Department of business and management

Bachelor's degree in management and computer science

How blockchain technology and smart contracts could revolutionize health and life insurance industry

Supervisor:

Prof.

Massimo Bernaschi

Candidate:

Alessandro Tursilli

249361

ACADEMIC YEAR – 2021/2022

Table of contents

Introduction ……3

Chapter 1: smart contracts and the blockchain

1.1 Introduction to the blockchain ……..……..5

1.2 What are smart contracts and how they work …….……6

1.3 Smart contracts and actual contract law …….……..10

1.4 What can smart contracts enable today?.....12

Chapter 2: health and life insurance possible applications

2.1 Moving towards more interoperable, comprehensive heath records……...…14

2.2 Supporting administrative processes with smart contracts……...16

2.3 Fraud detection…….....17

2.4 Making applications more client-centric……...…19

2.5 Establishing a more dynamic insurer/client relationship……..……20

Chapter 3: Current applications in insurance

3.1 Chainlink …….……23

3.2 Ethersic – generic insurance framework providers…….…….25

3.3 IBM partnership with Aetna…….……28

Conclusion…….……29

Bibliography……..……30

Introduction

The insurance industry is a cornerstone of modern economies, providing a safety net for people and business activities. However, the traditional insurance process is often slow, bureaucratic, and prone to fraud, leaving policyholders feeling frustrated and distrustful of the industry. With the advent of blockchain technology and smart contracts, the insurance sector has the opportunity to revolutionize the way it operates, delivering more efficient, secure, and transparent insurance products to consumers.

Smart contracts are self-executing agreements that automatically enforce the terms of a contract without the need for intermediaries. They execute on a secure and decentralized platform for managing and completing insurance transactions, reducing the need for manual processes and minimizing the risk of fraud. Meanwhile, blockchain technology provides a secure and decentralized ledger that can securely store and manage insurance transactions and records, further enhancing security and transparency.

In this paper, we will explore the potential of smart contracts and blockchain technology to transform the life and health insurance industry. Chapter 1 provides a comprehensive overview of smart contracts and blockchain technology, including their underlying principles and the key features that make them so transformative. We will examine the technology behind smart contracts and blockchain, and provide a general analysis of how they work and their potential applications. We will also discuss how current contractual law works and what are the challenges that smart contract will face with the present regulatory framework.

Chapter 2 will delve into the potential applications of smart contracts in the life and health insurance sector, including streamlined claims processing, reduced fraud, and increased transparency. We will analyse how oracles could connect real-time data to on-chain smart contracts to the purpose of establishing a more dynamic pricing approach resulting in a better client – insurer relationship. We will explore how making insurance applications more client-centric could benefit the industry by improving trust between policyholders and the insurance company.

We will also examine the challenges and limitations of adopting these technologies in the insurance industry, and provide insights into the best practices for implementing them. This chapter will provide a comprehensive overview of how smart contracts and blockchain

technology can transform the insurance sector, from the policyholder experience to the operations of insurance companies.

Chapter 3 will explore some of the current projects and initiatives in the insurance sector that are using smart contracts and blockchain technology. We are going to describe Ethersic and how this platform provides general frameworks for insurance related smart contracts. Then, we will introduce Chainlink oracles that provide the connection between off-chain data and on-chain smart contracts and the collaboration between IBM and Aetna to build a blockchain ecosystem to further develop decentralized health insurance.

In conclusion, this paper provides a comprehensive examination of the potential of smart contracts and blockchain technology to transform the life and health insurance industry, and offers valuable insights into the future of the industry. I believe that the adoption of these technologies has the potential to revolutionize the way insurance operates, delivering better products and services to consumers and improving the overall experience of policyholders.

1.0 Smart contracts and the blockchain

1.1 Introduction to the blockchain, why is it needed to support smart contracts

Blockchain technology has been a hot topic in the past few years, with proponents of the technology heralding it as a revolutionary new way to store, manage and transfer data securely. A blockchain is essentially a decentralized, digital ledger that records transactions on multiple computers in a secure, tamper-proof manner. Each block in the chain contains a record of multiple transactions and is linked to the previous block through cryptographic algorithms, creating a chain of blocks that is maintained by a network of nodes.

The most well-known application of blockchain technology is cryptocurrency, but the technology has the potential to be used in many other areas as well. One of the key benefits of blockchain is that it eliminates the need for intermediaries, such as banks, to process transactions. This not only increases the speed and efficiency of transactions but also reduces the cost and makes it easier for individuals to engage in transactions.

The working of a blockchain can be broken down into several key elements: blocks, nodes, and consensus algorithms. Each block in a blockchain contains a record of multiple transactions, and every block is linked to the previous block through cryptographic algorithms, creating a chain of blocks connected by nodes distributed on the whole network.

Nodes in a blockchain network can be thought of as participants that maintain and update the ledger. When a transaction is made, the nodes in the network validate the transaction and add it to the next block in the chain. The consensus algorithm is used to ensure that all nodes in the network have a copy of the same, up-to-date version of the ledger.

One of the most popular consensus algorithms used in blockchain technology is Proof of Work (PoW). In a PoW consensus algorithm, nodes in the network compete to solve a complex mathematical problem. The first node to solve the problem is allowed to add the next block to the chain, and in return, it is rewarded with a certain amount of cryptocurrency. This process ensures that the blockchain is secure and that all nodes in the network have a copy of the same version of the ledger. Another popular consensus algorithm is Proof of Stake (PoS). In a PoS consensus algorithm, nodes are selected to validate transactions and add blocks to the chain based on the amount of cryptocurrency they hold and are willing to “stake”. The more

cryptocurrency a node holds, the higher its chances of being selected to validate transactions and add blocks to the chain.

One of the key benefits of blockchain technology is its decentralization. This means that there is no central authority that controls the network, making it more secure and transparent. Transactions are verified and recorded on multiple computers in the network, making it nearly impossible to tamper with the ledger. In addition, all participants in the network have access to the same, up-to-date version of the ledger, increasing transparency and reducing the risk of fraud.

In the context of smart contracts, blockchain technology provides the necessary infrastructure to support their implementation. A smart contract is a computer program that automatically executes the terms of a contract when certain conditions are met. This means that contracts can be executed automatically without the need for intermediaries to enforce them. Blockchain technology provides the perfect platform for smart contracts because of its decentralized nature. This means that once a contract is written and deployed on the blockchain, it can be executed automatically without the need for any central authority. This eliminates the possibility of fraud or tampering with the contract, as all parties to the contract have access to the same, tamper-proof version of the contract.

