NEXUS MUTUAL

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

HUGH KARP, REINIS MELBARDIS

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 are 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 largely effective, barring a handful of high

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

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

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

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. 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 – An identity module will be required as part of the sign-up process to conform with legal and regulatory requirements.
10. Governance – A way to upgrade, enhance and fine-tune the code in line with the wishes of the membership base,

[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

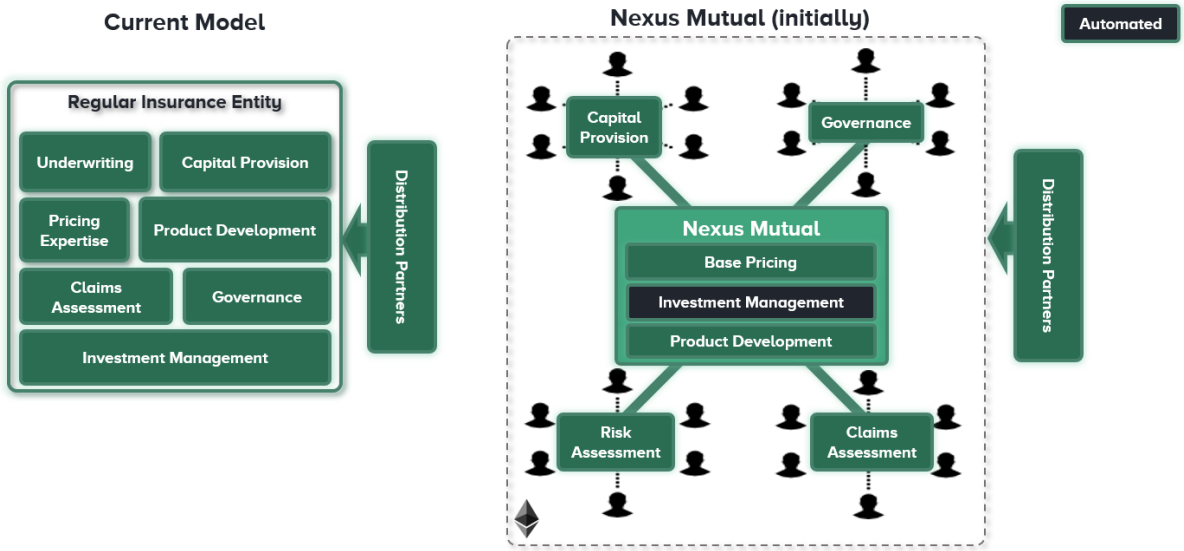
[6] See Appendix A

as well as the ability to interact with the non-blockchain world.

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, followed by a speculation-driven market on exchanges.

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

Note: Diagram illustrates funding level only. Price also varies with 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. INITIAL TOKENS – Some tokens will be set aside for founders and early contributors when the contract is deployed.
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 compensation 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 a fixed percentage of the cost of cover.
4. RISK ASSESSMENT REWARDS – Additional member tokens are allocated as an incentive for participating in risk assessment.
5. GOVERNANCE – Additional member tokens are allocated as an incentive for participating in governance.

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, risk assessment or voting in governance).

Membership tokens can be used in the following ways:

1. PURCHASING COVER – Member tokens can be used ("burned") to purchase cover. In this case the token value is determined by the continuous token model. 90% of

the tokens used are burned, with the remaining 10% locked for the cover period plus 35 days, as they are required to submit a claim.

2. CLAIMS ASSESSMENT STAKE – To participate in claims assessment and earn the resulting income, member tokens must be staked.
3. RISK ASSESSMENT STAKE – To participate in assessing risks and earning commissions a stake is required.
4. REDEMPTION - If the Capital Pool has sufficient funds redemptions of member tokens in exchange for Ether is permitted.

   The following restrictions will apply:

   1. Capital Pool needs to be above the MCR (MCR% > 100%).

   2. Redemptions are capped per transaction.

   3. The Capital Pool must have enough liquidity in Ether.

   4. Sell price will be 2.5% below the prevalent buy price.

Only members of the mutual will be able to own tokens. As such, tokens cannot be transferred to any Ethereum address that has not been designated as a member.

