FIRST BLOCKCHAIN BETWEEN SWISS HEALTH INSURANCES

Joachim Kreutzberg, CSS Insurances, Switzerland, joachim@kreutzberg.com

Konrad Durrer, CSS Insurances, Switzerland, konrad.durrer@css.ch

Simon von Däniken, CSS Insurances, Switzerland, simon.vondaeniken@css.ch

Christian Scharr, CSS Insurances, Switzerland, christian.scharr@css.ch

Dominik Odermatt, CSS Insurances, Switzerland, dominik.odermatt@css.ch

Abstract

Blockchain is a very promising technology that solves problems involving different parties in a secure and trustless manner. CSS insurance, based in Switzerland, has implemented a productive instance together with other Swiss health insurance companies. In doing so, the construct of the smart contract is used. The core of the application solves the problem of seamless switching from one insurer to the next, avoiding unnecessary waiting time. In addition to the core, additional contracts are needed to help the administration operate. This paper shows the experiences by CSS and the problems solved on the way to a productive implementation.

Keywords: blockchain, health insurance, Ethereum, pre and post-insurance coverage

1 Introduction

Blockchain is a promising technology that can be used in a wide variety of industries including the healthcare industry. It has a great potential for many comprehensive uses with disparate actors. Zhao et al. (2016) delivers a good overview about the opportunities in the scientific and economic arena.

CSS is one of largest health insurance companies in Switzerland. First we were only conceptually engaged with blockchain technology e.g. UK Government Office for Science (2016), but after having gained a greater depth of understanding, a foundation has been laid for concrete implementations. Initially, we were focused on a few rather simple cases. However, after a closer inspection, it has been shown that the so-called smart contracts offer a wide variety of possibilities in the insurance industry.

Smart contracts can be viewed as a series of rules (conditions with the subsequent actions) triggered by transactions. Our implementation of the later introduced use case is completely based on the idea of smart contracts through which many technical questions have already been successfully solved.

2 Objectives, which can be achieved using blockchain technology

The blockchain technology guarantees the following characteristics of individual transactions:

- Transactions are handled correctly (according to predefined rules),
- transactions cannot be changed after completion and
- transactions are fully transparent to the involved parties.

Every state changing call to a smart contract is handled as a transaction. This mechanism creates the trust necessary between the individual members by broadcasting this transaction to the participating nodes in the respective Blockchain.

Correctness is established by a commonly agreed, immutable implementation of the technology (e.g. Ethereum, Wood (2018)). This approach enables contracts that are facilitated on the Blockchain to be even more reliable and robust than typical classical legal contracts. Whereas, various lawyers can interpret classical contracts differently, the commonly agreed algorithm interprets individual smart contracts identically. This attribute is referred to as “code is law” by Lessig (2001) or also as “law is code” by De Filipi and Hassan (2018). The responsibility to write the contract without any deviation from its intention is delegated to the developer.

The impossibility to revoke a transaction is common sense in the accounting business. This feature ensures, that you can immediately react to transactions. It opens a huge potential use for automating processes und speeding up depending actions.

The resulting transparency helps to give all the involved parties the possibility to verify the history of the transactions and the state of the contract at any place or time. This is further promoted by the decentralized approach of the blockchain technology which allows each participating entity to store its local copy of the ledger.

3 The first blockchain among Swiss health insurance companies

3.1 Implemented use case: Pre- and post-insurer

The first implementation of a blockchain solution involves three independent health insurance companies. The implemented use case solves the problem of managing the pre- and post-insurance coverage without any gap. Each Autumn in Switzerland, many customers hange their compulsory insurance

provider. The reasons for these changes are manifold, e.g. the cheaper price of the competitor or the dissatisfaction with the services of the current insurance[1].

For a valid change certain governmental requirements must apply (cf. CH-Admin (2018)). Since this is a compulsory health insurance the change is highly regulated. The process guarantees that every person is insured at all times. As with a step-by-step transaction, both sides have to take certain actions to process a valid change. This structure of the case motivated us to look for a blockchain-based solution.

3.2 The implemented solution: The contracts

The contracts implement the following functions:

A person wants to terminate his insurance coverage. However, this can only be achieved if the previous insurance company confirms that the specific preconditions have been met based on Swiss law.

1. In the case of a new termination request, the smart contract checks the status of the smart contracts of all other insurance companies to see whether the confirmation is already available.
2. If the confirmation has been received from another insurer's smart contract (status: cancellation pending), the termination can be carried out immediately (status: termination of insurance accepted).
3. If this confirmation is not available, an entry is made with a hash value that is generated from a predefined set of attributes, which refers to a customer. This hash value is described in chapter 4.4 of this paper. Additionally, the corresponding status (status: termination pending) is stored on the Blockchain.