In conclusion, blockchain technology is needed to support smart contracts because it provides a secure, decentralized and tamper-proof infrastructure that allows contracts to be executed automatically without the need for intermediaries. This not only increases the efficiency of transactions but also reduces the cost and reduces the risk of fraud. The combination of blockchain technology and smart contracts has the potential to revolutionize the way in which we do business, making it easier, faster and more secure.

1.0 What are smart contracts and how they work.

In 1997 Nick Szabo was the first to introduce the concept of smart contract. He defined the smart contract as a "'a computerized transaction protocol that executes the terms of a contract"[1]. Szabo also proposed translating contractual clauses (collateral, bonding, etc.) into code, and embedding them into property (hardware, or software) that can self-enforce them, so as to minimize the need for trusted intermediaries between transacting parties, and the occurrence of malicious or accidental exceptions. As he quoted, Szabo also makes a real-life example of what is most similar to smart contracts: "A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas[2]"

Relating to this concepts, smart contracts could enable the exchange of money, property or information between parties in a transparent and more efficient way, this benefits could improve transaction costs every normal contract has.

Smart contracts really excel in data driven scenarios where the execution of the contract is purely deterministic. Within the blockchain context a smart contract is stored on the chain, and triggered by a transaction. It self-execute automatically in a prescribed manner on every node of the network according to the data contained into the triggering transaction. K. Christidis[3] provided a good scheme of how a smart contract could easy manage a data-driven interaction: Let's consider a blockchain network where Bob, Carol and Alice interact and where digital assets of type X and Y are traded.

Bob deploys a smart contract on the network that defines:

[1] Szabo N., Smart Contracts, 1994, http://szabo.best.vwh.net/smart.contracts.html.

[2] *Ibdem.*

[3] Christidis K., "Blockchains and Smart Contracts for the Internet of Things", p. 2296

1. A “deposit” function that allows him to deposit amount of X into the contract
2. A “trade” function that sends back 1 unit of X (from the contracts deposit) for every 5 units of Y it receives
3. A “withdraw” function that allows Bob to withdraw all the assets that the contract holds.

From this scheme we can suggest that the “withdraw” and “deposit” function can only be used by Bob (via his key) because Bob decided it; but those function could be written to let every user on the network could call them.

Bob now sends a transaction on the smart contract address calling a “deposit” function and moving 3 units of X to the contract. This transaction is recorded on the blockchain. Alice, who own 12 units of Y, then sends a transaction that moves 10 units of Y to the “trade” function and gets back 2 units of X. All of the transactions above are recorded on the blockchain. Bob then calls the function “withdraw”. The contract checks the signature key of Bob to check his identity and transfers all of its deposit (1 unit of X, and 10 units of Y) back to Bob.

Now we can observe the following:

1. The contract has is own state and can take “custody” of the assets on the blockchain[4]
2. An appropriately written smart contract should be able to describe all possible outcomes of the contract.
3. The connection between Bob and other users on the network is only driven by data. A transaction can be actually viewed as a signed data structure indicating a transfer of value[5].
4. Triggering a smart contract is done only by messages/transaction sent to its address
5. Smart contract are written is a deterministic way: to the same input will correspond always the same output. Writing a non deterministic contract on the blockchain could correspond to a error because an attempt to deploy the contract could not reach the consensus needed to register it on the blockchain ledger.
6. Smart contract that resides on the blockchain can be inspected by every used of the distributed network.

[4] Brown R. G., A Simple Model for Smart Contracts, 2015, http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts.
[5] Antonopoulos A. M., Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. Sebastopol, CA, USA: O’Reilly Media, Inc., 2014.

7. All interactions on the contract occur via signed messages on the network, this means that all users could get a cryptographically verifiable trace of all the transaction occurred on the blockchain.

Bitcoin-style blockchain can only support transfer of value between untrustful parties, smart contract take this concept even further. Furthermore, a blockchain that supports smart contracts like Ethereum allow for multi-step interactions to occur between mutually distrustful actors.

The main advantages are:

(a) All transacting entities get to inspect the code in a transparent manner, identify the all possible outcomes and decide to engage with the contract.
(b) Entities have also the certainty of the execution of the code, mainly because the contract is deployed on a network that no one actually owns and control fully.
(c) Actors have also identifiability of all the transaction occurred on the smart contract since those are registered on the distributed ledger.

The possibility of dispute is eliminated (only if all possible outcomes are accounted for) since the participants already verified and could not disagree over the outcome they engaged in.

Smart contract could be seen as autonomous parties, whose behaviour is deterministic and predictable. Smart contracts, also gave rise to the concept of DAOs “decentralized autonomous organizations” which are entities whose behaviour can be changed if a certain process that is coded into the contract is followed. An example can be of a smart contract that with a function calls another smart contract by address to perform its function. This address may be on the mutable part of the contract database containing a list of members, addresses (like public keys) that get to vote on a certain behaviour. A rule could be written in the contract so if the majority of the voters make a decision , the contract will modify its behaviour based on the voters decision by calling the address that received the majority of the votes.

1.1 Smart contracts and actual contract law: challenges

In this section of the paper some possible challenges of smart contract are highlighted and discussed. Such challenges can have a universal interpretation regarding different jurisdictions because they relate to the core principles of contractual law.

One could identify the nature of these challenges in the general adoption of smart contracts in a technical universe "parallel" to the legal realm, most of the time the pace at which technology evolves isn't backed up by appropriate regulatory frameworks, just as in the case of internet at the early stage.

The fact that provisions of smart contracts are enforced only by programming code could lead to the following issues:

(1) *Smart contracts don't create obligations in a legal sense.* The concept of obligation originates from Roman Law and is still key to actual law codes. Obligation defines a right, but to every right corresponds a duty. The term "obligation", then explains sometimes the duty, sometimes the right but more properly it describes the whole relationship[6]. The absence of this concept (understood in the classic legal sense) may lead to the conclusion that all of the legal laws associated to the concept of obligations are inapplicable. This affects the laws regulating to the mode of the performance and also to the consequences of non-performance. It's important to note that this doesn't imply that a smart contract can't be a legal contract of any form. In fact, the parties involved can still express their will just by agreeing to the contract, and they're still responsible for the result of their action. Furthermore, contract law also contemplates certain type of contracts that are performed instantaneously at the moment of the conclusion of it. So it would be more correct that implications of smart contract don't relay on actual "obligations" but the resulting of self-limitation of certain rights by technical means[7].

(2) *Unbreachability of a smart contract by a party.* One of smart contracts characteristics is their self-enforceability, which is a consequence of "code is law" nature. In this case any type of compensation for breach of the contract , e.g. liquidated damages, penalties

[6] B Nicholas, An Introduction to Roman Law (Oxford, 1962) 158.

