Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2019) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies

Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector

Rui Roriz[a], José Luis Pereira[a,b,*]

[a]*University of Minho, School of Engineering, 4804-533 Guimarães, Portugal*
[b]*Centro ALGORITMI, University of Minho, 4804-533 Guimarães, Portugal*

Abstract

Blockchain is a relatively new technology originally created to store Bitcoin's transaction records. The system is highly redundant and distributed, making it very difficult for fraudulent financial transactions. While cryptocurrencies might be the most well-known use case of blockchain technology, it is wrong to assume that this technology is restricted to the financial area. Indeed, many blockchain use cases are being developed today in different areas. Due to the complexity of certain processes, a new technology associated to blockchain has appeared – smart contracts. These digital contracts act like traditional contracts, with the major difference being their automaticity. In this article, we aim to discuss how blockchain and smart contracts may be used together in order to improve organizational operations. More specifically, we demonstrate how these technologies might be used to develop a solution that avoids certain types of fraud in the area of vehicle insurance.

Keywords: Blockchain; Smart Contract; Vehicle Insurance; Fraud Avoidance.

* Corresponding author. Tel.: +351 253 510 319; fax: +351 253 510 300.
E-mail address: jlmp@dsi.uminho.pt

1. Introduction

Presently, there is a very high expectation regarding the future of blockchain technology. Many startups are being created just to focus in blockchain technology development, while the major Information and Communication Technologies (ICT) companies are investing large amounts of resources to assure their position in this market. Indeed, according to McWaters [1], figures as high as $1.3 billion dollars are being invested by companies in blockchain, worldwide.

The insurance domain is an important economic area, with a high number of complex business processes and a lot of operational data produced. In the specific case of vehicle insurance the situation escalates as, by law, every vehicle owner must have her/his vehicle insured. Taking into account the astonishing number of vehicles presently in circulation, one might understand the magnitude of the situation.

Unfortunately, it is not only the processing work and stored data about insured vehicles that brings headaches to insurance companies. Fraud is also a major problem that costs them a lot of money, being very hard to fight some fraud situations without insurance companies working together. In this paper, we aim to investigate if blockchain technology may contribute to develop more sustainable and viable solutions to help insurance companies avoid frauds.

Regarding the structure of the paper, we begin by making some considerations about the vehicle insurance business sector, discussing the impact of insurance frauds in the sector and presenting the most damaging types of insurance fraud schemes. In the following, after a brief review of some basic concepts related to blockchain technology and smart contracts, we describe a blockchain-based solution to avoid a specific kind of vehicle insurance fraud, mentioning the tools used in its development. Finally, the most important functionalities of the proposed solution are presented and some conclusions are drawn.

2. Background

2.1. Vehicle insurance

By definition, in case of a traffic accident, a vehicle insurance aims to protect the victim's interest, independently if the responsible person for the accident has or has not the economic conditions to indemnify for the damages. A vehicle with no insurance, finds itself in an illegal situation, can be apprehended by authorities and its owner might pay a fine for that.

Since their creation, insurance companies have always been vulnerable to fraud because people are always open to engage in dishonest arrangements in order to make easy money. Vehicle insurance fraud is one of the most common type of frauds in the developed world, losing only for tax fraud [2].

In simple words, insurance fraud happens when a person tries to profit by violating the terms of the insurance contract. Fraudulent people intentionally create losses or damages their property, rather than acting like normal people that have no losses but want to be secure if something happens.

A fraud can happen in any phase of an insurance life cycle [2]:

- Individuals applying for insurance;
- Policyholders;
- Third-party claimants;
- Professionals who provide services to claimants.

There are two forms of insurance fraud: *hard frauds* and *soft frauds*. A hard fraud occurs when an accident is intentionally provoked in order to steal money from the insurance company. A soft fraud occurs when an accident happens naturally without intention of making it, but the insured client adds something more to the claim that has nothing to do with the accident, in order to gain more from it [2].

Insurance fraud has a major impact in the insurance companies profit and, consequently, increases the cost that clients pay to have an insurance policy. The losses for fraudulent claims may only be estimated because, usually, fraud is only discovered when a person starts to be greedy and the fraud arrangement becomes obvious for the company. So, many fraudulent claims might end up successfully without insurance companies notice them as frauds.

