Blockchain in Insurance: Exploratory Analysis of Prospects and Threats

Anokye Acheampong AMPONSAH[1]*
Benjamin Asubam WEYORI[3]
Department of Computer Science and Informatics
University of Energy and Natural Resources
Sunynai, Sunyani – Ghana

Professor Adebayo Felix ADEKOYA[2]
Department of Computer Science and Informatics
University of Energy and Natural Resources
Sunynai, Sunyani – Ghana

Abstract—**Ever since the first generation of blockchain technology became very successful and the FinTech enormously benefited from it with the advent of cryptocurrency, the second and third generations championed by Ethereum and Hyperledger have explored the extension of blockchain in other domains like IoT, supply chain management, healthcare, business, privacy, and data management. A field as huge as the insurance industry has been underrepresented in literature. Therefore, this paper presents how investments in blockchain technology can profit the insurance industry. We discuss the basics of blockchain technology, popular platforms in use today, and provide a simple theoretical explanation of the insurance sub-processes which blockchain can mutate positively. We also discuss hurdles to be crossed to fully implement blockchain solutions in the insurance domain.**

Keywords—Blockchain technology; insurance industry; hyperledger; ethereum

I. INTRODUCTION

Evolving technologies mostly help to change the driving forces underlying economic, social, and business developments [1,2]. Blockchain was developed and introduced in 2008 by a researcher or a group whose identity has remained anonymous even till now [3,4]. It was introduced as a financial application (Bitcoin), to facilitate peer-to-peer electronic cash transfer without requiring a centralized trusted system and for the resolution and prevention of the double payment problem [3,5].

In recent past years, Blockchain has ratcheted up and gained tremendous attention among the academic community [6], industry, and researchers demonstratively placing among the top five technology trends in 2018 [7,8]. According to [9], the output value of Bitcoin per day stands at 4.144 Million and the estimated transaction value of transactions on the blockchain is 158.932k as of September 17, 2020. Blockchain is categorized into three generations. The first generation – blockchain 1.0 was introduced in 2009 and used hardcoded special-purpose systems to focus primarily on digital currency and served potentially malicious public participants [3,10].

The second generation – Blockchain 2.0 commenced in 2014 and emphasized innovative ways of applying Smart Contracts in diverse situations and domains, championed by Ethereum [11] offering user-defined digital assets and partly turing complete functionality [10]. Blockchain 3.0 begun in 2017 with Hyperledger projects (Fabric, Composer, etc.) providing an all-purpose permissioned decentralized application system, mostly associated with user-friendly and highly configurable features. The second generation of blockchain saw significant systems being developed in logistics, certificates, and finance. Recently, the domain applications have expanded to include education, health, agriculture, Internet of Things (IoT), and governance [12,13] Smart Grid, Intelligent Transportation System, Data Center Networking, Electronic Voting System, and more [14,15,16,17]. All three phases are complementary and support one another to formulate the normality of blockchain technology [18].

According to [19,20], in case of an emergency, insurance is one of the essential assistance accessible to populations to neutralize their costs and assist them. The greatest challenge of the sector is how to detect and protect against counterfeit documents and stop the intentions of phoney participants. Consistent with [21], the impact of Blockchain technology has been seen by major insurers and reinsurers, where the majority have begun to invest in trial systems. A vivid example is the Blockchain Insurance Industry Initiative (B3i) launched in 2016 to examine the potential of BC to improve successes in data exchange among insurance and reinsurance enterprises [22]. The insurance companies provide a source of funding for the clients in a state of disaster and as a result, are engraved with enormous paper works and inefficiencies [23]. In the recent past, most insurance companies adopted a centralized architecture for system development as shown in Fig. 1a, and therefore by using a decentralized blockchain as in Fig. 1b, the insurance industry gets an exceptional chance to re-examine its complete value chain, which has continuously depended on utmost good faith and trust and develop novel insurance products for their consumers [24].

---

*Corresponding Author

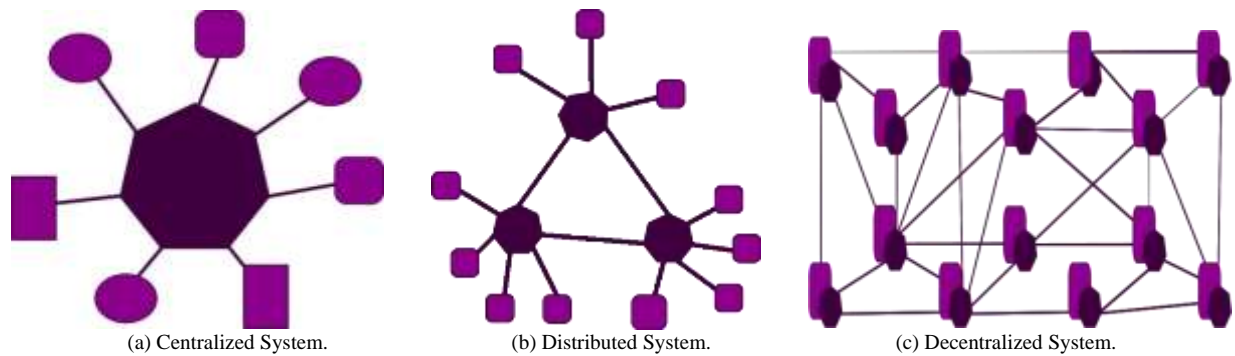(a) Centralized System.   (b) Distributed System.   (c) Decentralized System.

Fig. 1. Architecture of Existing Systems.

II. CONTRIBUTION OF THE PAPER

Currently many researchers have worked on blockchain in different perspectives. As indicated in Tables III and IV in appendix, some authors provided a general understanding of blockchain technology. The author in [10] used a meta survey to provide a strong foundation for their future reference model. The author in [14] built on previous surveys and produced a comprehensive importance of blockchain technology scoping the many different smart communities such as transportation, healthcare, proof-of-work algorithm, smart grid, finance, voting system, data center networking, consensus protocols, and process models, and many more. The author in [12] also provided a snapshot and proposed taxonomy of blockchain applications. There are further surveys for example [25], [26], [27], [28], [29] but they are all geared towards the financial aspects of blockchain and the underlining privacy and security issues. Equally, several surveys exist with a particular focus on other domains. For example, [30] concentrate on blockchain application in the Internet of Things (IoT), [31] authentication and identity management, [32,33] security and privacy, [34] Software Defined Networks (SDN) and a lot more. Closely related to this work as indicated in Table VI (in appendix) are [35], who purposely studied the repercussion of adopting blockchain technology on the operations and regulations of insurance companies with limited depth, and [36], who explained how blockchain can be significant to the insurance sector with the aim of assisting insurance industry players and major stakeholder to be aware of the applicability of blockchain in the sector. Equally, several researchers have reviewed blockchain applications in the insurance sector with a relatively strong introduction and ideas. For instance, as shown in Table IV and Table V [14] surveyed numerous blockchain applications and explained insurance processing using blockchain in the context of the financial sector. Also, [12] similarly acknowledged the application and acceptance of blockchain in insurance and touched on the various incomplete business processes that can be improved or reengineered. Other researchers also concentrated on other peculiar domains. Table VI consists of examples including [37], [2], and [38] with focus on Agric and Food Supply Chain, Business Models, and Construction Management respectively. It is evident that no comprehensive review has been done in assessing the impact or potentiality blockchain technology in the insurance industry. It the light of [14, 12] it is believed that a field like the insurance must have comprehensive and extensive representation in the literature in terms of blockchain's implications. Therefore, in this work, we fill in the gab by zooming in to review the significant Insurance business processes and how they can be enhanced by utilizing blockchain technology. We subsequently present major insurance sub-domains and how blockchain can be used to create new services and products. We also provide opportunities and describe our future directions.

The remainder of the paper is presented as follows. We first discuss the fundamental concepts of blockchain focusing on features of blockchain, components of blockchain, types of blockchain, and blockchain platforms in Section II. Also, the methodology applied to produce this work is described in Section III. We explain how we augmented systematic and gray literature methods to review the existing literature. There is a presentation of the major types of insurance and how blockchain can be leveraged in Section IV. Also, areas in insurance where blockchain can change are also discussed in Section V. And lastly, we present the limitations of blockchain technology in Section VI.

III. FUNDAMENTAL CONCEPTS OF BLOCKCHAIN

A. Blockchain Technology

Blockchain technology is a publicly verifiable, shared, immutable distributed ledger used for recording the history of transactions. As the name suggests, blockchain is a chain of blocks that contains information inside a block, and each block is connected with a hash of its previous and subsequent blocks to create a chain. Blockchain technology consists of nodes where each node maintains its local copy of the chain and is connected with peer to peer connections. Every block contains a header, an ID of the previous and next blocks, a timestamp, and a series of transactions. As a decentralized technology, blockchain (BC) enables completely new technological systems and business models [39]. BC typically combines previous technologies like digital signature, cryptographic hash, and distributed consensus mechanism [40].

Blockchain is the underlying digital foundation that supports applications such as bitcoin. The technology enhances the process of storing transactions and tracing assets in a cooperate network. Assets can be physical such as a house, car, phone, etc. and virtual like money, titles, bonds, equities, contracts, deeds, and virtually all other kind of assets that can be transferred from a peer to peer and stored securely,

privately, requiring no need for a third-party confirmation. This is so because trust is enforced and the confirmation is done by cryptography, network consensus mechanism, smart code, and collaboration without requiring controlling mediators like governments and banks [41]. Blockchain can be talked of in tandem with other similar algorithms like clustering and complex systems as they can all be described and examined based on the science of data structure serving as the basic building block of present algorithms where nodes are used for data packets and data stores, communicating with one another in consonance with agreed methods of nodes communication [42]. In BC, a transaction is requested which is broadcasted to the peer-to-peer network. Upon validation and verification, the transaction becomes complete when it is added to existing blocks on the blockchain. This is indicated in Fig. 2.

B. Features of Blockchain

Blockchain inherently provides the following features.

- Immutability and Security: Immutability makes blockchain a secure and transparent approach to storing and processing data among nodes in the blockchain systems using cryptographic functions [43]. Immutable transactions are sheltered from unauthorized amendments from mischievous users. Participants can create fresh transactions, but cannot remove or edit previous ones, facilitating that all nodes can keep track of all transaction history [44]. Once data is written and stored in the ledger, it can never be changed [45]. If an error exists in a transaction, a different transaction has to be created and the two are available. The distributed ledger diminishes the reliance on a trusted central party and the risk of a single source of a system failure or data manipulation as all nodes have the full information for authentication, verification, and validation [44].

- Transparency: By using a consensus mechanism, validation and acceptance rules are enforced in the blockchain network where any party after satisfying the protocols in the blockchain can apparently and publicly initiate and add transactions. The consensus, validation, and acceptance rules in blockchain guarantee trust among participants in the network since all transactions are endorsed by their prospective generators and once a block is accepted, miner nodes broadcast the block to all other nodes in the network [45]. In this case and the case of a public blockchain, all transactions are made available to all participating nodes while in a private blockchain all data are accessible to authorized nodes.

- Verifiability: The cryptography and consensus mechanism make the transactions implemented and managed in blockchain technology verifiable by both outsiders and insiders. So, for a transaction to be valid, at least fifty percent plus one participant must agree on its validity.

- Authenticity: Using smart contracts in blockchain applications offers the legitimacy of transactions. Also, the transaction in blockchain naturally contains the digital signature of the creator and responder and every block also consists of previous and subsequent hashed IDs.

- Accountability and Ownership: The immutability of transactions in the block, the connection among blocks, and the originators' endorsement could enable ownership control as well as accountability in applications powered by blockchain. Also, participants know the provenance of a block or transaction.
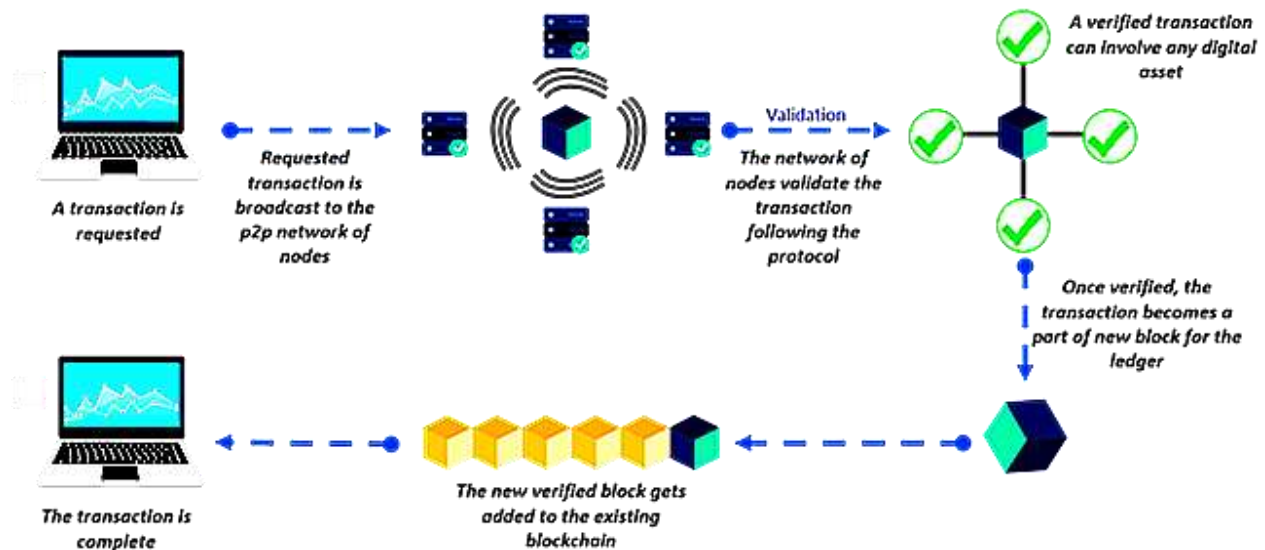

Fig. 2. Graphical view of how Blockchain Works. Source: Edureka.