[7] Alexander Savelyev (2017) Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, 26:2, 116-134

or penalties are not contemplated into smart contracts, unless they are explicitly written into the code itself. There is no actual need to address potential claims to a judiciary party or enforcement agency. This is actually one of the "selling points" of this types of contract. Though, in these cases this feature might be exploited by the potential vulnerabilities or imprecision of the code, by a party to the contract or a third party.

(3) *Vitiated consent or intent don't interfere with Smart Contract validity.* In this case, if a smart contract was concluded by mistake, unfair exploitation or as a result of fraudulent actions is completely irrelevant for its outcome. This is in contrast with contract law, in fact these action constitute a basis for legal claims. Therefore, in Smart contract a collision between intent and its expression is not contemplated; what is really important is the expression of intent via computer code. This approach could be viewed as an achievement for protection and market expectations. Needless to say, there is a possibility for applying provisions and limitation on the invalidity of a contract. Though, this is only possible if the malicious actor of the smart contract is identified and under the legal reach of a jurisdiction. This kind of action though, will not impact the content of the blockchain due to their immutability principle.

(4) *Smart contracts are egalitarian by nature.* Many jurisdiction across the world provide the consumer with special protection against unfair contract terms, this could be inapplicable to smart contracts. At the same time, consumer operating with smart contract might have more power to protect their interests. Nowadays, consumer have little to no power of choice as to not conclude or conclude a contract: it's long and hard to actually read and understand the terms and conditions of normal contracts provided by businesses, and consumer often don't have the bargaining power to change them; as they decide to go to another seller the terms and conditions are often the same. In the very near future Smart contracts could allow consumers to sign contracts with terms and conditions pre-established by them[8].

(5) *Illegal smart contracts.* Smart contacts treat legal and illegal subjects in the same way; what only matters is the feasibility of the smart contract terms. One example could be implementing a smart contract for illegal actions like hacking a website. A contract deployed on the Ethereum blockchain could control some type of cryptocurrency that can be automatically sent to a wallet in exchange of proof of the illegal act, in the form

[8] J Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection'

of a cryptographically verifiable string added to the attacked website[9]. Obviously, such contract would infringe normal laws, but it will still be executed by the programming code. The only solution would be to be able to pursue the individuals involved in the transaction in real life.

(6) *Autonomous nature of Smart contracts.* Is it possible to say, strictly speaking, that smart contracts don't need an actual legal system for their existence: they can operate across different legal systems. They may be interpreted as an alternative to the whole contractual law. Mathematics is a universal language, this highlights the transnational nature of those contracts which are regulated regardless of differences in national laws. The case of permissioned blockchain network though might be the best use case to let smart contracts be under the jurisdiction of a nation.

1.2 What can smart contracts enable today?

Smart contracts are designed to automate resolutions of contracts and allow parties to agree to an outcome without the intervention of intermediaries or a central authority, this can be achieved by 3 key features:

(a) A smart contract automatically process the outcomes of the contract

(b) *Multi-signature features* enable more parties to sign a contract and to approve a transaction – this is a key feature for multi-party contracts

(c) *Escrow capability* allows the locking of funds in the contracts that may serve has a collateral and can be unlocked under certain conditions defined by the contracting parties. Oracles are fundamental in this process, they're the bridge between real life inputs such as prices, performance or real-world data.

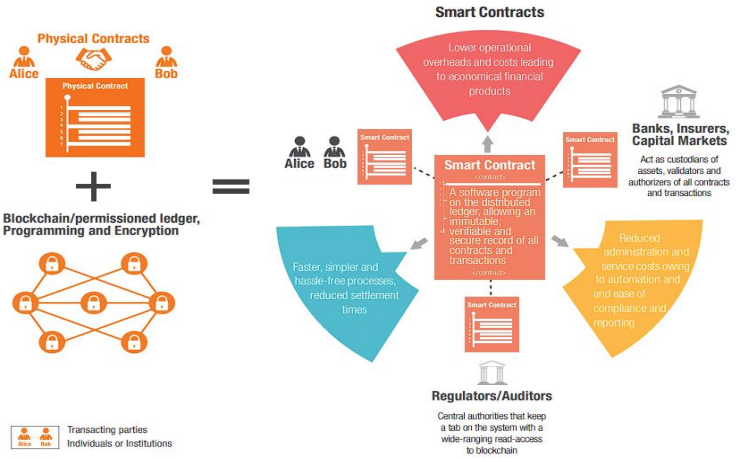
A permissioned blockchain ledger could be the best solution in financial services. It assures security privacy and scalability, which are all key features for all stakeholders:

- The transacting parties
- Banks and insurers: the can act as a custodian of assets and validators of transactions.

[9] P Duggal, Blockchain Contracts & Cyberlaw (E-book, 2015)

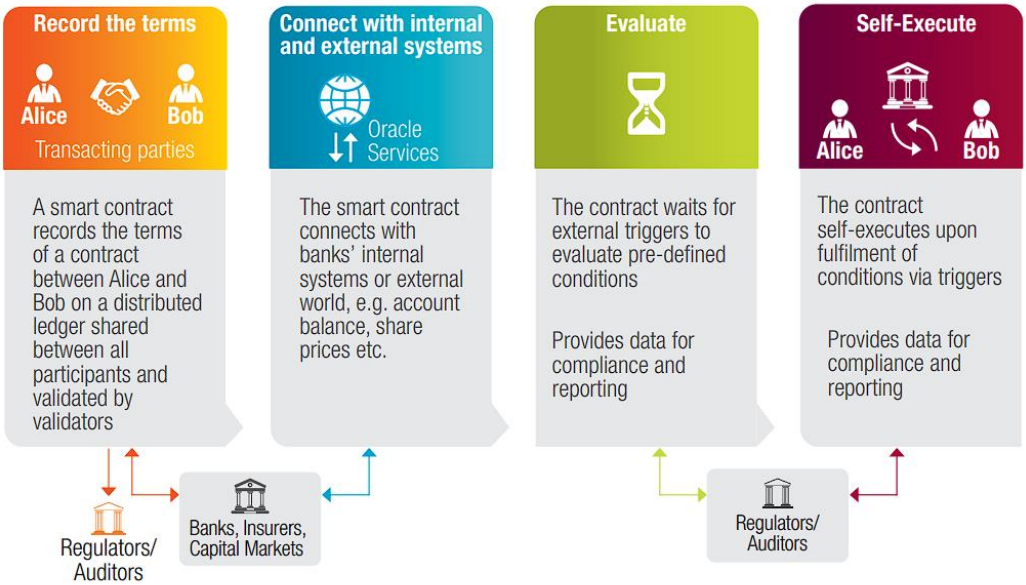
- Jurisdictions: they can have access to all registered transactions and keep watch on the whole system.