Accordingly, a new insurance request is handled vice versa.

At each transition to accepted status, the corresponding action is triggered in the backend system of the insurer via a log event of the smart contract.

An API layer is provided to simplify communication with smart contracts.

[1] The population of Switzerland is approximately 8 million. Historically, 6-10% of clients change their insurance provider, resulting in a potential of nearly 500,000 annual changes.

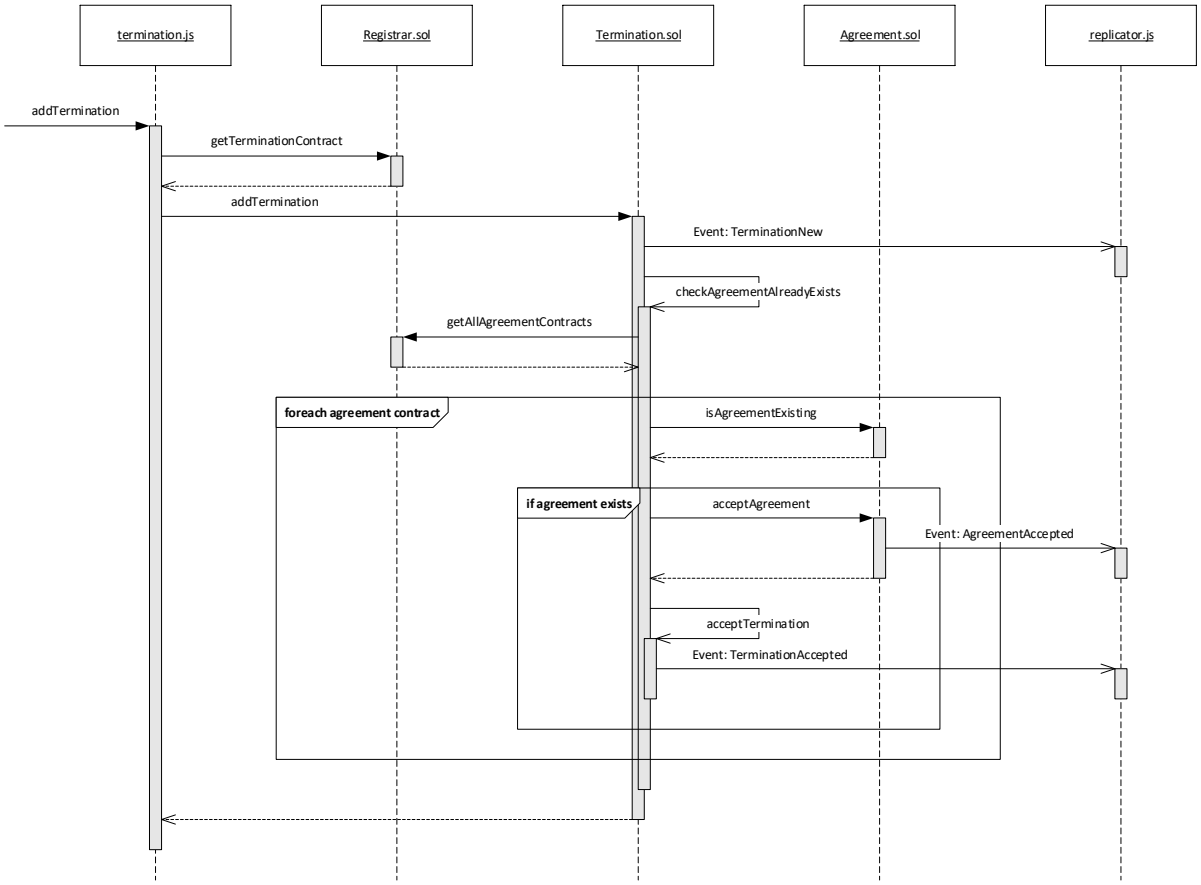

Figure 1 Interactions of contracts and events fired by adding a request for a new termination

3.3 The implemented solution: The chain

In order to select the appropriate blockchain, two essential questions had to be clarified:

1. First, which type of chain is suitable for this task? A chain can be open to everyone (public chain), open only to accepted members (federated or consortium chain) or fully private. Blockchainhub (2018) offers more details about the different types of blockchains.
2. Secondly, which concrete implementation meets our expectations?