C. Components of Blockchain

1) Assets: An Asset is a thing of value to an organization and by definition, it enables the transfer of nearly everything with economic worth over a blockchain network. Depending on the blockchain system, an asset may be intangible – currency, shares, patents, certificates, personal data, or tangible like food and beverage in a restaurant, properties in real estate, or any other tangible or intangible items. Unlike traditional -assets such as Apple Stock where the right of ownership is paper-based, blockchain asset is purely digital solely owned by the participant and does not require a third-party agent or agency in the case of transfer or sale.

2) Transactions: A transaction in blockchain refers to typical time-stamped events that happen to create blocks in the ledger. Transactions are stored using private or public keys giving the participants the option to be unidentified, however, identities can be accessed and verified by third parties. Trust and harmonization in the system are ensured as all transactions and other data are transparently certified before being joined in the ledger using Merkle tree presented by Ralph Merkle in Fig. 3 [46]. Merkle tree is a complete binary tree structure that aids in the verification and assurance of consistency of data [46] thereby helping to haste security authentication in big data systems. Each parent node hashes the value from its corresponding child node.

3) Consensus algorithm: In decentralized or distributed systems, a consensus algorithm helps in decision-making [47]. The consensus algorithm is an administrative process in a blockchain network where the majority of the distrustful participants agree upon what rules are used and the decision that is good for them all. The features of the blockchain consensus algorithm include assuring quorum structure, integrity, decentralized governance, authentication, non-repudiation, performance, and byzantine fault tolerance [47].

The decision affects whether a block will be appended to the chain or discarded. The consensus algorithm fulfils its aim by reaching an agreement, supporting collaboration and co-operation, ensuring equal rights and recognition, and also active participation by members. The following are examples of blockchain consensus algorithm. Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Leased Proof-Of-Stake, Proof of Elapsed Time, Practical Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Directed Acyclic Graphs, Proof-of-Activity, Proof-of-Importance, Proof-of-Capacity, Proof-of-Burn, and Proof-of-Weight. Reference can be made to [14] for a detailed explanation of these algorithms.

4) Cryptographic functions: Cryptographic Functions use complex mathematical computations to change the meaning of information into a form that is rendered valueless in the wrong hands. This component of blockchain allows potentially malicious members on a blockchain network to create and append blocks on to the "chain" and engage in secured operations on a network. Every block of the blockchain holds the hash of the previous block which is stored with the transaction data and timestamp. Unlike symmetric encryption, asymmetric (public-key) cryptography employs a public key that is willingly shared for encryption and then a private key for decryption. Hashing is also used to secure the operations of blockchain. Before a transaction is created, data from the previous block is hashed and stored. The transaction creator's public key is hashed and used to create a transaction identity and the address of the transaction [48, 49, 14]. Examples of hash functions are SHA-256, Ethash, SCrypt, RIPEMD-160, and One-Time Signature, X11, Equihash, Elliptic Curve Digital Signature Algorithm, Edwards-curve Digital Signature Algorithm (EdDSA), Ring, Borromean Ring Signatures and Multi-Signature [14].
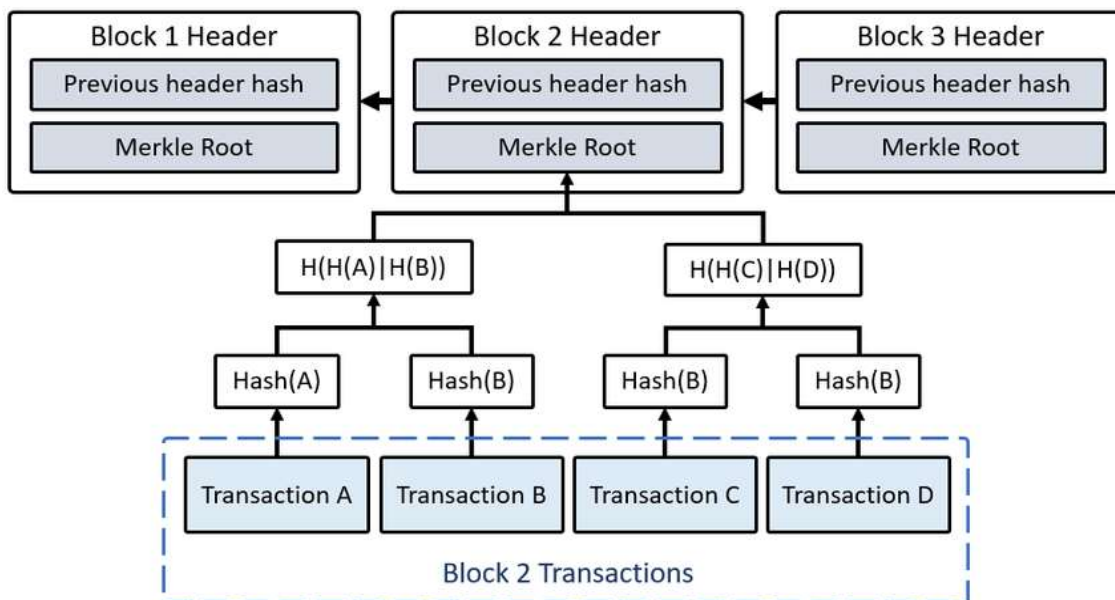

Fig. 3. Block Illustration in Blockchain using Merkel Tree.

5) Distributed ledger: A ledger is very crucial in business environments as it contains all transactional records for online and offline operations, users, and their credentials. In a normal business computing environment, a ledger is centralized. However in blockchain, the ledger is decentralized at the core, and depending on the type of blockchain, it is made available to some authorized participants (private) or all participants (public). Distributed ledger together with other characteristics of BC enforces auditability, security, transparency, and accountability.

D. Types of Blockchain

1) Public blockchain: Public blockchain uses proof of stake or proof of work to validate transactions before they are added to the block and the chain. This is done in a permissionless manner by allowing everyone to participate in the consensus process. All participants in public blockchain access, read, write, and transact on the network [50,51]. It is decentralized and has no reliance on a sole trusted entity for network control and administration. A public blockchain is protected by verification via cryptography where miners are incentivized. Transactions are consolidated and circulated by miners who can be anyone on the blockchain [50, 51]. Public blockchain uses computing resources and brute force mechanisms to verify transactions because no member on the blockchain is trustworthy and as a result, the miner who finally gets the correct results is given a reward. The most popular public blockchain is Bitcoin and Ethereum [50, 51].

2) Private blockchain: A private blockchain is permissioned blockchain where access control mechanisms are used to restrict network members from accessing parts of the blockchain. This enforces reliant on a centralized control system and permits only a few participants of the blockchain network to write to the blockchain. This type of blockchain is usually useful in the financial sector particularly because it complies with know-your-customer (KYC), anti-money laundering (AML), and Health Insurance Portability and Accountability Act (HIPAA) laws and regulations [51,50]. Hyperledger projects (Fabric, Iroha, Sawtooth, etc.) under the Linux Foundation are examples of the private blockchain.

3) Consortium blockchain: A consortium blockchain is permissioned and semi-decentralized type of blockchain. Unlike a public blockchain, a consortium blockchain requires permission to join, and also network control and administration power are given to a few sets of known nodes. Public participants may be given limited access to the ledger through API and may query the ledger in minimal ways. Consortium blockchain maintains the intrinsic security characteristics of public blockchain but also allows for a better level of regulation over the network. Examples of such platforms are R3, Quorum, Corda [52,50].

E. Blockchain Platforms

The following section discusses some popular blockchain platforms. This is summarized in Table I.

TABLE I. POPULAR BLOCKCHAIN SYSTEMS

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

1) Ethereum: Ethereum allows the blockchain community and developers to create and install blockchain-related systems. It is open-source and supports tokens, cryptocurrency, social apps, wallets and more to be deployed in the Ethereum Distributed Environment. Ethereum does not only support financial applications but also has an architecture that supports the application of distributed ledger technology in other fields. Ethereum supports several networks like Community Test Network, Community Ethereum Network, and other private BC networks.

The components of Ethereum comprises of

- Smart contracts are used to control all the events in Ethereum, written in Solidity programming language.

- Ether is the pillar of Ethereum transactions and cryptocurrency of the Ethereum network.

- Ethereum Clients develop and mine Ethereum blockchain. Examples are Geth, Eth, and Pyethapp.

- Ethereum Virtual Machine (EVM) is the blockchain engine behind Ethereum within which smart contracts run. EVM runs its language of bytecode which has necessitated the development of numerous smart contracts writing languages like Solidity.

- Etherscripter is a graphical user interface used to build smart contracts in Ethereum. In a few and simple steps, the drag and drop mechanism allows the automatic generation of backend codes in LLL, Serpent, and XML.

2) Hyperledger: Hyperledger is a worldwide partnership, accommodated by The Linux Foundation, and involves frontrunners in banking, finance, supply chains, Internet of Things, Technology, and manufacturing. Hyperledger is an open-source motivated by a community centered on mounting a collection of reliable bases, libraries, and tools for the development and deployment of enterprise-grade blockchain systems. More blockchain frameworks have been undertaken by Linux Foundation under the Hyperledger project including Fabric, Caliper, Sawtooth, Aries, Besu, Burrow, Cello, Composer, Explorer, Grid, Indy, Iroha, Quilt, and Ursa. Part of these frameworks is P permissioned (private) and others are permissionless (public) [53].

3) Corda: Corda was launched by R3 as an open-source blockchain platform in 2016 with provision from a strong community of developers and organizations. Corda is a blockchain with one key differentiator. It is a private blockchain platform that warrants the sharing of data among known participants. Corda was intended to ensure trust, transparency, security, and privacy.

4) Quorum: Quorum is a platform for enterprises to use blockchain. It is an enhanced branch of the public Ethereum client 'geth' to provide for business essentials. Quorum is also an open-source project and supports the very requirements of businesses – performance, privacy, and access control. The enterprise application requirements which predominantly include privacy, performance, and permissioning are all provided by Quorum augmenting them with the secrecy of all transactions, scalability, and speed, and ensures authorization.

IV. METHODOLOGY

We employed a methodology used by [12] and [54] and followed some of the steps in PRISMA [55] to allow for the production of reproducibility, transparent, scientific work. The following subsections describe the employed methods in detail. The following research questions were asked before the commencement of the literature search and the question determined the usage of whether gray or systematic literature review.

1) What are the major insurance sub domains that are currently draining the sector?

2) What are the major business processes in insurance that blockchain technology can mutate?

3) What are the current developments of the application of blockchain in the insurance sector?

A. Locating Studies or Data Extraction

To discover the latest papers for the resolution of the research questions, Mendeley Desktop and Google Scholar were used as the main sources for the papers. The search was done with no restricted timeframe. However specific search terms were used. For example, "Blockchain in Insurance", "Blockchain Insurance", and "Blockchain Application in Insurance" were used in April 2020. The process was repeated in November 2020. The search term with the highest results is "Blockchain in insurance" and was used to query a total of 578 papers.

B. Data Screening and Selection

As indicated in Table II, exclusion parameters were implemented before accessing the full papers. The types of papers that were included are peer-reviewed papers, book chapters, conference proceedings papers, short surveys, review papers, serials, white papers, official websites, etc. Enormous papers that satisfied any of the exclusion parameters (subject area, document type restrictions, and language) were excluded. Also, some papers were left out because of missing valuable information like authors' names, and abstracts. The search term fetched numerous articles but, most of them were rejected because their titles portrayed that they belonged to specific domains such as finance, legal, health, etc. All these were done without emphasizing author-specific or journal-specific papers. Other papers were excluded because they were not found although they appeared in the search query. Some papers also duplicated multiple times under different titles and were consequently excluded.

C. Descriptive Analysis

A total of 578 papers were fetched from the search term and a majority of them were excluded using the specified parameters in Table II. From Fig. 5, 455 papers were excluded resulting in the importation of only 123 into the reference manager. Out of the total number of excluded papers, nine papers were rejected after the importation because they appeared multiple times with different titles. Three papers

were included because they provided a strong theoretical foundation of blockchain technology although their titles were not in line with the thematic area. Twenty two papers were excluded because their contents were either unusable or not in line with the theme. Four papers were excluded by title but included by abstract and 15 papers could not be located by Google Scholar or regular Google search. Lastly, 12 papers were written in different languages other than English and

resulted in their exclusion. This resulted in the usage of 80 papers in this review. For the sake of simplicity, only the thematic papers are described and are depicted graphically in Fig. 4. In Fig. 4, it is observed that 6 papers in the area of blockchain technology and insurance were each published in 2016 and 2017. 21 papers were produced in 2018 and 27 papers were published in 2019. Lastly, 20 papers were published in 2020.

