NEXUS MUTUAL

A peer-to-peer discretionary mutual entity on the Ethereum blockchain.

HUGH KARP

ABSTRACT

The insurance industry has developed over time from a community based model to an adversarial one where large institutions dominate. It is also inefficient in many areas leading to large frictional costs being borne by customers. Blockchain technology allows individuals to efficiently transact directly with each other and therefore enables the core insurance entity to be replaced. Nexus Mutual uses blockchain technology to bring the mutual ethos back to insurance by creating aligned incentives through smart contract code on the Ethereum blockchain.

BACKGROUND

Before insurance companies existed, communities would group together themselves. They would pool resources to protect individual members from risks they all faced.[1] If an unfortunate event occurred the senior members of the community would decide whether to provide assistance or not. All funds raised were used to benefit the members of the community.

In developed nations we have largely moved away from this community approach primarily due to the underlying economics of insurance. Insurance economics is driven by diversification. The more individual risks that are pooled together the less capital is required to be confident all claims can be met.[2] Scale benefits are significant and community models don't have the means to access them easily.

Moving away from the community model brought other challenges, in particular the issue of "agency". An insurer is looking after customers money and then promising it will pay when a claim arises. As a result, the insurer is becoming an agent of the customer and history has proven this model doesn't work without heavy oversight from government institutions and complex legal frameworks. These frameworks are necessary primarily due to the lack of trust between customers and the institution and boil down to two main points:[3]

1. AGENCY - Insurers decide on how customers money is handled. Including how it is invested, which insurance risks it will back and when it gets paid out to shareholders. They also have an implied option where there is potentially unlimited upside but if the insurance company goes bust it is customers that suffer. Interests are not directly aligned.
2. TRANSPARENCY - A customer finds it extremely difficult to assess how safe a particular insurer is. There is a clear information asymmetry issue.

In developed nations both of these issues are dealt with primarily via law and prudential regulation. A complex combination of standards defining minimum capital levels, governance processes, reviews and regular financial reporting. Regulation in this way is

[1] https://en.wikipedia.org/wiki/Mutual_insurance

[2] https://en.wikipedia.org/wiki/Law_of_large_numbers

[3] http://fsi.gov.au/publications/

largely effective, barring a handful of high profile exceptions[4], but brings additional costs and reduced flexibility.

Even with this burden the institutional model has provided significant benefits to customers via reduced premiums and deeper pockets. The underlying diversification benefits have more than outweighed the regulatory burden. But there is still substantial unnecessary cost in the system. Estimates are that roughly 35%[5] of insurance premiums are lost due to frictional costs in the system. Only 65% of premiums are returned to customers via claims, the rest is lost in distribution, operational expenses (including regulatory), capital costs and profit.

Blockchain technology and smart contracts can strip out not only the administrative inefficiencies but a large portion of the governance and regulatory related costs. They can do this by providing trust in a different much more cost-effective way. Trust is moved from institutions and regulations to transparent code. Of the 35% of frictional costs we believe blockchain technology can cut out approximately 18%[6] due to administrative savings and reduced governance and regulatory costs, effectively halving the frictional costs in the system.

Additionally, through the use of membership tokens, blockchain technology can bring back the original goals of the mutual where all contributions are entirely for the benefit of members. Aligned incentives will foster a community spirit rather the existing adversarial and unbalanced relationship between individual and large institution.

Blockchain technology allows a peer-to-peer insurance mutual to be recreated in a cost effective and scalable way. It allows the cooperative ethos to be regained while preserving the benefits of diversification.

Solution Overview

The following components are necessary for a peer-to-peer risk sharing mutual:

1. Membership Tracking – A way to track individual members, including their proportional ownership.
2. Claims Assessment Methodology – A way for claims to be approved or declined.
3. Capital Model – To define how much capital is required to back the risks at any point in time.
4. Funding – Ability to attract capital to back the risks and reward that capital appropriately for the risks taken. Initially and on an ongoing basis.
5. Investment Returns – Insurers hold customers money until a claim event occurs. During this time they tend to invest these funds, usually quite conservatively, to earn additional return.
6. Product – A viable product to sell, including underwriting rules and other acceptance criteria.
7. Pricing – A method for determining the fair risk charge for the risk cover and a way for it to adjust over time.
8. Distribution – Tools and incentives to attract new members to the mutual.
9. Identity – Depending on the product it will probably be required to integrate an identity module as part of the sign-up process.