There are several known kinds of vehicle insurance frauds, including:

- *Ditching* – This type of fraud happens when the owner abandons her/his vehicle with the intention of it being stolen or stripped for parts. The point of this is to make some money from the insurance policy or to settle an outstanding loan. Frequently, the vehicle is expensive and purchased with a small down payment [2];
- *Cash for Crash* – This type of fraud happens when people intentionally make other drivers to crash into their vehicles in order to blame them. As an example, a driver is waiting to enter a roundabout and there is a vehicle in front of her/him. The driver behind the first vehicle sees that nothing is coming, concluding that it is ok to move forward. The vehicle in front advances as expected but suddenly breaks for no reason and consequently the vehicle behind ends up hitting it. What seems a normal accident, it's all staged by the criminals [3];
- *Double Dipping* – This type of fraud consists in claiming the same accident to multiple insurance companies, thus gaining more money for the same loss. As an example, a person has a health insurance from company A and an auto liability insurance from company B. In case of an accident, she/he might activate both insurances, which is wrong because she/he would get a pay-out from both companies, gaining twice from the same event [4]. In the auto insurance context, the double dipping fraud occurs when, because of a traffic accident, someone fills claims to different insurance companies.

Regarding the work portrayed in this article, the double dipping fraud arrangement is the use case for the developed insurance fraud avoidance blockchain solution.

2.2. Blockchain technology

On the 31st of October of 2008, an article was published by someone under the name of Satoshi Nakamoto, called "Bitcoin: A Peer-To-Peer Electronic Cash System" [5]. In this article, some of the features of bitcoin, which had the potential to revolutionize the financial sector, were described. Through this initial idea, the bases for the creation of bitcoin were established and later (9th of January of 2009) the first Bitcoin application was created. The success of the bitcoin comes from a cryptographic technology underlying it – the blockchain technology [6]. Since then, efforts have been made in order to separate the blockchain technology from the bitcoin application, so that it can be used in other industries [7].

In the words of Tapscott and Tapscott [8] "*This is much more than the financial services industry. Innovators are programming this new digital ledger to record anything of value to humankind – birth and death certificates, marriage licenses, deeds and titles of ownership, rights to intellectual property, educational degrees, financial accounts, medical history, insurance claims, citizenship and voting privileges, location of portable assets, provenance of food and diamonds, job recommendations and performance ratings, charitable donations tied to specific outcomes, employment contracts, managerial decision rights and anything else that we can express in code.*" Because of its potential, ten years after the creation of bitcoin, it is estimated that more than 25 countries are investing in blockchain technology, producing more than 2500 patents and making a total of 1.3 billion dollars invested [1].

In simple words, a blockchain is, essentially, a distributed database of records, or a public ledger of all transactions or digital events that have been executed and shared among participating parties [9]. All the transactions or digital events are inserted into blocks and these are added to the blockchain in a linear, chronological order [10].

Associated to blockchain is the concept of smart contract. In 1997, Nick Szabo published an article called "The idea of Smart Contracts". He defined smart contract as "*A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are 'smarter' than their paper-based ancestors*" [11].

Smart contracts have been designed to automate transactions and allow parties to agree with the outcome of an event, without the need for a central authority [12]. Nick described smart contracts as "*protocols within which the parties perform*", so when a transaction or an event occurs there is a set of rules which tells how the data should be processed, helping to produce the right outcome. This is accomplish by transforming the smart contract into computer code with clauses and agreements embedded as lines of programming code. Smart contracts seek to leverage the trustless, immutable nature of the blockchain to empower peer-to-peer, disintermediated agreements enforced automatically by code [13].

3. Proposed fraud avoidance blockchain-based Solution

Nowadays, the most widely used architecture for the development of distributed systems is known as *client-server*. In this architecture, *clients* request services from *servers* and deliver the results from those requests back to users via suitable interfaces. Servers store all the data and keep waiting to receive requests from clients, just to do the necessary processing and send back the results. While this is a very well-known and widely used architecture, with a vast number of successful applications developed and currently running, it suffers from a few problems:

- The server has a nuclear role in the system, being a major point of failure, in the sense that if the server goes down the entire system goes down as well;
- Even though security measures might be in place, there is always a chance that the data stored in the server can be changed/removed.