Figure 1. How smart contracts could work on permissioned blockchain systems



Source: Capgemini, "Smart contract in financial services", p.6

Figure 1.2 – Smart contracts lifecycle



Source: Capgemini, "Smart contract in financial services", p.6

From figure 1.1 and 1.2 we can have a practical framework of how a smart contract could work on a permissioned blockchain and his lifecycle, the advantages of this model could be extended

to all segments of financial services and will determine 3 key benefits: risk reduction, cost reduction and more efficiency[10].

2. Smart contracts – health and life insurance perspective

2.1 Moving towards more interoperable, comprehensive heath records

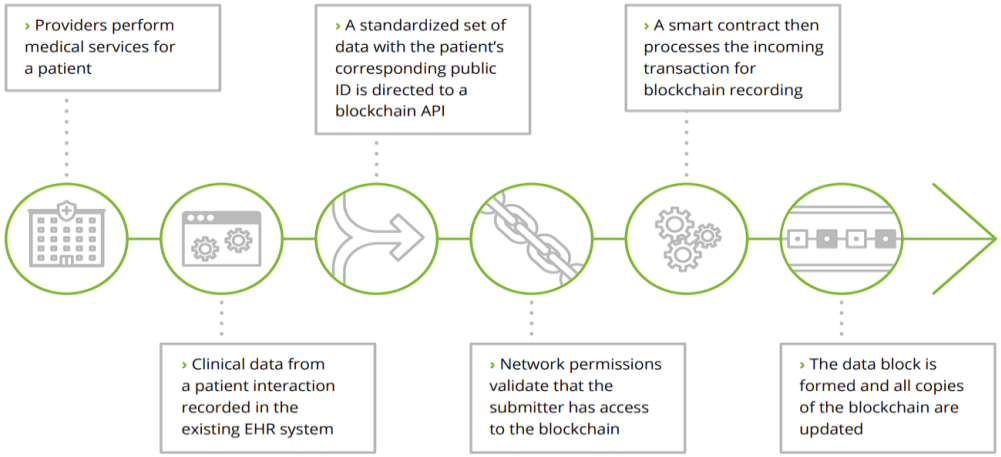
One of the main problems in health care today is sharing sensitive medical information across different users, providers and stakeholders. Blockchain feature to bring different entities together while enhancing data privacy and security might be the answer to this challenge.

The actual state of patient health records is not in a good position. Often, records are shattered among a multitude of entities, resulting in incomplete health records that are not sufficient to track patients in real time, which is one of the promises of coordinated care. In USA, only 18% of providers actually use electronic patient information from outside sources. Almost 36% of hospital providers rarely or never use electronic patient information[11]. The secure exchange of health information is already a priority to some insurer. Indeed, lack of interoperability can impact the quality and the cost of medical procedures by causing the repetition of useless diagnostic tests, medication prescribed that might impact negatively with other prescriptions, and relevant clinical information not to be shared when urgently needed. It can also result in poor clinical outcomes and readmission in hospitals if hospital loose track of patients sent home and develop conditions.

[10] *Ad ibidem*, p.8

[11] Vaishali Patel, JaWanna Henry, Yuriy Pylypchuk, and Talisha Searcy, "Interoperability among US non-federal acute care hospitals in 2015," Office of the National Coordinator for Health Information Technology.

Figure 2.1 – roadmap for adding medical information to blockchain systems



Source: *Blockchain:* A Comprehensive Look at Blockchain applied to Healthcare, Deloitte.

Two main reasons for blockchain to be the main answer to those problems are the ability of decentralized systems to establish trust and security between two or more entities. An interoperable and comprehensive health record could be mostly pulled out directly from existent EHRs in hospitals. Providers could also already select which information to be used when a patient goes to a doctor appointment or is recovered into a medical facility. Blockchain could also contain patient-generated data. Smart contracts can easily provide a secure identification process for the patient, resulting in readable and consistent data from all sources. Trust issues between different actors can be solved by blockchain's automated data verification. With the use of blockchain systems there is no need for an intermediary and users don't have to communicate. Participants will have control on who accessed their information, which is tamper-resistant once inside the blockchain. Blockchain provides a more secure environment to access data, for example a patient can provide access through private keys only to authorized users (hospitals, doctors and insurers).

One challenge blockchain systems might be facing is the scalability. These kind of environments will need a multitude of transactions to be executed every time and it's well know that some blockchain network are slow and have serious scalability problems. But, blockchain technology is constantly evolving and new generations of it are developed to be faster and more scalable. Some of today's interoperability problems might still be present even with the development and implementation of blockchain systems. Another question is who will be in charge to pay and maintain the blockchain. Also, even if these system are more secured, blockchain is not fool-proof. However, the benefits of developing this technologies, both in the

short and long term, should push stakeholder to invest and may impact how health information exchanges operate in the future.

2.2 Supporting administrative processes with smart contracts

Information is crucial in a insurance company. Properly acquiring, processing, securing and sharing information to make decision in a timely manner is important. Although, today's transaction can take days or weeks to process. It is important to note that many insurance companies still uses claims processes that were built decades ago. These technologies are now outdated, resulting in high cost for insurers. Also, the administrative infrastructure of these companies is inefficient and it is imperative to cost-effectively maintain them. Health insurer are often required to meet an acceptable medical loss ratio, which represent the proportions of their revenues which are paid out in reimbursements and those paid to manage administrative expenses.

The many millions of transactions and exchange of data an insurance companies and all the different actors involved in these environments like providers, customers, doctors, vendors and regulators should become much more efficient and easier to access, saving time and resources. Blockchain is capable of automatically collect all this data and valuable information sets, the link all together and act on the data using smart contracts.

Underwriting, pricing and claims processing are going to be faster with the implementation of smart contracts, due to their rules-based system and automatic verification of terms and conditions. For claims processing, as soon as medical services are rendered by a provider and the patient's updated EHR is uploaded and verified by the blockchain, the payment could be automatically initiated. This reduced the time needed to file a claim and review each one of them.

Another example is application review: the blockchain is capable of verifying applicants' information by comparing it, previous applicant approval, to applicant health record on the blockchain. If the information is correct, the blockchain could trigger an ID card or new member information. Even record maintenance such has change of addresses or updates – which often are challenging information to obtain and require multiple human interaction – could take place more quickly and easily through blockchain automatic documentation and verification.

Both health and life insurance are heavily regulated sectors, those companies would benefit from the transparency of organizational transactions and other activities. It is key for these companies to pull data together from different sources, the accessibility and security of blockchain ledgers could make reporting much faster, secure and easier.