[4] https://en.wikipedia.org/wiki/List_of_corporate_collapses_and_scandals

[5] http://www.mckinsey.com/industries/financial-services/our-insights/what-drives-insurance-operating-costs

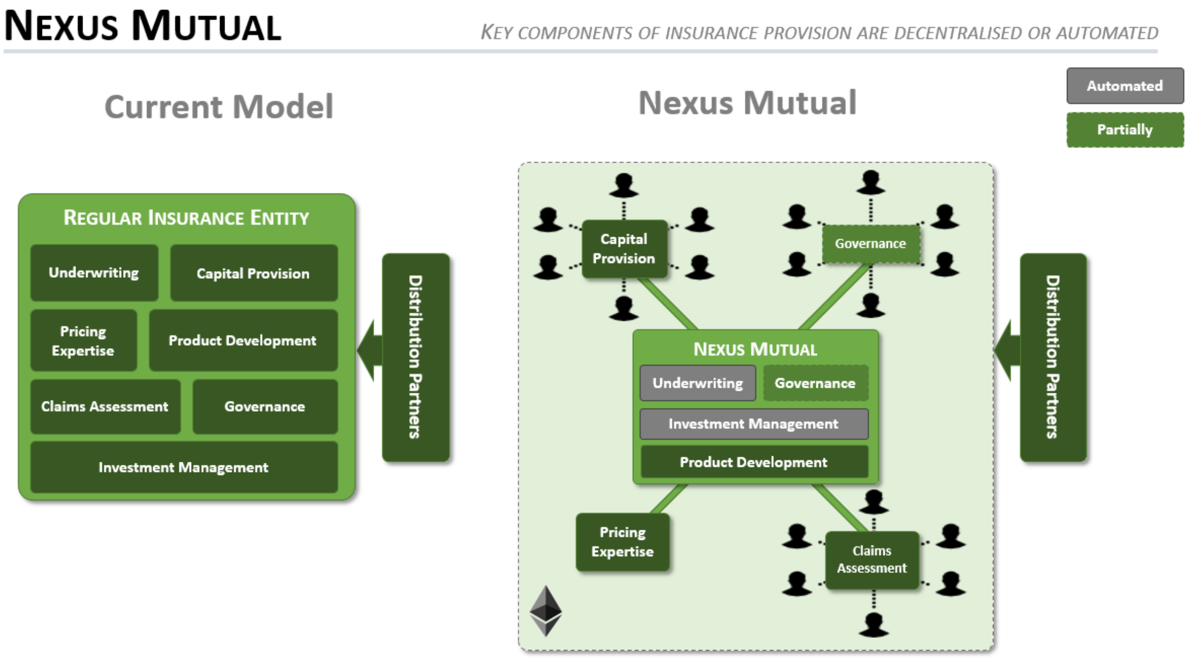
http://www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/Insurance_Risk_Benchmarks_Research_Annual_Statistical_Review.pdf

[6] See Appendix B

10. GOVERNANCE – Not all situations can be handled directly via smart contract code. There must be some way to handle unforeseen events. An Advisory Board will be set-up which can facilitate interaction with the real world, code upgrades and other decisions. Importantly, they will have no custodial rights over the fund pool.
11. TRANSPARENCY – Real time reporting of capital position and risk exposures.
12. LEGAL FRAMEWORK – A safe legal and regulatory environment to operate within.

The next sections of the paper will describe each of these components in turn, followed by additional comments on the competitive strategy.

A visual overview of the general structure, is shown below:

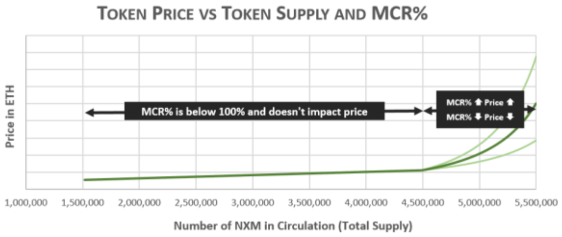


Membership

A simple ERC-20 compatible token will be created to serve as the key internal incentive mechanism to bind the mutual together.

A continuous token model will be used so that tokens can be purchased at any time but at a variable price. This contrasts to more common ICO type approaches where there is a fixed purchase period with set price change points.

The token price will vary based on 1) funding level of the capital pool and 2) the number of tokens in circulation:



$$TP = SF \times \left(1 + \left(\frac{TC}{Growth\ Step}\right)\right) \times Max(MCR\% \times MCR\%, 1)$$

TP *= Token Price in Ether*

TC *= Number of Tokens in Circulation*

MCR% *= Ratio of Capital Pool Funds to the Minimum Capital Requirement (calibrated to a 99.5% solvency level)*

SF = *Scaling Factor, to be calibrated based on the prevailing Ether price before launch.*

Growth Step *= will also be calibrated based on the prevailing Ether price before launch.*

Tokens can only be created in the following ways:

1. Founders Initial Tokens – Some tokens will be set aside for founders when the contract is deployed. A significant portion of these will be locked for up to 12 months, during which time they cannot be transferred.
2. Purchased via the Token Price Model – Anyone at any point can purchase tokens via the token price model. When funding is required (ie low MCR%) the price will be lower to encourage funds to be placed. Conversely the token price increases when funds are more plentiful. Price also increases based on the number of tokens in circulation which places a natural throttle on token issuance. The token model ensures a balance is reached between adequate return for the risks taken by early participants and allowing future members to join at any time.
3. Claims Assessment Rewards – Additional member tokens are allocated as an incentive to perform claims assessment. This will be limited to 1% of claims paid.
4. Capital Model Rewards – Additional member tokens are allocated as an incentive to run the capital model.

While the supply of member tokens is not fixed all methods of generating new member tokens require a specific contribution to the mutual. Contributions are made as either funds or services (claims assessment or running the capital model).