Having all these implications in mind it is convenient to search for new ways of mitigating these problems and blockchain could be just one of the answers. Building an application on the blockchain, in which every node is connected to every other node through the network, can help to eliminate the first problem. As for the security of the stored data, taking into account the blockchain inherent characteristics of data persistence and immutability and the consensus mechanisms used to store new data, the second problem is also solved.

Instead of the usual central server with a database, blockchain can be a network and a database combined. In the fraud avoidance insurance support system that we are proposing, the used data is available to all the insurance companies. By being part of this solution, every company has a copy of the data and code present in the blockchain. There is no more a single point of failure compromising the entire network, just multiple computers interacting with each other in the same network.

3.1. Vehicle insurance policy management

The process for creating an insurance policy is very simple. The client goes to the insurance company with the intention of making an insurance of her/his vehicle. Once there she/he talks to the insurance mediator about the deal. The insurance mediator asks for all the required information, for instance, vehicle plate, characteristics of the vehicle and client's age. After inserting that information into the system, it makes deal suggestions for the mediator to propose to the client. If the client accepts, the new insurance policy is submitted into the system.

With the integration of blockchain the business process would still be, essentially, the same, the only difference being when submitting the contract to the system. After the client accepts the terms, the mediator submits the contract into the blockchain, and a smart contract will automatically be activated. The purpose is to verify if the vehicle already has an active insurance policy in another company, in order to prevent a future double dipping fraud. If no insurance policy is found the new insurance policy is concluded and that information becomes available to all the companies in the blockchain network.

The prototype of our blockchain solution has been developed using the Ethereum technologies. In our proposal, every insurance company has a frontend and a backend present in their system. The frontend is where the employees interact with the DApp (Decentralized Application). The interface is quite simple and intuitive making use of two programming languages (HTML and CSS). As for the backend, this is where all the process to the blockchain is going to occur. Two languages were used in the backend development - JavaScript and Solidity.

Every insurance company system is represented by a node of the blockchain (see Figure 1). When an employee creates a new insurance policy, it first must pass all the criteria present in the smart contract and only then the transaction can be submitted to the blockchain.

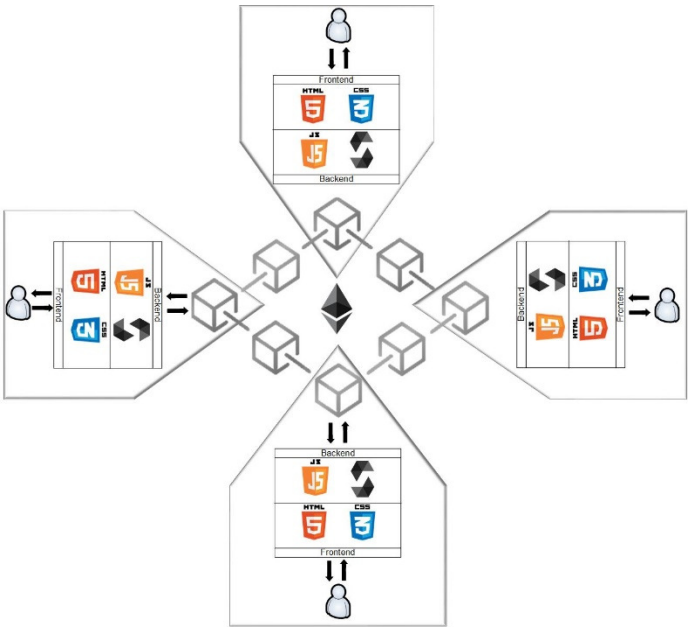

Figure 1. Blockchain solution architecture for insurance companies

3.2. Development tools

In the next paragraphs, a very brief description of each one of the tools used to implement the proposed blockchain solution is presented.

