THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

TECHNOLOGY

Transforming insurance settlements: Real-time processes through blockchain, Internet of Things, and explainable AI

MD MAMUNUR RASHID | STUART J. BARNES
MD ABDUR RAHMAN

WEALTH & ASSET MANAGEMENT

#51 APRIL 2020

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

INVESTMENTS

TECHNOLOGY

ESG

DEAR READER,

Welcome to edition 51 of the Capco Institute Journal of Financial Transformation.

The global wealth and asset management industry faces clear challenges, and a growing call for innovation and transformation. Increased competition, generational shifts in client demographics, and growing geopolitical uncertainty, mean that the sector needs to focus on the new technologies and practices that will position for success, at speed.

There is no doubt that technology will be at the forefront of a responsive and effective wealth and asset management sector in 2020 and beyond. The shift to digitization, in particular, will see the speeding up of regulatory protocols, customer knowledge building, and the onboarding process, all of which will vastly improve the client experience.

This edition of the Journal will focus closely on such digital disruption and evolving technological innovation. You will also find papers that examine human capital practices and new ways of working, regulatory trends, and what sustainability and responsible investment can look like via environmental, social and corporate governance.

As ever, I hope you find the latest edition of the Capco Journal to be engaging and informative. We have contributions from a range of world-class experts across industry and academia, including renowned Nobel Laureate, Robert C. Merton. We continue to strive to include the very best expertise, independent thinking and strategic insight for a future-focused financial services sector.

Thank you to all our contributors and thank you for reading.

Lance Levy, **Capco CEO**

TRANSFORMING INSURANCE SETTLEMENTS: REAL-TIME PROCESSES THROUGH BLOCKCHAIN, INTERNET OF THINGS, AND EXPLAINABLE AI

MD MAMUNUR RASHID | Senior Research Fellow, Consumer and Organizational Data Analytics (CODA) Research Centre, King's College London

STUART J. BARNES | Chair in Marketing, Consumer and Organizational Data Analytics (CODA) Research Centre, King's College London

MD ABDUR RAHMAN | Associate Professor, Department of Cyber Security and Forensic Computing, University of Prince Mugrin

ABSTRACT

The insurance industry continually struggles to identify the validity and justification of insurance claims, which put service providers and clients in a complicated trust relationship. The complexity is not only concerned with people who are involved in fraudulent claims, but due to the nature of certain businesses, genuine claims are often handled with a mindset of potential fraud. The current insurance business model is largely a traditional, paper-based, error-prone claiming mechanism. Current practices comprise complex and costly processes, often resolved by the involvement of the legal administrators. The overall process also has a multi-point authentication issue, as it needs to maintain an immutable ledger, which is distributed and validated among different parties. Recently, technology has made evolutionary advancements in the area of distributed ledgers. In this paper, we present a novel architecture that will allow a massive amount of heterogeneous data to be used for insurance claims evidence. Our framework leverages the state-of-the-art networking technology and both blockchain and off-chain decentralized repositories. The framework also employs explainable artificial intelligence (XAI) for bringing trust within the reasoning and deep learning algorithms and helping in different ecosystems of the insurance industries. Our solution uses advanced technologies in the insurance industry that could potentially enhance transparency, trust, and automation in handling insurance claims.

1. INTRODUCTION

In the U.K. alone, 469,000 fraudulent claims and applications were detected in 2018, a rise of 3 percent in 2017, with their value up by 6 percent. Every day, 1,300 insurance scams are uncovered, each with an average value of £12,000 [ABI (2018)]. New methods are needed to ensure claims are more transparent, foolproof, and financially more viable for both clients and insurance service providers. Due to the explosion of smartphone-based online services, almost all the services associated with insurance lifecycle are offered through online systems. Such a solution will require a number of state-of-the-art technologies and tools to work together for its proven success.

Artificial intelligence (AI) solutions create a paradigm where computer systems can sense what is occurring within an environment, and think, learn, and act in response to what they are sensing. Internet of Things (IoT) has environmental sensors that are designed to measure a variety of conditions, storing all the data in a decentralized database. Current technology advancements, including high-speed Internet availability and 5G networks for IoT data [Cero et al. (2017)], decentralized data storage computing through cloudlets, smartphone technology, blockchain-based decentralized security [Khan et al. (2017)], mobile edge and fog computing [Yang et al. (2018)], ubiquitous M2M (machine-to-machine) connectivity

[Li et al. (2018a)], IoT for device to device (D2D) monitoring systems [Rahimi et al. (2018)], location-aware systems, crowdsourcing and crowdsensing, and web services, to name a few, contribute to the potential for creating systems that transform insurance claim management [Rahimi et al. (2018)].

Current smart health and home monitoring systems already produce big data designed to alert users after an event has occurred. This creates the possibility of continuously collecting and analyzing that massive amount of data, utilizing it to predict, alert, and prevent risky behavior autonomously, and proactively warn of an event that is about to happen. AI software platforms can analyze a multitude of environmental sensor measurements to create information and messages that are sent instantaneously to the mobile devices of property owners and managers [Ehsan et al. (2019)]. AI systems have the potential of empowering and enabling faster and better decision-making and mitigating property damage and personal injury risk; an early warning AI system can identify and predict the onset of fires, water damage, equipment failures, food/medicine spoilage, and other catastrophic events [Weitz et al. (2019)].

We believe that insurers should modernize and personalize policies, with swifter rollouts and more meaningful tracking of trends and results. One-quarter of those operating in the sharing economy, who believe there is a risk of doing so, said they want coverage they can activate or deactivate as needed. A further 22 percent indicated they were interested in being automatically insured when buying/renting services or possessions to manage this risk [Riikkinen et al. (2018)]. In this paper, we outline a novel framework, employing state-of-the-art technologies that have the potential to radically transform the insurance claims business. We examine the technologies, their applications, changes to insurance industry processes, and the overall benefits of the proposed solutions.

2. TECHNOLOGIES UNDERPINNING A NEW INSURANCE CLAIM FRAMEWORK

The next generation of smart cities will face the challenge of convergence of technological advancements, where a massive amount of data will be generated on a daily basis, all of which needs to be digested, processed, and responded to, both for real-time user queries and historical Spatio-temporal related queries. Blockchain, IoT, Mobile Edge Computing (MEC), and AI are key technologies that can work together to solve smart city solutions. In this section, we outline some of the key technologies and the role that they play in a potential solution.

2.1 Key technology components in an insurance platform solution

Although MEC [Chen et al. (2019)] is a popular topic, its application in insurance claims processing has received less attention. Recent advancements in IoT devices has led to an increase in connected devices, with greater processing capability [Fernandez-Carames, and Fraga-Lamas (2018)]. The existing IoT device to cloud communication architecture needs to be redesigned to leverage the full potential of MEC. MEC can work as an intermediary between entities related to the physical world and IoT nodes and the cloud in the cyber world [Wang et al. (2018)]. Furthermore, MEC shows the potential to address the availability and improved connectivity, resilience, scalability, low latency, and real-time delivery of a massive amount of data, which the traditional cloud-only solution fails to guarantee [Chen et al. (2018)]. For real-time insurance applications, such spatio-temporal multimedia data generated by each business process consists of a very large volume of data to be shared with the cloud [Zhang et al. (2018)]. The introduction of a MEC layer [Liu et al. (2017a)] at the vicinity of the IoT sensors or users related to insurance claims processing would make it possible to save bandwidth and processing resources, and incorporate security solutions before the processed data is sent to the cloud. However, due to stringent requirements for privacy, security, and anonymity in data sharing within insurance processing ecosystem, MEC will typically require technologies such as Tor and Blockchain [Zhou et al. (2018a)].

The use of blockchain within the insurance industry can bring transparency, as most of the claims are managed by multiple parties. These disruptive technologies, together with MEC, can allow for anonymous and secure sharing of data with any intended stakeholder without the need for a central authority. This will allow IoT and user data to be secured and anonymized. Moreover, the incorporation of blockchain and Tor will enable security implementation to become more robust. A user can carry out any insurance-related business activity or conduct any financial transaction without the need for central authority or middleman. On the other hand, the chain of blocks containing the timestamped history of spatio-temporal activities and transactions related to insurance business process or a user's history containing multimedia data can be linked by cryptographic hashes within the blockchain [Liu (2017b); Yin et al. (2018); Li et al. (2018b)]. This will allow for securing the data from cyberattacks or unauthorized access from anyone in the middle, thereby saving the relevant institutions from penalties or criminal punishments. This makes insurance claims more secure, and dictions can, therefore, be taken with more confidence.