Membership tokens can be used in the following ways:

1. Purchasing Cover – Member tokens can be used ("burned") to purchase cover. Where; Token Value = Mutual Pool Funds (V) / Number of Tokens. 95% of the tokens used are burned, with the remaining 5% locked for the cover period plus 35 days, as they are required to submit a claim.
2. Claims Assessment Bond – To participate in claims assessment income member tokens must be posted as a bond.
3. Capital Model Bond – To participate in running the capital model member tokens must be posted as a bond.
4. Underwriting Bond – To participate in assessing risks and earning commissions a bond will be staked.

5. SURPLUS DISTRIBUTIONS - Pricing will be calibrated so the capital pool expects to generate surpluses over time.

   Members can participate in surpluses by locking their tokens for a period, 100 - 365 days. The longer the lock period the higher the proportional share of surplus.

   Weight = Number of Locked Tokens x Days Locked/100

   If the MCR%$_{(Full)}$ is greater than 180% then a surplus is distributed to those members who have locked their tokens. The total surplus distributed each week is the minimum of A, B or C:

   A. 0.1 ETH per locked NXM token;

   B. 5% of the MCR∈ $_{(Full)}$; or

   C. 50% of the total amount of ETH held in the capital pool V$_{(Full)}$.

   A surplus cannot be distributed if a previous surplus was distributed less than 1 week ago. So there is a maximum of one surplus distribution per week. The 180% threshold is checked once each day after the capital model results are available on-chain.

CLAIMS ASSESSMENT

There are two main approaches to claims assessment using blockchain technology. Firstly, use an oracle which is either a trusted off-chain information provider (eg to trigger parametric insurance events) or secondly to crowd-source information and assess claims using voting mechanics (eg a prediction market).

Under a mutual model there is a legal requirement that a group or sub-group of members decide on how funds are distributed. This immediately focusses efforts on the crowd-source approach but there are other arguments against parametric trigger based cover:

1. BASIS RISK[7] - This can lead to poor customer outcomes especially when customers have suffered a loss but the trigger has not technically been met.
2. ORACLE FAILURE - Back-up claims process mechanisms will be required if the oracle were to fail.
3. LIMITED PRODUCT SET – Product development requires a reliable data oracle to exist. The data must also be sufficiently granular data to construct a meaningful consumer product. IoT devices are expected to bring many more potential data oracles in the future but are currently not widespread or reliable enough to act as oracles.

Returning to the crowd-source model, there needs to be an incentive for people to report and a strong disincentive to prevent fraudulent reporting. This is somewhat difficult to achieve in an insurance context because there is a clear incentive to defraud the pool by 1) purchasing cover for a low percentage of the sum assured, 2) using a substantial portion of the sum assured to pay-off claims assessors and then 3) pocketing the difference.

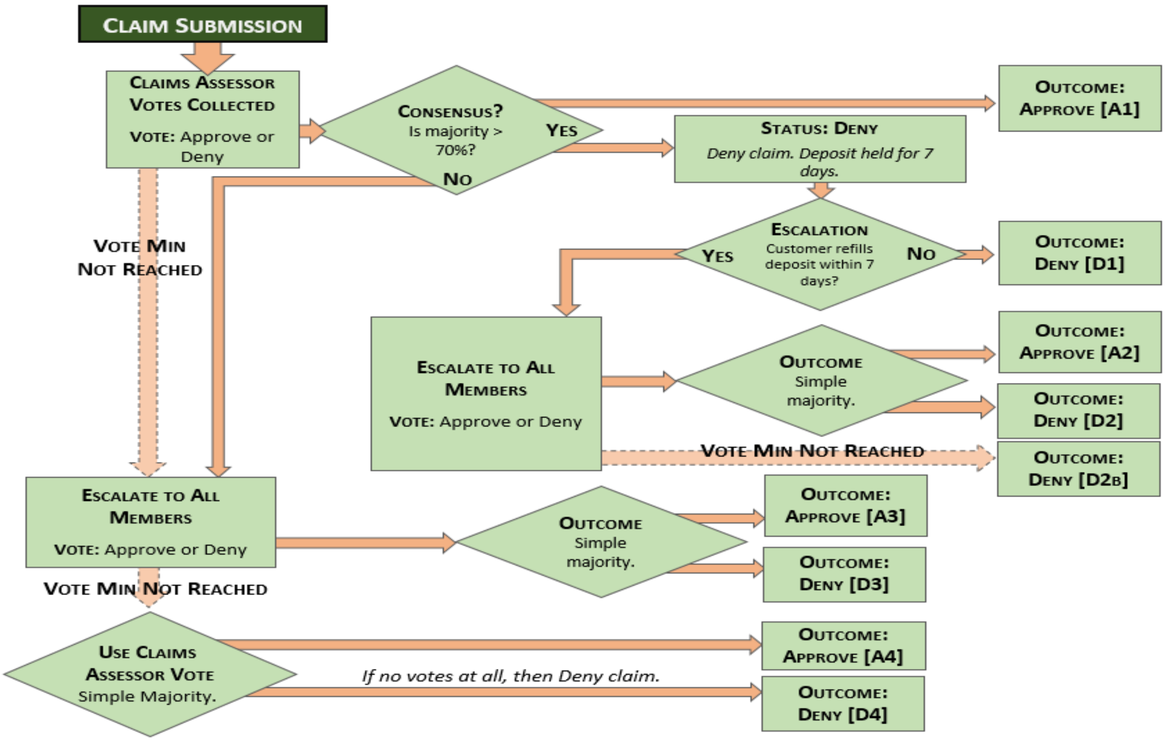
A solution to this issue is to require claims assessors to have a significant stake in the success of the overall pool and a high disincentive to act dishonestly. This can be achieved by requiring a bond be posted in the form of membership tokens. The bond is deposited for a specified period of time and provided claims are assessed honestly it is returned. If the Advisory Board deems a claims assessor to be acting dishonestly it has the power to burn the deposited member tokens.