- *Solidity* - As the blockchain platform used for the system is Ethereum, it is necessary to use its own language – Solidity [14]. Solidity is used to code all the business logic into the smart contracts so the verifications upon creating an insurance can be checked. Ethereum was the first decentralized app platform and because of that it is the blockchain platform that has the higher number of developers building real-world applications on top of it. Besides this, since the creation of Ethereum many developers have developing multiple tools (Truffle, Infura, Web3.js, among others) to help other developers create their DApps easily. So, for several reasons, availability and easy access to information, tools and notorious success of the technology, the Ethereum was chosen for the development of this DApp.
- *Node.js* - An open source and cross-platform runtime environment for executing JavaScript code outside of a browser. Node.js is used to build back-end services, also called APIs. These are the services that power client applications like a web app running inside of a web browser or a mobile app running on a mobile device. These client apps are simply what the user sees and interacts with. They're just the surface they need to talk to some services sitting on the server or in the cloud to store data, send emails or push notifications, etc. For the development of this system, we used the Node Package Manager from node.js. Node Package Manager (npm) is a package manager for the javascript programming language and is the default package manager for the JavaScript runtime environment Node.js. It consists of a command line client, also called npm, and an online database of public and paid-for private packages, called the npm registry. The registry is accessed via the client, and the available packages can be browsed and searched via the npm website. The package manager and the registry are managed by npm, Inc [15].
- *Truffle Framework* - A development environment, testing framework and asset pipeline for Ethereum. It is one of the most widely used IDEs among the Ethereum community. Developers can use it to build and deploy DApps for testing purposes with many features that make it more attractive to users with a Web 3.0 dev background. It

has built-in smart contract compilation, linking and deployment, so it takes care of managing the contract artefacts. Includes support for custom deployments, library linking and complex Ethereum applications. When used along with Ganache (see below), it helps to develop DApps quickly and get real code deployed, fast. Truffle has a console which allows access to all deployed contracts for a quick test of the system functioning. The point of using Truffle in this work is to help to organize the DApp development asset and not have to worry about manually setting up a test environment [16].

- *Ganache* - A personal blockchain for Ethereum development that can be used to deploy contracts, develop applications, and run tests. It is available as both a desktop application as well as a command-line tool (formerly known as the TestRPC). Ganache is available for Windows, Mac, and Linux. This tool was used as our blockchain [16].
- *MetaMask* - A browser plugin which allows users to make transactions to Ethereum or other networks through browsers, eliminating the need for dedicated user interfaces for Ethereum or other networks. Regular web browsers do not know how to connect to an Ethereum node and read and write to the blockchain, so it would be necessary a special browser like Mist. This is where MetaMask helps, it makes regular browsers being capable of writing such transactions into the blockchain, by injecting a JavaScript library called web3.js into the name space of each page the browser loads. Browsers are then capable with functions that can make requests write and reads to blockchain. It also allows users to specify to which Ethereum node these requests are sent to. In this system, MetaMask was used to facilitate the process of confirming and inserting transactions into the Ganache Ethereum [17].

4. Proposed fraud avoidance blockchain-based solution demonstration

While the fraud avoidance blockchain-based solution that we are proposing is only a prototype for now, it already showed us its applicability. In the present, it offers three main functionalities:

- *Creation and termination of insurance policies*

Once the goal of this solution is to support insurance companies in their activity, it is important to allow the creation and termination of insurance policies. The creation of insurance policies needs to go through a validation process in order to prevent any duplicate creation. The values inserted in the blockchain need only to be enough to identify a certain vehicle in the context of a certain insurance company. For this example, the data chosen for an insurance policy to be created are “platnumber”, “idcard”, “startdate” and “enddate”, but the insurance companies only insert information about “idcard” and “platnumber”, the other two data elements are filled by the system. These data identify a vehicle and a person, allowing us to know if an insurance policy is still active or not. In this system, to know if an insurance policy is still active, the “enddate” is used. Upon creating an insurance policy, this field will get the value 0 (zero), which means that the insurance policy is still active. If it gets a certain valid date, as seen in Figure 2, it means the insurance policy is no longer active.