Seeking quality providers for insurance companies is fundamental, data sharing across organizations could help insurers in seeking out the right and cost-effective provider. With smart contracts, it would be also much easier verifying if contracted providers are meeting their obligations. Smart contracts could automate drafting complex terms and condition and could ensure their executions automatically, the immutability of smart contracts could also ensure that all parties are confident that terms will be consistently executed. Smart contract will also make the whole transaction record available to all see and review.

There are still challenges into the implementation of blockchain systems into insurance companies back-office processes. Implementing new technology requires to all actors to fully understand and operate it effectively, this could result in costs for teaching users. In addition, quality of data is crucial – information need to be accurate and properly formatted in order to be combined with data from different resources. In fact, combining data from different sources such as health care providers, users and financial institution might result in the need for data reformatting and manual migration. Integration and migration costs need to be considered, along with allocating resources to train employees. However, the benefits might be more than the costs especially in the long term.

2.3 Fraud detection

Insurance companies loose approximately more than 80$ billion annually[12]. Frauds in health insurance ranges from submitting claims for medical services that were never rendered to up-coding services to receive higher payments. Insurance policyholders commit fraud by not reporting other types of insurance coverage that would already cover the billed services or filing claims on behalf of ineligible members/dependents. Into the life insurance scenario frauds typically occur during filing the application – often, applicants try to cover key medical information like past diseases, cancer, diabetes or hearth conditions. It is important for health

[12] Coalition Against Insurance Fraud, "By the numbers: fraud statistics," http://www.insurancefraud.org/statistics.htm, 2016.

and life insurers to protect themselves and their shareholders and policyholders from frauds in order to decrease costs.

Like said before, when false information is submitted by applicants via false claims, false applications or other false information, smart contract could be enable to detect and help determine if the submission is invalid. All data types can't be verified by smart contracts, but they can validate the submitter and the completeness of the information. A health insurer could verify these types of claims by linking the submission to a patient's interoperable health record to verify that the patient had rightfully claimed for the medical procedure he requested. A life insurer could also analyse different elements of the patients health record – like whether the applicant was been treated for dangerous diseases, or if the patient was a smoker – to even public employments record to check if the information submitted by the applicants are correct. If everything is correctly confirmed, the claim can be processed and paid. If not, the claim would either be not paid, or at least the insurer could start an investigation.

Blockchain's ability to easily and securely check data from different resources at any stage of the claim processing and data analytics can help insurer to detect, and fight fraudulent actions. Into the health insurance world, some providers can intentionally bill different insurance companies for the same medical service; nowadays, without a interoperable system like blockchains and smart contract all the different companies could have not enough information to detect this fraudulent action or to even understand if the bills were made intentionally wrong or by accident by the provider. If all the payer's information are brought together into an interoperable system, trends are easier to recognize and fraud could be easily exposed. By using analytics, insurance companies could build model made to detect strange trends and indeed possible frauds, systemic waste and abuse – companies could also share information between them to link fraud cases made among different insurers.

Collaboration including different organization like health insurers, law enforcement, health care providers and financial institution is crucial to link different and external blockchains in order to detect, identify and fight fraudulent actions. The sharing of data and collaboration mentioned above may take big investments in time and resources to develop and maintain.

2.4 Making applications more client-centric

Applications for life and health insurance might be difficult and time consuming when users are required to gather past medical information and apply for new medical tests for underwriting and pricing their personal policy. A study by LIMRA, a life insurance association, revealed that 70% of people who got their insurance plan by their employer where satisfied with the application process and described it "comfortable". Instead, a more recent, LIMRA repo highlighted that whose didn't have the opportunity to obtain insurance by the employer, but instead tried to buy individually life insurance policies on their own were far less pleased with the experience – some described it "intimidating"[13] . In fact, normal applicants are likely to not apply for life or health insurance; part of this is that they not perceive any benefits in applying for such a complicated and time consuming process.

Deciding which policy is the best for consumers is really challenging. A survey of organizations helping individual choose the right policy reported that 73% of their clients struggled understanding basic concept of insurance.[14] In addition, accessing to health information is difficult, and is one of the biggest obstacles in providing effective health care today.[15]

With easier-to-access, more complete and comprehensive set of medical records on the blockchain, the application proves could be easier and less time consuming. It would change the mind of many people who struggle with the application process and are discouraged by such an intrusive procedure. Furthermore, a blockchain facilitated data repository could become a key feature to enhance customer experience and strengthen relationships. This could help raising the number of people having prospect to apply to a policy, which is faster and more user-friendly. Increasing the number of people with life and health insurance.

If the total of a consumer's medical and wellness record could be contained and registered in a blockchain systems, the application process could be shortened from an average period of 45 days to almost real-time. Health insurers, could benefit from obtaining verified and secured patient information, making the addition of new policyholders information more

[13] LIMRA, "Insurance Barometer Study".
[14] Karen Politz, Jennifer Tolbert, and Rosa Ma, "2015 Survey of Health Insurance Marketplace Assister Programs and Brokers".
[15] David Blumenthal, "The biggest obstacle to the health-care revolution," Wall Street Journal.

faster and easier. In this way, the consumer wouldn't have the burden of manually collect and provide old and new information to the insurer.

This benefits could help lower the uninsured population, even considering people that don't trust normal information systems and see the blockchain as the perfect digital lockbox for them.

2.5 Establishing a more dynamic insurer/client relationship

Insurer/client relationship has always been problematic, one of the main reasons relays in stressful and difficult claims process and lack of clarity in terms and conditions of contracts. Life insurance, also, tends to be a one-dimensional product – in the sense that the conditions are simple and after subscription there isn't big interactions between the insured and the insurer. When the insured dies it pays out, when the term expires, it lapses. Once the sale is closed, the only interaction between the parties is the payment of periodic premiums. With little incentives other than death benefits, life insurance product struggle to drive sales growth. As a matter of fact, younger and healthier people often don't have life (or even health) insurance because is perceived like a low-return, high-cost product that offer really little relevance in a policyholder's daily lifestyle.

EHRs securely stored on a smart-contract based blockchain could help the foundation of integrating a policyholder lifestyle and habits into the insurer/insured dynamic relationship. In example, blockchain could be used not only to safely store patients data and medical record, but it could also be used to store real-time data (trough oracles) about the insured lifestyle via telematic devices like smartwatches. In this way, the insurer could establish dynamic prices and premiums based on the continuous assessment of a person's risk profile. This could allow a scenario in where discounts are applied for certain good habits like diets and exercises achievements , or even gamification-driven competitions. Health insurers could sponsor and support wellness programs and trigger discounts on premiums.