[7] https://www.questia.com/library/journal/1P3-1252828171/understanding-basis-risk-in-insurance-contracts

In addition, the following other incentive structures will be put in place:

- Voting with the consensus outcome entitles claims assessors to a share of the fee pool. Fees will be paid as additional member tokens and valued at 1% of sum assured.
- Voting against the consensus outcome results in locking of the bond for a longer period. Assessment is often challenging and automatically burning high values of member tokens for genuine differences of opinion needs to be avoided.
- No consensus results in a reduced fee pool for claims assessors and the claim is then escalated to all members (token holders) for a vote.
- Voting power must add up to greater than at least 5x the sum assured value, where voting power is determined by a proxy of the member tokens value used to vote.
- Member tokens contributing to claims assessment voting become "inactive" and cannot contribute to another claims assessment for 12 hours. This prevents posting a bond, submitting many fraudulent claims of value well above the deposited bond and then approving them all. The Advisory Board has time to step in and burn tokens before too many fraudulent claims are approved. In this case the members would benefit overall as the accretive benefit from the burned member tokens would outweigh the fraudulent claims cost.
- Calibrations of the incentive mechanisms need to be refined in testing.

Designing incentive structures resilient to game theoretic attacks is very challenging. The approach described has a basic incentive structure at its core and then overlays timing windows and human intervention to prevent more extreme scenarios.



CAPITAL MODEL

The capital model determines the minimum capital the fund needs to hold. The funding rules in the next section then reference the Minimum Capital Requirement (MCR) and determine actions such as the token price and surplus distribution.

The capital model will be calibrated to handle events up to the 99.5% or a 1-in-200 event. Capital at this level is consistent with Solvency II[8] methodology now in place in the EU, as well as the regulatory standards of many other nations such as Australia[9], Bermuda, Japan, Mexico and Singapore who either have specific targets of 99.5% or are on the way to gaining "equivalence" with the SII regime.

An alternative approach is to 100% collateralise the insurance contracts, essentially holding the full sum assured value at all times. In combination with the immutability of the blockchain this would give the consumer an extremely high level of security. This comes at the cost of severely reduced capital efficiency and the ability to raise funds at an appropriate price. As a simple example, assume we have 10,000 (n) identical policies each with a chance of claim of 1% (p) for a sum assured of \$100 (v). Assuming independence the 99.5% minimum capital requirement (MCR) is given by:

Mean = $\mu = p \cdot n = 100$

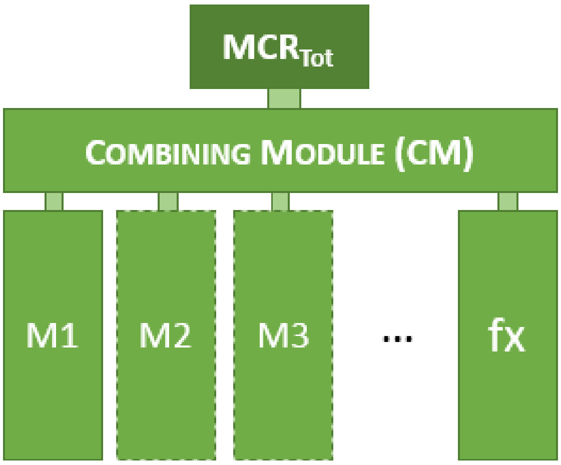
Std Dev = $\sigma = \sqrt{n \cdot p \cdot (1-p)} = 9.9499$

MCR = $v \cdot (\mu + 2.58 \cdot \sigma) = \$12,567$

Total Exposure = $n \cdot v = \$1,000,000$

To back 10,000 contracts we only need 1.26% of the total exposure to be confident the fund will be solvent in 199 out of 200 scenarios. This diversification benefit needs to be leveraged otherwise we cannot be competitive with existing institutions.

The capital model is structured in multiple modules, where each module represents a product and currency pair. In addition, there is a currency module (fx) to account for currency risk. The modules are then combined at a total level to get the MCR. In its simplest form, with one product and one currency there are three modules, M1, fx and CM.



The base calculation currency is Ether as dividends and capital raisings will be done in Ether. Each individual modules MCR is calculated in local currency (ie GBP, USD, EUR etc) and then converted to Ether in the combining module.