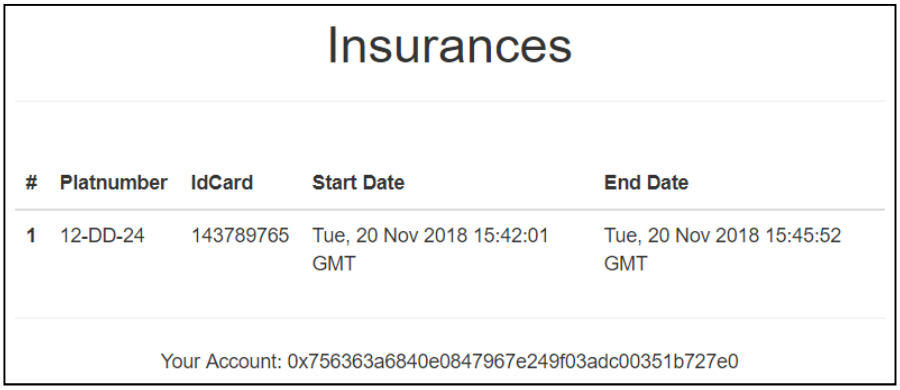

Figure 2. Data about an Insurance Policy

- *Creation of Claims*

Creation of claims is the third kind of events in an insurance company and like the other two (creation and termination of insurance policies) they have a major influence in the business. For the creation of claims, there is also a validation made by a smart contract. It is only possible to create claims if there is an insurance policy active. Otherwise, the process ends. This functionality is needed in order to save the claims history of every vehicle.

- *Record of the Life of a Vehicle*

Blockchain is notably known by its immutability regarding the data it stores, so it can also be viewed has a source of unchangeable records. As the insurance companies systematically insert in the blockchain data regarding every event a vehicle has been involved in, just by using a vehicle plate number it is possible to know how many insurance policies it had in the past or how many claims were filled (Figure 3). All this information is relevant to an insurance company upon creating a new insurance policy, as the price will be determined according to this.

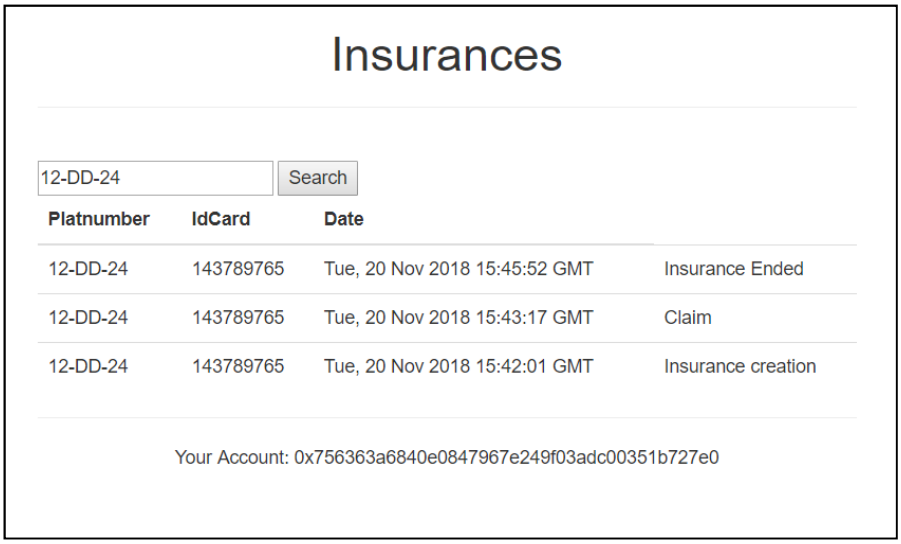

Figure 3. Insurance Events occurred with a Vehicle

Besides these functionalities, our solution may bring many other benefits that can be hard to obtain otherwise. It is a fact that a company never desires to share crucial business information with a competitor, as it may have consequences in terms of its market share. In the specific case of fraud prevention, while insurance companies might benefit from sharing some information elements about their clients, they hardly would do so. In the best case, they could accept an independent and trustworthy entity that would centralize relevant information about insurance policies giving access to data needed to prevent insurance frauds. A solution like the one we are proposing might eliminate the necessity for this central entity as the system itself stores relevant data that allows insurance companies to avoid a specific kind of frauds. The shared data stored in the blockchain has no competitive value for the insurance companies but may allow them to avoid some future headaches.

