOR SMART CONTRACT

FRAMEWORK ALGORITHMS AND COMPONENTS

Blockchain technology is applied in this design to protect and process a portion of the insurance environment. Blockchain technology guarantees the accountability of insurance and the security factor of bogus claims.

Figure 5 illustrates the framework's primary use case functions. These insurance policy qualities are supported by scattered smart digital contracts that are essentially temper proof, reliable, and trustworthy. Client and policy information will be stored in a database as objects using smart contracts. The client has the choice to register and submit applications for the initialization, claiming, and refund of the insurance, as can be seen by paying closer attention. The internal working of the insurance company includes agents and validators. The agents will deal directly with clients.

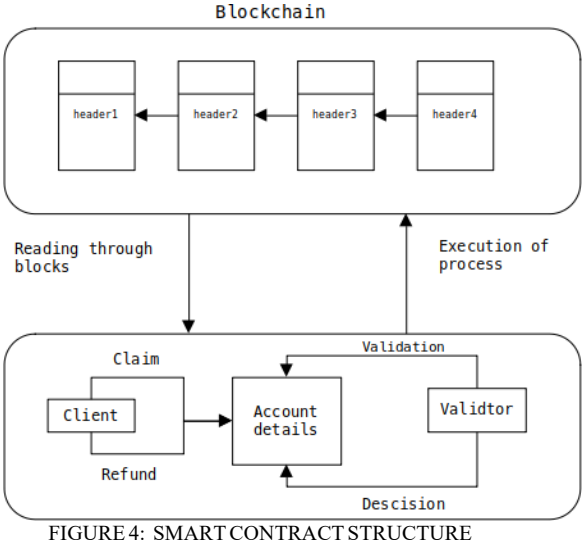

FIGURE 4: SMART CONTRACT STRUCTURE

They'll assist the customer or have access to the register and handle customer service requests, policy initialization, and issues. The validators have access to the validation of the transaction block, refund, and policy claims.

I. CLIENT REGISTRATION

Clients are registered in the insurance system by the use of smart contracts. A client object structure (StructCO) is built in the database to initialize a client. The client object has properties such as a special id, name, age, contact, etc. An agent creates a composite key (*Ckey*) and a client object (*CO*) using the *CKey* in order to register that client object.

Algorithm 1 *[Client Registration]*

StructCO ⟵ (clinet_id,client_name,client_age,contact,);

Database ⟵ StructOC;

CKey ⟵ (agent_id, client_id);

Composite key and Client Object is stored in Database;

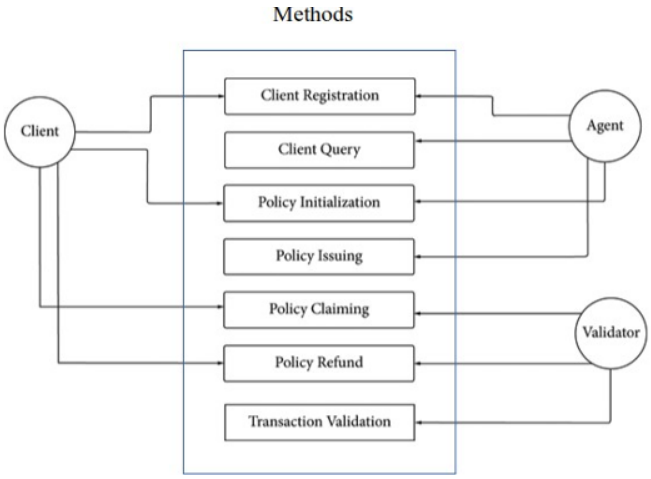

Figure 5: Low Level Design of the Framework

II. CLIENT QUERY

A client's information, including all of his attributes, is saved in the blockchain network after registration. Now, the insurance agent must establish a composite key in order to get any individual client information.