Focussing on module one to begin with, and assuming the product has a fixed sum assured MCR_{M1} is defined as follows:

$$MCR_{M1} = \sqrt{\sum_{i,j} Corr(i,j) \cdot Exp(i) \cdot Exp(j)}$$

Where, Corr(i,j) is the correlation matrix of the individual pricing risk cells:

$$Corr(i,j) = \begin{bmatrix} 1 & \cdots & corr(j,i) \\ \vdots & \ddots & \vdots \\ corr(i,j) & \cdots & 1 \end{bmatrix}$$

[8] https://en.wikipedia.org/wiki/Solvency_II_Directive_2009

[9] http://www.apra.gov.au/Policy/Documents/Regulation-Impact-Statement-LAGIC.pdf

http://www.aon.com/attachments/reinsurance/052011_ab_latin_america_solvency_regulation_paper_051911.pdf

https://www.munichre.com/site/corporate/get/documents_E-2113795143/mr/assetpool.shared/Documents/5_Touch/_Publications/302-08131_en.pdf

And Exp(i) = Total exposure (or sum assured) in pricing risk cell i.

The correlation matrix may be very simple if independence between cells can be assumed in which case $\mathrm{MCR}_{\mathrm{M1}}$ reduces to:

$$\mathrm{MCR}_{\mathrm{M1}} = \sqrt{\textstyle\sum_i Exp(i)}$$

It is possible that each product module may have a different formulaic logic to get to an assumed 99.5% confidence capital requirement. In particular, this would be required with indemnity based products rather than fixed sum assured values.

The next step is the currency module (fx) which takes the MCR's of each module in a particular currency (k), compares that to the value actually held in the pool, V_{j}, and applies a currency shock of 50%, both up and down, and then chooses the maximum value. The sum of all these becomes $\mathrm{MCR}_{\mathrm{fx}}$:

$$\mathrm{MCR}_{\mathrm{fx}} = \Sigma_{\mathrm{k}} \mid (\Sigma_{\mathrm{k}} \mathrm{MCR}_{\mathrm{i}} - \mathrm{V}_{\mathrm{k}}) / 50\% \mid \cdot \mathrm{fx}_{\mathrm{k\ to\ \Xi}}$$

Where $\mathrm{fx}_{\mathrm{k\ to\ \Xi}}$ is the exchange rate to Ether.

The combining module then takes a similar approach to the $\mathrm{MCR}_{\mathrm{M1}}$ calculation, treating each module as its own pricing risk cell and assuming a correlation between different modules:

$$\mathrm{MCR}_{\mathrm{Tot}} = \sqrt{\textstyle\sum_{l,m} Corr(l,m) \cdot MCR(l) \cdot MCR(m)}$$

subject to a minimum value.

Where, Corr(l,m) is the correlation matrix of the modules:

$$\mathrm{Corr(l,m)} = \begin{bmatrix} 1 & \cdots & corr(l,m) \\ \vdots & \ddots & \vdots \\ corr(l,m) & \cdots & 1 \end{bmatrix}$$

The total MCR will need to be calculated regularly, probably at least once per day, as it is needed as a reference item for funding triggers. Operationally this will work as follows:

- Calculation will need to be performed off-chain, due to gas requirements, with the result being notarised on-chain.
- The capital model code will be open-source and all inputs will be available on-chain (either directly or via oracles for currency exchange rates) or as part of the model itself.
- Correct running of the model will be verified on-chain.
- Updates to the model or input parameters will be handled via the Advisory Board governance process.
- There will be a specified block number on which calculations are made. This locks the data inputs to the calculation model and gives enough time for the model to be run off-chain.
- Running the capital model will be incentivised via a member token reward that ticks up depending on the time since the last verified model result was placed on-chain. It also requires posting a bond in the form of member tokens which can be burned by the Advisory Board if the capital model is repeatedly run incorrectly.[10]

FUNDING

The fund will target a capitalisation, or funding, level of 180% of the minimum capital requirement. This is broadly consistent with existing insurance institutions.[11] The total current pool value is V, which is calculated as the sum of all the currency pools converted into Ether. The funding levels are all

[10] Possible alternative solutions https://truebit.io/ http://www.ethereum-computation-market.com/

[11] https://www.moodys.com/research/Moodys-Solvency-II-ratios-Not-Fully-Comparable-Generally-Comfortable-Level--PR_345910

effectively governed by the continuous token model described in the membership section.

When the fund is first launched no policies can be purchased until an MCR% of 100% is achieved (which will be the minimum capital requirement). Once that happens the fund goes live and the token model interacts with the capital model to increase or decrease the token price as required.

Another aspect of funding is the multi-currency pool of funds. As member fees and claim payments will be constantly flowing in and out of the pool rules are required (both trigger limits and targets) to ensure the right level of funds is allocated to each currency pool. Also, as the capital model punishes mismatches in fund pools vs MCR's by currency (via greater $\mathrm{MCR}_{\mathrm{Tot}}$) a decision on allocation is required. Targets and trigger limits will be set, though the Advisory Board will have the authority to update these as necessary.