With blockchain and smart contracts architecture it will be easier to effectively integrate different types of health and wellness information sources, rather than the more traditional, disperse, and often siloed digital infrastructure. A medical record stored on a interoperable blockchain system could easily be updated with diversified, lifestyle-related data in near real-time, driving more frequent and dynamic risk calculations and establishing dynamics insurance

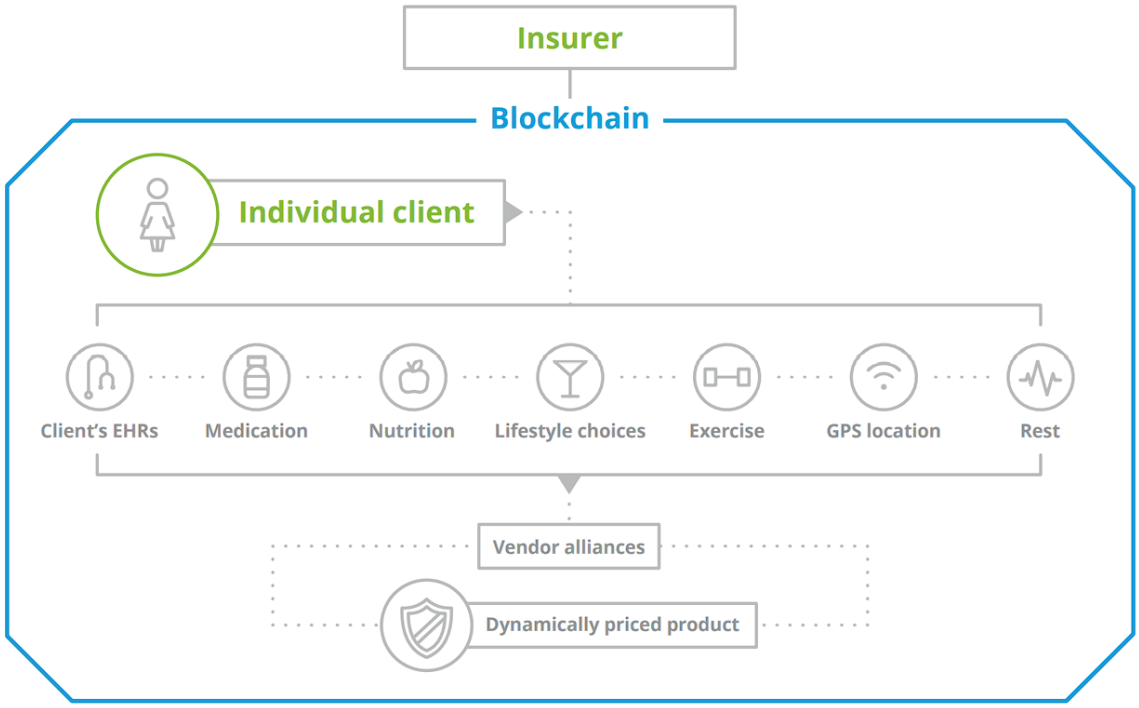
premiums pricing. Life insurers could potentially use this data to incentivize risk-reducing behaviours on an individual's basis, also stimulating healthier lifestyle behaviours by aligning with and offering promotions and discounts for vendors (nutrition facilities, gyms, spas, etc.).

In addition, such real-time data could be tied into health insurance smart contracts to help reminding policyholders to take medications or to schedule check-ups. Data collection could also incentivize contacts from a medical care provider if changes in hearth rate, blood pressure or other factors that might sett off important alarms.

Advanced analytics, blockchain-facilitated data repository and real-time data sources could make subscribing to a life and health-insurance a more integral part of a policyholder's lifestyle. For traditions term life insurance, there could be a shift in the perception from a product based on the inevitability of death to a one focused on tracing a path towards a healthier "policy for life". In a similar way, in health insurance, instead of interacting with the insurer only for payments of insurance premiums or filing claims for illness or injuries, consumers could establish a positive relationship with the insurance company. If healthier lifestyle and exercise can result in immediate tangible benefits – like discounts or reduced deductibles – users could associate health insurance not only with illness and medical expenses but also with benefits and wellness. On the other side, insurers could benefits with healthier and risk-adverse clients.

Leveraging blockchain and smart contracts to interactive, dynamic client-insurer relationships could encourage more people to purchase a life or health insurance and stick with the same insurer one subscribed (particularly if discounts may not apply if clients change policy plan or insurance company).

Figure 2.2 – How blockchain could facilitate dynamic pricing for policyholders.



Source: Deloitte centre for financial services.

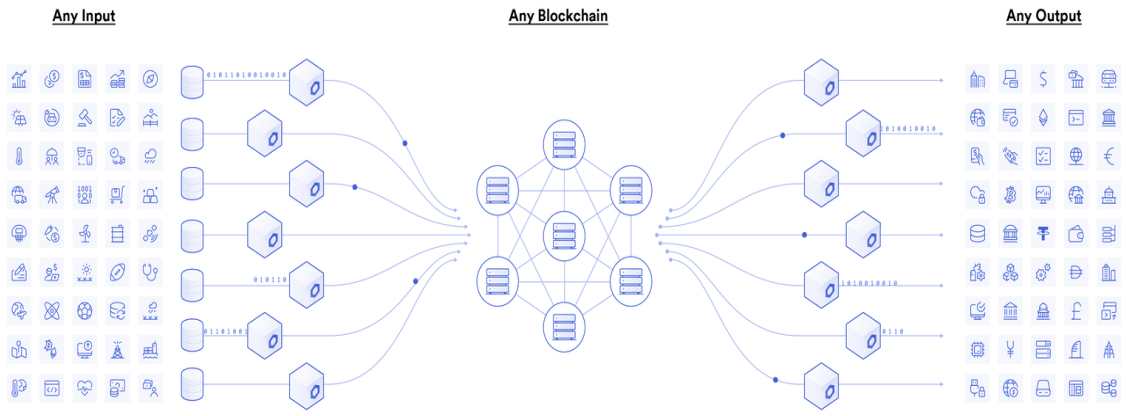
The addition of real-time information that may minimize arbitrary pricing decision and set a more dynamic relationship between the insured and the insurer, cannot be accomplished by blockchain alone. Granular lifestyle data points – uploaded manually or collected automatically via sensor connected to the Internet of Things (IoT) – will need to be securely stored and properly used in the blockchain in order to turn data into effective customer insights and incentives. Furthermore, monitoring 24/7 and possibly penalizing those who don't/can't maintain an healthy lifestyle could affect some consumers to rejects these kind of dynamic – priced policies, while insures could face regulatory constraints to protect the interest of clients that won't participate in these policies.

