Token Mechanics for a Decentralized Insurance Platform

v.1.0 (Published Review Version) 19.06.2017

Christoph Mussenbrock

Table of Contents

1 Summary **4**

2 Acknowledgements **5**

3 Analysis **5**

3.1 Principles of insurance 5

3.2 Problems with traditional insurance 8

3.3 Requirements and consequences of a decentralized implementation 9

4 Proposal for a platform token **10**

4.1 Protocol 10

4.2 Platform 11

4.3 Role of the platform token 11

4.4 Use of the protocol outside the platform 12

4.5 Many platforms? 12

4.6 Platform without token? 12

Version Control

Version	Date	Author	Remarks
0.1	06.05.2017	Christoph Mussenbrock	Initial
0.2	11.05.2017	Christoph Mussenbrock	Results of Neuchatel workshop
0.3	14.05.2017	Christoph Mussenbrock	Elaborate token model for Transaction costs
0.4	18.05.2017	Christoph Mussenbrock	Continued work on Tx Cost Model
0.5	27.05.2017	Christoph Mussenbrock	Merging Stephans Comments
0.6	08.06.2017	Christoph Mussenbrock	Internal Review Version
0.7	16.06.2017	Christoph Mussenbrock	Proposals for resolving comments
1.0	19.06.2017	Christoph Mussenbrock	Resolving internal review

1 Summary

The purpose of this document, which will be part of the Etherisc White paper soon, is to give an analysis of basic principles of insurance and a deduction on how we can build a token system on top of these principles, which is sustainable and sound (later in this paper we will describe which kind of tokens we consider to be "sustainable" and "sound").

In Chapter 3, we analyze insurance and and break costs and capital flows down into three elements:

1. Expected value of risk
2. Capital costs for long tail risks
3. Transaction costs

We show that the first isn't a source of profit, because it is only a redistribution of capital corresponding to sharing risks among the participants.

The second are a source of fixed income, at a certain risk. Capital has to be locked for a certain period in time, and there is a potential risk of losing the capital provided, e.g. in the case of a rare but catastrophic event, also known as "black swan event". Capital providers are compensated for this risk. This compensation is calculated based on the lock-up time and on the risk of what is being insured.

The third are a source of entrepreneurial revenue and increase with higher efficiency of the business processes.

We argue that today insurance companies are the predominant way to organize these elements and that blockchain technology provides an opportunity to replace insurance firms by decentralized structures using a standardized protocol. Capital and revenue streams can then be represented by tokens.

Our conclusion from this analysis is that we need two types of tokens, one for representing risks - this type will come as a collection of similar tokens, one for each risk pool, we call those "risk pool tokens". These "risk pool tokens" will be discussed in a separate document, as they underlie a different economic dynamic.[1] The second type of token supports the coordination and economical incentivization of actors in a decentralized insurance system. This is the token to be discussed for a token sale to fund the development of a protocol and platform for decentralized insurance. We call these "platform tokens".

In a distributed environment with many participants, building products as a collaborative effort, the platform token serves as glue, as collateral, and as representation of the material and

[1] In https://www.etherisc.com/whitepaper, we already described a possible implementation of a "risk pool token", which aggregate similar risks and which can be sold and traded to provide the necessary funds to cover "long-tail-risks".

immaterial value of the network, much as Ether serves as a means to secure the stability of the Ethereum Blockchain.

In Chapter 4, we detail our proposal for a platform token. Chapter 5 lists some requirements for the sale process of the platform token, and Chapter 6 contains the objectives we try to fulfill with our design.

2 Acknowledgements

The ideas in this paper are a collaborative result of many talks and discussions, online and in person, with some brilliant minds of the crypto-economic space. I would like to say “thank you” especially to the following people, who added considerable value to the draft:
Ron Bernstein, Jake Brukhman, Alexander Bulkin, Alex Felix, Stephan Karpischek, Renat Khasanshyn, Micah Zoltu and last but not least all those members of our gitter channel, who gave valuable feedback and criticism and encouraged us to follow our path.