CLAIMS ASSESSMENT

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

Under a discretionary 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 that limit the usefulness of 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 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.

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 cover amount, 2) using a substantial portion of the cover amount to pay-off claims assessors and then 3) pocketing the difference.

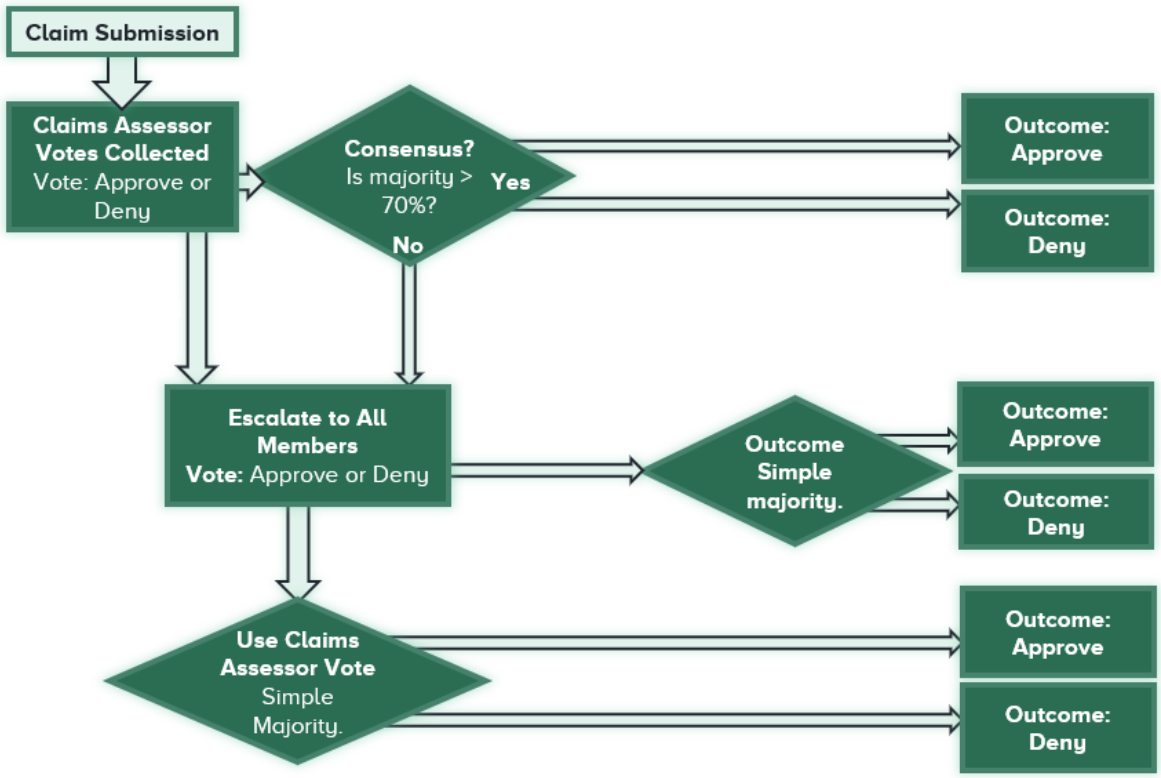
A solution to this issue is to require claims assessors to have a significant stake in the success of the overall pool and a high disincentive to act dishonestly. This can be achieved by requiring a stake be posted in the form of membership tokens. The stake is deposited for a specified period of time 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 staked 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 a fixed percentage of the cost of cover.
- 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.
- Voting power must add up to greater than 5x the cover amount, where voting power is determined by the number of staked member tokens used to vote.
- No consensus results in a reduced fee pool for claims assessors and the claim is then escalated to all members for a vote.
- Member tokens contributing to claims assessment voting become "inactive" and cannot contribute to another claims assessment for 12 hours. This prevents posting a sufficiently high stake, submitting many fraudulent claims of total value well above the staked amount 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 redemption restrictions.