Additionally, some trust-less way of converting fiat-crypto tokens to Ether is required to balance the pool. One solution is to automatically deploy exchange contracts with a specified starting price (via an Oracle) and the required volume of tokens. The contract then incrementally lower the price until a third party interacts with the contract and exchanges the funds. Other decentralised exchange solutions are expected to develop (and already exist) that could be used instead. More investigation is required on this aspect.

More broadly, there is an implicit assumption throughout the paper regarding the availability of a fiat-based crypto token for all currencies the mutual wishes to trade in. At present no viable solution to this exists, though many companies and organisations have publically stated they are developing solutions and MakerDAO has recently gone live. It is expected an acceptable solution will eventuate in the short term. There is no intention to build such tokens but rather use them when they are developed by others. Therefore, Nexus Mutual is will only be able to transact in Ether denominated coverage until viable fiat-crypto tokens exist.

Investment Returns

Investment returns are an often underappreciated aspect to insurance as it allows the insurance entity to earn returns on the reserves it holds.

Nexus Mutual will hold all funds on-chain and will restrict itself to assets of ERC20 tokens only. At present this asset universe is quite small but it is expected to grow substantially over time.

The investment process will be entirely automated using the 0x[12] protocol to initiate trades. Essentially a buy and hold investment strategy will be defined and trades will rebalance the pool as required. There will also be trading triggers to deal with liquidity needs arising from claim payments.

The assets chosen will need to change over time (via the governance module) and are expected to be relatively conservative. Ideally, the assets list would include some dividend bearings assets like tokens that contribute to Proof of Stake or earn by lending ETH on margin.

Such an approach means basic investment management can be entirely automated and conducted in a trust-less way.

The current lack of investment options is not considered a major issue in the short term as enough viable ERC20 tokens currently exist.

[12] https://0xproject.com/

PRODUCT

Initially the mutual will be launched with only one product, Smart Contract Cover with a fixed sum assured. The product will cover “unintended code usage” where someone, not necessarily the cover purchaser, has suffered a financial loss on the contract. As an example, the cover would pay out on the DAO hack, and the two Parity multi-sig wallet issues. It is not intended to pay-out on loss/misuse/phishing of private keys as this cannot be verified.

This product is seen to have a very good market fit for the early adopters of the platform. Security of smart contracts is a well-publicised issue within the Ethereum community with many technical efforts being led to improve the situation. Longer term, the intention is to expand the product range into more regular insurance products and become an alternative risk carrier for the insurance industry.

The initial product has been chosen for several reasons:

- Claims assessment can be done entirely remotely using publicly available data from block explorers.
- A fixed sum assured means claims assessment is a simple “yes” or “no” rather than requiring an assessment of how much damage has been caused.
- The product underwriting can be automated.
- It is not necessary to identify the end consumer or even confirm that they have an insurable interest in the specific contact.
- The product in new to market with no alternatives existing. Many developers are very worried about deploying code to main-net, as even with many security audits and thorough testing you can never be completely sure bugs don’t exist.

Numerous future products can be developed such as indemnity based cover, life cover, auto cover etc. Many of them will require some form of underwriting processes, an identity module and much more complex claims assessment procedures. The goal is to initially build a product with a clear consumer need in our target audience before expanding into regular product lines.

PRICING & CAPACITY LIMITS

Given the lack of historic data on smart contract hacks related information on code security will be used to assist pricing. Additionally, it is expected that most new contracts will start off with a very high (or even uninsurable) premium that is then reduced over time as the code is more battle tested in the real world. However, by itself this is not of any material benefit to code developers as they will often want cover immediately. Therefore, we will introduce the concept of underwriting, which is essentially underwriters (think smart contract security auditors) staking tokens against specific smart contract addresses to reduce the price of cover.

If there is an early claim then part of the stake will be lost but in return the underwriter will earn commission in the form of tokens for cover sold on that particular address.

In this way, we are combining a standard pricing algorithm with decentralised underwriting approaches to provide protection for the Ethereum community and its smart contracts. In addition, it will be possible to provide cover for smart contracts written on different blockchains, not just on Ethereum.

Another important aspect is capacity limits. A relatively simple approach will be taken whereby exposure to any single smart contract (or related and similar contracts) will be limited to a fixed percentage of the pool value. This ensures that any one claim event does not put the solvency of the fund at risk.

From an upgrade perspective, the Advisory Board (or membership) can propose a detailed one-off review of pricing at any time. This would re-set the with a new set of rates/algorithm. Alternatively, pricing can be provided off-chain via an API to a specialised pricing provider. This option is a likely first step which is easier to implement and more flexible but introduces a level of trust in the pricing provider.

Pricing will also be flexible enough for cover periods in daily increments. With a formula used to determine non-yearly cover period rates.

DISTRIBUTION

Distribution will initially focus on the small group of cryptocurrency enthusiasts, entirely within the cryptocurrency sphere. This will enable any teething issues to be identified before building out more product and attempting a large scale up. We believe there is ample opportunity in the short to medium term to provide meaningful growth with the initial product, in particular:

- Well-funded projects looking to deploy code could purchase cover in case something goes wrong. This would help minimise reputational damage and provide a fund to compensate users if necessary.
- Individuals looking to interact with smart contracts may want extra confidence before exposing funds. Very few individuals have the capability to assess code quality by themselves. This is especially important when large values are involved.
- ICO contracts looking to provide confidence to prospective funders may want to pre-purchase cover for their ICO code.
- Multi-sig wallet contracts could be insured. While not addressing private key management issues this gives greater confidence funds won't just disappear. This could form part of a more comprehensive custody solution designed by 3rd parties.