Algorithm 2 *[Client Query]*

CKey ⟵ (agent_id,client_id);

If (CKey in Database):

retrieve desired CO

else return Error;

III. POLICY INITIALIZATION

Policy issuance, claims, refunds, and other transactions will beincluded in the smart contract. The policy structure (*Struct_PO*) and policy client structure (*Struct_PCO*) are initialized in the database. The identity, name, premium, reimburse, and term information will all be included in the policy structure. The *Struct_PCO* include the customer id, policy id, claim amount, indicator of claim acceptance, claimsubmission date, etc.

Algorithm 3 *[Policy Initialization]*

IV. POLICY ISSUING

Customer selects a policy from the available options (id_Policy) from the database. After deciding on an insurance plan, the customer pays a premium to the salesman. An associated policy-client object *(PCO)* is produced and saved in the database if the transaction is approved and passes all validity checks.

Algorithm 4 *[Policy issuing]*

find if PCO exists in DB or not;
Check whether Clients Smart contract id is already linked withan agent id or not;
Check if Customer Premium match Policy Premium; Ckey_PolicyClient ⟵ (agent_id, clinet_id, id_policy);

PCO ← Struct_PCO ← (client_id, id_policy, true, data);
Add Ckey_PolicyClient , PCO in the Database;

V. Policy Claiming

The Customer provides his credentials to his corresponding agent in order to process a claim. The relevant requirements are verified, and the refund is then started as a result.

Algorithm 5 *[Policy Claiming]*

Ckey_PolicyClient : {agent_id, client_id, id_policy}; Find if PCO exists in DataBase using Ckey_PolicyClient;
If PCO found,
Check if(PCO_acceptance == True);
If amount + Customer_Reimburse <= Reimburse_Policy:
then pay(agent_id, client_id, id_policy, client_reimburse);
else refund
end

VI. Policy Refund

The prior claim process is the basis for the refund process. Here, the database updates total number of claims in the policy-client object.

Algorithm 6 *[Policy Refund]*

CKey_PolicyClient : {agent_id, client_id, id_policy};
find if PCO exists using CKey_PolicyClient in the DataBase.
Update the amount = amount + Customer_reimburse in PCO

TABLE I. Security of the Proposed Framework

Sr. No	Table Column Head	
	Threat	***Prevention***
1.	Modification client Information	PoA consensus algorithm
2.	Chaning the Meaning	Endorsement Plans
3.	False Outcome during Audit	PoA consensus Algorithm

The potential dangers to the framework are listed in Table 1 together with the measures taken to combat them. The immutable design of the blockchain network makes it secure already, but the table also shows how various malevolent acts might damage the foundation. The unauthorised changes and removal of data is handled via the consensus algorithm we've chosen. Because the endorsement and other policies are encoded in the Ethereum network's smart contract, any incorrect endorsing will be obvious and detectable.

Analysis of Consensus Algorithm

For the purposes of this framework, the PoA algorithm performs admirably. Permissioned blockchain networks use Proof of Authority (PoA) consensus. Both platforms with and without permissions can use the consensus technique. In the permissionless systems, any block can become node. The permissioned system is more secure because all of the nodes and validators are pre-selected. PoA is a kind of consensus that has a high degree of fault tolerance and can produce excellent performance.

Only the nodes in this algorithm that have established themselves as authorities are permitted to produce fresh blocksor transaction logs. The validators are permitted to create transaction logs and other monitoring tools once they have been chosen. To gain the right to validate and produce the blocks, the validators just need to use their reputation. In contrast to every other consensus systems we have seen so far. Additionally, they are not required to stockpile their coins or invest in expensive technology or storage. The foundation of Proof of Authority is the confidence in the chosen validators. This algorithm works well in trust-distributed private and public networks.

Conculsion

This study aims to present an insurance smart contract architecture built on the blockchain. An extremely secure private, decentralised system based on Ethereum is used to conduct insurance transaction processes. The conventional insurance contracts are created in this architecture using smart contracts. The decentralised Solidity smart contracts employed in this system streamline the insurance and claim settlement procedures due to their immutability. By utilising the PoA algorithm in this design, money and storage are saved. Asa result, the framework offers an effective and secure means ofconducting business in the insurance sector.