The capital model will borrow heavily from EIOPA's Solvency II[8] methodology which is calibrated to withstand events in a year with a 99.5% probability, or, in other words, a 1-in-200 year event. This is consistent with many other regulatory standards of 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 = $\mu = p \cdot n = 100$

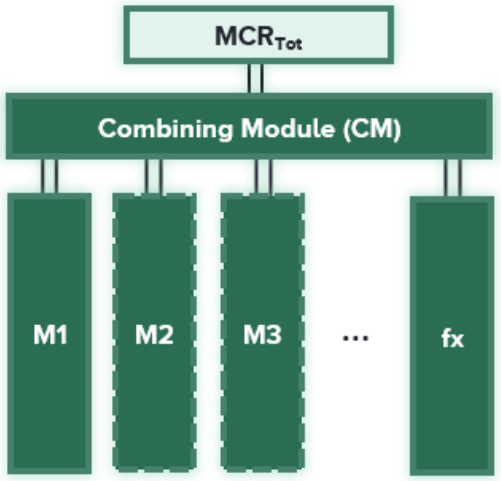
Std Dev = $\sigma = \sqrt{n \cdot p \cdot (1-p)} = 9.9499$

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

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

In this example, we expect 1% of the total exposure to be paid out in claims, but with 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 compete 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 the pool will be Ether dominated to start with. The MCR of each individual module is calculated in its currency (ie ETH or DAI[10]) 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;

[8] https://eiopa.europa.eu/regulation-supervision/insurance/solvency-ii

[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

[10] https://makerdao.com/whitepaper/DaiDec17WP.pdf

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

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

And Exp(i) = Total probability-weighted exposure (or cover amount) in pricing risk cell i.

The correlation matrix may be very simple if independence between cells can be assumed in which case MCR_{M1} reduces to:

$$MCR_{M1} = \sqrt{\sum_i Exp(i)}$$

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 cover amount 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 MCR_{fx}:

$$MCR_{fx} = \Sigma_k \, | \, (\Sigma_k \, MCR_i - V_k \,) \, / \, 50\% | \cdot fx_{k \text{ to } \Xi}$$

Where $fx_{k \text{ to } \Xi}$ is the exchange rate to Ether.

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

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

subject to a minimum value.

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

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

A minimum MCR value will be set when the pool launches and the MCR value can never drop below this.

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 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.
- To begin with it is likely the MCR will be run in a trusted manner off-chain due to technical limitations. In the future trust minimising options for complex computation will be investigated further with a strong intention to remove this reliance.

FUNDING

The funding levels are all effectively governed by the continuous token model described in the membership section. The total Capital Pool value is V, which is calculated as the sum of all the asset values converted into Ether.

When the fund is first launched no covers can be purchased until an MCR% of 100% is achieved (which will be once the Capital Pool

is equal to 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 are held in each currency. Also, as the capital model punishes mismatches in fund pools vs MCRs by currency modules (via greater MCR_{Tot}) a decision on allocation is required. Targets and trigger limits will be set, which can be updated via the governance process as necessary.

Additionally, some trust-less way of converting fiat-crypto tokens to Ether is required to balance the pool. As per the investment returns section, this will be handled via the 0x protocol[11].

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 widely adopted solutions to this exist, though many companies and organisations have publicly stated they are developing solutions and MakerDAO has recently gone live with DAI (a USD stable-coin). Initially, Nexus Mutual will use Ether and DAI ($USD) as its initial currencies and wait for further solutions to develop and become more widely adopted.

Investment Returns

Investment returns are an often under-appreciated aspect to insurance as it allows the insurance entity to earn returns on the reserves it holds. This is a key component to insurers' profitability and therefore must be replicated in some fashion if Nexus Mutual is able to compete with existing insurance entities longer term.