For many insurers, the cloud-computing debate is over [Benhamouda et al. (2018)]. With seven in ten carriers using the cloud in their businesses, it is already an integral part of their technology environment and business platform strategies. Cloud providers are actively evolving their capabilities to offer advanced solutions in partnership with system integrators to create industry-specific solutions [Esposito et al. (2018)]. For example, the number of U.S. insurers with claims systems fully deployed in the cloud has seen a steady rise from 13 percent in Ovum's 2016 survey to 26 percent in 2018 [Juniper (2017)].

Blockchain has gained traction due to its fully decentralized peer-to-peer redundancy solution, providing a secure identity for each stakeholder and support of smart contracts, which can be activated on spatio-temporal logic [Turkanovic et al. (2018)]. This ensures secrecy of block data through secure wallets and strong encryption, guaranteeing the service level agreement through the transparency of the historical blocks, all at a low cost in managing distributed databases. Furthermore, blockchain offers immutable and non-hackable transaction storage for different smart city applications [Gao et al. (2018)], which is particularly useful when the users are mobile, i.e., moving among inter-MEC nodes, which requires decentralized yet secure and seamless integration and interaction for cyber profiles [Valtanen and Backman (2018)].

Although Blockchain supports strong security, it does not deliver perfect anonymity because each transaction added to the block reveals the address of the miner, and the transaction parties, which is visible to the public [Zhou et al. (2018b)] . In order to add anonymity to blockchain transactions, researchers have proposed a multitude of solutions, such as via Tor, usage of a one-time pad address for each transaction, secure wallets, TumbleBit, and Zcash, to name a few [Zhao (2018)]. The raw IoT data and the multimedia payload emanating from applications can thus be anonymized and at the same time added to the blockchain at the MEC node before it can be sent to the cloud. The MEC node is assumed to host the cloudlet architecture acting as a high-end computing platform that can run blockchain nodes or Tor virtual machines [Moubarak et al. (2017)]. In addition to security and privacy, the MEC node can also be used in tandem with other scalability solutions incorporating 5G and IoT communication [Marjanovic et al. (2018)].

We envision further leveraging the fog computing paradigm by assuming that "edge devices" will perform a large portion of the cloud activities related to insurance claims, such as storage, communication, and processing, and in return will receive a substantial number of incentives for sustainable growth [Ni et al. (2018)]. Moreover, depending on the scenario and available bandwidth, edge devices will carry out as much local processing as possible and offload to the cloud backend only when a favorable network condition is observed. Hence, together with blockchain-based security, each user within an insurance ecosystem takes control of their usage data, granting permission to whomever they want and when they want [Yeow et al. (2017)].

With the massive volume of data collected, the amount of data processing and event detection in different scenarios is a daunting task. However, advanced AI, with the support of multi-tier machine learning, deep learning, and other types of data science advancements, have made it possible to analyze such massive volumes of data and find phenomena of interest [Porambage et al. (2018)]. AI has been successful in automatic reasoning by following some predefined workflows, the big data set to work on, and the types of output to deal with [Ehsan et al. (2019)]. These technologies together show promising prospects for various smart city challenges, including in the insurance industry. Existing insurance policies are often processed on paper contracts, which leaves claims and payments error-prone, and numerous steps requiring human supervision. This inherent complexity of insurance involves consumers, brokers, insurers, and reinsurers [Raikwar et al. (2018)]. New technologies can enable each part of the insurance lifecycle to leverage and provide improved quality of services [Lamberti et al. (2018)].

About one-third of CIOs at insurers surveyed by Ovum said their biggest challenge with IoT is the cost and complexity of implementation. About 25 percent cited a lack of consumer demand for products incorporating IoT, while just over 20 percent said associated compliance issues, particularly around privacy, were too complex. Notwithstanding, several insurance companies have moved towards technology-driven models, e.g., in Asia, AIA Hong Kong has launched a blockchain-enabled "bancassurance" platform, allowing the life insurer and its bank distributors to share policy data and digital documents in real-time, streamlining the onboarding process, improving transparency, and reconciling commissions automatically through smart contracts [Bhushan (2015); Code (2018)]. The Hong Kong Federation of Insurers is also working to establish a blockchain-based auto insurance platform [Ledger (2019)]. In Europe, AXA is offering flight-delay insurance over a blockchain platform with parametric triggers and smart contracts [PwC (2019)]. In the case of health insurance, a blockchain smart contract can store the cryptographic public ID of the patient, therapist, hospital, caregiver, and other community of interest and their relationship, along with the permission and authorization level by different entities. During insurance claims processing when access to health data is needed, the smart contract is used to validate access control, permissions, relationships among the entities, and sharing the hash of the actual off-chain health data with joint ownership [Hawkins et al. (2018)]. Finally, the off-chain health data can be queried with the session key obtained from the smart contract execution [Rahman et al. (2018)].

2.2 Explainable AI considerations

AI has been successful in solving many problems by enabling a robust algorithm to take major decisions too time-consuming and complex for humans. AI has been under development in the insurance industry for many years, but it could not completely succeed in solving a fundamental problem. Current AI models work in a Blackbox mode, where it is not always known how the outcome of an action is derived. It is not possible to trace back to the raw data in different sub-processes, since many assumptions are made within the algorithm, which cannot be explained to humans. The reproducibility of individual steps or semantic explanation of the evidence that will convince stakeholders is very important for the insurance industry – and this is where Blackbox AI fails. Any complex insurance claim decisions need to fully visible and justified. Transactions in each stage of an AI-operated system must be recorded to ensure transparency and traceability for clients and industry experts. To resolve this, we propose to use explainable AI, which records all transitions and logs outcome-driven decisions. We believe our proposed framework is the first XAI solution to be considered for automated insurance claims processing. In this paper, we proposed to combine XAI with IoT, and blockchain, to ensure that insurance-related data processing is more transparent, less human-error prone, and faster.

We envision an XAI algorithm that will be tailored to understand the evidence needed for different types of insurance industries, the workflows, and the decisions that will be made via the human-AI algorithm teams. This reference point helps subsequently, when a claim is being challenged by a client. The XAI also assists insurance industry stakeholders to gain confidence in the decisions made. Several insurtechs are already engaging in real-time, as-needed coverage. Trov, a global on-demand insurance agency, uses an application that enables consumers to insure single items such as cameras and digital devices with coverage that can be activated and terminated at any time over a mobile app [Insurance Journal (2018)]. Another advanced feature that we envision is the use of XAI data for improving system performance. In the future, we expect to capture the most relevant data on a live system, but at present, we leverage all transaction data to create a benchmark dataset for future systems to make decisions more quickly and precisely. We believe that this will transform the insurance industry's operational methods, where technology will be able to take over all major legal liabilities with minimal legal involvement.