5. Conclusion

The goal of this article is to describe a blockchain-based solution that demonstrates the potential use of this emergent technology in the specific case of insurance fraud avoidance. A real problem which causes important business losses to insurance companies. The proposed solution intends to avoid one specific kind of fraud – double dipping –, which consists in making several insurance policies of the same vehicle in different companies with the

intention to later simulate a traffic accident and, thus, receive money from several insurance policies regarding the same event.

The proposed solution consists in the creation of a blockchain-based system, in which every insurance company would be a node of the network. To eliminate the risk of double dipping insurance frauds, before the creation of a new insurance policy companies access the blockchain to verify if the vehicle is currently involved in another insurance policy. Thus, avoiding the simultaneous existence of several insurance policies for the same vehicle.

In this solution, insurance companies maintain their confidential information about clients and insurance policies in their own systems. They only store in the blockchain information that can be shared with other insurance companies without incurring into competitive risks. Additionally to insurance fraud avoidance, the system allows insurance companies to easily access vehicles insurance history, without having to rely in other parties.

Currently, our proposed solution is in a prototypical stage. It has been tested with data from hypothetical insurance companies, clients and vehicles and has proved to work. In the future, we intend to add more functionalities to the solution and, maybe, to evolve to a final product.

Acknowledgements

This work has been supported by national funds through FCT – Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2019.

References

[1] McWaters, R. J. (2016) “A Blueprint for Digital Identity—The Role of Financial Institutions in Building Digital Identity,” *World Economic Forum*.

[2] Whitaker, J. E. (2018) “Insurance Fraud Handbook,” *Association of Certified Fraud Examiners*.

[3] Nolan, S. (2014) “Staged Collisions: Separating Accidents from Fraud,” *Insurance Institute of Ireland*.

[4] Johnston, B. (2008) “Identifying, Avoiding & Curing the Double Dip,” *TenPoint Insurance Solutions*.

[5] Nakamoto, S. (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System.”

[6] Pilkington, M. (2015) “Blockchain Technology: Principles and Applications”, in F. Xavier Olleros and Majlinda Zhegu (eds) *Research Handbook on Digital Transformations*, Edward Elgar..

[7] Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017) “Blockchain,” *Business & Information Systems Engineering* **59** (**3**): 183-187.

[8] Tapscott, D., and Tapscott, A. (2016) “Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World”, Penguin.

[9] Crosby, M., Nachiappan, P., Verma, S., and Kalyanaraman, V. (2015) “Blockchain Technology: Beyond Bitcoin,” *Sutardja Center for Entrepreneurship & Technology Technical Report*, UC Berkeley.

[10] Swan, M. (2015) “Blockchain: Blueprint for a new Economy”, O’Reilly Media, Inc.

[11] Szabo, N. (1997) “The Idea of Smart Contracts,” Nick Szabo’s Papers and Concise Tutorials, 6.

[12] Cant, B., Khadikar, A., Ruiter, A., Bronebak, J. B., Coumaros, J., Buvat, J., and Gupta, A. (2016) “Smart Contracts in Financial Services: Getting from Hype to Reality,” *Capgemini Consulting*.

[13] Brennan, C., and Lunn, W. (2016) “Blockchain: the trust disrupter,” *Credit Suisse Securities (Europe) Ltd.*: London, UK.

[14] Ethereum. (2018) “Solidity Documentation” Retrieved from https://media.readthedocs.org/pdf/solidity/develop/solidity.pdf.

[15] Node.js. (2016) “About Node.js.” Retrieved from https://nodejs.org/en/about/.

[16] Truffle. (2018) “Truffle Suite Documentation.” Retrieved from https://truffleframework.com/docs/truffle/overview.

[17] Kumavis, J. and Finlay, D. (2018) “MetaMask Browser Extension.” Retrieved from https://github.com/MetaMask/metamask-extension.