3. Current applications in non-health and health insurance

3.1 Chainlink – how oracles could help connect blockchain to the real world

One of the main challenges faced by decentralized insurance is the lack of trust in data sources and the difficulty in verifying events that trigger insurance pay-outs. Chainlink[16] is a decentralized oracle network that provides secure and reliable data to smart contracts on the blockchain. It enables smart contracts to access off-chain data and interact with real-world events and systems, making it an ideal solution for decentralized insurance. In the traditional insurance model, insurance companies rely on third-party sources, such as government agencies and data providers, to verify and validate claims. However, in a decentralized insurance model, there is no central authority to rely on. This is where Chainlink comes into play. By acting as a bridge between smart contracts and real-world data, it enables decentralized insurance to access accurate and reliable data to verify claims and trigger pay-outs.

Figure 3.1 – How Chainlink connects off-chain and on-chain data



Source - https://blog.chain.link/

Another benefit of using Chainlink for decentralized insurance is that it helps to mitigate the risk of fraud and mismanagement. Chainlink provides a secure and reliable way for health insurance smart contracts to access and verify off-chain data, such as medical records

[16] https://chain.link/

and test results. This enables decentralized health insurance providers to offer insurance products that are based on real-world data and events, without the need for intermediaries.

For example, a decentralized health insurance policy that covers hospitalization due to a specific medical condition can use Chainlink to verify if a policyholder has been hospitalized and if they meet the conditions specified in the insurance policy. This ensures that policyholders receive the benefits they are entitled to in a timely manner, without the need for manual verification and claims processing.

Chainlink also helps to reduce the risk of fraud in the health insurance industry. In traditional health insurance, fraud is a major challenge that leads to billions of dollars in losses every year. In decentralized health insurance, smart contracts could provide a transparent and tamper-proof way of verifying and managing insurance claims. This reduces the risk of fraudulent claims and helps to keep health insurance costs under control.

Moreover, Chainlink offers a high degree of customization, allowing health insurance providers to tailor their insurance products to meet the specific needs of their target audience. For example, a health insurance provider can offer insurance products that are based on specific medical conditions or demographic groups, such as elderly people or people with pre-existing medical conditions.

In conclusion, Chainlink has the potential to revolutionize the health insurance industry by providing a secure and reliable way for decentralized health insurance providers to access and verify off-chain data. This enables health insurance providers to offer insurance products that are transparent, trustworthy, and tailored to the specific needs of their target audience. As the decentralized health insurance industry continues to grow, it is likely that we will see more and more health insurance providers adopt Chainlink to provide their customers with the best possible health insurance experience.

3.2 Ethersic – generic insurance framework providers

Ethersic was first founded in 2016 as an hackathon project, its whitepaper was released shortly after the competition, in its version 0.3. The focus of the first document was to outline a general framework for decentralized insurance policies and to outline the core of a blockchain based reinsurance market. Since now in 2023, two other whitepapers were released: 1.01 and 2.0. A this moment Ethersic is a large community made of investors, developers and policyholders. The 1.0 whitepaper outlined the DIP token which is used has a staking token to cover collateral damage and claims pay-outs. In 2019 the GIF framework was implemented, resulting in a big innovation in the sector.

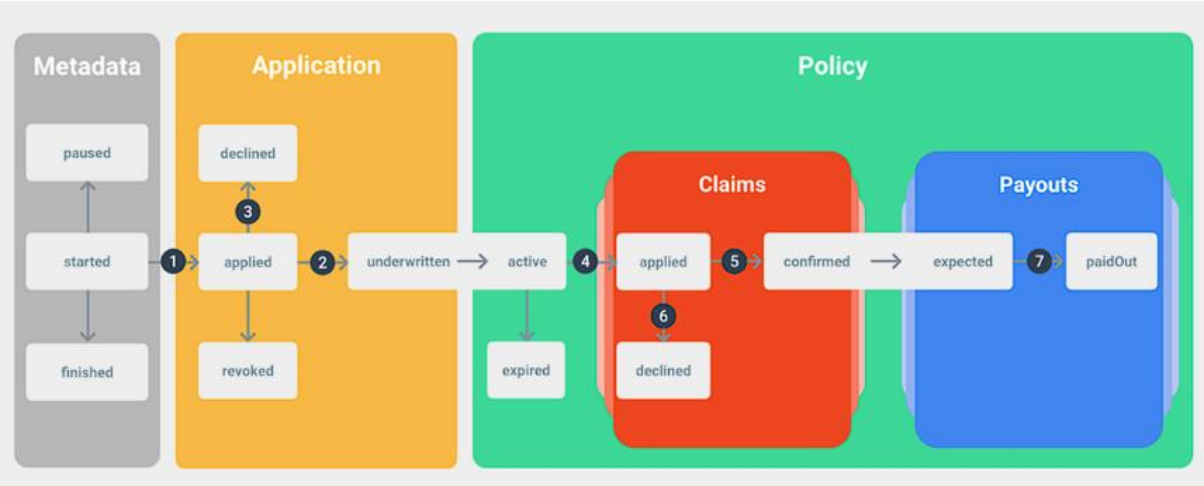
GIF is an acronym for "Generic Insurance Framework". It's made of open-source smart contract able to implement generic insurance products and policy lifecycle functions. Thus, GIF enables a wide range of insurance types. GIF fully operates on a blockchain and is multi-chain and multi-tenant capable. Right now, the GIF is most suited to host parametric insurance products. Parametric insurance cover pre-established loss events immediately when they occur, pay-outs are deterministic, rather than offering compensation for actual damage. GIF already offers cover for flight delay, heavy rainfalls, drought, or damage by hurricanes but a social life insurance is being implemented and will be the next step of integrating more and more different types of insurance products.

The GIF is open source, so everyone can deploy it's own products, modify the code, fork it etc. Any GIF instance can optionally be registered in a global ledger which is supported by a DAO (decentralized autonomous organization), all DAO's stakeholder are able to participate in governance of the network. In order to successfully register a GIF instance, some rules need to be followed, which ensure that clients will feel safe when they subscribe with a registered GIF instance.

GIF instances are managed by an instance operator. The primary task of an instance operator are the administration of products and oracles. The instance operator is linked by and Ethereum address. Any operator can be a natural person owning the private key of the address or a smart contract – either multisignature or represented by a DAO structure. This process fully decentralized the governance and control of any GIF instances. One address can also manage and operate on different instances.

Ethersics provides a standard lifecycle of a policy, which can be also personalized by any product designer.