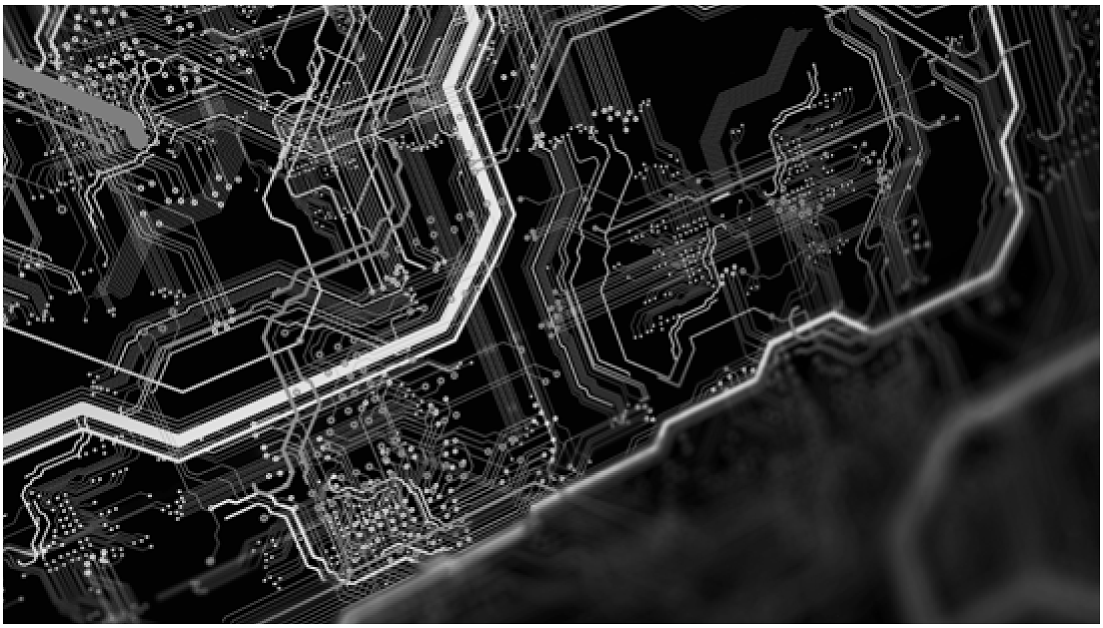
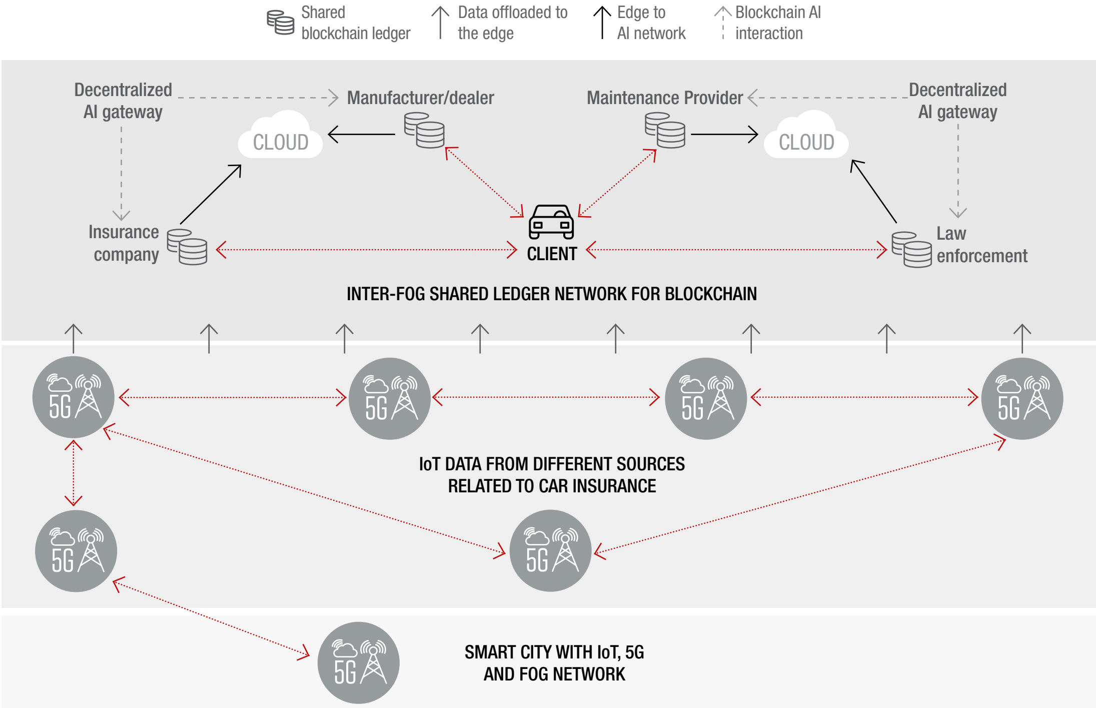
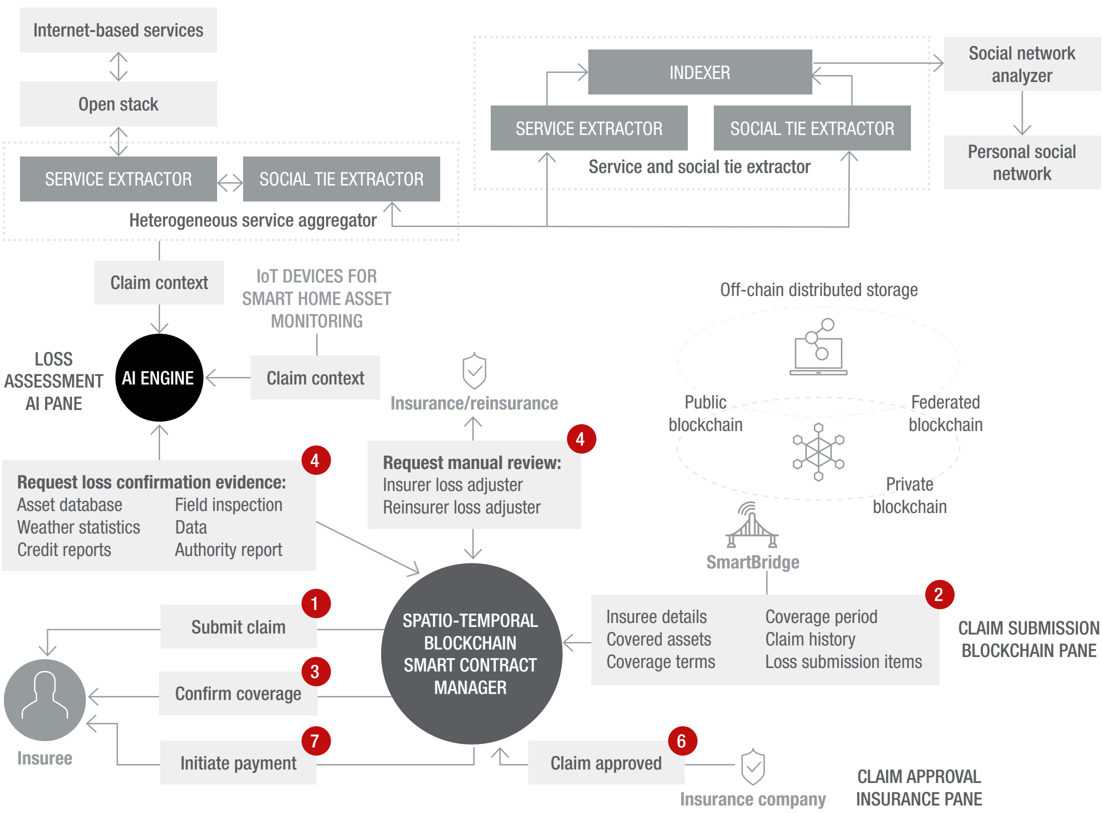


Figure 1: Managing insurance-related data through the proposed infrastructure

(a) A high-level architecture where different lifecycles of car insurance are being captured in a smart city



(b) Different steps during a typical claims process, which can be supported by the proposed framework



3. A NEW, DATA-DRIVEN FRAMEWORK FOR INSURANCE CLAIMS

In this section, we present a design to illustrate how the insurance-related data will be managed through our proposed infrastructure. Figure 1 is a very high-level illustration, where infrastructure is shown at the component level. As shown in Figure 1a, IoT data related to the insurance industry in a smart city is collected via the 5G, Mobile Edge/Fog network, which is then stored within the blockchain and off-chain storage for evidence purposes. The immutable and distributed blockchain ledger can then be used in different use-cases and by different stakeholders of the insurance ecosystem. Figure 1b shows a generic insurance claims process in which blockchain and off-chain storage is used by the XAI so that the claims-processing human agents can understand the steps and intervene during the claim's preparation lifecycle.

3.1 Core system components

Let us take the example of auto insurance. There are two ways in which blockchain can prove to be beneficial for the auto insurance industry. First, it can connect all users and service providers with the help of shared ledger in which all the information will be readily available. It will help auto insurers reduce risk and fraud. Second, with the help of smart contracts, claims processing will be faster.

Figure 2 shows the cloud, edge, client nodes, and their communication pattern. As shown in Figure 2, IoT devices forward their insurance-related data traffic to the MEC nodes first, which does the security handling, small scale analysis, and then shares the final results with the cloud. The task of decentralization and anonymity of the captured insurance-related data also takes place in the MEC nodes. Hence, with the help of advancement in 5G technologies, the MEC nodes can provide many IoT-Edge centric services to the underlying applications, thereby reducing the load on the cloud. Since the MEC node supports both security and anonymity of the IoT data, once deployed near public places, it can securely support underlying insurance applications with mobility of the users. A cloudlet server can be hosted at the house of a subject, at relevant organizations, or the premises of the 5G base station. The cloudlet server acts at the IoT edge network to support IoT data processing, security, storage, and analytics at the edge. This will allow the high data rate IoT sensors that are used to capture insurance-related evidence to be processed with low