Distribution in the short term will come primarily via community engagement and promotion within the cryptocurrency community driven from within the project.

Longer term, when the product range is expanded to regular insurance products the main challenges to wider distribution are:

- ACCESSING CRYPTO TOKENS – As future products require purchasing fiat-crypto tokens the development of consumer wallet tools and processes is needed to achieve any meaningful scale. Approaches whereby distribution partners handle the crypto aspects and allow consumers to conduct business entirely outside the crypto sphere will be the primary focus.
- FIXED SUM ASSURED – Most consumers are accustomed to indemnity based products where claims paid cover losses actually incurred.
- DISTRIBUTION PARTNERS – Many insurance policies are sold through brokers, so enabling an attractive financial distribution model will be key to attracting larger volumes. Distribution tools and marketing material will need to be developed.

In summary, the longer-term vision is not for products to be mass marketed to consumers directly, but rather as a B2B2C platform that distribution partners can integrate with via blockchain's inherent open API architecture.

Therefore, a key aspect to the long-term success of the mutual are the distribution partners. The smart contract platform is designed to be as open as possible and therefore quite flexible for distributors to interact as they see fit (subject to any compliance obligations).

IDENTITY

For several insurance applications the identity of the customer will be required. This entails a controlled space where accounts have been verified and sign-up can be restricted to customers meeting certain criteria.

As the initial product does not require the identity module this will be considered as a future development. In addition, there is no intention to build a new identity model from scratch but rather integrate an existing one, like Uport[13] or Thomson Reuters Block One ID[14] once they become established.

GOVERNANCE

Ideally all potential actions can be defined by the code but reality is much more complex and a fall-back option is required in several circumstances. As such an Advisory Board will be set-up to make decisions requiring interaction with the real world as well as govern some of the more extreme scenarios. Importantly, the Advisory Board has no custodial rights over the fund pool and cannot release funds to any particular person.

The Advisory Board will operate under two core principles:

1. SUSTAINABILITY – Protect existing customers by ensuring the overall fund is sustainable
2. GROWTH - Enable sustainable premium and customer growth

It will contain at least five individuals who are all members of the mutual and contain a mix of insurance business expertise, mutual governance and blockchain development.

Advisory Board members will have the following broad authorities, which will be specified in more detail:

1. Conduct reviews of and implement changes to the Capital Model and Pricing Rates.
2. Facilitate the implementation of proposals through a process of review, recommendation and development.
3. Ensure contract code is fit for purpose.
4. Punish bad actors with regards Claims Assessment and Capital Model incentives.
5. Meet all the legal and regulatory requirements of Nexus Mutual Ltd.
6. Facilitate engagement of services required for Nexus Mutual Ltd.

Detailed authorities will list what Advisory Board members can agree on by themselves and what they need to go to Members for a final decision.

All proposals put to a Member vote must contain a defined list of the possible voting outcomes as well as the Advisory Board recommendation and vote result. Members are then given a specified timeframe to vote on the proposal. If a specified quorum is not met then the vote proceeds as per the Advisory Board recommendation. Otherwise the majority outcome prevails.

Individual Members can develop proposals for the Advisory Board who will have some discretion whether to proceed with them or not.

Any individual Member owning more than a specified number of the total member tokens may request to join the Advisory Board. The

[13] https://uport.me/

[14] https://blockone.thomsonreuters.com/

Advisory Board puts this to a member vote along with their recommendation.

Transparency

A key requirement for operating a well-run mutual entity is providing members, potential members and other interested parties with accurate information regarding the financial health of the mutual. Blockchain technology lends itself quite naturally to transparency due to the public ledger. As such, a website interface will be developed which reports on key metrics in real-time. These will include:

- Capitalisation ratio.
- Exposure by pricing cell, and groupings.
- History of capital metrics and token price.
- Number of total member tokens outstanding split by locked vs transferrable.
- Details on claims assessment results, with summary statistics.

Legal Framework

Nexus Mutual will be set-up as a real world legal entity in the UK as a company limited by guarantee. Holders of member tokens will have a legal right to proportional ownership of the mutual and will also be responsible for providing the guarantee.

The guarantee will be set at £1 per a specified number of member tokens.

A discretionary mutual structure is legally not providing insurance, it is just a legal structure that enables members to trade with each other. Therefore, it is not required to conform with all the insurance regulatory and legal requirements. In addition, products are not subject to Insurance Premium Tax (IPT) in the UK with any distributed surpluses being taxed in the hands of members. The mutual will pay tax on any trade outside of the mutual, for example VAT on services and corporate tax on investment income.

A discretionary mutual based in the UK can legally trade in the UK but cover can be provided anywhere in the world. As such, global cover is available as long as members are able to legally become a member of the UK company.