3 Analysis

3.1 Principles of insurance

Lots of literature has been written on the theory of insurance, but the basic principles are simple.

Let's start with an example (I took this from the German wikipedia[2]). The example is not meant to be “realistic” but serves the sole purpose to explain the principle; neither the mentioned time spans nor the used interest rates will be found in actual markets; and of course, most houses are not fully paid as Alice’s house in the following example.

Alice has a house. The house is worth $100K. The probability of a complete disaster by fire is 0,1% per year (that is one devastating fire in 1,000 years). Alice wants to ensure that she has access to enough funds to get a new house in the case of a fire. So she decides to get a loan of $100K and has to pay redemption (also called principal) and interest rate. Statistically, she will need one such loan every 1.000 years in the average, so so she will pay $100 redemption each year (this will sum up to $100K in 1,000 years). The mathematical term for this amount is “expected value” of the random variable representing the risk.
Additionally, she pays an interest rate of maybe 1%, so she has yearly costs of $1,100 ($100,000 loan * 1% interest rate plus $100 annual redemption = $1100.00).

Now we show how pooling risks in an insurance scheme reduces these costs drastically.

Assume 100,000 house owners are coming together in a pool. Again, everybody pays a $100 share; this amount is now called the “premium”. They collect a total of $10,000,000 in premiums. But now there is a difference to Alice, who takes care only for herself: because of

[2] https://de.wikipedia.org/wiki/Versicherung_(Kollektiv)#Beispiel

the law of large numbers[3], with a very high probability there will only be about 100 fires, causing a damage of about $10,000,000! And because the sum of all premiums is also $10,000,000, the whole damage can be paid out of the collected premiums, there is no need for every house owner to take on a loan. (Because premiums are collected at the beginning of the year, and all the houses "expected" to burn don't all burn at the beginning of the year, but more or less are equally distributed over the year(s), there is a so called "float"[4] of liquidity which can also generate a significant revenue. For simplicity, we won't focus on this effect in this paper.

So the costs for each single house owner are now reduced from $1,100 to $100!

Such a pool may be designed solely to benefit its' participants, and to not make any "profit". If the pool did generate profits, these profits could be distributed back to the participants, effectively reducing the premiums again to a level where no profits are generated.

This is the very basic effect of risk transfer in insurance. Please note that the effect increases with the pool size.

But still, this is not the whole story.

In some years, there are more fires, in other years, less. To account for these variations in damages, the whole pool has again to raise some money, e.g. $10M, to cover the unlikely event of a burst of many fires in one particular year. And let's suppose that the interest rate for this capital is even particularly high, e.g 20%. We will have total costs for this capital of $2M. The interest rate for the capital is a function of the risk and the riskless interest rate on the capital market; in an efficient market, the interest rate will compensate for the higher risk in comparison with a risk-free investment and will also contain a fair profit. So basically, this is where profits are generated for providing capital in an insurance structure.

The overall costs of $2M are distributed among all house owners, yielding an additional cost of $20 per house owner per year, which is added to the premium.

So after this, there is also a protection against "long tail risks" or "black swan events", at a cost of $20 per house owner. Again, the risk diversification effect increases with the pool size.

Overall, participants now pay $120 per year for their house insurance.

To organize 100,000 people in a pool, a professional structure is needed, otherwise, every single participant would have to talk to every other, which would simply be impossible. The operation of this professional structure adds transaction costs to the premium. This is the reason why insurance companies have come into existence: They provide a way to decrease

[3] https://en.wikipedia.org/wiki/Law_of_large_numbers
[4] http://www.npr.org/sections/money/2010/03/warren_buffett_explains_the_ge.html

transaction costs for the participants of the pool, creating an economy of scale and coordinating a huge number of participants and employees[5].
The three elements described above; pooling or risk, risk transference, and efficient administration are necessary. You can't have insurance without each of them.
For the purposes of this paper, I will call them:

1. expected value of the risk
2. capital costs for long tail risks
3. transaction costs

As we have seen, a community may not wish to generate profit from the first element. The second element yields a risk fee for binding capital which depends on the structure of the particular risk: It is typically lower if the risks are granular and uncorrelated; it is typically higher if the risks are clustered or correlated. The third one depends on the complexity of the process. A simple and highly standardized insurance "product" has a smaller transaction complexity than a more complicated, non-standardized product. This will reflect in lower transaction costs.