TABLE II. EXCLUSION AND INCLUSION PARAMETERS

| Parameter	Systematic Review	Grey Literature
Inclusion	• Peer-reviewed papers • Book chapters • Conference proceedings papers • Short surveys • Review papers • Serials etc.	• Regular Google search • Official websites
Exclusion	• Subject area (other domain-specific papers) • Language (Non-English) • Missing authors' names • Missing abstracts • Undiscoverable papers • Papers with unusable contents	
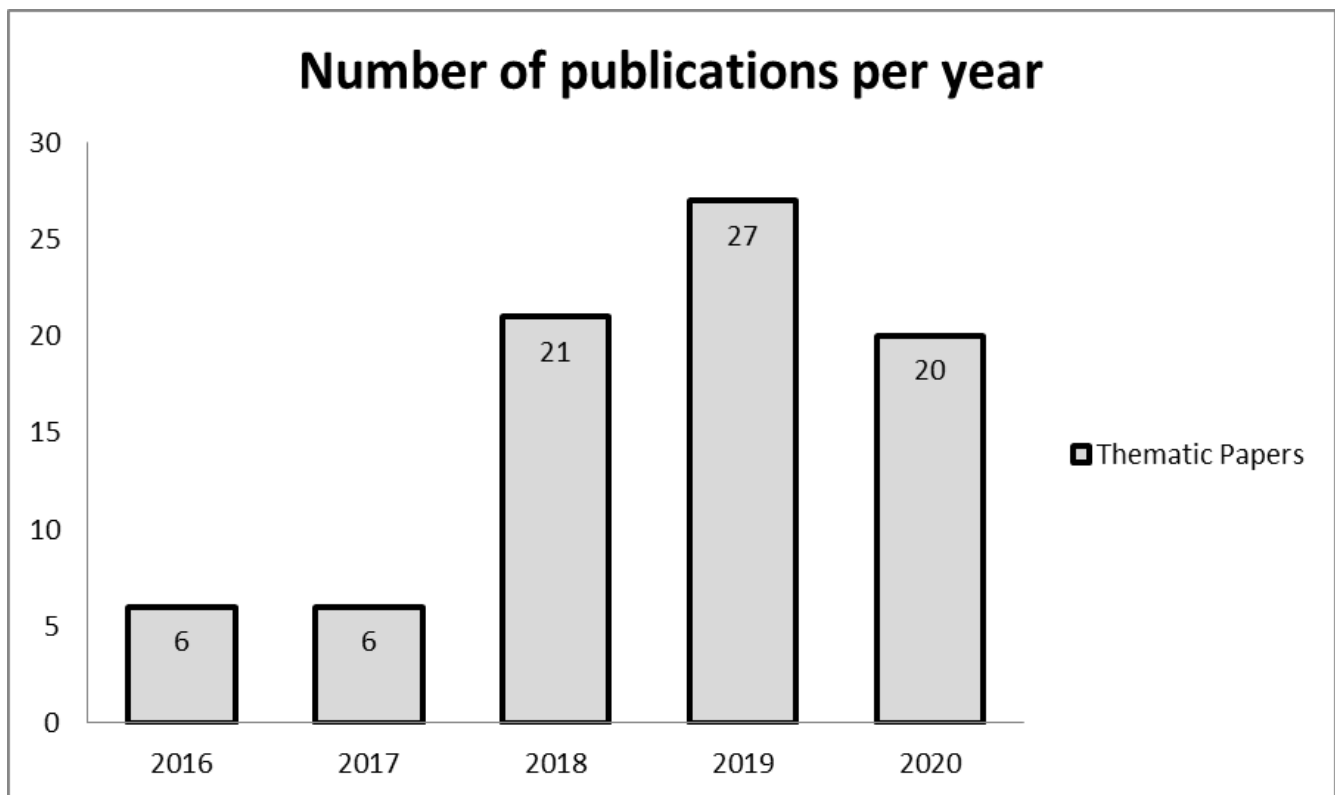
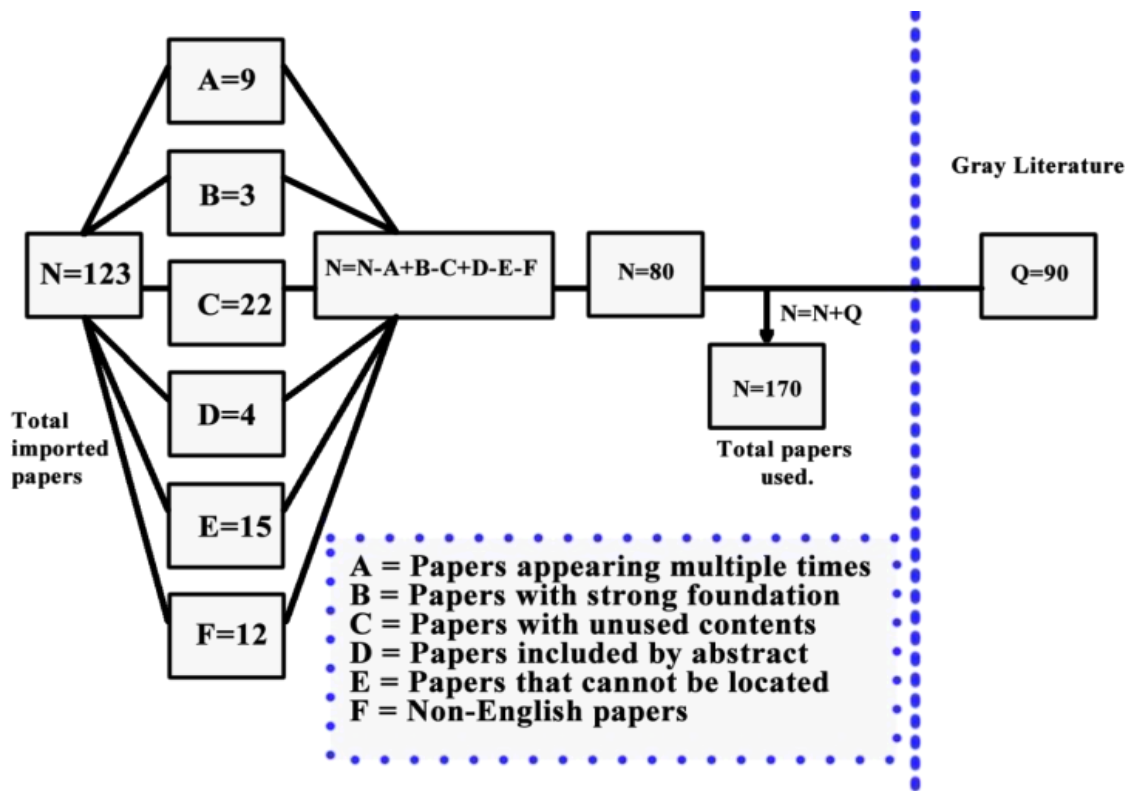Fig. 4. Yearly Publication of Thematic Papers.

Fig. 5.   Graphical view of the Search Strategy.

V.   RESULTS AND DISCUSSION

A. Major Types of Insurance

According to [56], although contemporarily found with numerous challenges, insurance is an avenue to provide financial risk mitigation that pays the policyholder in case of the occurrence of an unforeseeable adverse event or loss of property [57]. However, the industry is profoundly reliant on various processes between transacting parties to initiate, maintain, and close different classes of policies. Consequently, the processing time of transactions, settlement, and payment time of claims, and the security of the process execution are major concerns [58].

Futuristically, several existing breakthroughs in computing like Cloud Computing [18], Internet of Things (IoT) [59], Artificial Intelligence (AI), machine learning methods [60], and data analytics [61] will be joined and leveraged to automate and drastically transform the manner in which insurance processes are handled contemporarily. The following are the major types of insurance being provided by modern companies and how blockchain's contribution can be implemented.

1) Vehicle insurance: Vehicle insurance is an insurance policy covering motorcycles, trucks, cars, and other vehicles that apply roads. The main purpose of vehicle insurance is to ensure vehicle users' financial fortification against physical or property damage or bodily injury which results from an accidental collision on the road and also against any hostile traffic and vehicular happenings [62]. It was first introduced in

the United Kingdom in August 1930 by an act to regulate traffic motor vehicles on the road and to protect third parties from the dangers associated with vehicular movements [177]. In some cases, vehicle insurance offers a monetary bulwark against vehicle theft and other events like vandalism and natural disasters.

The overwhelming rate of road accidents and related fatalities and injuries necessitates vehicle insurance. Annual road traffic deaths stand at 1.35 million in 2016 [63]. The economic repercussions besides the deaths and injuries are enormous with over $300 billion annual costs which include travel delays, property damage, medical costs and pain, legal costs, loss of productivity, and loss of quality of life [64]. Without vehicle insurance, injured people would rarely get any recompense in a case of an accident, and motor drivers will mostly cope with considerable charges for injury and destruction of their car and property difficultly or find themselves in an illegal situation, apprehension, or might pay a fine [62]. In most countries, insurance premiums are paid regardless of vehicle usage or not [65]. For efficiency and customer satisfaction, vehicle insurance companies have offered discount programs [66] and designed enhanced business models to reduce the risk of losing revenue [67]. A classic example is the development and institutionalization of Usage-Based Insurance (UBI) [68, 69] which requires customized payable premiums based on vehicle usage to reward good or other driving habits. UBI supports the use of on-board devices [70], and telematics devices to capture relevant information like G-force, speed, mileage, time, location, and trip duration, informing the insurance company

about drivers' driving behaviour [71,69,67,72]. Policies in UBI are categorized as Pay As You Drive and Pay How You Drive [73,74] which makes them economical and precise for drivers [75,76]. Blockchain can be leveraged together with smart contracts to process claims promptly without going through tiresome bureaucracy which mostly results in the rejection of enormous claims. Also, the conditions that must be satisfied before payments can be automated quantitatively, therefore insured drivers or vehicles with rejected claims may accept the rejection and may not lead to further litigations which may also amount to extra costs [77,78]. Again blockchain can be linked with the IoT combined with efficient data capturing devices to collect, store, and process real-time data collected from targeted vehicles resulting in objective monitoring of vehicular movements [45]. This apparently will be particularly useful in usage-based premiums. The author in [65] designed a BC-based system that supports transparent management and analysis of data in a pay-as-you-go car insurance application to allow drivers who rarely use their vehicles to pay premiums on trips of interest. A blockchain system can be combined with smart contracts and sensors installed in customers' vehicles to manually modify policy coverage using environmental conditions for claims settlement and adjudication [79,80].

2) Home insurance: Many individuals and societies in the United States have been affected by natural disasters like Hurricane Harvey resulting in the destruction of their homes [81]. Home insurance – building or content insurance insures against events like fire, which destroy homes or domestic properties. In the United States, regular homeowners' insurance policies support costs resulting from hail, wind, and fire, but disregard damages caused by earthquakes and floods [82,81]. Without home insurance, disaster losses are possibly going to impact affected people to live sub-standard lives and in destitution. The wholesale insurance and reinsurance aggregated about 520 billion USD in Gross Written Premiums in 2013 [83]. In areas with great dangers of devastation, governments intervene and take obligation. Countries like the United States, Chile, France, Mexico, Germany, Japan, and the United Kingdom practice this when the risks are considered uninsurable [84].

Blockchain technology can be leveraged to automate claim applications and processing. Once a natural disaster is confirmed by the mandated state institution with the magnitude and level of impact, a smart contract can be triggered to effect payments to the affected communities. The monetary losses incurred by insurance companies from natural disasters ratcheted from $528 billion (1981–1990) to $1.6 trillion over the period 2001–2011 [84]. Between 2005 and 2006 the total loss in Europe was about $1 billion and $ 400 million in Australia [85]. In 2017 Hurricane Harvey resulted in about $25 to $37 billion in flood damage to homes in Texas. Presumably, administrative costs may take a huge chunk of the costs. Consequently, blockchain can be used to cut excessive human involvement and paper works by employing smart contracts [23]. Privacy issues may lead to the adoption of public or private blockchain where exact damage and recompense of individuals are accessed by authorized

users only. An example of such platforms is HurricaneGuard implemented on Etherisc [86].