Figure 3.2 – Representation of policy lifecycle in GIF



Source: Ethersic whitepaper 2.0, https://etherisc.com

The default policy lifecycle delineates the following functions:

1. newApplication (to store and create a new policy for a customer)
2. underwrite (to sign an application)
3. decline (to decline an application)
4. newClaim (to file a new claim for a loss or damage)
5. confirmClaim (to confirm a claim and generate a payout)
6. declineClaim (to reject a claim)
7. payout (to confirm and initiate a payout)

It's important to note that the GIF ecosystem is indifferent on how payments are made, pure crypto payments can be made directly to the product contract, fiat payments require a fiat gateway and an external banking or credit card system.

In the final section of the whitepaper, Ethersic describes how funds for claims and investments in the platform are gathered and managed. In the Ethersic ecosystem, staking comes in two different ways:

1. The first type is staking DIP tokens in a "Global staking Pool". This first type of staking ensures that participants have an interest into the growth of the platform,

and also ensures that users are economically incentivized to behave according to the platform rules.

2. The second type of staking is allocating crypto-assets, usually stable coins, into risk pools. These assets carry the insurance risk.

To be sure that there is always liquidity in order to start or continue selling policies or carrying pay-outs, Ethersic planned two risk pools. Both risk pools will collect premiums form all policies and also collect additional liquidity from investors.

Net premiums (after deduction of costs) from the purchase of policies from clients are paid into the risk pool, and claims are fully covered by the funds present into the same risk pool. An investor can choose his tolerance to risk and portfolio structure. By providing funds for risker policies, investor tend to gain better yields for staking. Investor can also make ethical choices on which kind of policies to cover, like environmental friendliness, climate neutrality, or social commitment. Premiums paid by investors are credited proportionally in the ratio of personal risk capital / total risk capital. If a claims happens to be approved, the refunds are shared proportionally by all risk capital providers who have contributed to the premiums since policy subscription.

In summary, Ethersic's focus on building a general framework for decentralized insurance plans is really interesting. The platform is still in early stages of developments but great objectives have been achieved. Many policies are active and easy purchasable by users, and investors on the platform are incentivized by the staking of the DIP token. In theory, their framework is able to provide many different types of policies and it's possible for every user to have a personalized insurance plan. The GIF framework is open source, and the community is really active. This could incentivize even more the optimization of the whole platform and solve problems that might be encountered.

3.3 IBM partnership with Aetna

American insurance giant Aetna, now owned by CVS health, launched a collaboration between PNC bank and IBM. The aim of the collaboration was to design a blockchain network, supported by smart contracts, that will improve transparency and interoperability in the industry.

The project also includes Anthem and Health Care Service Corporation, it focuses on using blockchain to address and solve different types of industry challenges like claims and payment processing, to allow secure and frictionless health data exchanges, and to maintain current and accurate provider directories. The main objective is to create a collaborative blockchain ecosystem that can benefit multiple members involved into the healthcare industry, maintaining a highly secure, shared environment.

With 500 blockchain's projects in various industries, IBM has been working on blockchain technology for several years. According to Bill LaFontaine, general manager, intellectual property at IBM, the platform from the IBM-led group is already prepared for blockchain experimentation by the participating companies.[17] The initiative stands out from others that are in various stages of completion because the platform is accessible to member companies right away so they can start testing blockchain technology.

According to the IBM-led blockchain initiative, the distributed ledger technology can be used to ease the transition to value-based care, such as bundled payment arrangements. This initiative is also aiming to reduce administrative waste in the healthcare industry and find areas of inefficiency and redundancy. The technology also presents a chance to simplify the administrative procedures in order to reduce transaction costs.

[17] Aetna, IBM launching new blockchain healthcare network. https://www.fiercehealthcare.com

Conclusion and personal opinions

Smart contracts have been gaining significant attention in recent years as a tool for automating and streamlining various business processes. In the context of the health and life insurance industries, smart contracts have the potential to bring about a number of key benefits.

One of the most significant benefits of using smart contracts in the health and life insurance industries is the removal of intermediaries. By relying on secure, tamper-proof code, smart contracts can simplify the claims process, reduce the time it takes to process claims, and eliminate the need for manual intervention. This results in cost savings for both insurance companies and policyholders.

In addition, smart contracts can provide greater security and privacy for sensitive health and personal information. Since the information is stored on a decentralized blockchain, it is protected from unauthorized access, tampering, and other forms of cybercrime. This is particularly important in the health insurance industry, where the security of personal health information is a top concern. Another benefit of smart contracts is their ability to promote transparency and trust. Policyholders can have greater confidence in the claims process, knowing that their information is being handled in a secure and transparent manner. Insurance companies can also benefit from the increased trust and transparency, as it may result in higher customer satisfaction and increased customer loyalty.

As said before, application of using smart contract in the health and life insurance industries could result in many benefits, but here are still some challenges to overcome. For example, the development of smart contract technology is still in its early stages, and there is a lack of standardization and interoperability. Additionally, there are questions about how smart contracts will be regulated, and whether they will be able to comply with existing regulations.

Despite these challenges, the use of smart contracts in these environments is promising, and is likely to become increasingly important in the coming years. As technology continues to advance and more organizations adopt blockchain and smart contract technology, we can expect to see even more innovative applications of this technology, leading to a more efficient, secure, and fair system for all parties involved.

Bibliography

1. **Szabo N., Smart Contracts, 1994**, http://szabo.best.vwh.net/smart.contracts.html
2. **Christidis K.,** "Blockchains and Smart Contracts for the Internet of Things", p. 2296.
3. **Brown R. G.**, A Simple Model for Smart Contracts, 2015**,** http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts.
4. **Antonopoulos A. M.,** Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc., 2014.
5. **B Nicholas,** An Introduction to Roman Law (Oxford, 1962) p. 158.
6. **Alexander Savelyev**, Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, p. 116-134.
7. **J Fairfield,** 'Smart Contracts, Bitcoin Bots, and Consumer Protection'
8. **P Duggal,** Blockchain Contracts & Cyberlaw (E-book, 2015)
9. **Vaishali Patel, JaWanna Henry, Yuriy Pylypchuk, and Talisha Searcy,** "Interoperability among US non-federal acute care hospitals in 2015," Office of the National Coordinator for Health Information Technology.
10. **Coalition Against Insurance Fraud,** "By the numbers: fraud statistics," http://www.insurancefraud.org/statistics.html
11. **LIMRA**, "Insurance Barometer Study".
12. **Karen Politz, Jennifer Tolbert, and Rosa Ma**, "2015 Survey of Health Insurance Marketplace Assister Programs and Brokers".
13. **David Blumenthal,** "The biggest obstacle to the health-care revolution," Wall Street Journal, 2016.
14. **Chainlink official website**, https://chain.link/
15. **Ethersic whitepaper**, https://etherisc.com
16. **Aetna, IBM launching new blockchain healthcare network.** https://www.fiercehealthcare.com