Figure 2: Three tier protocol architecture

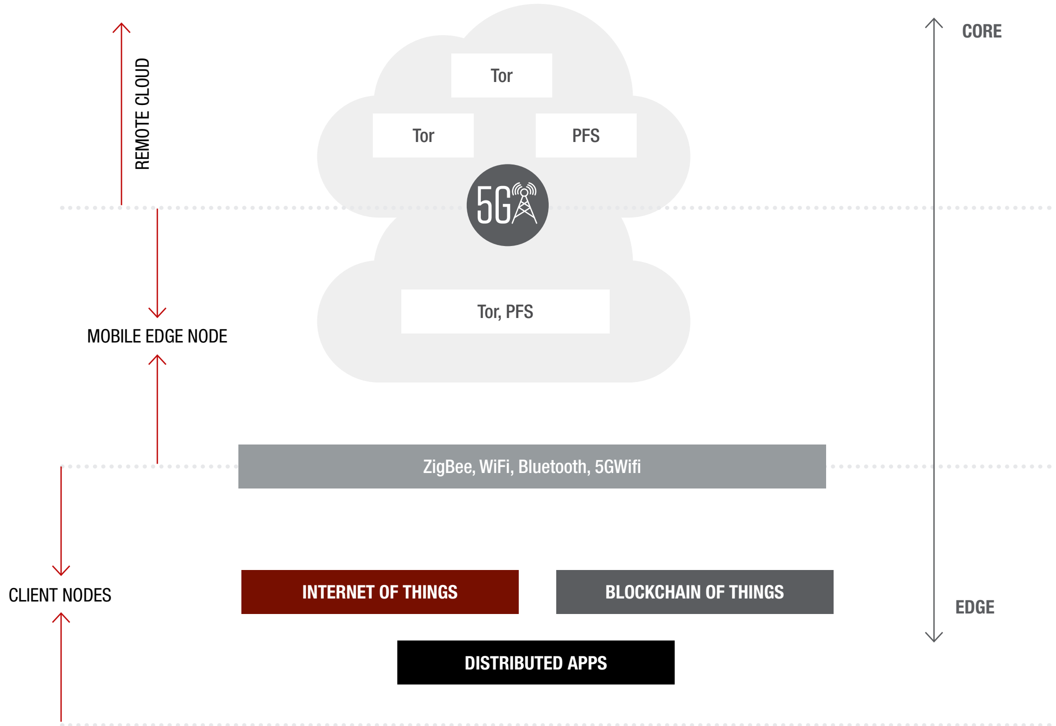
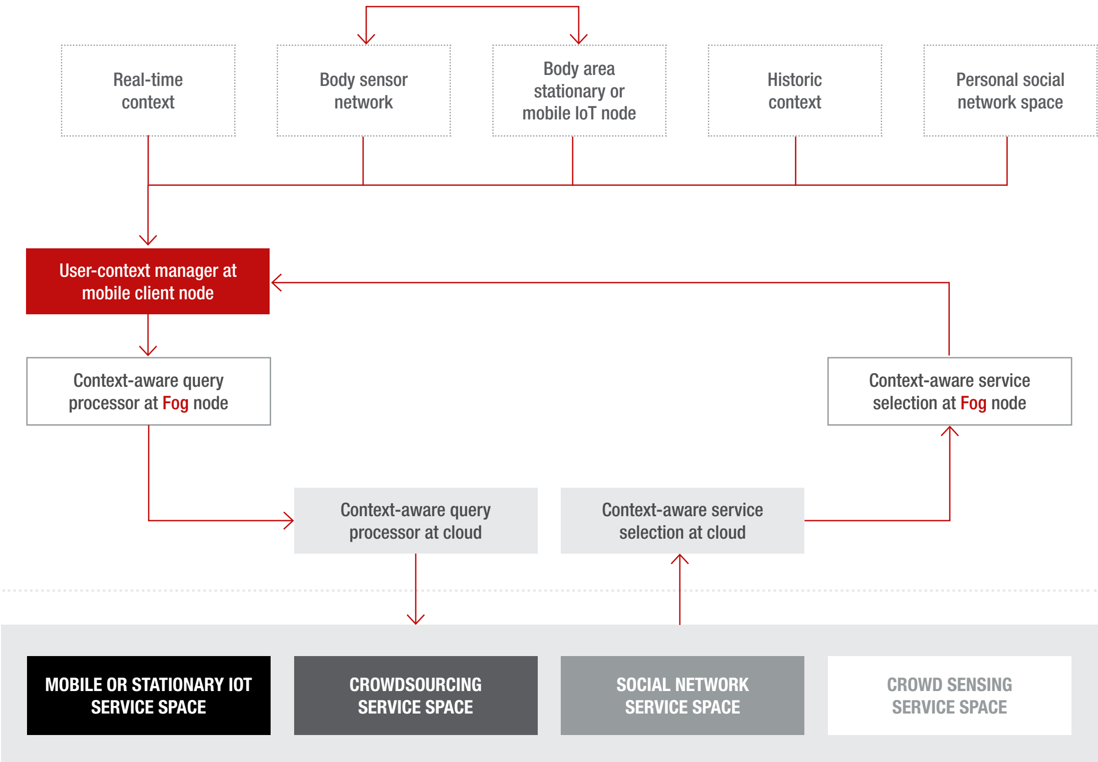


Figure 3: Context-aware AI-based insurance assistance framework



latency and high security in a decentralized manner. In the absence of a mobile edge tower, a smaller server can be used as an edge router such as a laptop, or a smartphone that can intake the sensory data and share it with the cloudlet or the mobile edge network for further processing.

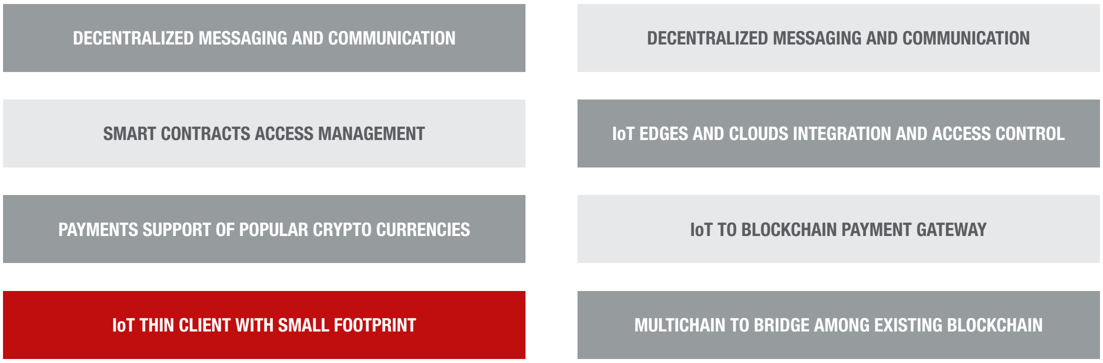
We can also use mobile edge/fog nodes to act as virtual clouds within the fog tier to handle the offloading and reduce the latency. The fog tier tries to answer most of the insurance-related queries from the fog tier, provide high bandwidth, support low latency, help in smart-phone low battery consumption, and local and low computation need that can be used to provide navigation to users in the same physical proximity. The boundary and coverage of each client node and fog node determine the sub-boundaries of the fog tier and those of the D2D communication possibility. If two or more insurance-related stakeholder nodes are within the same fog tier boundary, they can start a D2D (device-to-device) communication. However, each fog node acts as an opportunistic node, such that whenever good network bandwidth is available, the fog nodes upload the fog tier transactions to the core IP-based cloud backend.

3.2 Context-aware insurance data collection

The proposed framework aims to provide context-aware insurance services through the following: collection of insurance evidence from IoT, crowdsourced, and social media data; storage of the incoming multimedia data initially at the distributed fog nodes and finally to the big data repository; and inter-correlation of context-aware clusters of crowd data rendered back via spatio-temporal services to each individual, based on context. As shown in Figure 3, different insurance applications allow a query or task to be sent by a requester to a very large crowd or a set of IoT nodes through the proposed platform, which leverages both fog and cloud computing architecture. The requester then receives complex insurance-related results in a personalized fashion. Figure 3 shows details about different components within the framework.

We assume that to support the insurance ecosystem, numerous stationary IoT devices will have been deployed around a city, within vehicles, within houses, and so on, for collecting different types of insurance phenomena data. Furthermore, we assume that each person within a massive crowd has a smartphone and is optionally surrounded by both

Figure 4: IoT protocol stack to support the blockchain-based AI insurance assistance framework



a "body sensor network" (BSN) and a subset of IoT devices, whether stationary or mobile, forming a "body IoT network". The smartphone in our framework has 4G LTE-A/5G internet connectivity through which an individual can be connected to personal social networks. The built-in smartphone sensors, the sensors within the BSN, and the IoT sensors together allow collecting real-time user and ambient context data.

4. STAGES IN THE DEVELOPMENT OF THE NEW SYSTEM

Insurance data handling is a complex process, and hence, modular development is needed so that the insurance data can be recorded at every step of data migration. In this section, we delineate the proposed development steps for the full deployment of the system.