3) Life insurance: Life insurance is a signed bond between an insurer and a policyholder or insured, where the policyholder is required to trade a premium in exchange for an assured amount of money in the case of the death of the insured [87]. A life insurance policy provides for the insured and their dependents in the case of bad events which lead to grief and the seizure of income. The amount to receive or the event to trigger the payment is highly dependent on the investment or the contract which can either be a terminal illness or a critical accident. Insuring oneself against life's uncertainties gives a cover of life risks, death benefits, return on investment, tax benefits, loan options, life stage planning, assured income benefits, and riders. The policies of life insurance are lawful agreements that stipulate the terms and describe the limits of the events insured. For example, some policies may exclude events of suicide, war, fraud, civil commotion, and riot. A major challenge of life insurance perhaps is that the beneficiary of a policyholder is required to present documents like a death certificate and the paper form of the policy [88] which can be destroyed by a natural disaster like flood and other occurrences. Also in the case where the policyholder holds numerous policies, the beneficiary may not be aware of their existence and therefore can also lead to inefficiencies and raise administrative costs unintentionally [89] as is the case in the United States where about 7.4 billion dollars exist in unclaimed life insurance money from insured people [90]. The life insurance industry can leverage blockchain as it helps to ensure information is accurate, secure, and trusted and ensure the transparent sharing of information between two or more parties [91]. Typically, instead of using contracts and agreements in paper form, blockchain-related smart contracts can be programmed to trigger and respond to all predefined services. As a substitute to trusting the insured to keep a copy of the policy, it can be recorded in the distributed ledger of blockchain making it available to the beneficiary, insured, insurer, and other entities (police, deaths and births registry, etc.) and transparently updated when necessary [89]. Smart contracts can also observe already existing platforms like Oracle to confirm and validate the demise of an insured together with other participants on the blockchain network through the consensus algorithm. Real-time clinical information can also be shared and digital proof can be easily amalgamated into insurance underwriting and the anticipation is a prospective mutation in the subdomains of product development and consumer pricing [91].

4) Disability insurance: Disability insurance (DI) is a type of insurance that protects the insured against loss of income resulting from disability. It is a social insurance program that provides income and health benefits to people who cannot work because of some form of disability [92]. It covers funded sick leave, temporary disability, and longstanding disability benefits [93]. According to 2015 statistics, the percentage of

people living with disabilities among the civilian population in the United States of America increased from 11.9 to 12.6 in 2014 [94]. Over 51 million (18%) American population stand to be categorized as disabled. Again, in every second and four minutes, incapacitating and deadly incidents occur respectively resulting in 3 out of 10 entry-level workers becoming disabled before retirement [95]. In 2014, the percentage of employed civilians between the ages of 18-64 living with disabilities was 34.4% of US civilians compared to 75.4% for people without disabilities, signifying a difference of 41 percent. The same report indicates that about thirty percent of working-age civilians living with disabilities were living in poverty as of 2014. DI is large and growing faster [92]. In 2012 the DI program in the United States paid beneficiaries about $136.9 billion. The programs of DI are associated with enormous impediments including a huge number of false rejections and minimal false acceptances [96,92]. With the characteristics of blockchain, numerous problems characterizing the DI programs can be solved. Certainly, there would be a database of civilians with disabilities indicating their level of severity. Smart contracts can also be used to determine the time to disburse payments and the amount to be disbursed to every participant depending on predefined parameters. This can be done transparently and automatically.

5) Health insurance: Due to low or loss of income, poor folks and most women in developing countries and all over the world become particularly vulnerable and suffer in the case of sickness because of the overburdened cost of medical expenses [97]. Most people are unable to save, own properties like lands or any valuable ornaments which can be sold to cater for the cost of seeking medical attention if the need be. It is a known case that health-related bills are the cause of depleting personal and family accounts into bankruptcy [97]. Diseases can propel well-living individuals and their families to deplete their accounts and or lead to deteriorating health conditions. Hypothetically, governments are supposed to provide their poor with health insurance schemes and health-related programmes [98]. The reverse is the case in practice [97]. This may be caused by the embezzlement of funds, increased administrative costs, social and political influence, unstructured processes, and mischievous intentions of hospital workers [99]. The process of medical billing is fraught with enormous challenges [99]. It begins when a patient enters the hospital and ends when the patient leaves which involves different stages like arrival, monetary restraints confirmation, coding, and billing, sending the bills to the insurance company, and receiving reimbursement [99]. A major challenge with the medical billing scheme is extreme billing, partly due to the absence of trust and transparency among the parties involved (patients, nurses, doctors, and insurers). Unceasingly, billing and claims are abused in the healthcare zone [99, 100, 101]. This is relatively so because medical bills are prepared on the blind side of the patient but this can easily be resolved by taking advantage of blockchain technology.

For example, by adopting a hybrid blockchain system, patients will be fully aware of the hospital services and prescriptions that lead to the payable amount and they may be required to validate the transaction before committing to the block and the transparency, decentralization, auditability, and immutability of blockchain will make all data in the ledger unchangeably available to all authorized participants [102,99]. Information sharing in the health care sector is extremely important regarding the sensitivity of medical records like patient's health status, medical records ([103]. A patient will be required to see numerous health specialists for a particular treatment or in a lifetime [104]. The manual information-sharing system is fraught with excessive complications and results in unnecessary charges and hassle for the patient [105]. Also, there is a lack of transparency and privacy [106]. Consequently, a cryptographically protected blockchain ensures patient privacy while providing an industry-wide, co-ordinated warehouse of healthcare data, bringing the industry billions in finances a year [105,107]. In this line, [107] and [18] proposed, designed, and implemented a blockchain prototype to ensure verifiability, privacy, and integrity of transactions in a health insurance claim. Medrec and Gem Health are examples of frameworks and blockchain-based systems used for information sharing and administration of medical health records [108]. Also, [109] propose MIStore to provide efficient verification and homomorphic computation, decentralization, and secured data.

6) Long-term care insurance: Long-term care insurance protects persons against the cost of receiving regular assistance for chronic disabilities (cognitive or physical). This form of insurance is different from health insurance in the sense that it is not meant for out-patient or specific diseases but to assist insureds in fundamental daily living activities like dressing, eating, and bathing and tasks that are essential for living like cooking, shopping, and any other housework [110]. Long-term care costs are usually covered by state programs (Medicaid, Medicare, etc.), private insurance companies, and the recipients and their families. The cost of long-term medical care is very expensive and as a result, government programs have limited the service coverage. Indeed, most of the expenses are covered by the beneficiaries and their families which exert enormous strain on their finances. For those who satisfy the complex and varying state eligibility rules, Medicaid pays for some amount to cover expenses like domestic health care, nursing home services, and community-based service to enable beneficiaries to remain in their respective communities [110]. Private companies in the domain of long term care insurance remain significantly low, mostly due to sector risks and liabilities. Confidently, support from private and corporate donors, philanthropists, charitable givers, and rich individuals can be very valuable to the beneficiaries and governments in general. An ability of blockchain is the quality of being leveraged to provide financial support for start-up companies and small businesses – Initial Coin Offering (ICO). ICO provides the platform for

company executives and individuals to request funds to start a company or business. One opportunity here is for public programs and private insurers to leverage blockchain to solicit financial support to cater for the substantial cost of seeking long term health care.

7) Marine insurance: Voyage transportation is loaded with enormous threats such as piracy, and cross-border shoot-outs as well as natural occurrences that can harm the cargo, ships, terminals, and vessels and cause massive monetary loss to individuals and companies [111]. This has necessitated the development and implementation of marine insurance which protects sea-based transport-related losses. The current initiative by major industry players like EY, Guardtime, Microsoft, A.P. Møller-Maersk, and insurance industry leaders like ACORD, XL Catlin, Willis Towers Watson, and MS Amlin – Insurewave, a built blockchain system to support marine vessel insurance. The initial capacity support is about half a million automated ledger transactions intended to deal with about one thousand vessels [112]. The leverage of blockchain and related distributed ledger helps to bring participants in a single network and ensure efficient execution of processes and maintain an immutable and accurate audit trail.

Since marine insurance is one of the oldest commercial insurance, most of the processes, practices, customs, and policy terms are structured and can be easily translated into programmable lines of code. Consequently, the brokerage purchasing process could be simplified by eliminating financial intermediaries and transparency can be improved among the parties by making quoting, binding coverage, and related activities visible to all participating stakeholders. Marine insurance processes would be greatly enhanced. For example, payments of premiums will be fast and straight into the accounts of the insurer and the policy will be made available upon receipt of funds. With transactions immutably and transparently stored in the blockchain ledger, conflicts will be resolved as quickly as possible [113]. In events of cargo loss, total loss, or products and goods contamination as in pharmaceuticals and food, smart contracts can be developed to trigger payments when the necessary notification and verification have been done and the proof has been submitted to the blockchain ledger.

B. Implementation of Blockchain in Insurance

According to [91], the following are the general blockchain benefits in insurance. Event-triggered smart contracts, increased back-end efficiency, disintermediation, better pricing, and risk assessment, new types of insurance, and reaching the underserved Blockchain-based applications can be very valuable to all insurance companies - travel, agriculture, Assets, medical Insurance, because of the inherent facility to provide long-lasting strategic benefits in terms of lowering operational costs by reducing or eliminating overlapping processes, enhancing automation, reducing counterparty risks and providing secure, transparent and decentralized transactions [114].

Most of the contemporary insurance applications adopt the client-server architecture which has worked well for quite a long time now. However, it must be mutated to enhance security and efficiency [45]. Client-Server Architecture is a computing model in which the server keeps, provides, and controls most of the services and resources to be consumed by the client. Clients request and access resources over a computer network or through an internet connection. Although systems using this architecture perform better and serve the needs of enterprises, their very nature makes them suffer some limitations. Systemic failure can affect all operations that rely on the server. Although safety procedures might be put in place, there is still a higher probability that the data can be manipulated in the server accidentally or deliberately [62]. The following are some key areas in the insurance domain that Blockchain technology can enhance and/or help prevent.

1) Claim submission and processing: The author in [114] designed a blockchain-based system that supports quick insurance claim processing. Insurance claim processing can be very tedious, time demanding, inefficient, and susceptible to human errors especially where validation is done through paperwork processes [115, 116]. Also, there is a lack of transparency in the submission of claims and the processing is associated with adverse effects of delays and blunders leading to unsatisfactory customer services [40,45, 117]. Insurance claims is a circulated process involving several entities – insurer, insured, regulators, and third party entities, mostly characterized by inefficiencies and malicious intentions [118].

Blockchain can drastically reduce the claim creation, accepting, and processing time and make it hassle-free, and less costly using smart contracts once the policy conditions for payment are unambiguously clear [119,118,21, 120,121]. Blockchain can be employed to create immutable and auditable statements at the various stages in the insurance claim processing that can be re-accessed by all participants. The benefit would be to reduce the risk and cost of transactions and improve trustless computations. Blockchain has also emerged as impressive technology to provide high efficacy solutions to the problems of contemporary insurance systems (45,122,117]. As an example, a novel system is being worked on by ANZ Bank, Suncorp of New Zealand, and IBM to ensure efficient and smooth transmission of data and premium payments between insurers and brokers. By involving blockchain in the storage and update of data, there would exist a single version of truth between insurers and brokers and smart contracts can execute to commence payments automatically [20]. Also, Allianz has employed digital tokens to pay its worldwide affiliates thereby alleviating the challenge of currency exchanges [20]. Also, AXA French insurance company launched a smart contract based flight-delay insurance product to reduce cost, improve customer engagement, and develop new insurance products [123]. InsureETH a startup in UK, and the project of American International Group (AIG) have similar objectives [124]. Fig. 6 shows a theoretical way of handling claims using blockchain as proposed by [125].
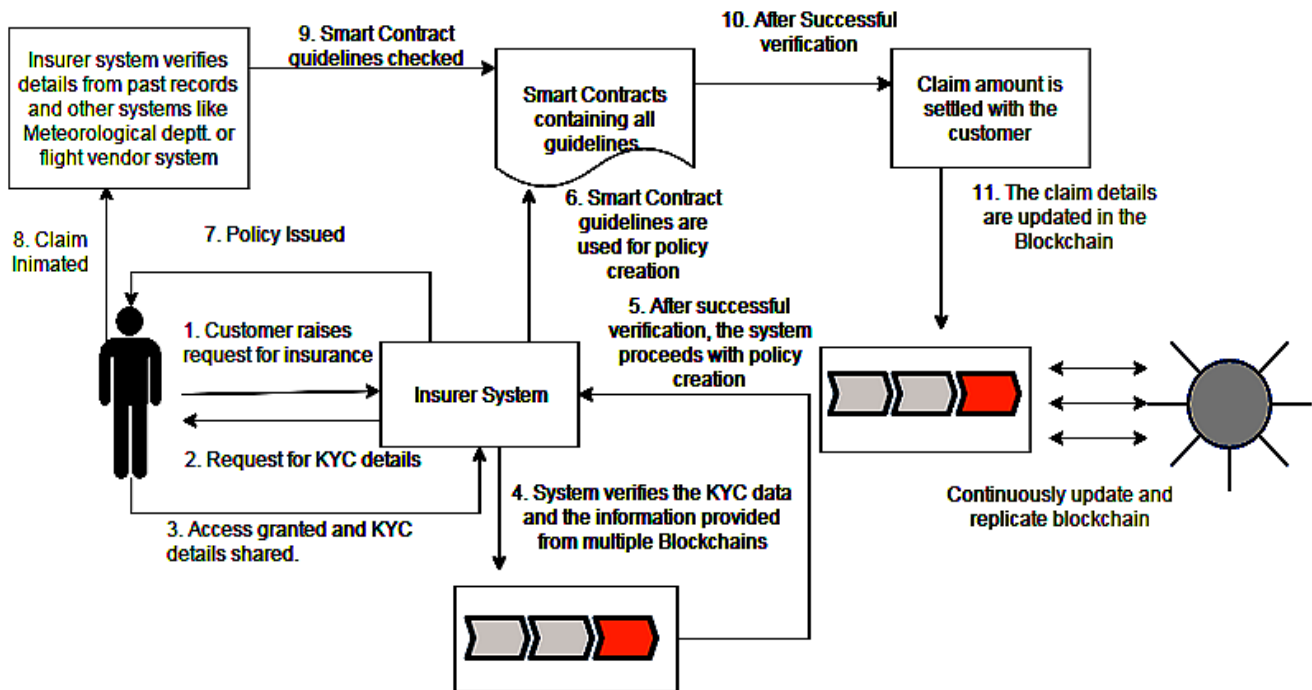
Fig. 6. Claim Submission and Processing using Blockchain.