As Nexus Mutual will hold all funds on-chain, it will restrict itself to assets of ETH and 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 protocol to initiate trades. 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, with the changes initiated and approved via the governance module.

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

Ideally, the assets would generate a positive return over time with very high probability, akin to the portfolio composition of traditional insurers which tend to be dominated by corporate and government debt instruments[12]. In the Ethereum world, we see the current most appropriate candidates for generating a return on ETH as:

- locking up ETH to generate interest in the proposed Proof of Stake system,
- investing in financial instruments based on collateralised lending[13]
- acting as a guarantor in state channel and payment channel networks.

Unfortunately, we are still some time away from Ethereum moving to a Proof of Stake system. With insufficient scale and liquidity currently available in the various ETH-based lending markets, becoming a payment channel guarantor is more likely to be viable

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

[12] http://www.oecd.org/investment/Evolution-insurer-strategies-long-term-investing.pdf

[13] https://dharma.io/

in the short term, but the technology still needs to mature and be adopted more widely by other blockchain applications. The current lack of investment options is not considered a major issue in the short term given the expected short policy durations of the initial product. It is therefore likely that Nexus Mutual will initially launch without any investment assets, only holding currency assets closely matched to the liabilities of the mutual.

An alternative approach would be to invest a portion of the funds into a basket of ERC20 tokens, in the hope that they gain in value relative to ETH. We do not see any reason to believe that such investments exist and, if they do, that we would be able to pick out such a basket from the outset. However, such investments could be made via the member governance process.

PRODUCT

Initially the mutual will be launched with only one product, Smart Contract Cover with a fixed cover amount. The product will cover "unintended code usage" where someone, not necessarily the cover purchaser, has suffered a financial loss on the smart 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 cover amount means claims assessment is a simple "yes" or "no" rather than requiring an assessment of how much damage has been caused.
- The product pricing can be largely automated allowing covers to be issued without any mandatory manual underwriting.
- It is not necessary to confirm the member has an insurable interest in the specific contract.
- The product is 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.
- The likely short-term nature of the covers is a good fit given the (lack of) on-chain investment options available.

Numerous future products can be developed such as indemnity-based cover, life cover, auto cover etc. Many of them will require some form of initial underwriting process 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) cost which is then reduced over time as the code is more battle-tested. However, by itself this is not of any material benefit to code developers as they will often want cover immediately.

Therefore, we are introducing the concept of decentralised risk assessment, which involves knowledgeable experts (think smart contract security auditors) staking value in the form of member tokens against specific risks to reduce the price of cover.

If there is an early claim then part or all of the stake will be lost. In return, the risk assessor 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 risk assessment to develop a complete pricing framework.

Another important risk mitigation technique employed by the mutual involves capacity limits. A relatively simple approach will be taken whereby exposure to any single smart contract (or related and very 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 mutual at risk.

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

Unlike traditional insurers, pricing will also be flexible enough for cover periods in daily increments, with a formula used to determine rates for specific, non-yearly cover periods.

DISTRIBUTION

Distribution will initially focus on the relatively small group of cryptocurrency enthusiasts, entirely within the cryptocurrency sphere. This will enable any teething issues to be identified before building out more products and attempting significant scaling by offering the product to a mainstream audience. 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 funds 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.
- PROJECTS LAUNCHING AN ICO looking to provide confidence to prospective funders may want to pre-purchase cover for their ICO contract 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 more typical 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. This is similar in nature to the concepts behind existing insurance distribution and the latest trends in open-banking in the UK.

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

It will be necessary to identify all members of the mutual. This is because each member becomes a guarantor of the company and is required by company law in the UK to be identified.

There will be a simple identity process where KYC is conducted that links an Ethereum address to the customer, noting that all identifying information is not held on-chain. This will be a one-time process when signing up as a member.

From then on, the Ethereum address will be linked to the member. This serves a dual purpose of legal compliance and providing some level of Sybil attack prevention, noting that the system is designed to be Sybil resistant anyway.

