17.07.2017 – Author: Jonathan Staude

Democratic CELLPHONE Protection

# EXECUTIVE SUMMARY

This document describes how to realize a fully digitalized insurer based on smart contracts on the Ethereum blockchain. Since Insurance is a highly digital product it is possible to digitize nearly all process steps in the product lifecycle. However the touchpoints with the customer for a) risk assessment at point of sale and b) Claims assessment and payment are hard to automate. At each point experts are needed to evaluate the respective amount to pay by the customer or by the insurer.

The idea is, to use swarm intelligence to automate even these steps. Participants in the insurance ecosystems may estimate the appropriate premium to be paid for this coverage and object. Furthermore in case of a claim, the swarm may also evaluate if a claim is acknowledged and estimate the amount to be paid out by the contract.

All of these automatic processes can be performed by the blockchain for maximum automation, fairness and transparency to the customer. The platform itself –as an equivalent to the insurance company- has no leverage to control premium/claims payments. Thus the participants, which also own the collective have the complete power over claims. Since all participants are insured by the collective, there is a high incentive to create fair claims/premiums.

# PRINCIPLES

Want to insert a picture from your files or add a shape or text box? No problem! In the Insert tab of the ribbon, simply tap the option you need.

Find even more easy-to-use tools in the Insert tab, such as tools to add a hyperlink or insert a comment.

Contract

A contract is defined by

1. A coverage period

This is the period, for which the contract is valid. Any claims need to be proven to take place during this coverage period.

For the MVP, we can only use 1-year contracts.

1. A coverage

This is the risk covered by the contract for example theft, accident or fire. Claims payments can only be expected for claims that were caused by the events defined in the coverage.

For the MVP, we can only use accident and theft.

1. An insured object

This is the object, that is insured against a risk described in the coverage. An object can only be insured once and it must be insured by the owner of the object.

For the MVP, we can use Cellphones.

1. A sum insured

This is the sum up to which payments can be made based on the insurance contract. This sum cannot be higher than the total time value of the object.

1. A premium

This is the premium paid for a contract. The premium amount is based on the time value of the object and the coverage. Since premiums are calculated on the equivalence principle Premium=Expected Cost+Expected claims, we assume the premiums for this digital insurance model to be lower due to much lower costs.

For the MVP, we can use Market price –x%

# THe Insurance Mechanics

Generally, insurance as a mathematical product is easy to automate. The very nature of the product is distributed, so it’s an obvious application for blockchain. Anyhow, there are two processes in the product lifecycle of a (P&C) insurance contract that require decisions that are not easy to automate. At first, the assessment of risk –the pricing actuary’s job – depends on criteria that are hard to generalize. A price depends on information about the insured object, the insured person and after all also on the competition.

The second process in the product lifecycle that is hard to automate are claims payments. The rightfulness of a claim and the size of the claim depend on a set of structured and unstructured information about the claim and the insured person.

In the blockchain environment, those two processes –for now- can’t be fully displayed in a smart contract. Anyhow it is possible to feed the smart contract with all the information needed to continue the pricing or claims process. This concept chooses a democratic approach for each of those manual steps.

## Underwriting/Risk assessment

Once a participant want to transfer risk to the pool, participants of the pool – “judges” - decide on the price and whether the object and the person are insurable. For this, we suggest five random people to vote on the price and on the insurability of the contract. The proof of insurability lies with the possible customer. Once enough participants agree on price and insurability, the smart contract executes automatically. The product is expected to give guiding information for the judges based on past experience with the insured object and person.

## Claims payments

The claims payment is addressed in a democratic way. The pool decides whether to pay out a claim to a participants. This can be achieved by randomly selecting “judges” that vote on size and rightfulness of a claim. Since all of the “judges” are insured in the network themselves they are incentivized to judge claims in a fair way. The product is expected to give guiding information for the judges based on past experience with the insured object and person.

### Acknowledgement of a claim

## Similar to insurance companies, we expect the policyholder to proof that a claim is valid. The collective will then decide whether this proof was sufficient for a payment or even whether a fraud is suspected.

## A simple approach for this process would be via voting. Ten randomly selected participants of the insurance system can vote whether the claim is justified. If a claim is voted as justified for example nine times, the claim is automatically paid.

## In this process there are several variants thinkable, the options voters have can vary from yes/no to yes/no/proof again or to a scale of trustworthiness. Furthermore it is thinkable to let the participants vote on the actual percentage of payment.

## In this theoretical state it is not advised to fix the process, but to test several systems against each other to assess which voting system is the most effective.

### Estimation of a claim

### Similar to i) there are several ways of estimating the claims value possible. For a simple prototype we may only choose to have full payments or no payments. For part-payments an estimation model may be developed.

### It is planned to support the decision making process with competitor’s data.

### Fraud assessment

### There are several fraud scenarios thinkable like multiple claim for one event, false information provided or teams of fraudsters that manipulate the voting process. Anyhow, the state-of-the-art machine learning techniques are well-suited to detect fraudsters and warn participants in the voting process.

### Payment

### Once determined, payments are processed automatically via the ethereum blockchain.

## Investments

## There is no plan to invest funds in anything else than Ethereum yet. The funds will be collected and paid out. The growth of the cryptocurrency market will provide revenues for the start. Mid-term, classical investment strategies can be implemented.

# Technology

# All contracts are realized as smart contracts on the Ethereum blockchain. Thus, there is maximum information symmetry between all contract holders, the platform itself and possible investors/reinsurers. There is no way to withhold or reduce claims by any central authority or to overprice since this central authority does not exist. Furthermore, instead of having employees working on claims regulation and pricing, the collective is taking this task over. This reduces the overhead costs of the insurance mechanism to a minimum.

# Risks

## Currency volatility

## The price of ethereum is still quite volatile. To address this issue, payments can be transferred to fiat currency via a platform directly.

## Fraud

## Fraud is always existent in insurance and for this product it will be no different. Anyhow, the business model incentivates participants to play fair and punishes participants that do not play by the rules.

## Scalability

## The whole world can take part in this pooling of risks at once. Thus it is important to address technical scalability of the DAPPS in an early process of the implementation. The product counts on the scalability solutions for Ethereum in general.

## IT security, Hacking attacks

## The implementation needs to strictly consider IT security in every step of the process. Security leaks can easily lead to high losses and the insurance pool is an attractive target for hackers. Thus a funds distribution concept for the mitigation of IT risks is necessary.