2) Fraud detection and prevention: The insurance companies stand high chances of losing good treasure as a result of claims of fraudulent nature [45,126]. Inadvertently, fraud increases yearly [18] and by estimation, about 5 to 10 percent of all annual claims are fraudulent and the FBI indicates that it costs US non-health insurers over 40 billion every year [127,128] which results in extra costs for policyholders in increased premiums. Similarly, in the UK, claim fraud results in about £3 billion annually [128]. Ditching, Cash for Crash, Double Dipping are some recorded frauds in vehicle insurance [62]. Again the centralized nature of insurance systems affects the integrity and transparency of the data stored in them [45]. Identity theft is another way of fraudulently acquiring and using another person's information thereby impersonating the genuine owner to enjoy unbefitting benefits [129, 130]. An authorized malicious insider can manipulate internal data for financial benefits which can be very detrimental to the company. Blockchain can eliminate the limitations of client-server architecture to prevent fraud. The transactions in Blockchain are visible to all participants and

original statements, policies and contracts are very difficult to mutate [118,62]. The consensus protocol ensures that without any central governing body, any modification to the database happens at an agreeable rate and does not affect the integrity of the data. Again Blockchain can minimize forgery, document or contract alterations, multiple booking [118] as the distributed ledger can be shared among multiple trusted parties like medical doctors and security agencies to create and update [79,130].

The validation of the authenticity, provenance, and ownership of goods and documents is made easy with blockchain. The encryption method applied by blockchain can prevent cyber liability where personally identifiable information can be impaired by third party entities who store such data. Blockchain can eliminate trusted third-party companies whose presence adds value and overheads by authenticating the validity of submitted documents [79]. Fig. 7 demonstrates a framework to detect and eliminate fraud during claim submission and policy issuance as proposed by [125].
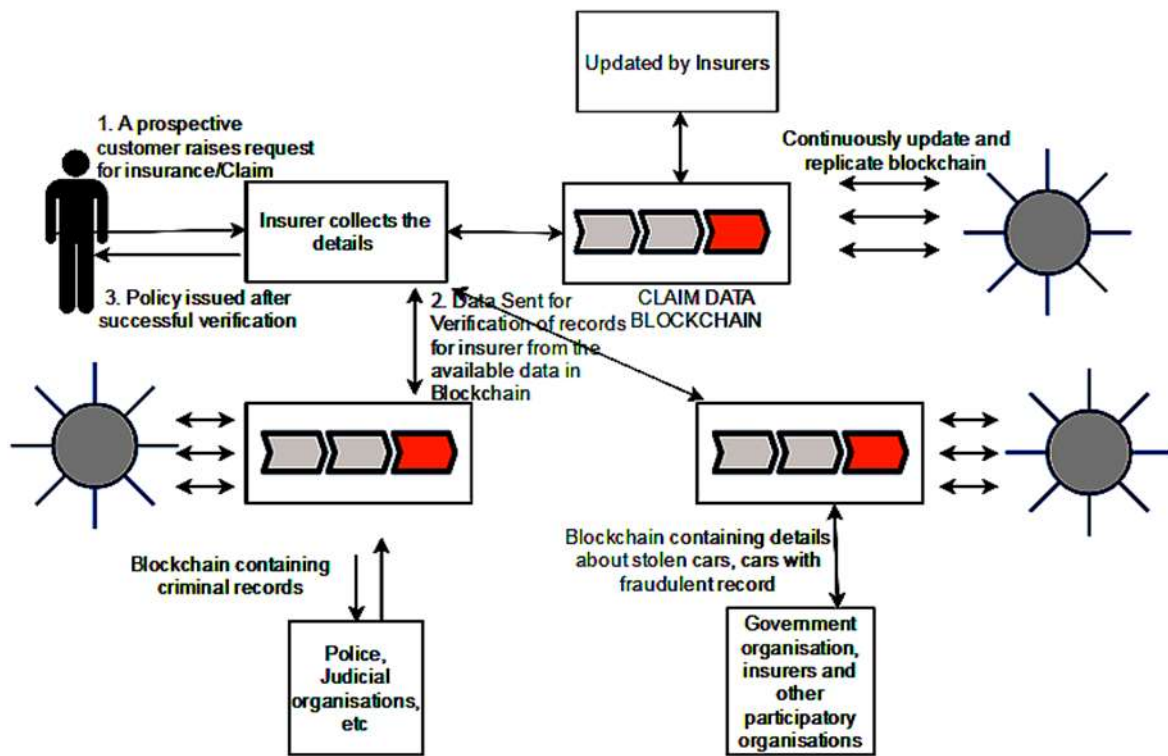
Fig. 7. Framework for Fraud Detection during Claim Submission or Policy Issuance.

3) Data entry and identification: A little over sixteen percent of the world's population is without recognized proof that they exist [131]. Consequently, there is a need for virtual identification systems. Fortunately, there exist numerous means to electronically and accurately identify people for who they are and to authenticate their characteristics [132,12,133]. In insurance, the storage of wrong and unverifiable data can have extremely negative effects and support for fraudulent activities [79]. The employment of blockchain in insurance can prevent writers from modifying previously stored data, as data are shared among all participating members in an unchangeable and append-only manner. Immutably hashing the IDs of data originators enforces non-repudiation, data integrity, and authenticity.

4) Sharing of intelligence data: Insurance systems face numerous systemic flaws that are exploitable by malicious persons [118]. This results from creating multiple policies and synthetic Identification numbers with the same device. Apparently, insurers invest in public data and subscribe to service providers to get informed about fraud investigation and prevention. In the past, insurers have tried to share intelligence but suffered technological, commercial, and legal roadblocks as a result of confidentiality and national and corporate access control policies [118]. Health records exist in digital formats however communication of such data among healthcare providers remains a challenge [134]. Cyber-insurance has not been widely accepted by insurers and coverage is restricted to business interruption, stolen of digital

assets, and data breach, mainly because of the unavailability of accurate data, legal and procedural approaches for auditing, and assessment of organizational security strength [135; 136]. The comprehensive and palpable benefits of employing blockchain to share insurance-related data will comprise accountability, ledger immutability and transparency, data decentralization, and security [137,138, 139,140]. A group of insurers can team up to initiate a Blockchain network for the system, to host enormous distributed processes on the network, with no single proprietor [118]. The financial sector keeps a record of the credit history of their customers which is accessible to all permitted financial companies and other institutions. Similarly, BC can be used to record insurance premium payments history and other records for access and usage by other insurance companies almost instantly and accurately [21]. [141] propose a scheme to authenticate insurance transactions based on blockchain to solve the problems of security, high cost of data management, and easy data manipulation.

5) Peer to Peer insurance: Peer to Peer insurance (P2P) is a new type of insurance that gives like-minded insureds with the same insurance needs and interests the chance to consolidate their funds and manage their private insurance. P2P insurance is different from traditional insurance in the sense that, there is a drastic reduction in the expenses of managing the insurance policy, re-insure insureds when claims surpass the pool and also pay themselves using reserves. This is as a result of bureaucracy bypass, reduction in paper works,

minimal workers, and more [142]. P2P insurance companies make filing a claim and receiving payment less costly, easy, automatic, fast, and transparent mostly by using online service or mobile application. Examples of P2P insurance companies are Tong JuBao in China [143], Guevara in the UK [144], and Friendsurance in Germany [74,145). Dynamis is a P2P complementary protocol for unemployment insurance that replaces the underwriters with policyholders' social capital and Enigma while ensuring complete privacy, provides the platform for diverse parties to mutually store and perform computations on data [146]. The core characteristics of blockchain have a direct link with the characteristics of P2P insurance – decentralization, speed, automatic, ease of use. A smart contract can be used for claim filing and processing and also automate payouts. Claims are approved by the majority of the blockchain participants before disbursement of the amount after which the reserve is shared among the remaining insureds or given to charity homes [147]. At this point operations research techniques can be applied together with a smart contract running on the blockchain network to ensure the fair and transparent distribution of payouts and reserves.

6) Getting rid of middlemen: Middlemen exist in the insurance companies for numerous reasons – for claims data or document preparation and submission on behalf of the claimant, ensuring the right documents are acquired and submitted. The use of middlemen in insurance offers some value for the insurers and the insureds. However, their existence introduces bottlenecks in the process – delay in claims processing and extra cost for the participants involved [148,127].

The architecture of Blockchain eliminates all brokers [6], thereby attributing to each partaking company, the original copy of the ledger. The peer-to-peer nature of blockchain and the consensus algorithm allows the peers to interconnect and transfer data among themselves. The employment of this technique may drastically reduce the approval time of transactions from days to seconds automatically thereby meaningfully improving efficiency at a minimal cost [148,6]. Indeed, by eliminating the need for a middleman, the technology has the potential to disrupt many activities in sub-sectors of the insurance that currently rely on a trusted authority or intermediary operator.

7) Know-Your-Customer and Anti-Money Laundering (KYC/AML): Insurers, reinsurers, and brokers perform auditing processes to know their customers and also prevent money laundering and it usually involves multiple entities like individuals and legal personnel [21]. In a case where an insured deals with a broker who works with numerous underwriters which in turn deal with reinsuring brokers, such a transaction will involve multiple participants who have to follow the KYC/AML processes along the value chain. Obviously, this overlay of processes adds to processing cost and time [21]. London's leading commercial think-tank Z/Yen has commenced IDChainZ which is a scalable, globally available, and subject-cantered operational proof of concept fabricated using ChainZy mutual distributed ledger technology which allows several parties to add, certify and exchange KYC and AML documentation [149]. IDChainZ is intended to reduce processing time and cost, make time-critical transactions presently uninsured and reduce operational risk [21]. Fig. 8 is a framework for KYC/AML as proposed by [125].
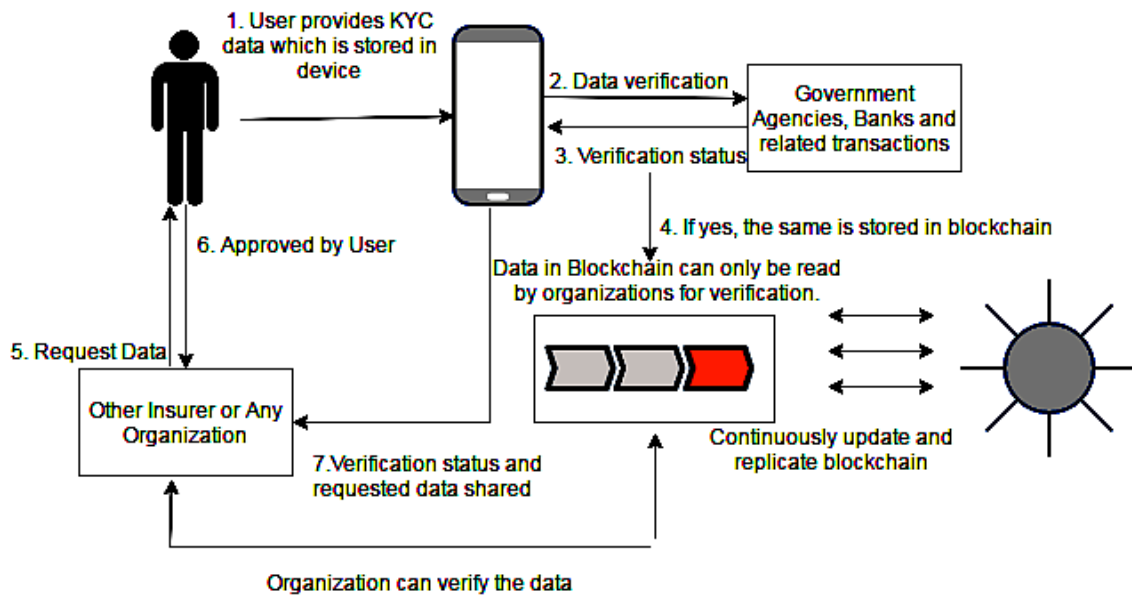

Fig. 8.   KYC Compliance Framework using Blockchain.

C. Limitations of Blockchain Technology

Despite blockchain technology's tremendous potential in advancing existing systems with smart contracts, major gaps remain within its implementation as a libertarian-rooted, privacy-minded, decentralized cryptocurrency and a technology stack that fully satisfies business, security, and regulatory requirements [41]. As an emerging technology hurdles exist to impede its wide acceptability and the realization of its full potential. Blockchain is no exception. The following are the challenges of adopting Blockchain in insurance [129,127].