The three elements are completely independent of the underlying technology, economic environment or currencies. They are the atomic building blocks of every risk-sharing system[6].

What conclusions can we draw from analyzing these elements for designing a blockchain-based, decentralized insurance system?

The distribution of expected value (element 1) and capital costs for long-tail-risks among participants (element 2) is inevitable and not specific for a blockchain solution. Therefore, let's focus on the third element.

Blockchain is essentially - among other aspects - a way to solve the transaction cost problem without firms. Without the "design pattern"[7] of firms, transaction costs are subject to combinatorial explosion. The coordination costs for n participants are roughly of Order $O(n^2)$ and firms reduce this to $O(n)$. Because of this huge gain in efficiency firms have many ways to hide profits in the transaction costs, and on the other side internal inefficiencies don't show up fast.

---

[5] The downside of this is the fact that inefficiencies tend to hide in the organization. The bigger the organization, the lesser people are doing the real work (people at the "rim" of the organization) and the more people are needed in the center to organize the people at the rim (the "management"). Furthermore, to limit internal inefficiencies, companies need a plethora of control mechanisms (that's the old style) or complicated incentive systems (that's the more modern way).

[6] There is a fourth element - reinsurance. The purpose of reinsurance is to reduce the cost of risk diversification by categorizing and securitizing different risks. Reinsurance and "wholesale" risk transference enabled by reinsurance adds another layer of complexity, and therefore we won't discuss reinsurance in this paper.
[7] On the importance of design patterns, see also: Design Patterns, by the "Gang of Four" https://www.amazon.com/s?search-alias=stripbooks&field-isbn=0201633612

Transaction costs also appear in another context: regulations, which are deemed necessary to protect customers in a context with built in conflicts of interest. Regulations form a very effective "competitor" barrier to entry. While insurance companies often complain about the burdens of regulations, they actually don't have much interest in reducing these burdens, as they discourage new competitors from entering the market.

3.2 Problems with traditional insurance

Transaction costs cannot be eliminated completely. But blockchain can help to solve three main problems which pile up costs in traditional insurance companies:

1. Coordination ("managerial") costs.
2. Conflict of interest between customers and company.
3. Information asymmetry between customers and company.

Advantage 1. In traditional firms, you have two types of employees: the first group is doing the actual work, the second group is coordinating the whole system. The larger a company grows, the more energy flows in the second group (like a circle, the first group forms the rim of the circle, the second the area; the larger the circle, the less efficient are the processes, and the more energy flows into the coordination of the coordinators). Blockchain can help reduce these coordination costs. Instead of a posse of managers, "smart contracts"[8] can act as trustless hubs between the agents at the rim of the system, and thus eliminating most of the costs and the inefficiency of the management.

Advantage 2. In a traditional insurance company, the company "owns" the whole process, including the tasks which tend to raise conflicts of interest between customer and company. An obvious example is claims management: The claims manager has the explicit goal of minimizing payouts for damages, because he is employee of the insurance provider! Of course there is a guild of "independent" appraisers and experts, but who pays their bills?

Blockchain can solve this conflict of interest, by enabling truly independent experts (who for example may be publicly ranked by their reputation for efficiency or fairness), and whose work is independent of the insurance provider, as well as being transparent and auditable by the whole community.

The same is valid for another area, where the conflict of interest is (intentionally) not obvious; consider Product Design. An insurance company has a big advantage over customers, because they can design products in a way which perhaps unfairly maximizes revenues (sales) and minimizes payouts (expenses).