The following criteria were used for selection:

- For environmental reasons, we want to use a proof of authority, not a proof of work algorithm.
- We are not willing to pay real crypto currencies for every transaction.
- We want to allow for (distributed) control over the participants.
- We want to profit from reusable know-how and to rely on the broadest possible community.

In our case, we decided to create a consortium chain[2]. We built this consortium chain, based on Parity implementation (Parity (2018)) of Ethereum and the Aura proof of authority mechanism. Atzei Net al. (2017) show the risks using this technology.

[2] There are specific implementations like R3, B3i, Hyperledger Fabric, Corda or variants of Ethereum.

CSS health insurance has made a technical implementation with two other Swiss health insurance companies. Overall, a six-node chain was built (cf. figure 1). In addition to these three main participating companies, each insurer also has his subsidiary involved.

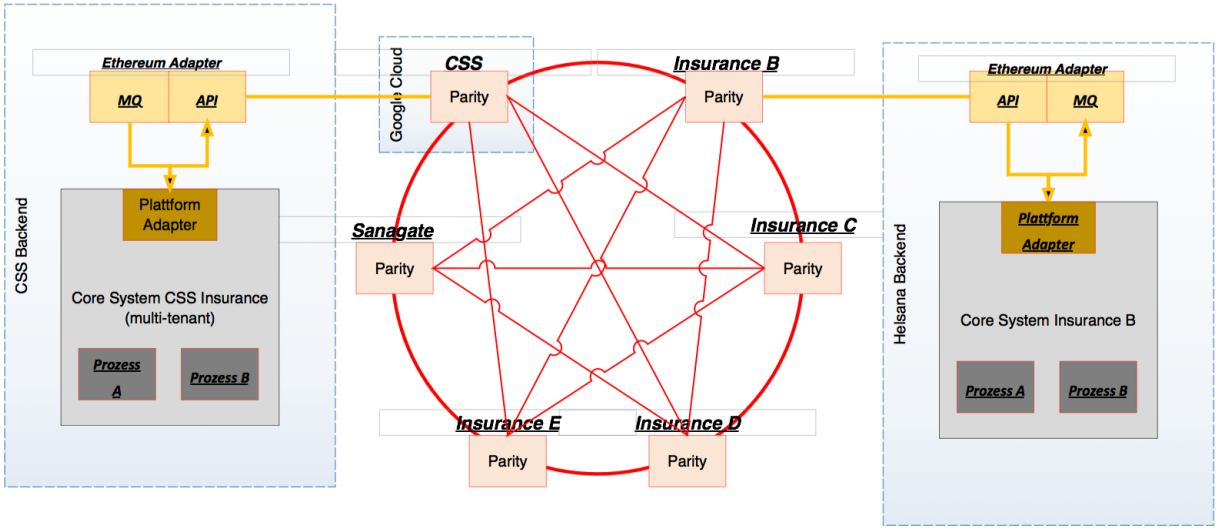

Figure 22 Implemented blockchain in Swiss health industry

4 Results of PoC

4.1 Need for a common body: The tasks of the consortium

The need for a consortium emerged quickly with the implementation. There are already many of these consortiums in existence (e.g. b3i (2018), r3 (2018)), however they are not in alignment with the objectives of the participating parties.

4.1.1 Regulation

As far as content is concerned, the smart contracts must be worked out as they are in the ordinary contracts. It must also be regulated and agreed upon if and when new smart contracts are deployed. If there is a need for corrections (e.g. a new contract has to be deployed), the procedure must be determined off-chain.

In our case, it must be regulated from the time the participants are allowed to submit notices of termination for the following year (see versioning) and vice versa when they no longer have to be accepted for the previous year.

4.1.2 On-/Offboarding

One of the procedural tasks is to onboard new members to the blockchain. In addition to the admission, the ordinary resignation of a consortium member must also be regulated. This can be voluntary or after breach of certain obligations.

The so-called technical committee is responsible for the documentation of this process. The decentralized approach of blockchain technology fully emerges with introducing a new authorization-node. The mechanism of this node is explained in detail in Authority (2018). The implemented node is asking for acceptance and one after the other existing nodes sends his approbation till the new node reaches its quorum. In the case of a resignation of an existing member the remaining members will remove the departing member from their list of trusted authorities.

4.1.3 Deployment

Coordinated deployment of new smart contracts is an essential task of the consortium. The timespan between the implementation of new functionality and the decommissioning of old functionality must be understood by all participants both on a technical and content-wise level.