4.1 Source insurance data extraction

Figure 4 shows the protocol stack of collecting, analyzing, and visualizing IoT data. Since the IoT devices are thin, we assume there is limited capacity for connecting with edge devices running full blockchain nodes. The framework allows an IoT node to communicate with nearby edge nodes running smart contracts, to use decentralized messaging services, to save raw IoT sensory data into a decentralized repository via the edge networks, to add IoT data of interest to the blockchain, and to connect to cryptocurrency exchanges and gateways. The IoT data is fed to the AI engine for logic extraction and finding patterns of interest as evidence.

The modules are responsible for collecting the raw contents from heterogeneous internet-based sources and IoT devices. The framework embeds a suite of protocols and algorithms that can communicate with complex and proprietary sources of existing heterogeneous internet-based services and retrieve online multimedia content. To manage load balancing and scalability, the framework uses proxy servers, where each proxy server actually listens to each type of content retrieval service request and, depending on the number of concurrent service requests, a greater number of proxy servers may be employed within the system. A proxy server stores the list of content retrieval services available within the framework. A properly designed service client algorithm is envisioned to: store the path to an internet resource, bandwidth, round trip time, delay, URL patterns, HTTP access methods, response types, and authentication patterns, inter alia. The indexer stores each extracted service in an index server, referred to as a "personal social network". This serves as the AI dataset for a particular subject.

4.2 Insurance data semantics extraction

This module is responsible for pre-processing and analyzing content, extracting logic, indexing the emotion primitives, presenting the claims results to the user, and adapting the emotion value from the user feedback to train the system. In its upstream data collection path, the Controller receives raw content from the Web Data Extractor. The Controller also issues requests to extract new content in the downstream path. Upon receiving raw media content, the Controller delegates the content to the model component, i.e., insurance phenomena extraction logic. This component mashes up all the logic extraction services available within the framework and delegates the content to the most optimal service, depending on media and user requirements. It also leverages the metadata of each API (application programming interface) in the form of types of media support, response type per unit content, size of each payload per request, types of request and response (i.e., JSON, XML, REST), number of requests per API call, type of domain knowledge supported, types of functionalities supported, types of logic values supported (positive, negative or neutral), ranges of logic value, and semantic attributes, such as affection friendliness, sadness, amusement, contentment, and anger, to name a few. The unit could be horizontally enriched with various services. There are three different working phases.

4.2.1 TRAINING PHASE

The system makes use of a supervised learning method to classify the semantics of the retrieved content, assuming conditionally independent classification features. Classifications would include positive, negative, or neutral sentiments. We use this theorem to evaluate the posterior probability of sentiment membership for classifying new input samples according to its associated features (i.e., content/text keywords). We do the same for all possible classifications. Thus, we are able to classify a new event as the classification with the highest posterior probability.

4.2.2 EXECUTION PHASE

When the system receives new content to be classified, it tries to analyze the data before classification. Using the AI engine, we get the probability of a certain classification given the input data. Our proposed algorithm employs a fast and reliable technique to classify raw data with great certainty and against the training dataset even with noise in the data.

4.2.3 FEEDBACK PHASE

The use of the AI algorithms provides highly accurate results to classify the emotion tag for the input feed. However, for different reasons, we might receive an incorrect or undefined decision. Thus, we add the capability for the user to train the system at run-time to refine the algorithm's knowledge base and improve its overall efficiency.

4.3 Insurance primitives

Insurance Primitives, which work as an atomic type of insurance process repository, store the output of "claims extraction logic". Each API stores its result to a separate repository. Some APIs use the stored emotion primitives as a training dataset and use their stored emotion data as an input to the claims' extraction logic. This dataset gets enriched throughout the lifecycle of the emotion extraction service. The richer this database is, the more accurate the logic behaves.

5. PROOF OF CONCEPT APPLICATION SCENARIOS

In the proposed framework, we use blockchain in different scenarios, which can then be linked to the insurance policies. The collected data through our proposed framework can help insurance transparency greatly. In this section, we will present our visionary architecture for supporting different use-cases.

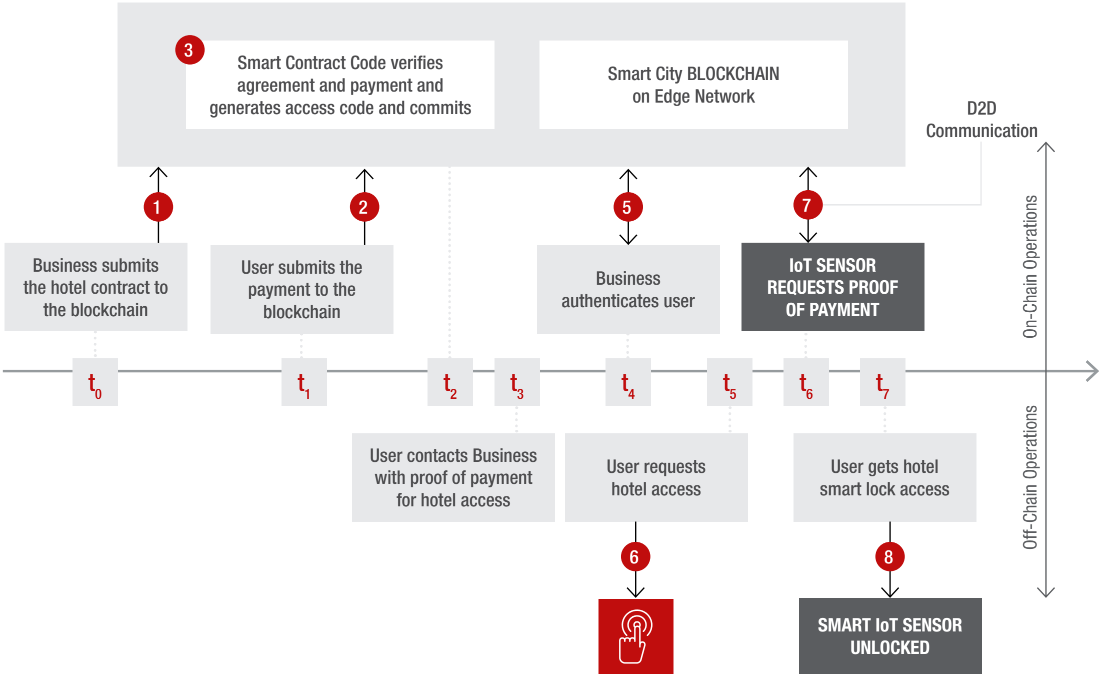
5.1 Property rental scenarios

Figure 5(a) shows a scenario in which a user rents a hotel using cyber-physical interaction between blockchain and IoT devices. Figure 5(b) shows the interaction between the smart lock and the rest of the blockchain clients to successfully and securely handle the complete device-to-device contractual agreements. The IoT smart lock cannot store the complete blockchain record and cannot run the complete Ethereum virtual machine (EVM) due to its storage and processing limitations. Hence, it has to rely on a set of miners for proof of payment and a smart contract logic execution operating within the edge or in the decentralized cloud. The smart lock will use the proof of payment from which it also has to pay to the miner nodes that calculated the hash as proof of payment from the complete blockchain. The proposed approach, as shown in Figure 5(a), will allow the property owner to rent rooms to the user in exchange for money. Although the property owner is not trusted, and may try to maximize the benefit by different approaches, including concurrently renting the property to different users, the system will block such security holes. Similarly, the renter will be able to book a room from the owner through the blockchain, even though not fully trusted or known to the owner, with potential for minimizing costs by avoiding payment to the owner.