[8] On some blockchains like Ethereum (which we use) you can write programs (called "smart contracts") that are un-censorable, immutable, and permanent. These smart contracts can interact with each other to perform a wide variety of actions, including financial and escrow transactions. This makes possible direct and transparent interactions between two parties who may be and may remain anonymous, that previously required a third-party intermediary to be effective. The term was originally coined by Nick Szabo, but in a slightly different meaning. Note: The above definition was thankfully supplied by Ron Bernstein, who was not successful in finding the original author - please contact us if you are the author.

For example if a customer expects a payout from an insurance policy they bought for a particular “event” but the insurance company does not provide the payout because the company maintains that the policy bought doesn't actually cover that “event”, the customer experience is severely degraded and trust is eroded between consumers and insurance providers.

Advantage 3. Information asymmetry is in itself a source of inefficiency and high transaction costs. Insurance companies gather data and information in huge private silos by proprietary means and the data is often not shared., This data and the companies’s experience in analyzing the data is considered one of the main differentiators in the market. The reasoning behind decisions made based on this data is opaque and difficult to challenge. In a blockchain environment, all fundamental data and the decisions based on the data can be transparent and objectively validated.

3.3 Requirements and consequences of a decentralized implementation

Requirements and consequences for implementing a decentralized insurance protocol on a blockchain:

1. A protocol needs some means to incentivize participants to use it. Fostering “Network Effects”[9] is one such mean and can lead to a sustainable and growing user base.

   Why do we need a protocol and not only a single smart contract? While a single contract can handle a single product, this singularity will not generate the network effects which are desirable to form multiple large pools of similar risks needed to get the benefits of the “law of large numbers” working.

2. A decentralized insurance protocol and platform can replace “the firm”, by implementing a standardized set of rules for how stakeholders in the system interact with smart contracts and with each other using the protocol. By this, most of the coordination costs are replaced by autonomous and automated contracts and procedures and enforce efficiency by open market mechanisms.

3. The development and operation of a protocol needs funding. Even if we can drastically reduce the coordination costs, there are still the costs for the initiation of the system – e.g. acquisition of licenses, development of smart contracts, audits, as well as costs for agents at the “rim” of the system which we cannot eliminate completely. Therefore we need a way to collect these costs from the ultimate customers and distribute them amongst these agents.

[9] Network effect is described as the effect that one user of a good or service has on the value of that product to other people. The classical example is telephone: the more people use it, the more valuable the telephone is for all.

4. We also need a way to calculate and distribute the expected value of the risk and the capital costs for covering long tail risks amongst the customers.

5. Tokenization may be the solution for these requirements - but only if the token is intrinsically required for the protocol to operate efficiently; i.e. "baked into" the protocol itself ***and*** usage of the protocol is only possible via tokens.

   If the token were not intrinsic to the use of the platform, then some new actor could replicate the protocol except without the token, and migrate users to the new protocol without the friction of a purely "rent seeking" token.

   The initial distribution of tokens in a "token generating event" has two primary functions; the funding for protocol development is collected and a first user base for the protocol develops.

6. Which tokens do we need and with which properties?
   a. For the distribution of the *expected value*, and for the *distribution of the capital costs for covering long-tail-risks*, we need a type of token which generates a foreseeable profit. The profit solely depends on the underlying risk structure, the number of risks, their correlation, and so on. The value therefore depends only on the knowledge of the risk parameters (which can be incomplete) and mathematics.
   These tokens will e.g. yield a fixed revenue or generate an equivalent rise in price for their owners (which is equivalent).

   b. For the *distribution of the transaction costs* we need a different type of token. This token has to be designed in a way that incentivizes the use and the efficiency of the protocol: the revenue associated with this token or its price should increase with the efficiency and use of the underlying processes.
   In the next chapter, we describe a proposal for a token with these properties.

4 Proposal for a platform token

The proposed platform token is an integral part of a system consisting of a protocol and a platform.