1) Scalability: Blockchain is expected to grow in popularity and acceptance and when these are realized, the current infrastructure may not be able to support the growth. Practically, the available computing resources limit the insurance industry from reaching the apogee of implementing blockchain technology. Theoretically, with the current infrastructure, about 1000 transactions should be verified by Ethereum in a second. The number reduces to about 10 which is very small compared to Visa and Paypal, which can verify about 1670 and 193 transactions per second respectively [150]. The current consensus algorithm for permissionless blockchain requires 50 percent plus one participant to agree on the validity and authenticity of blocks and transactions. The case for permissioned blockchain is different with pre-known nodes. In a blockchain, every block has a limited block size, and time interval [150,151]. As the number of network nodes increases, the number of transactions to be processed also increases, however, the scalability decreases. Conceptually, sharding was proposed to enhance blockchain's scalability likewise Super Quadratic Sharding. However, results from implementation may prove otherwise. The decentralization of data and processing capabilities require that individual nodes be possessed with the capability to handle transactions for a growing number of users. At the moment, blockchain works well with a smaller number of participants however, to validate data on a real-time basis and ensure efficiency, the broader as-is nature of the insurance industry needs a different perspective for its larger population. Consequently, there is a need for gargantuan storage space, enhanced consensus algorithms, and robust computing power.

2) Expertise: Blockchain technology is a relatively novel innovation and a broad specialization with minimal books and technical knowledge distributed across multiple websites [152]. The technical and technological know-how are other limitations of blockchain systems development. The proficiency and expertise essential to create, apply, and maintain blockchain systems are still at the juvenile stage [129]. There are some successes as few platforms use blockchain without hindrance. However, stability and speed would be required if the technology would be extended to other industries.

3) Security, Data privacy and management: Blockchain in its current form has a lot of vulnerabilities and limitations in terms of security privacy and data management [153,154,155]

and a lot of field practitioners and academicians have pointed out that blockchain does not adhere to existing privacy laws such as the EU General Data Protection Regulation [156]. Bitcoin, the famous blockchain application operates the public ledger type and the source code is open which defies privacy and confidentiality [12]. This can be solved by implementing the private type of blockchain [129]. Also, enormous encryption and anonymization techniques can be used successfully but also come with challenges in terms of speed, portability, and scalability [129,12]. In the contexts where the number of nodes is expected to grow tremendously like IoT, implementing such a mechanism can be too challenging [157,12]. Again to prevent the release of sensitive data, secure file sharing protocol methods like telehash, Whisper [158], or content-addressed file system can be used [157].

Although blockchain is 'tamper-proof', the nodes writing to and reading from the blockchain applications can be vulnerable. In case of an attack, the target is not the blockchain application or ledger itself but the external systems such as cryptocurrency wallets. If the data input node is compromised, it will lead to the storage, processing, and usage of inaccurate and misleading information [156]. It is known that the transactions of bitcoin can release massive confidential data [159,12] which confirms the transactional privacy problem of blockchain [160]. In the case of public blockchain applications, the data stored is made available to all involved nodes and it is similar to posts made onto the public Internet [156]. Just like any other computer program, smart contracts also usually comprise bugs that can lead to serious consequences [12]. Decentralized Autonomous Organization (DAO) attack (Siegel, 2016) is an identified weakness in SC which led to a loss of about 47 million dollars and the Parity wallet weakness which also allowed the orchestration of about 280 million dollars [161,12]. Besides the aforementioned susceptibilities of SCs, there are other numerous ones. Solutions have been proposed to mitigate the effects of the identified vulnerabilities [162] and the most encouraging is the approach that attempts to submerge the expressiveness of the underlying programming language [12,158]. Other frameworks exist [163,164], which look for bugs by verifying the correctness and fairness of smart contracts. With Discouragement Attack, [165] propose the use of insurance contract theory to ascertain the withdrawal delay case studying cyber insurance to thwart the attack victims damage.

4) Regulation, standardization, and taxation: It is important to note the effective law scheme and the applicable risk management that can be used in public blockchain systems. Nevertheless, in private blockchain systems, the consensus algorithm can be designed to enforce some internal governance scheme and legal framework which will store the rules that will apply to transactions [156]. The conflict resolution process is also required in private blockchain systems. At the moment there is no comprehensive universally acceptable regulatory response to blockchain [166] despite efforts by government and supranational organizations [167]. In a 2018 survey [168], it was discovered that the most

frequent government involvements in blockchain-related issues are the issuance of public educational notices mainly about the vulnerabilities and risks associated with cryptocurrency investments by the central banks. In such cases, the people are warned about the difference between cryptocurrency and actual currency and as such indicate the cryptocurrency is not unregulated and guaranteed by the state. Hence any form of investment in cryptocurrency is perilous [168]. Various countries also issued a warning indicating how cryptocurrency provides a fertile ground for dishonest deeds like terrorism and money laundering. In effect countries like Canada, Australia and the Isle of Man changed their laws to include cryptocurrency and related companies and activities under the laws of financing counterterrorism and money laundering. In countries like Algeria, Vietnam, Nepal ban all events involving cryptocurrencies. Qatar and Bahrain ban and permit their citizens from engaging in cryptocurrency within and outside of their borders respectively. Readers can refer to the [168] for a full report of how countries are regulating cryptocurrency. In particular, understanding who is accountable and legally responsible is a major challenge.

The extension of the existing tax framework to the virtual companies is extremely difficult and has presented enormous challenges globally [156] and taxation of cryptocurrencies is a major question posed by many [168]. Even so, not many countries support the use of cryptocurrency and consequently do not have appropriate taxation structures for cryptocurrencies. As of 2018, only a few countries had instituted measures to tax virtual currency [168]. These countries are indicated in Table III. Taxation of blockchain faces bottlenecks partly because there is a debate Among European Union Member States Cryptocurrency investments are not subject to Value Added Tax (VAT) primarily due to the European Court of Justice ruling in 2015 [168]. No country in Sub Sahara Africa has applied a taxation scheme to cryptocurrency except South Africa. Contemporarily, Ghana has not regulated the employment of blockchain and in effect, blockchain-related systems that intends to take a virtual currency or cryptocurrency payments could be considered illegal when multiple nations participate.

5) Suitability and compatibility: The suitability of blockchain in all situations is questionable especially in data management, although the future looks promising and a lot of companies are enthused about the potential of blockchain to transform the virtual infrastructure and solve numerous [12,169]. Because most IT Officers do not understand the basics of blockchain, they hike their interest and predict the use of it in every IT project [12]. In a project where data storage is not required blockchain will probably be of no significance. Furthermore, if only one administrator is needed to read and write content, then blockchain is inappropriate.

Contrarily, blockchain is powerful in a computing environment where trustless entities transact and data need to be permanently stored [12]. Typically blockchain can be very useful when known mistrusting entities will store and change the content of the ledger [170].

6) Sharding: Contemporary centralized applications and storage systems may not work efficiently in this age of Artificial Intelligence, IoT, machine learning, Big Data, all running in the cloud [171]. To accommodate scalability, availability, manageability, security, and reliability, existing systems have to be modified [171,50]. The concept of sharding has been around for some time now and works well in database systems providing low-cost high-performance computing. Traditional non-sharded databases usually installed on a single database are prone to a single source of failure leading to the crumbling of the complete business application [171]. AES256-CTR is used to encrypt files at the client-side before they are sharded as in Fig. 9 and the encryption key is completely controlled by the data owner so contents are protected from the company providing the storage space [50].

In blockchain, sharding can be considered a challenge. According to [50], shards can be described as well-designed self-governing blockchain which interconnects with one another. Validators are used to monitor shards and if the total number of shards is $S = O(c)$, where c is the overall number of transactions supported by a shard, then the method can take a maximum of $O(c^2)$ transactions. If the number of shards increases in a composite manner, then the number of transactions will exponentially grow to $O(exp(c))$ [50]. When an application has a shard with minimal interactions or users, then the implementation may be easier and cross-shard communication can be enabled by securely passing information using receipts. Most blockchain systems recently in use are not scalable so most operations can be run on a single shard. However, introducing multiple shards and subsequently implementing cross-shard interaction and asynchronous communication can have serious operational impediments [50].

TABLE III.   COUNTRIES WITH BLOCKCHAIN LEGAL FRAMEWORKS AND REGULATIONS

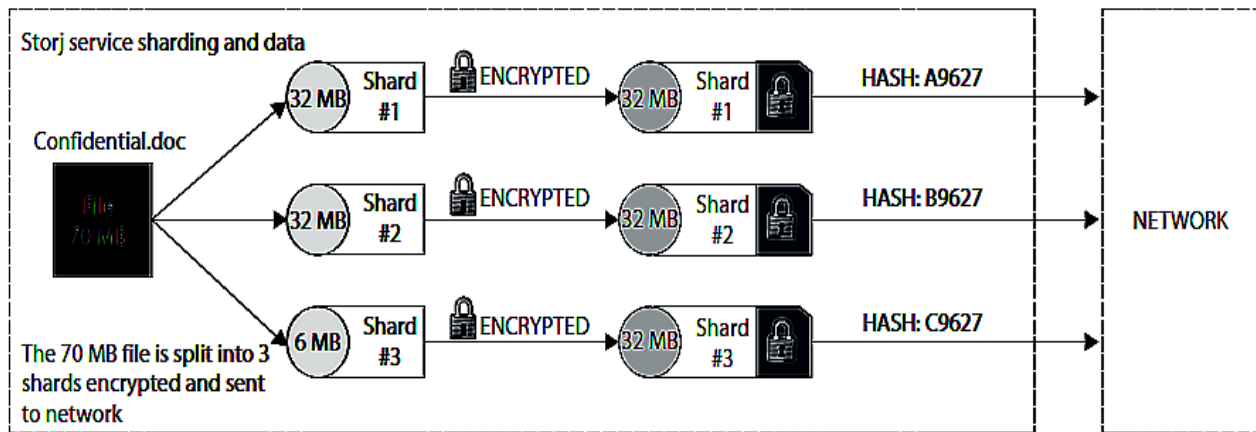| Country	Form of Taxation
Israel	Asset
Bulgaria	Financial Asset
Switzerland	Foreign currency
Argentina	Income tax
Spain	Income tax
United Kingdom	Corporate tax, income tax, capital gains tax

Fig. 9.   Sharding Processes. Source:[50].

D. *Discussion*

Blockchain technology has emerged as contemporary disruptive technology. As indicated in section II, numerous works have been done to expand the applicability of blockchain 3.0 to other domains other than the financial sector. However limited works exist in the insurance industry. Therefore we review various opportunities and threats available in this endeavour. It has been observed by industry and academic researchers that the most important business processes that can be improved or re-engineered in the insurance sector are issues of claims and fraud. The nature of blockchain and its features like cryptography, consensus algorithm, decentralization, etc. make it an ideal solution for the insurance sector. Hashing of the identities of the participant in the blockchain network provides a solution to the problem of data identification and sharing of intelligent data. The blockchain P2P could create a new line of insurance products and get rid of trusted middlemen. This review was done to uncover the prospects to position us well to embark on our future works. At the moment blockchain technology also possesses numerous challenges including security and data privacy, scalability, regulation, and taxation. Although the individual technologies upon which blockchain is mounted is matured, their integration presents come susceptibilities. Blockchain will become a very powerful tool so mitigate many of the technology problem facing the insurance industry.

VI.   Conclusion and Future Direction

Ever since blockchain gained public attention, researchers have proposed and developed numerous frameworks, systems, and applications. The financial sector has almost fully benefited from blockchain and so the trend has moved to other domains like supply chain management [175], health, government, law, and more. This work focused on reviewing and producing a simple literature review on blockchain technology with a peculiar interest in the opportunities and threats in the insurance domain. It was discovered that the insurance sector as enormous as it is now can also leverage blockchain technology to enhance core internal processes like claim submission and processing, fraud detection and prevention, etc. Blockchain can also be used to mutate and possibly produce new brands of insurance and also enhance existing ones. It is also a discovery that BC possesses several challenges including scalability, security, and privacy, taxation and regulation, etc. The Insurance sector has not received the beneficial exploitation of blockchain 3.0. As indicated all initiatives by the insurance industry players are at the beginning stages. Therefore, subsequently, several pieces of research will be conducted to broaden the existing academic literature in terms of leveraging blockchain to enhance the core insurance business processes (Claims submission and processing, fraud detection and prevention, etc.) and mutate existing InsurTechs like Usage Based Insurance in vehicle insurance. We will also employ operations research techniques like game theories to enhance and theoretically create multiple insurance products like the Peer to Peer insurance, health insurance, etc. Again, in private blockchain systems, presumably, not all data are needed by all nodes so decentralization of the full ledger may be technically insignificant and may add to the storage, scalability, and performance issues. Consequently, to increase performance we are is going to research how to extract and store the most contextually relevant data especially in a private blockchain.