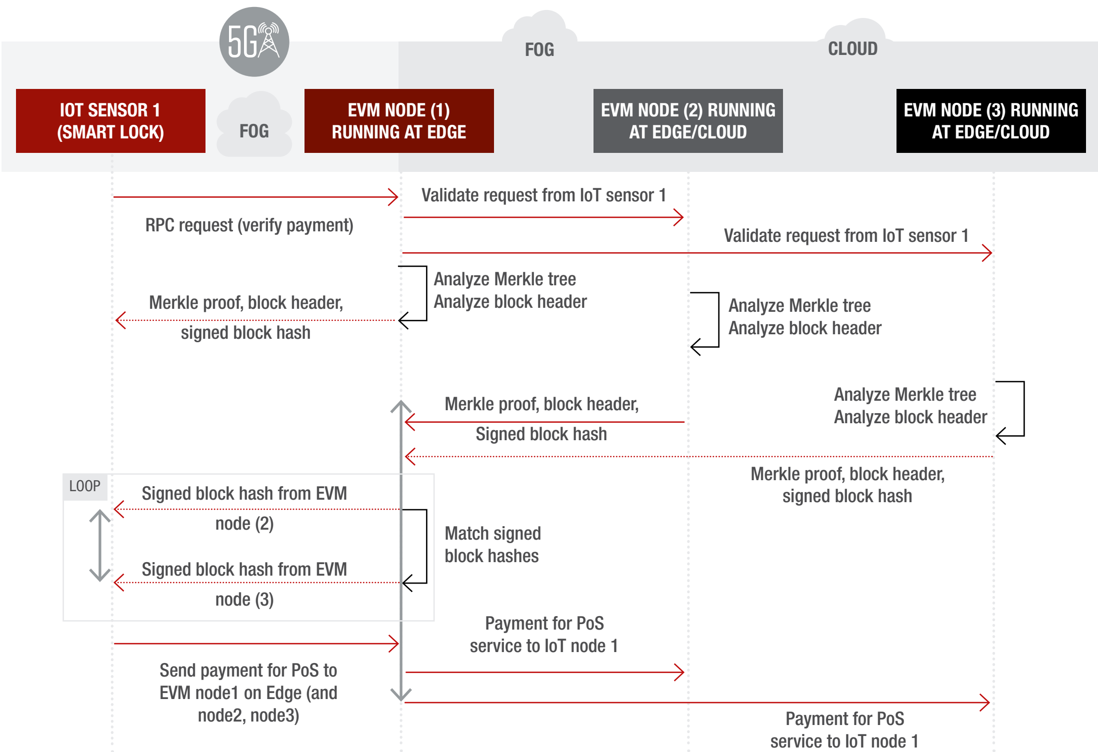
The framework will ensure that the owner and the renter have the incentive to protect their privacy. The physical property is controlled by IoT devices and pre-determined protocols and is, therefore, trusted, i.e., the property is programmed to follow decisions made by the blockchain smart contract system. It is also assumed that the physical property will not disclose information to any third party and will use the blockchain platform to carry out transactions between owners and renters by recording agreements/payments and tracking agreement execution. Trusted properties will always follow instructions accepted by the blockchain system. The secure transactions will allow insurance claims processing transparent and trustworthy by different stakeholders.

Figure 5: Proof of concept design architecture for real life deployment

(a) A scenario where a user books a hotel with the help of blockchain and IoT devices



(b)The detailed machine-to-machine communication among different blockchain nodes to commit the transactions



5.2 Smart home monitoring scenarios

Figure 6 shows a scenario where data is collected from smart home IoT sensors, which is then shared with both blockchain and a decentralized repository storing the sensory data payload for the XAI engine, which can then be used as insurance claim evidence for analysis. The multi-dimensional data types collected from the smart home include those sensing ambience, user activity, energy usage, aspects of security, and human physiological data. This data is fed to the XAI engine for event analysis, event indexing in the blockchain, saving the payload in the off-chain solution, or further inquiry of other blockchain bridges, if deemed necessary, and alert generation for various threshold values of sensory data. The smart contract can also interface with the external cryptocurrency gateway and exchange in the case of payment for any third-party services. Finally, the owner of the house can share smart home data with an insurance service provider. The service uses distributed apps to connect to the decentralized databases.

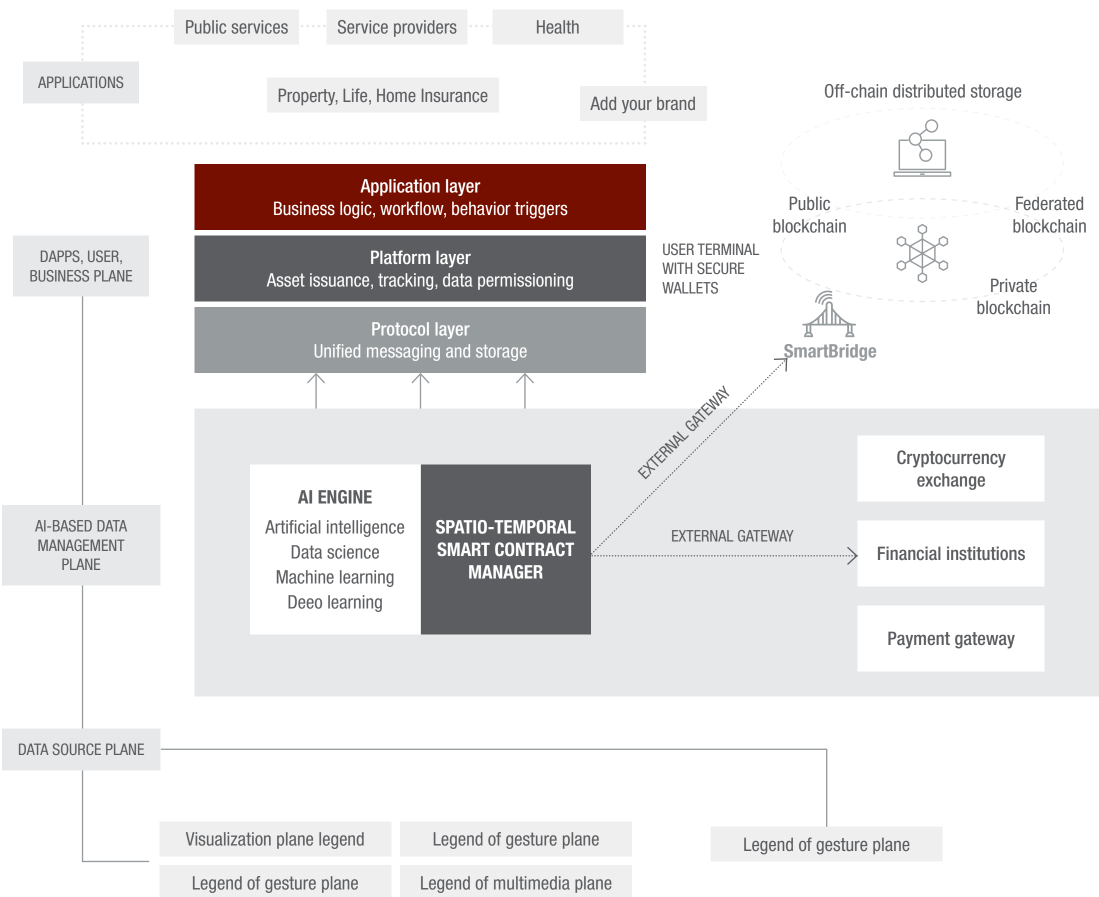
6. NEW ERA OF OPERATIONAL PROCESSES

The proposed solution will require numerous changes in the current operational model of the insurance business. This will not only help in bringing transparency into the insurance industry but also make its operational costs more manageable via changes in the current operational model. In this section, we examine the possible areas where operations will be transformed.

6.1 Underwriting

The department responsible for verifying the authenticity of a claim and deciding on claim coverage requires a trustworthy repository of data. Blockchain, IoT, and XAI offer a central repository of truth. Using the blockchain, underwriters can obtain data from external sources to automate some aspects of underwriting, since the data in the blockchain is trustworthy and is from verified sources (see Figure 1b above). On blockchain, external data from off-chain can be included as

Figure 6: A complete smart home scenario where different types of data are recorded in the blockchain and shared with community of interest



evidence using smart contracts to decrease risk liability and provide semi-automatic pricing (see Figure 5). This can help to automate and shorten the underwriting process, reducing the cost of operations (see Figure 6). Blockchain also brings transparency and improves trust in the underwriting process by enabling shared visibility in complex multinational programs, providing transparency across underwriting coverage and premiums at local and international levels.

6.2 Claims processing

Improving claims processing methods is often considered a priority for insurance companies. For the consumer, submitting a claim and getting it approved is yet another tedious process. Processing can take quite a while, especially considering the number of data points needed for verification and the amount of manual effort required. With blockchain and XAI, most of the necessary information that is required for claims verification can be processed in either real-time or near real-time. Since blockchain can take inputs from a variety of different sources without altering any information, insurers can use the data available in the blockchain to track the usage of an asset. Provenance is one major area where insurers can take advantage of blockchain. A shared ledger and insurance policies executed through smart contracts can bring an order of magnitude improvement in efficiency to property and casualty insurance.

Alongside big data, mobile and digital technologies, blockchain is essential for establishing an efficient, transparent, and customer-focused claims model based on higher degrees of trust. Within claims prevention, new data streams can enhance the risk selection process by combining location, external risk, and analytics. Thanks to the proof of location protocol of blockchain, a distributed ledger can enable the insurer and various third parties to easily and instantly access and update relevant information (e.g., claim forms, evidence, location of the event, police reports, and third-party review reports). The use of data from a mobile phone or IoT sensors can streamline claims submission, reduce loss adjuster costs, and increase customer satisfaction, with blockchain systems facilitating communications and coordination among all parties. IoT sensors can trigger alerts to insurers that a crash has occurred (thereby initiating a new claim), and then route secure and relevant data to preapproved and conveniently located medical teams, towing services, and/or repair garages. Blockchain is in the middle of connecting and ordering data from the multiple devices and apps involved in the multidimensional process. Similarly, the combination of sensor data, satellite imagery, mobile technologies, and blockchain could be used to facilitate claims payments and rescue services when natural disasters occur in remote areas. Data from weather stations could determine claims amounts based on actual weather readings, with blockchain enabling greater automation, more efficient data sharing, and stronger safeguards against fraud.