4.1 Protocol

The Protocol is a collection of Smart Contract Templates, Rulebooks, Standards, Best Practices which are developed and maintained by the community. There are many possible governance schemes for such a protocol; we intentionally don't make a prejudice on which model should be chosen, this will be part of the protocol development. The governance should fit to the participants using it. Of course, meanwhile blockchain offers some interesting tools to formalize governance, but that should be left to developers and users.

4.2 Platform

The platform is the (sub) community of all entities which make use of the protocol, and which are connected by a common economic interest.
Providing insurance is a complex process, involving possibly many participants, as we have seen above.

- Customers of an insurance need to rely on the smooth operation of these participants.
- Fees have to be distributed along the value chain, but only if all parts of a process have been appropriately fulfilled
- Participants supplying critical parts (e.g. a risk model) have to assume liability for their work.
- Some services are needed by many participants, so it makes sense to offer them as shared services.

The platform will serve as marketplace for insurance-related services, which are offered according to the open protocol standard and which are therefore always interoperable.

4.3 Role of the platform token

To make long story short, we need some strong economic principles to ensure the proper working of all participants and their cooperative, mutually supportive behaviour. Therefore, we have designed the platform tokens to bind participants to the platform and to assure the quality of the provided services. We are effectively implementing what is known as "Proof of Stake", - a method of achieving consensus between multiple actors, - focusing on the specifics of the risk transfer.
We would like to decompose the value chain as far as possible and to engage market mechanisms to select those participants which offer a service at the best value.
This is quite similar to the operating mode of a blockchain: Miners have an economic incentive for cooperative behaviour.
Some aspects of “good-behavior” comprise stability properties like:

- Promise to offer a certain service over a certain time (service stability)
- Promise to offer a certain service in a certain quality / with a certain SLA (quality stability)
- Promise to offer a certain service at a certain price (price stability)
- Promise to take a certain liability for a service (guarantees)

We propose to secure the platform and the products built on that platform via the platform token. Participants (not customers) will need a certain amount of tokens to enter the platform “ecosystem”. These tokens are locked as collateral. Depending on the service offered, a different number of token will be required to avail of the platform or provide services on the platform.. Simple services require a small number of tokens, complex or critical services will require a higher number of tokens. The amount of tokens which have to be provided as collateral will correlate to the potential damage from participant misbehavior or from the violation of the platform terms. These parameters may be subject to a platform governance model (in the future) where participants have voting power based upon tokens owned. Or, governance may be conducted automatically by the use of smart contracts.

The proceeds from token sale(s) are used to nurture the development of the platform and to establish or provide central services as long as there is no independent participant providing them.
The exact definition of “Proof of Stake” in this context is subject to ongoing research and discussion.

A certain insurance product needs a collection of services chained together to some business process. Participants offering these services can organize to offer such a product (maybe there is a market for such services and a “product management service” doing the coordination work). It is even possible that the fees for some of the services offered by participants in the ecosystem may be negotiated on an open-market platform. The protocol will offer ways to distribute the premium to the various risk pools and to the participants who provide product “processing”.

4.4 Use of the protocol outside the platform

The protocol can - of course - be used outside the platform. However, every single use of protocol standards outside of the platform will always lack the following:

- the support of the platform
- economies of scale and cost benefits proved by the platform
- access to the platform’s “commons” - i.e. services offered by the community of all participants for the benefit of all.
- the securing and integrity mechanisms
- the stability assertions (service, quality, price, liability)

4.5 Many platforms?

It can be argued that in principle several platforms could exist in parallel. That’s true - nothing prohibits to launch a second, identical platform. This is analog to the existence of altcoins. However, an altcoin can be launched at substantially lower costs than an insurance platform, making the existence of parallel platforms quite improbable.

4.6 Platform without token?

Can the platform exist, and maybe even be better, without a token? We argue that it cannot as the core function of the token is to serve as the collateral to enforce the proper behaviour of all participants of the platform. A platform without a (similar) token will simply not have the trustworthiness needed for insurance applications, because the participants would not have incentives to behave as they should.