References

[1]   B. Cohen, J. Ernesto Amorós, "Municipal demand-side policy tools and the strategic management of technology life cycles," Technovation 2014. https://doi.org/10.1016/j.technovation.2014.07.001.

[2]   V. J. Morkunas, J. Paschen, E. Boon, "How blockchain technologies impact your business model," Bus Horiz 2019. https://doi.org/10.1016/j.bushor.2019 .01.009.

[3]   S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Manubot 2008. [Google Scholar].

[4]   C. S. Wright, "Bitcoin: A Peer-to-Peer Electronic Cash System," (August 21, 2008).

[5]   T. Ahram, A. Sargolzaei, S. Sargolzaei, J, Daniels, B. Amaba, "Blockchain technology innovations". IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017, 2017.

[6]   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.

[7]   J. Kietzmann, C. Archer-Brown, "From hype to reality: Blockchain grows up" Business Horizons. 2019 Jan 1; 62(3):269-71.

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

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

[10] 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).

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

[12] F. Casino, T. K. Dasaklis, & C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues" . Telemat Informatics 2019.

[13] 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.

[14] 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.

[15] 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.

[16] D. E. Kouicem, A, Bouabdallah, H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks. 2018 Aug 4;141:199-221.

[17] 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.

[18] W. Liu, Q. Yu, , Li, Z., Li, Z., Su, Y. and Zhou, J., "A Blockchain-Based System for Anti-Fraud of Healthcare Insurance," In *2019 IEEE 5th Int. Conf. on Compu. Commun. (ICCC)* (pp. 1264-1268). IEEE.

[19] M. Sharifinejad, A. Dorri, J. Rezazadeh, "BIS-A Blockchain-based Solution for the Insurance Industry in Smart Cities," arXiv, 2020.

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] M. Tsukerman, "The Block is hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future," Berkeley Technol Law J 2016.

[26] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, R. Brooks "A brief survey of Cryptocurrency systems," 14th Annu. Conf. Privacy, Secur. Trust. PST 2016, 2016.

[27] M. Conti, E. S. Kumar, C. Lal, S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Comm. Surveys & Tutorials, 2018 May 31;20(4):3416-52.

[28] M. C. Khalilov, A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," IEEE Comm Surveys & Tut. 2018 Mar 26;20(3):2543-85.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," Proc. - IEEE Symp. Secur. Priv., 2015.

[30] H. N. Dai, Z. Zheng, Y. Zhang, "Blockchain for Internet of Things: A Survey," IEEE Internet Things J 2019.

[31] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," Int J Adv Sci Eng Inf Technol 2018.

[32] B. K. Mohanta, D. Jena, S. S. Panda, S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges," Internet of Things 2019.

[33] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, "A survey on privacy protection in blockchain system," J Netw Comput Appl 2019.

[34] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," IEEE Access 2020.

[35] R. Brophy, "Blockchain and insurance: a review for operations and regulation," J Financ Regul Compliance 2019.

[36] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V, Santamaría. Blockchain and smart contracts for insurance: Is the technology mature enough? Futur Internet 2018.

[37] A. Kamilaris, A. Fonts, F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," Trends Food Sci Technol 2019.

[38] Ž. Turk, R. Klinc, "Potentials of Blockchain Technology for Construction Management," Procedia Eng., 2017.

[39] K. Valtanen, J. Backman, S. Yrjola, "Blockchain-Powered Value Creation in the 5G and Smart Grid Use Cases," IEEE Access 2019.

[40] 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.

[41] A, Tapscott, D. Tapscott, "How Blockchain Is Changing Finance," Harv Bus Rev 2017.

[42] 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.

[43] N. P. V. Sravan, P. K. Baruah, S. S. Mudigonda, "Use of Blockchain Technology in integrating Heath Insurance Company and Hospital," Int J Sci Eng Res 2018.

[44] S. Ølnes, J. Ubacht, M. Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov Inf Q 2017.

[45] 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.

[46] Y. C. Chen, Y. P. Chou, Y. C. Chou, "An image authentication scheme using Merkle tree mechanisms," Futur Internet 2019.

[47] L. S. Sankar, M. Sindhu, M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017, 2017.

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

[49] 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.

[50] 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.

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

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

[53] C. Saraf, S. Sabadra, "Blockchain platforms: A compendium," IEEE Int. Conf. Innov. Res. Dev. ICIRD 2018, 2018.

[54] R. B. Briner, D. Denyer, "Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool," Oxford Handb. Evidence-Based Manag., 2012. Google Scholar.

[55] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," PLoS Med 2009.

[56] O. Mahmoud, H. Kopp, A. T. Abdelhamid, F. Kargl, "Applications of Smart-Contracts: Anonymous Decentralized Insurances with IoT Sensors," Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree, 2018.

[57] H. Mohamed, "Takāful (Islamic insurance) on the blockchain," Growth Islam. Financ. Bank., 2019.

[58] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay, K. Y. Lam, "A Blockchain Framework for Insurance Processes," 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc., 2018.

[59] M. Vahdati, K. G. Hamlabadi, A. M. Saghiri, H. Rashidi, "A Self-Organized Framework for Insurance Based on Internet of Things and Blockchain," Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud.

[60] N. Dhieb, H. Ghazzai, H. Besbes, Y. Massoud, "A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement," IEEE Access 2020.

[61] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. Mong Goh, X. Liang, "Blockchain and IoT Data Analytics for Fine-Grained Transportation Insurance," Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS, 2018.

[62] R. Roriz, J. L. Pereira, "Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector," Procedia Comput. Sci., 2019.

[63] World Health Organization, https://www.who.int/gho/road_safety/ mortality/traffic_ deaths_number/en/ unpublished.

[64] S.L. Poczter, L. M. Jankovic, "The Google Car: Driving Toward A Better Future?," J Bus Case Stud 2013.

[65] H. T. Vo, L. Mehedy, M. Mohania, E. Abebe, "Blockchain-based data management and analytics for micro-insurance applications," Int. Conf. Inf. Knowl. Manag. Proc., 2017.

[66] L. M. Palma, F. O. Gomes, M. Vigil, J. E. Martina, "A Transparent and Privacy-Aware Approach Using Smart Contracts for Car Insurance Reward Programs," InInternational Conference on Information Systems Security 2019 Dec 16 (pp. 3-20). Springer, Cham.

[67] S. Husnjak, D. Peraković, I. Forenbacher, M. Mumdziev, "Telematics system in usage based motor insurance," Procedia Eng., 2015.

[68] P. Handel, I. Skog, J. Wahlstrom, F. Bonawiede, R. Welch, J. Ohlsson, "Insurance telematics: Opportunities and challenges with the smartphone solution," IEEE Intell Transp Syst Mag 2014.

[69] J. Wahlström, I. Skog, P. Händel, "Driving behavior analysis for smartphone-based insurance telematics," Proc. 2nd Work. Phys. Anal., 2015.

[70] Lin W-Y, Lin FY-S, Wu T-H, Tai K-Y. "An On-Board Equipment and Blockchain-Based Automobile Insurance and Maintenance Platform," In Int Conf on Broadband and Wireless Comp, Comm & Appl pp. 223-232, 2020.

[71] F. Li, H. Zhang, H. Che, X. Qiu, "Dangerous driving behavior detection using smartphone sensors," IEEE Conf. Intell. Transp. Syst. Proceedings, ITSC, 2016.

[72] R. Harbage, "Usage-based Auto Insurance (UBI)," 2011 https://www.casact.org/community/affiliates/sccac/1211/Harbage.pdf unpublished.

[73] A. Kumar, A. Prasad, R. Murthy, "Application of blockchain in Usage Based Insurance," Int J Adv Res 2019.

[74] V. Aleksieva, H. Valchanov, A. Huliyan, "Application of smart contracts based on ethereum blockchain for the purpose of insurance services," Proc. Int. Conf. Biomed. Innov. Appl. BIA 2019, 2019.

[75] H. Qi, Z. Wan, Z. Guan, X. Cheng, "Scalable Decentralized Privacy-Preserving Usage-based Insurance for Vehicles," IEEE Internet Things J 2020.

[76] Z. Wan, Z. Guan, X. Cheng, "Pride: A private and decentralized usage-based insurance using blockchain," In2018 IEEE Int Conf Internet of Things IEEE Green Comp & Comm (GreenCom) and IEEE Cyber, Phys Soc Comput (CPSCom) IEEE Smart Data 2018 Jul 30 (pp. 1349-1354). IEEE..

[77] M. Demir, O. Turetken, A. Ferworn, "Blockchain based transparent vehicle insurance management," 6th Int. Conf. Softw. Defin. Syst. SDS 2019.

[78] M B. Abramowicz, "Blockchain-Based Insurance," SSRN Electron J 2019.

[79] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gomez, V. Santamaria, "Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage," IEEE Consum Electron Mag 2018.. 2816247.

[80] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, S. Jha, "B-FICA: BlockChain based Framework for Auto-Insurance Claim and Adjudication," Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree, 2018.

[81] A. Drexler, A. Granato, R. J. Rosen, "Homeowners' financial protection against natural disasters," Chicago Fed Lett (409):1 2019.

[82] H. Kunreuther, "All-Hazards Homeowners Insurance: Challenges and Opportunities," Risk Manag Insur Rev 2018.

[83] R. Hans, H. Zuber, A. Rizk, R. Steinmetz, "Blockchain and smart contracts: Disruptive technologies for the insurance market," Am. Conf. Inf. Syst. A Tradit. Innov., (AMCIS) 2017.

[84] B. Hagendorff, J. Hagendorff, K. Keasey, "The Impact of Mega-Catastrophes on Insurers: An Exposure-Based Analysis of the U.S. Homeowners' Insurance Market," Risk Anal 2015.

[85] R. E. Munich, "Natural Catastrophes 2011 Analyses, assessments, positions," 2012 unpublished.

[86] A. Sheth, H. Subramanian, "Blockchain and contract theory: modeling smart contracts using insurance markets," Manag Financ 2019.

[87] B. Beers, "A Brief Overview of the Insurance Sector," 2020, unpublished.

[88] S. Lesley, "Life Insurance Industry under Investigation," CBS NEWS (Apr. 17, 2016) unpublished.

[89] A. Cohn, T. West, C. Parker, "Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids," Georgetown Law Technology Review, 1(2), 273-304.

[90] D. A. Disparte "Blockchain Could Make the Insurance Industry Much More Transparent," unpublished.

[91] M. Lounds, "Blockchain and its Implications for the Insurance Industry," 2020 unpublished.

[92] H. Low, L. Pistaferri, "Disability insurance and the dynamics of the incentive insurance trade-off," Am Econ Rev 2015.

[93] B. Olmsted, "How to Buy Disability Insurance," 2019. unpublished.

[94] L. Kraus, "2015 Disability Statistics Annual Report. A Publication of the Rehabilitation Research and Training Center on Disability Statistics and Demographics," 2016, Institute on Disability, University of New Hampshire.

[95] Disability statistics and Facts, https://web.archive.org/web/ 20110727133227/http://nteu-chapter78.org/documents/member_benefits /Disability%20Statistics.pdf unpublished.

[96] J. Gera, A. R. Palakayala, V. K. K. Rejeti, T. Anusha, "Blockchain technology for fraudulent practices in insurance claim process," Proc. 5th Int. Conf. Commun. Electron. Syst. ICCES 2020, 2020.

[97] M. K. Ranson, "Reduction of catastrophic health care expenditures by a community-based health insurance scheme in Gujarat, India: Current experiences and challenges," Bull World Health Organ 2002.

[98] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, L. Tawalbeh, "Health Care Insurance Fraud Detection Using Blockchain," 2020. In 7th Int. Conf. Soft. Def. Syst. (SDS) 2020 (pp. 145-152). IEEE.

[99] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," Appl Sci 2019.

[100] Z. Chang, "Research of medical insurance based on the combination of blockchain and credit technology," Proc. 2020 Asia-Pacific Conf. Image Process. Electron. Comput. IPEC 2020, 2020.

[101] H. Andre, A. K. Dewi, F. Pangemanan, G. Wang, "Designing blockchain to minimize fraud in state-owned national insurance company (Bpjs kesehatan)," Int J Emerg Trends Eng Res 2019.

[102] V. Dhillon, D. Metcalf, M. Hooper, "Blockchain enabled applications: understand the blockchain ecosystem and how to make it work for you," Apress; 2017 Nov 29.

[103] H. Limin, Y. Jianmin, "Application Research of Blockchain in the Field of Medical Insurance," Int. Conf. Econs., Mgt. Eng. Edu. Tech (ICEMEET) 2019.

[104] H. Gajera, M. L. Das, V. Shah, "Blockchain-powered healthcare insurance system," In Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions, Inst. Eng. Tech. 2019. 362-410.

[105] CBInsights. How Blockchain Is Disrupting Insurance. CB Insights 2018 available at https://www.cbinsights.com/research/blockchain-insurance-disruption/accessed November 24, 2020 unpublished.

[106] C. Sandland, D. Schilling, A. Marke, "A Critical Analysis on the Capacity of Blockchain-Based Parametric Insurance in Tackling the Financial Impact of Climatic Disasters," Strengthening Disaster Resilience in Small States: Commonwealth Perspectives. 2019 Oct 7:87.