7. EXAMPLE INSURANCE APPLICATION AREAS FOR THE PROPOSED SOLUTION

We propose the above technology solution in a variety of areas of insurance, in each case improving speed, efficiency, and transparency, and reducing operational costs; hence improving overall profitability. The proposed method will be customized based on industrial rules and policies. Notwithstanding, the technological aspects remain the same regardless of the business characteristics of the different insurance industries.

7.1 Health insurance

Blockchain and IoT can potentially interconnect medical care facilities, insurers, patients, physicians, and other parties, thereby improving the level of care provided to patients. Furthermore, processes can be streamlined, as all the data is held in a central, secure repository. Through a blockchain of IoT health data, medical records can be cryptographically secured and shared between health providers, increasing interoperability in the health insurance ecosystem. An individual can be surrounded by a set of gesture tracking sensors and ambient intelligent IoT sensors supporting in-home therapy sessions. IoT nodes and gesture tracking sensors are secured by the private/public encryption keys. A patient may allow access to their data to the community of interest, including caregivers, therapists, insurance company, medical doctors, hospital authority, and so on. Patient-related data can also be digitally signed and saved into the blockchain by trusted parties and an individual can authorize a subset of personal therapy data on an ad-hoc basis. The smart contract embeds the access policy of the patient. Any transaction that enters the edge network gets parsed by the geographically distributed, permission mining/consensus nodes to get approved and added to the blockchain. With investment from Munich Re, among others, insurtech company Bought by Many has created a way for customers to sidestep traditional routes to purchase niche products that legacy insurers often avoid, such as travel insurance for those with pre-existing medical conditions [Lamberti et al. (2018)]. Our system provides key data and methods to enable the provision of such services in a low-cost, transparent, and secure way.

The collected health data includes an enormous amount of multimedia data in the form of text, image, audio, and video. An offline centralized cloud or decentralized cloud storage can be used to store the multimedia data while the transaction in the blockchain stores the hash of the pointer of the files distributed in the cloud storage. Using XAI to automatically process the massive amount of health data would bring trust and efficiency. While reading or querying the file, the patient must first authenticate with a private key to obtain the hash of the distributed file pointers before accessing the actual file providing the distributed hash to the cloud controller. Since the cloud storage pointer hash is saved in the blockchain and then goes through a Tor anonymity network, the security, immutability, integrity, and backup of the hash is guaranteed. To improve secure storage, distributed (to avoid the single point of access), a cryptographic P2P cloud storage architecture such as StorJ, BigchainDB, or IPFS can be adopted. Since the customer is at the center of ownership for their therapeutic data stored in different autonomous and private health institutions' computer systems, they may share data on-demand with any institution through the cryptographic signature in the blockchain [Sreehari et al. (2017)].

7.2 Automobile insurance

Blockchain and car IoT can connect consumers, service providers, and others, with the help of a shared ledger of readily available information. This will help auto insurers reduce the risk of fraud. Second, with the help of smart contracts, claims can be automated and processed more quickly. By creating a consortium of automobile stakeholders, government agencies, and so on, one can obtain all the information easily. Moreover, insurance companies can use smart contracts to issue automatic pay-outs to medical facilities and other beneficiaries. Consumers increasingly want more control over their specific coverage. A survey of life insurance consumers indicated that 90 percent of buyers revealed a preference for self-management of existing policies through digital channels [Juniper (2017)].

8. ADVANTAGES OF THE PROPOSED SYSTEM

The proposed solution has a number of key advantages. We believe that it can be used in many different areas and sectors of the insurance industry. However, this is based on a common regulatory requirement in some sectors. To take full advantage of this system, we need to customize it based on the sector of insurance and local regulatory considerations. The performance of the system can vary by sector, but in general, it should be more transparent and cost-efficient.

8.1 Identity theft and cost savings

Key problems faced in the insurance industry are false claims, fraud detection, and the time taken to validate each application. Blockchain shows promises as a solution since it can serve as a distributed register which has both internal and external customer data. Once the personal information is entered in the blockchain, the platform can automatically validate the documents, such as address proof, medical reports, and so on. This will not only speed up the entire process but at the same time, it will reduce human intervention, thus minimizing the probability of errors. Blockchain offers more efficient data processing and reduction in fraud, thereby saving an estimated 15-25 percent of expenses incurred during the insurance process, potentially saving billions of dollars [Insurance Journal (2018)]. In a blockchain, transactions are time-stamped and immutable, so identities are secure, and all data is far more trustworthy. This means that fraud is more easily detected, which could have profound implications in the insurance industry, where 65% of all fraudulent claims go unnoticed. According to the Institute of International Finance, some U.S.$60 billion of fraudulent claims are submitted annually in the U.S. and Europe alone, any meaningful reduction would bring substantial benefits to insurers' bottom lines [Ralph (2017)].

8.2 XAI for automated customer support

AI-powered, customer-service chatbots can be better equipped to meet the expectations of providing context-aware customer support for a real-time touchpoint and customized assistance while fulfilling a company's need to cut costs. XAI powered chatbots will further become more powerful as voice recognition technology with an explanation of internal steps improves, adding trust, lowering the cost, and shortening the time of each insurance claim. XAI can also bring drone technology to a new level of utility for insurers, such as in hard-to-reach disaster areas to record loss and damages. XAI can provide drones with increased computational abilities that might allow them to spot a damage in an image that is not apparent to the naked eye or to make on-the-spot decisions about how to use the data they are capturing, potentially speeding up the claims process. XAI can also analyze crowdsourced spatio-temporal multimedia data to find event details that will allow pinpointing and forensic analysis of the actual cause of an event.

8.3 IoT for forensics and evidence

As more devices and objects are connected to the IoT, the amount of data that will be created and collected will increase significantly. This data will be hugely valuable to insurers as they look to develop more accurate actuarial models, or new products such as usage-based insurance (UBI) models. In the auto insurance market, for example, encrypted data gathered about driving times and distances, acceleration and braking patterns, and other behaviors can be used to identify high-risk drivers, validate information included on applications, and give consumers more control over their premiums. The challenge in this future state, however, is not only how to manage the sheer volume of data and logic related to insurance industry, as thousands or millions of devices are communicating with each other, but to also protect from ransomware or other distributed denial of service (DDoS) attacks [Pan et al. (2018)].

Via blockchain, one can manage large, complex networks by having the devices communicate with each other on a peer-to-peer basis securely, instead of building an expensive data center to handle the processing and storage load. Having these devices manage themselves is significantly cheaper than the data center model. For example, sensor-equipped devices such as fitness wearables can measure a person's activity, diet, and vital signs. This can help health insurance companies assess and predict health, which potentially means fewer customer ailments and fewer claims. Telematics-based car insurance, in which insurance rates are influenced by a customer's actual driving frequency and habits (e.g., reckless versus safe), relies on IoT sensors to supply the data for analytics to help determine "good driver" rates. Smart home monitoring systems enable homeowners to optimize security and lower the risk of break-ins through IoT-powered devices such as connected doorbells, which activate motion detectors, deploy night vision, and allow users to speak to persons at the door from anywhere in the world.

8.4 A Decentralized insurance big data repository

A fundamental problem across business sectors is the security of the business and customer data. Traditional systems in use, whether in the banking industry, insurance, or healthcare, have significant weaknesses, providing possibilities for exposure of data to third parties, as demonstrated by widely reported breaches of consumers' social media data (e.g., Facebook) and insurance data. Blockchain emerges as a solution that can circumvent key weaknesses in traditional platforms. Unlike current systems, in blockchain, the data is not present at a central location, thus making it safe and secure. Furthermore, the information is encrypted, maintaining anonymity.

8.5 Smart insurance contract

Blockchain supports "smart contracts," which can automate self-executing agreements that were largely theoretical before blockchain existed. For instance, a life insurance smart contract could immediately release funds to a beneficiary upon the death of a policyholder through electronic checking of death certificates. By dramatically reducing the need for human involvement, claims processing is accelerated, errors and delays are reduced, and improved service is delivered to insurance customers in their greatest area of interest. This will bring transparency in every transaction on the distributed ledger. The aim is to transfer this logic to every possible transaction in the future.