References

[1] "Estimated Size of the Global Insurance Market 2020," https://www.statista.com/statistics/1192960/forecast-global-ins urance-market/

[2] E. M. Immergut, "Health policy," in *International Encyclopedia Of the Social & Behavioral Sciences*, pp. 6586–6591, Elseiver, Amsterdam, Netherlands, 2001.

[3] A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, NJ, 2016.

[4] "Bitcoin.org," https://bitcoin.org/bitcoin.pdf.

[5] M. Lischke and B. Fabian, "Analyzing the bitcoin network: the first four years," *Future Internet*, vol. 8, no. 4, p. 7, 2016.

[6] Government Office for Science, "Distributed ledger technology: beyond block chain," in Government of United Kingdom, 2

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smartcontracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] W. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view offinancial blockchains," in *Proceedings of the 2016 IEEE Symposium On Service-Oriented System Engineering (SOSE)*, pp. 450–457, Oxford, UK, March 2016.

[9] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," *in Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics* (SMC), pp. 2567–2572, Banff,Canada, October 2017.

[10] J. Ellul and G. Pace, "Blockchain and the common good

reimagined," 2019, https://arxiv.org/abs/1910.14415.

[11] O. Alfandi, S. Otoum, and Y. Jararweh, "Blockchain solution for iot-based critical infrastructures: byzantine fault tolerance," in Proceedings of the *NOMS 2020 - 2020 IEEE/IFIP* Network Operations and Management Symposium,Budapest, Hungary, April 2020.

[12] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: is the technology mature enough?" *Future Internet*, vol. 10, no. 2, 2018.

[13] H. Luo, M. Das, J. Wang, and J. C. P. Cheng, "Construction payment automation through smart contract-based blockchain framework," in *Proceedings of the 36th International Symposium on Automation and Robotics in Construction (ISARC 2019)*, pp. 1254–1260, Banff Alberta, Canada, May 2019.

[14] S. N. Khan, F. Loukil, C. G. Ghedira, E. Benkhelifa, and A. H. Bani, "Blockchain smart contracts: applications, challenges, and future trends," *Peer-to-PeerNetworking and Application*, vol. 14, pp. 1–25, 2021.

[15] M. Raikwar, S. Mazumdar, S. Ruj, S. G. Sen, A. Chattopadhyay, and K. Y. Lam, "A blockchain framework for insurance processes," in *Proceedings of the 2018 9th IFIP International Conference On New Technologies, Mobility And Security (NTMS)*, pp. 1–4, Paris- France, February 2018.

[16] P. K. Singh, R. Singh, G. Muchahary, M. Lahon, and S. Nandi, "A blockchain-based approach for usage-based insurance and incentive in its," in *Proceedings of the TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, pp. 1202–1207, Kochi, India, October 2019.

[17] K. Sayegh, *Blockchain Application in Insurance and Reinsurance*, SKEMA Business School, Lille, France, 2018.

[18] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Proceedings of the International Conference on Principles of Security and Trust*, pp. 164–186, Uppsala, Sweden, April 2017.

[19] F. Holotiuk, F. Pisani, and J. Moormann, "Radicalness of blockchain: an assessment based on its impact on the payments industry," *Technology Analysis & Strategic Management*, vol. 31, no. 8, pp. 915–928, 2019.

[20] P. Tasca, "Insurance under the blockchain paradigm," in *Business Transformation Through Blockchain*, pp. 273–285, Springer International Publishing, Cham, Switzerland, 2019.

[21] Nath, "Data exchange platform to fight insurance fraud on blockchain," in *Proceedings of the 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pp. 821–825, Barcelona, Spain, December 2016.

[22] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A survey of blockchain applications in different domains," in *Proceedings of the 2018 International Conference On Blockchain Technology And Application - ICBTA 2018*, Xi'an,China, December 2018.