In our case, for example, we plan to deploy a new contract per year (see versioning).

However, each participant must therefore know whether he or she can still count on a reliable answer from the other parties of the previous smart contract. Furthermore, every participant has to be willing to implement the enhancements that are made on the shared smart contract layer into his back-end systems.

4.2 Monitoring

There is no need for an additional task in monitoring. Monitoring of the nodes and the chain can be established, decentralized and individually by every participant. The API of the Parity implementation is fully sufficient to be integrated in the overall monitoring systems. Parity (2018) shows how to use the implementation.

4.3 Versioning

As mentioned above, our use case and selected design of technology allows us to deploy a new contract every year. This offers the possibility of introducing changes and fixing bugs once a year.

4.4 Security

Everyone can read each item on the chain. This is a basic principle of the Blockchain technology. We deliberately decided not to rely on implementations that suppress this aspect in a proprietary way. As a result, the requirements for the implementation of a Smart Contract in our chain are similar to those in a public chain.

We derive a hash value from the customer's social security number, the current year and a confidential value (actual contract number) known only by the two parties involved. Along with the state, only the hash value is stored on the chain.

On the one hand, it is possible to match the hash-keys using a smart contract, but on the other hand, only the companies involved can draw conclusions about the individual persons. A record matching to the plain text must therefore be stored in the back-end systems of the insurances involved.

5 Outlook for further use cases

In addition to the mentioned and implemented case of pre- and post-insurer, we are looking for more use cases.

We see great potential in the case of demarcation between cases labeled as accident or sickness/disease. While in case of illness the health insurance covers the costs, in cases of accident the accident insurance (as a rule SUVA) is obligated to cover the costs. It frequently occurs that cases are reported to the health insurer first, under the assumption of a medical condition, but then must be regrouped and treated as an accident. The transfer of the case could be realized on a blockchain.

Other potential use cases concern fraud management, be it by the service provider or the insured. In addition to fraud management, the overlapping claims (of two different insurers) from compulsory and voluntary insurance presents another problem, which could potentially be solved with a blockchain.

From a research perspective we are following the discussion around upgradable smart contracts closely. We are aware that the upgrade of the code only once a year might not be sufficient. Therefore, we

are investigating procedures to ensure a smoother and less bureaucratic way to enhance smart contract functionality or fix existing bugs. One way of fulfilling these requirements could be by implementing upgradable smart contracts. There is currently no corresponding standard in place but there are various initiatives underway which attempt to solve this problem as Tanner (2018) mentions.

References

Atzei N., Bartoletti M., Cimoli T. (2017) A Survey of Attacks on Ethereum Smart Contracts (SoK). In: Maffei M., Ryan M. (eds) Principles of Security and Trust. POST 2017. Lecture Notes in Computer Science, vol 10204. Springer, Berlin, Heidelberg

Authority. (2018). Retrieved August 2018 from https://wiki.parity.io/Proof-of-Authority-Chains

Blockchainhub. (2018). Retrieved August 2018 from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

b3i . (2018). Retrieved August 2018 from https://b3i.tech/home.html

CH-Admin. (2018). Retrieved August 2018 from https://www.admin.ch/opc/de/classified-compilation/19940073/index.html

De Filipi P. & Hassan S., (2018), Blockchain Technology as a Regulatory Technology. From Code is Law to Law is Code. Harvard University. Retrieved August 2018 from https://arxiv.org/ftp/arxiv/papers/1801/1801.02507.pdf

Ethereum (2018), Retrieved August 2018, from https://www.ethereum.org/

Lessig L., (2001), Code is Law. On Liberty in Cyberspace. Harvard Magazine. Retrieved August 2018 from https://www.harvardmagazine.com/2000/01/code-is-law-html

Parity. (2018). Retrieved August 2018 from https://www.parity.io/

r3. (2018). Retrieved August 2018 from https://www.r3.com/

Tanner J., (2018), Summary of Ethereum Upgradeable Smart Contract R&D. Retrieved August 2018 from https://blog.indorse.io/ethereum-upgradeable-smart-contract-strategies-456350d0557c

UK Government Office for Science. (2016). Distributed Ledger Technology: beyond block chain. Retrieved June 27, 2017 from https://www.gov.uk/government/uploads/system/ uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Wood G. (201?). Ethereum: A secure decentralised generalised transaction ledger. Retrieved August 2018 from http://gavwood.com/paper.pdf

Zhao, J.L., Fan, S. & Yan, J. Financ Innov (2016) 2: 28. https://doi.org/10.1186/s40854-016-0049-2