GOVERNANCE

Ideally all potential actions can be defined by the code but reality is much more complex and fall-back options are required in several circumstances. As such an Advisory Board will be set-up to facilitate decisions requiring interaction with the non-blockchain 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, with each Board member liable to be replaced at any time via the member voting process.

The Advisory Board will operate under two core principles:

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

At the start, it will contain several individuals who are all members of the mutual and contain a mix of expertise within insurance, mutual governance and blockchain development.

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

1. Facilitate and implement the wishes of the membership base, particularly where the code doesn't specifically allow automatic implementation.
2. Punish bad actors within the Claims Assessment process.
3. Meet all the legal and regulatory requirements of Nexus Mutual Ltd.
4. Implement emergency pause functionality if required.
5. White-list and vote on proposals where required.

A detailed list of authorities will lay out what Advisory Board members can agree on by themselves and what proposals 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 (eg Yes/No) as well as the Advisory Board recommendation and vote result. Members are then given a specified timeframe to vote on the proposal. The majority outcome prevails unless a specified quorum is not met – then the vote proceeds as per the Advisory Board recommendation.

Individual members can develop proposals for the Advisory Board who will have some discretion whether to "white-list" the proposal or not. The aim is to "white-list" all reasonable proposals.

Any individual member may propose that they join the Advisory Board. This type of proposal is automatically put to a full member vote without proceeding through the "white-listing" process. This ensures the members ultimately maintain full control of the mutual as any Advisory Board member can be replaced without interference from the Advisory Board.

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 information such as:

- Capitalisation ratio (MCR%).
- 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.

In combination this information will provide an accurate real-time financial position of the mutual. Compared to a regular insurer's financial reporting, which generally takes 3 months (at best) to determine a quarterly result, blockchain can provide orders of magnitude improvement in both timeliness and transparency.

LEGAL FRAMEWORK

Nexus Mutual has been set-up as a company limited by guarantee in the UK and will operate under a discretionary mutual structure. Members of the mutual 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 member. This means if the mutual was ever to run out of money, each member is liable for a further £1 only.

A discretionary mutual is not a provider of insurance, it is a legal structure that enables members to trade with each other under the banner of one legal personality. 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 distributions or surplus 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;

1. Members are able to legally become a member of the UK company, and;

2. Local laws and regulations of the members jurisdiction are adhered to.

Practically, this means Nexus Mutual will be able to provide cover in most countries with some being restricted for various local legal reasons, such as securities laws, insurance regulation and tax.

As a real world legal entity, the mutual can interact directly with non-blockchain 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 to facilitate faster growth

Nexus Mutual will adhere to the principles in the Association of Financial Mutuals (UK industry trade body) code of conduct and will investigate the process of becoming a full member.

All of the above views are formed based off informed research and discussion with business and legal experts. While many aspects have also been verified through formal legal advice there still remains uncertainty with how products and platforms like Nexus Mutual interact with the legal system, especially as many aspects still require guidance from various regulators. As such, when joining, any members of the mutual agree that they will withdraw their membership should it be required for legal or regulatory reasons that would endanger the ongoing operation of the mutual. Nexus Mutual fully intends to comply with all regulation.