[107] X. He, S. Alqahtani, R. Gamble, "Toward Privacy-Assured Health Insurance Claims," Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree, 2018.

[108] S. Maganahalli, "Blockchain: The Future of Insurance," Int J Res Appl Sci Eng Tech , 8(5), 2020.

[109] L. Zhou, L. Wang, Y. Sun, "MIStore: A Blockchain-Based Medical Insurance Storage System," J Med Syst 2018.

[110] R. W. Johnson, C. E. Uccello, "Is private long-term care insurance the answer?," (Vol. 29, 2005). Center for Retirement Research at Boston College.

[111] KaranC, "What is Marine Insurance," 2019 available online at https://www.marineinsight. com/know-more/what-is-marine-insurance/ accessed November 1, 2020 unpublished.

[112] EY. World's first blockchain platform for marine insurance now in commercial use, 2018, unpublished.

[113] C. Reed, "Blockchain and the World of Marine Insurance," 2017. available online at https://www.marinelink.com/news/blockchain-insurance429260 unpublished.

[114] P. K. Meduri, S. Mehta, K. Joshi, S. Rane, "Disrupting Insurance Industry Using Blockchain," In Int. Conf. Intell. Data Comm. Tech. Internet of Things 2018 Aug 7 (pp. 1068-1075). Springer, Cham.

[115] T. Mohan, K. Praveen, "Fraud detection in medical insurance claim with privacy preserving data publishing in TLS-n using blockchain," Commun. Comput. Inf. Sci., 2019.

[116] 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," Br Actuar J 2020.

[117] A. Borselli, "Smart Contracts in Insurance: A Law and Futurology Perspective," In: P. Marano, K. Noussia (eds) InsurTech: A Legal and Regulatory View. AIDA Europe Res. Ser Insur Law Reg, vol 1. Springer, Cham.

[118] I. Nath, "Data Exchange Platform to Fight Insurance Fraud on Blockchain," IEEE Int. Conf. Data Min. Work. ICDMW, 2016.

[119] R. Huckstep, "What does the future hold for blockchain and insurance?," Available online at https://dailyfintech.com/2016/01/14/ what-does-the-future-hold-for-blockchain-and-insurance/ unpublished.

[120] J. Xu, Y. Wu, X. Luo, D. Yang, "Improving the Efficiency of Blockchain Applications with Smart Contract based Cyber-insurance," IEEE Int. Conf. Commun., 2020.

[121] [1] J. L. Liu, X. Y. Wu, W. J. Yu, Z. C. Wang, H. L. Zhao, and N. M. Cang, "Research and design of travel insurance system based on blockchain," 4th Int. Conf. Intell. Informatics Biomed. Sci.,2019.

[122] A. W. Singer, "Can Blockchain Improve Insurance? Risk Manag 2019.

[123] S. O. Nam, "How much are insurance consumers willing to pay for blockchain and smart contracts? A contingent valuation study," Sustain 2018.

[124] A. J. Pagano, F. Romagnoli, E. Vannucci, "Implementation of Blockchain Technology in Insurance Contracts against Natural Hazards: A Methodological Multi-Disciplinary Approach," Environ Clim Technol 2019.

[125] A. Sehgal, "Blockchain's Insurance Business Implementation," Int J Comput Appl 2017, 174(3):32-7.

[126] J. Sun, X. Yao, S. Wang, and Y. Wu, "Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS," IEEE Access, 2020.

[127] N. Lorenz, J. T. Münstermann, B. Higginson, M. Olesen, P.B. Bohlken, "Blockchain in Insurance-Opportunity or Threat? McKinsey & Company Report; McKinsey & Company," McKinsey Co. Insur., 2016.

[128] J. A. Tarr, "Distributed ledger technology , blockchain and insurance : Opportunities , risks and challenges," Insur. Law J., 2018.

[129] M. A. Henk and R. T. Bell, "Blockchain: An insurance focus," 2016. Unpublished.

[130] İ. YILDIRIM and E. E. ŞAHİN, "Insurance Technologies (Insurtech): Blockchain and its Possible Impact on Turkish Insurance Sector," Uluslararası Yönetim Eğitim ve Ekon. Perspektifler Derg., 2018.

[131] J. J. Roberts. "Microsoft and Accenture Unveil Global ID System for Refugees," 2017 unpublished.

[132] J. H. Lee, "BIDaaS: Blockchain Based ID As a Service," IEEE Access, 2017.

[133] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," Records Manage. J. 26 (2), 110–139 2016.

[134] L. Mertz, "(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution," IEEE Pulse, 2018.

[135] I. Vakilinia, S. Badsha, and S. Sengupta, "Crowdfunding the Insurance of a Cyber-Product Using Blockchain," 9th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. (UEMCON), 2018.

[136] T. Lepoint, G. Ciocarlie, and K. Eldefrawy, "BlockCIS - A blockchain-based cyber insurance system," Proc. - 2018 IEEE Int. Conf. Cloud Eng. IC2E 2018.

[137] P. Tasca, "Insurance Under the Blockchain Paradigm," in Business Transformation through Blockchain, 2019, (pp. 273-285). Palgrave Macmillan, Cham.

[138] L. Zhao, "The Analysis of Application, Key Issues and the Future Development Trend of Blockchain Technology in the Insurance Industry," Am. J. Ind. Bus. Manag., 2020.

[139] [1] J. Bramblet, "Ultimate Guide to Blockchain in Insurance - Accenture Insurance Blog," Accenture, 2018 unpublished.

[140] L. Xiao, Y. Cheng, H. Deng, S. Xu, and W. Xiao, "Insurance Block: An Insurance Data Security Transaction Authentication Scheme Suitable for Blockchain Environment," In Int. Conf on Smart Blockchain (pp. 120-129). Springer, Cham., 2019.

[141] L. Xiao, H. Deng, M. Tan, and W. Xiao, "Insurance Block: A Blockchain Credit Transaction Authentication Scheme Based on Homomorphic Encryption," Commun. Comput. Inf. Sci.,2020.

[142] S. Pritzker, "Everything You Need To Know About Peer-To-Peer (P2P) Insurance," 2020, unpublished.

[143] D. Oleynikova, T. Loaec, "P2P Protect – TongJuBao," unpublished.

[144] H. Terry, "Guevara Peer to Peer Car Insurance," 2020 unpublished

[145] https://www.friendsurance.com/ unpublished.

[146] K. Wang, A. Safavi, "Blockchain is empowering the future of insurance," 2016, accessed December 06, 2020, unpublished.

[147] fidentiaX, (2018), "Peer-to-Peer Insurance: How Blockchain is challenging the traditional insurance model," unpublished.

[148] Norton, S. (February 2, 2016). CIO explainer: What is blockchain? Wall Street Journal. Retrieved May 10, 2020 8:05AM. Unpublished.

[149] ChainZy. IDChainZ, 2020, unpublished.

[150] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and Scalability," Proc. - 2018 IEEE 18th Int. Conf. Softw. Qual. Reliab. Secur. Companion, QRS-C.

[151] K. Qin, A. Gervais, "An overview of blockchain scalability, interoperability and sustainability," Hoch. Luz. Imp. Coll. Lon. Liq. Netw. 2018 May.

[152] K. Saeedi, A. Wali, D. Alahmadi, A. Babour, F. AlQahtani, R AlQahtani, R. Khawaja, Z. Rabah, "Building a Blockchain Application: A Show Case for Healthcare Providers and Insurance Companies," Adv. Intell. Syst. Comput., 2019.

[153] I. Eyal, E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," In Int. conf. fin. Crypto. data sec. 2014 Mar 3 (pp. 436-454). Springer, Berlin, Heidelberg.

[154] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, "Where is current research on blockchain technology?—a systematic review," PloS one. 2016 Oct 3;11(10):e0163477.

[155] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," Int. J. Netw. Secur., 2017.

[156] J. Salmon, G. Myers, "Blockchain and associated legal issues for emerging markets," 2019. [Google Scholar].

[157] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access. 2016 May 10;4:2292-303.

[158] D. Chris, Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress, New York. 2017.

[159] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Proc. Pri. Enh. Tech. 2018 (4):179-99.

[160] N. S. bt Abd Halim, M. A. Rahman, S. Azad, M. N. Kabir, "Blockchain security hole: Issues and solutions," In Int. Conf. Rel. Infor. Commun. Tech. 2017 Apr 23 (pp. 739-746). Springer, Cham.

[161] Parity Technologies, November 2017. Security Alert, https://paritytech.io/security-alert-2/. Unpublished.

[162] M. Suiche, "Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode," Def Con, 2017.

[163] S. Kalra, S. Goel, M. Dhawan, and S. Sharma, "ZEUS: Analyzing Safety of Smart Contracts," DEF con. 2017.

[164] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale," In Proceedings of the 34th Ann. Compu. Sec. Appl. Conf. 2018 (pp. 653-663). 2018.

[165] J. Li, D. Niyato, C. S. Hong, K. J. Park, L. Wang, and Z. Han, "A Contract-Theoretic Cyber Insurance for Withdraw Delay in the Blockchain Networks with Shards," Int. Conf. Commun., 2020.

[166] V. Akgiray, "The Potential for Blockchain Technology in Corporate Governance," OECD Corp. Gov. Work. Pap., 2019.

[167] S. Grima, J. Spiteri, and I. Romānova, "A STEEP framework analysis of the key factors impacting the use of blockchain technology in the insurance industry," Geneva Pap. Risk Insur. Issues Pract., 2020.

[168] Global Legal Research Center, https://bravenewcoin.com/insights/regulation-of-bitcoin-in-selected-jurisdictions 2014. unpulished.

[169] J. Umeh, "BLOCKCHAIN: DOUBLE BUBBLE or DOUBLE TROUBLE?," *ITNOW*, 2016.

[170] K. Wust and A. Gervais, "Do you need a blockchain?," *In 2018 Crypto Valley Conf. Blockc. Tech. (CVCBT)* (pp. 45-54), IEEE 2018, doi: 10.1109/CVCBT.2018.00011.

[171] S. Bagui and L. T. Nguyen, "Database Sharding," Int. J. Cloud Appl. Comput., 2015, doi: 10.4018/ijcac.2015040103.

[172] O. Ali, M. Ally, Clutterbuck, and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: A systematic literature review," Int. J. Infor. Manag. 2020.

[173] F. R. Batubara, J. Ubacht, and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," ACM Int. Conf. Proc. Ser., 2018.

[174] X. Wang *et* al., "Survey on blockchain for Internet of Things," Comp. Commun.. 2019.

[175] H. Min, "Blockchain technology for enhancing supply chain resilience," Bus. Horiz., 2019.

[176] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," Dig. Comm. Net.. 2020.

[177] Road Traffic Act 1930 unpublished.

APPENDIX

TABLE IV.   CURRENT BLOCKCHAIN SURVEYS IN INSURANCE AND THEIR LEVEL OF DISCUSSION: A COMPARATIVE SUMMARY

Authors	Year of publication	Level of discussion		
		Low	Medium	High
[14]	2019	*		
[12]	2019	*		
[35]	2019		*	

TABLE V.   BLOCKCHAIN TECHNOLOGY GENERAL SURVEYS

Author(s)	Year of Publication	Domains of interest	Other domains
[12]	2019	- Financial Application - Integrity and Verification - Governance (Citizenship and user services, Public sector and Voting - Internet of things - Healthcare - Privacy and security - Business and industrial applications (Supply chain management and Energy sector) - Education - Data management	- Crowd-funding - Humanitarian and philanthropy - Intelligent Autonomous transport - Environmental management - social media - grid computing - cloud computing
[14]	2019	- Financial system (Insurance processing, Banking system, Enterprise sector and Stock exchange) - Intelligent transportation system (Unmanned Aerial Vehicles, Electric Vehicles, and Vehicular Adhoc Networks) - Internet of Things (Device communication, supply chain management, Access control, Fault tolerance and Energy-efficiency) - Smart grid (Energy trading, Demand response, and Dynamic pricing) - Healthcare networks (Record management, Access control policy, Data sharing and Data storage,) - Voting system (e-voting database manipulation and Tamper-proof vote counting) - Data center networks (Cloud computing, Edge/fog computing, - Process models	
[32]	2019	- Healthcare - Financial - Internet of things - Legal perspective - Government - Power grid - Intelligent transportation systems - Commercial world (digital rights management, production management, copyright management, construction industry, transaction management and users behavior management for network media) - Cloud computing - Reputation system - E-business - Supply chain	

TABLE VI.   BLOCKCHAIN TECHNOLOGY SPECIFIC SURVEYS

Author(s)	Year of Publication	Core Domain	Other Domain(s)
[37]	2019	Agric and Food Supply Chain	
[2]	2019	Business Model	
[38]	2017	Construction Management	
[174]	2019	Internet of Things (IoT)	
[175]	2019	Supply Chain	
[176]	2020	Cyber Security (IoT)	
[173]	2018	e-Government	
[172]		Financial Sector	
[33]	2019	Privacy in blockchain systems	
[36]	2018	Insurance	
[35]	2019	Insurance operations and regulation	