As a real world legal entity, the mutual can interact directly with real world service providers as well as regulated insurance entities. The latter is particularly useful as excess-of-loss insurance coverage may be required for high exposures.

Bridging from the fiat world to the crypto world will require AML/KYC compliant processes. These have to be investigated in more detail but the project will be fully compliant with these regulations.

Other compliance activities relating to sales processes and treating customers fairly type regulation will be investigated as part of the compliance activities required to set up the new mutual.

All of the above views are formed based off informed research and discussion with business experts, however, they do need to be verified by formal legal advice.

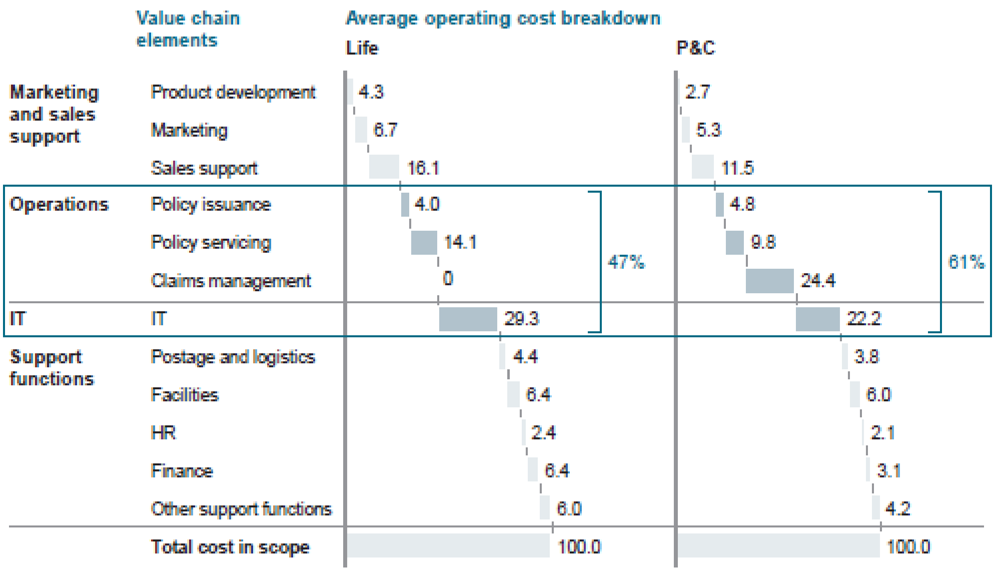
Competitive Strategy

A key challenge in open source business is retaining a competitive advantage when anybody can copy your entire code base, decrease margins slightly and poach all your customers. To remain relevant the business must establish meaningful barriers to potential competition. In open-sourced blockchain systems this is largely achieved through the network effect where a community gathers around a certain technology, becomes bought into it (usually financially as well as emotionally / philosophically) and continuously improves it to remain relevant. The following barriers and frictional costs are designed to keep Nexus Mutual relevant to current members and continually attract new ones:

- UNDERWRITING NETWORK – Establishing a meaningful underwriting network of smart contract auditors and providing them adequate incentives to participate.
- SIZE OF FUNDING POOL – The faster scale can be achieved the larger the funding pool can grow and the greater the diversification benefits exist. This ensures efficient capital usage, lower prices and provides more resilience to claims shocks. Additionally, the greater the pool value the higher the barrier to replicate.
- CONTINUAL DEVELOPMENT – A continued focus on improvement of the product. Including, releasing new products and providing easy to use infrastructure surrounding the core blockchain code will heighten the barrier to replicate.
- MEMBER TOKENS – All customers are members and have a vested interest in the success of the mutual through token ownership. If members shifted to another provider their current holdings would drop in value. Member tokens therefore provide an indirect incentive to remain with the mutual and an additional barrier to competitors.

Whilst all of these barriers have the potential to be overcome the goal is to gain networks effects and scale benefits that will prevent copy-paste competitors taking significant market share.

Appendix A – Cost Reduction Enabled by Blockchain Technology



Operations and IT account for around 50% of a typical insurer's cost base

Percent of total costs,1 Western European peer group as of H1 2015

1 Total costs excl. commissions

SOURCE: McKinsey's Insurance 360° benchmarking [15]

Focussing on the P&C column, the costs in the above diagram account for roughly 25% of premium, so most of the 35% of premium that gets lost in frictional costs. The most notable exclusion is commission.

Marketing and Sales Support E – These costs will largely remain as is. There are likely to be some small savings in sales support costs due to efficiency in the underlying systems but there won't be any material savings overall.

Operations and IT – The major area where large cost savings can be realised. The only material costs that will remain will be gas costs, decentralised claim assessment and smart contract upgrades. We will assume these costs are reduced by 90% as the majority of IT upgrades will be handled as part of the product development budget.

Support Functions – Large cost savings will materialise across a number of sub-functions primarily because the number of people employed will be dramatically reduced. Only the Advisory Board is required. We will assume 90% of these costs can be avoided.

Converting this back to a percentage of premium we get a cost reduction of roughly 18%, which is close to half of the 35% total frictional costs.

[15] http://www.mckinsey.com/industries/financial-services/our-insights/what-drives-insurance-operating-costs