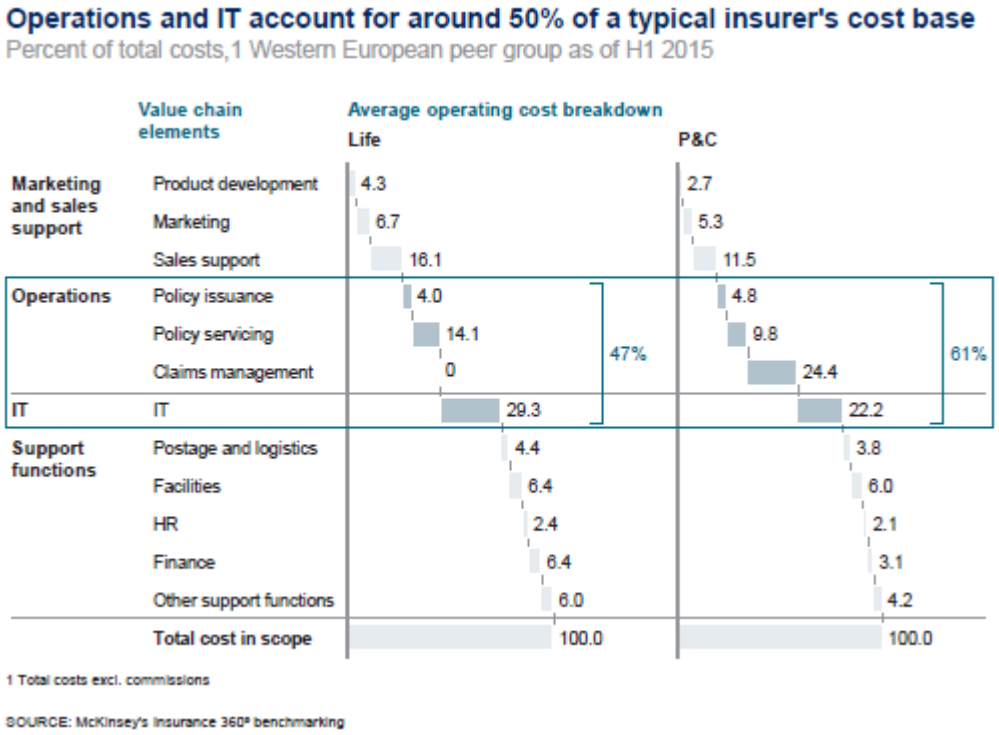
Competitive Strategy

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 and 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:

- Risk Assessor Network – Establishing a meaningful network of risk assessors (smart contract auditors to begin with) and providing them adequate incentives to participate.
- Size of Capital Pool – The faster scale can be achieved the larger the Capital Pool can grow and the greater the diversification benefits. 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. Releasing new products and providing easy to use infrastructure surrounding the core blockchain code will heighten the barrier to replicate. This will be increasingly driven by all members of the mutual over time.
- 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. Membership 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 network effects and scale benefits that will prevent copy-paste competitors taking significant market share.

APPENDIX A – COST REDUCTION ENABLED BY BLOCKCHAIN TECHNOLOGY



14

Focussing on the P&C column (Property and Casualty, i.e. short-term non-biometric insurance more akin to the initial offering of Nexus Mutual), the costs in the above diagram account for roughly 25% of premium, representing most of the ~35% of premium that gets lost in frictional costs[15]. The most notable cost excluded from the above is commission.

MARKETING AND SALES SUPPORT – These costs will largely remain as is for mainstream products. 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 affect the proposed mutual will be gas costs, rewards for decentralised claim assessment and smart contract upgrades. We estimate these costs are reduced by 90%, as policy issuance and servicing are entirely automated, claims management is simplified and crowdsourced and systems normally required by insurers are made vastly more efficient by availability of the distributed ledger.

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 at the start, with potential for some support functions if the marketing and sales support teams have grown large enough. We assume 90% of these costs can be avoided.

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

[15] Typically, claims costs account for about 65% of insurance premium income (e.g http://www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/Insurance_Risk_Benchmarks_Research_Annual_Statistical_Review.pdf), with expenses making up the rest up to the point where typically most of the premium income gets spent (e.g. https://www.verisk.com/siteassets/media/downloads/insuranceresultsreport2016q4.pdf).

Therefore, combining the above estimates, we expect to reduce the non-commission frictional costs by approximately 72% compared to a traditional insurance company. Converting it back to a percentage of premium income, this equates to a further 18% of premiums accruing in the mutual for the benefit of the members.

Note that the above discusses a comparison to established insurance companies assuming comparable products and sales channels applying to Nexus Mutual. Initially, the cost base is likely to be reduced further due to the niche nature of the product resulting in pre-incurred product development costs and a fully digital marketing approach aimed at the blockchain community.