8.6 Client on-boarding

Every customer is required to verifying their identity with the insurance company. Insurers and customers waste a lot of time verifying their documents and identity. This can be reduced with a blockchain platform that can talk to other blockchain platforms to verify the identity of the user. The records in the blockchain can be made available to those who have permission to view the information. All the user records are securely stored in the blockchain using cryptographic techniques.

9. CONCLUSION

In this paper, we have addressed key efficiency and transparency challenges in the global insurance industry. We discussed technologies that can be used for the improvement of current practices. Subsequently, we propose a technical framework that can potentially be used to solve key problems. Two of the most important elements of the claims process are access to the data in real-time and providing a secure and trusted platform for sharing insurance data. We propose an IoT-based 5G network for super-fast data sharing and the use of blockchain for data sharing and maintaining security. We have discussed key technologies that are important in minimizing the aforesaid risks. Through the integration of XAI, our proposed solution will not only reduce the operational costs of insurance claims but also bring transparency to this process. The proposed XAI-driven system will be able to operate independently and should be able to calculate adjustments via its own AI capacity. We believe that our method can help to significantly build trust among insurance customers and help to rebuild sustainability in the global insurance industry.

REFERENCES

ABI, 2018 "Detected insurance frauds in 2018," https://bit.ly/2t2OXyQ

Benhamouda, F., S. Halevi, and T. Halevi, 2018, "Supporting private data on hyperledger fabric with secure multiparty computation," 2018 IEEE International Conference on Cloud Engineering, 357–363

Bhushan, P., 2015, "Bancassurance: the Indian scenario," 2014 NIT-MTMI International Conference on Emerging Paradigms and Practices in Global Technology, Management & Business Issues

Cero, E., J. B. Husic, and S. Barakovic, 2017, "IoT's tiny steps towards 5G: Telco's perspective," Symmetry 9:10, 1–38

Chen, X., Z. Zhou, W. Wu, D. Wu, and J. Zhang, 2018, "Socially-motivated cooperative mobile edge computing," IEEE Network 6, 12–18

Chen, W., D. Wang, and K. Li, 2019, "Multi-user multi-task computation offloading in green mobile edge cloud computing," IEEE Transactions on Services Computing 12:5, 726-738

Code, S., 2018, "Leading a healthier century," AIA

Ehsan, U., P. Tambwekar, L. Chan, B. Harrison, and M. O. Riedl, 2019, "Automated rationale generation: a technique for explainable AI and its effects on human perceptions," IUI 2019, 263–274

Esposito, C., A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, 2018, "Blockchain: a panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing 5:1, 31–37

Fernandez-Carames, T. M., and P. Fraga-Lamas, 2018, "A review on the use of blockchain for the internet of things," IEEE Access 3536:c, 1–23

Gao, J., K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, 2018, "GridMonitoring: secured sovereign blockchain based monitoring on smart grid," IEEE Access 6, 9917–9925

Insurance Journal, 2018, "On-demand insurance agency Trov expands into U.S., launches in Arizona," Insurance Journal, July 5, https://bit.ly/35JpQhv

Juniper, C., 2017, "2018 Trends to watch: insurance," Ovum

Khan, C., A. Lewis, E. Rutland, C. Wan, K. Rutter, and C. Thompson, 2017, "A distributed-ledger consortium model for collaborative innovation," Computer 50:9, 29–37

Lamberti, B. F., V. Gatteschi, C. Demartini, M. Pelissier, A. Gómez, and V. Santamaria, 2018, "Blockchains can work for car insurance: using smart contracts and sensors to provide on-demand coverage," IEEE Consumer Electronics Magazine 7:4, 72-81

Ledger, D., 2019, "Key blockchain trends impacting Hong Kong's logistics industry," KPMG

Li, M., F. R. Yu, P. Si, and Y. Zhang, 2018a, "Green machine-to-machine communications with mobile edge computing and wireless network virtualization," IEEE Communications Magazine 56:5, 148–154

Li, L., J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, 2018b, "CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Transactions on Intelligent Transportation Systems, 1–17

Liu, M., Y. Mao, S. Leng, and S. Mao, 2017a, "Full-duplex aided user virtualization for mobile edge computing in 5G networks," IEEE Access 6, 2996–3007

Liu, W., S. S. Zhu, T. Mundie, and U. Krieger, 2017b, "Advanced block-chain architecture for e-health systems," 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), 1–6

Marjanovic, M., A. Antonic, and I. P. Zarko, 2018, "Edge computing architecture for mobile crowdsensing," IEEE Access 6, 10662–10674

Moubarak, J., E. Filiol, and M. Chamoun, 2017, "Comparative analysis of blockchain technologies and TOR network: two faces of the same reality?" 2017 1st Cyber Security Networking Conference, 1–9

Ni, J., S. Member, X. Lin, and X. S. Shen, 2018, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," IEEE Journal on Selected Areas in Communications 8716:c, pp. 1–14

Pan, J., Y. Liu, J. Wang, and A. Hester, 2018, "Key enabling technologies for secure and scalable future Fog-IoT architecture: a survey," arXiv:1806.06188 [cs.NI]

Porambage, P., J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, 2018, "Survey on multi-access edge computing for internet of things realization," IEEE Communications Surveys & Tutorial 20:4, 2961–2991

PwC, 2019, "Blockchain, a catalyst for new approaches in insurance," https://pwc.to/2FMzgP0

Rahimi, H., A. Zibaeenejad, and A. A. Safavi, 2018, "A novel IoT architecture based on 5G-IoT and next generation technologies," (arXiv:1807.03065v1 [cs.NI])

Rahman, M. A., E. Hassanain, M. M. Rashid, S. J. Barnes, and M. Shamim Hossain, 2018, "Spatial blockchain-based secure mass screening framework for children with dyslexia," IEEE Acces 6, 61876–61885

Raikwar, M., S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, 2018, "A blockchain framework for insurance processes," 2018 : 9th IFIP International Conference on New Technologies, Mobility and Security, 1–4

Ralph, O., 2017, "Bought by Many expands niche insurance role," Financial Times, January 16, https://on.ft.com/2ThPK9x

Riikkinen, I., M., Saarijärvi, H., Sarlin, P. and Lähteenmäki, 2018, "Using artificial intelligence to create value in insurance," International Journal of Bank Marketing 36:6, 1145–1168

Sreehari, P., M. Nandakishore, G. Krishna, J. Jacob, and V. S. Shibu, 2017, "Smart will: converting the legal testament into a smart contract," 2017 International Conference on Networks &. Advances in Computational Technologies (NetACT), pp. 203–207

Turkanovic, M., M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, 2018, "{EduCTX}: a blockchain-based higher education credit platform," IEEE Access 6, 5112–5127

Valtanen, K., and J. Backman, 2018, "Creating value through blockchain powered resource configurations: analysis of 5G network slice brokering case," IEEE Wireless Communications and Networking Conference Workshops (WCNCW): Workshop on Intelligent Computing and Caching at the Network Edge, 185–190

Wang, S., J. Xu, N. Zhang, and Y. Liu, 2018, "A survey on service migration in mobile edge computing," IEEE Access 6, 23511–23528

Weitz, K., D. Schiller, R. Schlagowski, T. Huber, and E. André, 2019, "'Do you trust me?': increasing user-trust by integrating virtual agents in explainable AI interaction design," IVA'19, 7–9

Yang, Y., Y. Ma, W. Xiang, X. Gu, and H. Zhao, 2018, "Joint optimization of energy consumption and packet scheduling for mobile edge computing in cyber-physical networks," IEEE Access 6, 15576-15586

Yeow, K., A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, 2017, "Decentralized consensus for edge-centric internet of things: a review, taxonomy, and research issues," IEEE Access 6, 1513–1524

Yin, H., D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, 2018, "Hyperconnected network: a decentralized trusted computing and networking paradigm," IEEE Network 32:1, 112–117

Zhang, K., S. Leng, Y. He, S. Maharjan, Y. Zhang, 2018, "Mobile edge computing and networking for green and low-latency internet of things," IEEE Communications Magazine 56:5, 39–45

Zhao, Y., Y. Li, Q. Mu, B. Yang, and Y. Yu, 2018, "Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems," IEEE Access 6, 12295–12303

Zhou, E., S. Hua, B. Pi, J. Sun, Y. Nomura, K. Yamashita, and H. Kurihara, 2018a, "Security assurance for smart contract," in Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security, 1–5

Zhou, X., J. Liu, Q. Wu, and Z. Zhang, 2018b, "Privacy preservation for outsourced medical data with flexible access control," IEEE Access 6, 14827–14841

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO