ABSTRACT

Insurance is often regarded as either being a mutual organism, where everyone is going to the same place, together; or an adversarial system where the objectives of policy holders and shareholders stand opposed.

We want to demonstrate that blockchain technology enables us to create ecosystems of cooperation, where individual objectives can be mutually aligned, so instead of *everyone going the the same place* we can all *go in the same direction...* towards a better financial futuer.

To achieve this outcome, we propose a hybrid mutual–investment model, where we create an ecosystem for everyone to mutually benefit, even though we all aren't in the same space.

WHAT IS INSURANCE?

At its core, insurance is simply an agreement or contract between two parties, where one party takes on the risk of the other for a fee. This contract is typically represented by a policy and the policy holder receives protection against an unintended outcome, such as loss or damage, which is carried by the insurer (underwriter). The insurer receives a fee for taking on this risk, and is under obligation to carry the loss in the event of a claim.

Insurers leverage risk aggregation and risk pooling to mitigate the risks they carry and to provide more attractive fees (insurance premiums).

1. RISK AGGREGATION AND RISK POOLING

If we lived in England, specifically London, during the 17th century as investors, we would have had ample opportunity to invest in merchant ships trading with British Colonies and the New World. These ships would sell goods from Britain to the colonies and return with exotic treasures, such as tobacco and pineapples, that made very lucrative sales under British high society.

However, the risks involved were significant, as storms, pirates, mutinies, colonial revolts and numerous other unintended events could completely eradicate not only our profit margins, but our entire investments.

AGGREGATION

The first strategy to effectively deal with these risks is to spread our investments over a number of ships or share our risks with other investors (risk aggregation), as the chances for all of them to encounter such unintended events are significantly reduced.

For example, if the average merchant ship has a 10% (1 in 10) chance of complete loss then ten merchant ships would have a mere 0.00000001% (1 in 10,000,000,000) chance of complete loss.

However, the chance for a single loss at this point is practically guaranteed, for the moment we pool 7 ships each with a 10% chance of loss we get to a 94.8% chance for a single loss, and at 10 we are guaranteed that one ship will not make it, and a further 60% chance that a second ship will be lost as well.

POOLING

The second strategy involves dealing with these "guaranteed losses" by pooling our risk, as we do not know which of the ten ships will not make it, only that we can reasonably expect at least one loss and likely a second.

The contributions we make must be sufficient to cover the expected losses for this voyage. Thus, in the event the loss occurs we reimburse that particular investor from the pool.

2. UNDERWRITING PROFITS AND LOSSES

However, not every voyage will yield predictable losses, as statistics is a science of historic averages and of predictive probabilities, not an account of current events. Thus it turns out that our first voyage into the New World was a spectacular success as all ships have returned safe and sound with cargo and profits in tow.

One ship has suffered minor storm damage and is repaired from the pool utilizing only a fraction of the funds. At this point we may liquidate the pool and disburse the surplus (underwriting profit) to each policy holder proportional to their initial contribution (dividends) or reallocate the funds for a subsequent voyage requiring each policy holder to only contribute the calculated difference (premium adjustment).

Sadly, our next voyage turned out less fortuitous and we lost three entire ships, along with their crews and cargo to a nasty hurricane. This time around our pool does not have sufficient funds to honour all claims and a loan must be made with a creditor to cover the shortfall (underwriting loss). For our next voyage the premiums are adjusted not only to take the greater risk into consideration, but also to cover the shortfall and commensurate debt the pool has incurred.

3. MUTUAL VS STOCKHOLDER INSURANCE

Unfortunately, the losses we suffered during our last voyage has left some investors in a position where they cannot afford the premiums and consequently withdraw their policies. This leaves our pool severely underfunded and hugely impact our premiums as our aggregation benefits are diminished. In order to address our funding requirements we vote to demutualize the insurance and turn to a stockholder model.

The insurance would no longer be "owned" by the policy holders, we will attract additional investors just for the purpose of underwriting. The insurance now becomes stockholder owned and any underwriting profits or losses in the pool are exclusively for stockholders to benefit or bear.

4. FLOAT

One of the largest new stockholders is an investment bank and they leverage their considerable experience to conclude a plan to augment underwriting profits. Essentially, the seven remaining ships still have a mere 0.0000001% (1 in 10,000,000) chance of a complete loss and a 94.8% chance of a single loss (thus we can reasonably expect it) for which a claim will be paid out. However this claim will only occur at the end of the voyage, which takes approximately 12 months.

The insurer technically owes that claim to the claimant, but being a future event there is no way to know who the claimant may be, there is also a very small chance that there may be no claim made after the voyage concludes.

Thus, once the contributions are made for this voyage, the pool will be invested in another investment instrument to yield a profit while we wait for the voyage to conclude and a possible claim to be made. The float is thus the amount of premiums received and the period between receiving them and honouring claims against their active policies.

5. RISK OF MORAL HAZARD

Calculating each policy holder's contribution would be a straight forward matter if all things were equal, but in reality it rarely if ever is. Each policy holder may invest different amounts in different type of ships (Carrack vs Barquentine) with different loads of goods going to different target destinations presenting wildly varying risk profiles. As long as we are aggregating our risks and pooling our resources with other investors and policy holders we are at the risk of moral hazard where one party deliberately acts to the detriment of the others. One policy holder may deliberately withhold information pertaining to faced risks (such as suffering mast damage during the previous voyage), another may deliberately attempt to trade in riskier waters simply because of having the insurance policy, yet another may realize their investment is unlikely to turn a profit and then take deliberate action to ensure a loss so that they can make a claim against the pool in order to at least recover their investment. External investors (stockholder) may endeavour to pay as little claims as possible in order to maximise underwriting profits, unexpected events resulting in loss may be reclassified as an expected event not covered by the policy.

BEHAVIOUR MODIFICATION

Some actions pertaining to moral hazard can be regulated against (and often is), such as deliberately withholding relevant information (which may void a policy)and taking deliberate action to cause loss for purpose of filing a claim (insurance fraud). But, subtle psychological interactions such as acting less risk averse due to having an insurance policy cannot be regulated against. For these, insurers need to engage in behaviour modification by providing policy holders with incentives for continuing risk averse actions.

Many insurers engage in two forms of behaviour modification, namely disincentivising undesired behaviour and incentivising desired behaviour.

DISINCENTIVISE UNDESIRED BEHAVIOUR

With our ship insurance we may implement a mechanism that requires each ship owner to carry a small part of the risk, thus if they make a claim they must stake it by "paying up" this associated risk. This is known as an excess payment (paying for the additional risk) and serves a twofold purpose, 1) it serves to lower the overall premium and 2) it serves as a disincentive for arbitrary claims, as it requires this out of pocket payment from the policy holder when a claim is made.

INCENTIVISE DESIRED BEHAVIOUR

As part of our now stock based insurer, we may also elect to implement a mechanism to incentivise ship owners to not make unnecessary claims by allocating a small portion of the underwriting profits and/or investment income (from the float) to policy holders that make no claims over the course of the respective journeys (predefined periods), effectively refunding them a portion of the premiums paid. We may even structure this in such a way that this payout is proportional to the pool's profit performance, further incentivising the principle of mutuality.

Our objective with behaviour modification is to create a situation where there is greater benefit in honouring the principle of mutuality, than there is to game the system for illegitimate individual gain.

So what do these premiums entail? Firstly, the insurance company accepts the risk of loss from a policy holder at a determined price of risk (risk premium). The overall policy premium must further also make provision for additional expenses such as administrative costs, operational overheads, possible agent commission fees and any other business related expenses. The net premium is the insurer's revenue and is used to fund the risk based capital pool in order to maintain sufficient liquidity to pay any outstanding claims.

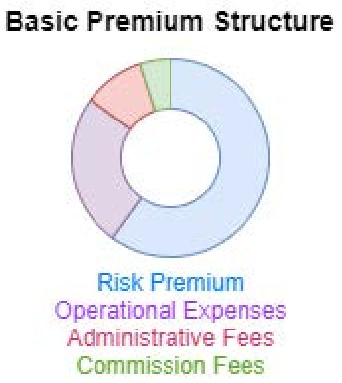
6. REVENUE MODEL

Now that a number of journeys have concluded and a fair number of seasons have passed, some of us have transformed from being shipping and trading investors to being insurance investors. At this point our little trading insurance operation has grown into somewhat of a big deal. We have transformed from an informal group of shipping and trading investors meeting in a London coffee shop, into a full blown insurance operation (this is actually how Lloyd's of London originated). We leverage two separate revenue streams, and with prudent management and underwriting practice we can ensure that both streams are individually profitable. In fact, we may then regard this operation as being paid to borrow and invest money (as Warren Buffet wrote in a famous Berkshire Hatthaway shareholder letter). To understand this statement, let's take a closer look at the detailed revenue models.

PREMIUMS

Premiums collected from policy holders are the starting point for all revenues earned by all types of insurance operations. So what exactly do these premiums entail? Firstly, our insurance company accepts the risk of loss from our policy holders at a determined price of risk (risk premium). The overall policy premium also includes additional fees to make provision for additional expenses such as operational overheads, administrative costs, service fees, possible agent commission fees and any other business related expenses. The net premium (the remaining portion after all these expenses) is our first revenue stream and is used to fund the Risk Based Capital Pool from which we must pay any outstanding claims.

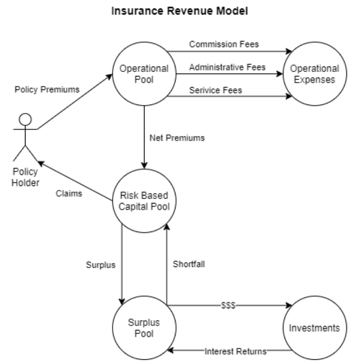
Basic premium structure here



INVESTMENTS

If our revenue earned exceeds the claims, we are making an underwriting profit. If the pool keeps growing it may far exceed the amount of funds required to honour outstanding claims (surplus) and we will be able to invest this in interest earning instruments, our second revenue stream. Further to this, we have the float (the period between receiving premiums and paying claims) that can also be invested, and this is what Buffet refers to as “borrowing” money: as the insurer is actually under obligation to pay any legitimate claims against the policy, but is free to invest any premiums received until a claim becomes due and payable. Thus, if our first stream is profitable, we are technically being paid to borrow money (the float) and invest it to generate even further (and often greater) revenues.

Insurance revenue flows here



7. CONCLUSION

The above time traveler’s journey gives a good overview of the insurance industry and some of the key concepts and terms used in the domain. However, there are lots more to know and to learn about the industry and a great depth to each of the concepts eluded to in this article. Use this as a starting point and delve deeper using online resources and industry publications. You will be amazed by what you can be lear from public domain resources, even within such a protective industry.

SURE X IN A NUTSHELL

- Built on the Binance Smart Chain network.
- Users can buy or coverage for items such as technological devices (phones, cameras, computers etc) — stakers split profit and yields as a reward.
- Purchase coverage using stablecoins.
- Coverage funds are invested on platforms such as Aave, Curve, Balancer, etc.
- Coverage holders can place claims easily on the SureX Platform.
- Tribunal claims mechanism to ensure every claim is assesed fairly.
- SRX tokens govern the platform.

VALUE PROPOSITION

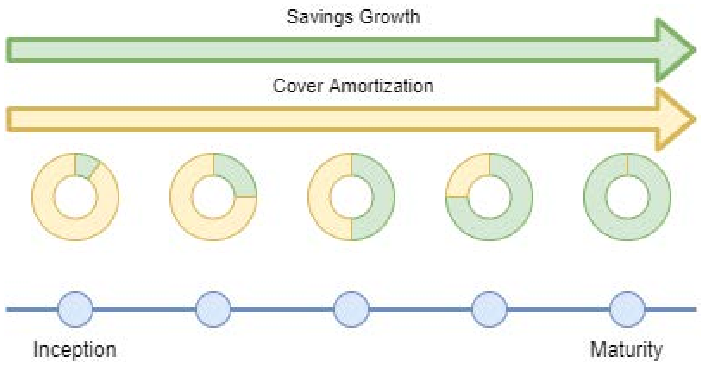
1. UNIQUE DECENTRALISED SAVINGS COVER

- Worried about your expensive equipment?
- Saving towards your next upgrade?
- Paying too much?

Join SureX Mutual. We have each other covered.

2. HOW IT WORKS

Mutual provides members with a hybrid savings insurance policy. This policy provides both insurance coverage, as well as a savings instrument that grows toward a specific target over a specific period. As the savings grow, the risk is reduced, and so too the cost of insurance, because the policy covers the outstanding balance of the savings target instead of the associated equipment.



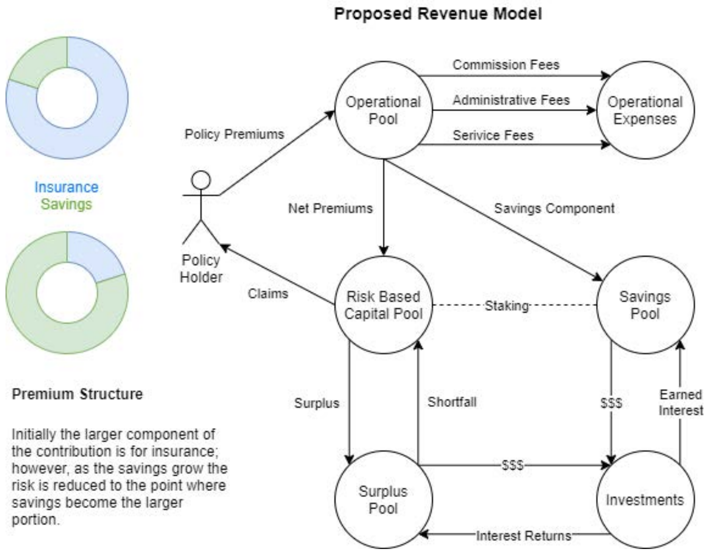
BUSINESS MODEL

1. OVERVIEW

REVENUE MODEL

Our mutual insurance model provides members with a hybrid savings insurance policy. This policy provides both insurance coverage, as well as a savings instrument that grows toward a specific target over a specific period.

As the savings grow, the risk is reduced, and so too the cost of insurance, because the policy covers the outstanding balance of the savings target instead of the associated equipment.



Initially the larger component of the contribution is for insurance; however, as the savings grow the risk is reduced to the point where savings become the larger portion.

STAKING

The staking of tokens form the basis of our governance and claims procedures. This gives the system the mechanism to either reward or punish behaviour. This ensures that shareholders engage in governance actions and honour the principle of mutuality and dissuade them from acting in their own selfish interests.

Savings Pool

This additional savings pool is pertinently not ours, but the policy holder's. It is part of our smart contract though, and thus under our control (like a custodian account).

The policy holder's premium essentially gets divided into two parts: one part goes into the risk pool and the other part goes into the savings pool.

RISK HANDLING: FIXED AMORTIZATION

Let's look at our professional photographer Kate: if she needs to replace her equipment in 3 year's time, and she insures it for $3000, we don't actually insure the equipent that she wants cover for, we insure her savings deficit.

Here a model of fixed amortizaton is applied as we innitially insure the $3000 as her savings will have a zero balance, but as the policy matures the savings grow and the deficit shrinks.

TYPES OF COVER WE OFFER

We insure against loss or damage. We can grow our offering as the product matures.

2. GOVERNANCE

The two primary functions of our governance model are:
1. Electing claims assessors
2. Making investment decisions regarding the funds' investments, surplus, profits and float.

In order to be considered for the role of an insurance administrator (will be limited to a legal jurisdiction, geographical area or number of wallets owned), users can submit a Request for Bid (RFB) in the form of staked tokens. If they are not successful in their bids, the stake is released, and if they win the bid, their stake is put into escrow.

If the claims administrator approves bad claims, and these claims are identified, the stake bears the cost and not our pool.

If their stake diminishes below a safety threshold, their contract is terminated and they cease earning administrative fees and revenues from the associated policies, and a new bid is opened.

WHAT IS A "MEMBER"?

Users are seen as members of the insurance community. We want to incentivise long-term policy investments for members to become benefactors.

WHAT IS A "BENEFACTOR"?

That is when a member's (Alice) contribution become the underwriting for the claim of another member (Bob), thus making Alice the benefactor of Bob's policy risk premium.

3. CLAIMS

STAKING REQUIREMENT

Users are required to stake a certain amount of tokens in order to file a claim. These tokens will automatically be staked from their savings account and they will have to deposit any deficit if needed.

If the claim is successful, the stake is released and the claim is paid from the risk pool. If the claim fails, the stake is "taxed".

This reduces the chances of fraudulent or just incompetent claims, since the entire stake or the administrative portion therof is lost to the claimant.

The above mechanism will allow us to deal with claims on policies associated with wallets that have no standing history, risk or credit score.

IMMEDIATE COVERAGE AND CLAIMS

Well-known wallets such as those with a good history and good risk score, are allowed to open a new policy and be eligible for immediate cover without the claim waiting period.

This differentiates us from and makes us more competitive than traditional insurance products on the market.

Other users can also qualify for immediate cover if they're willing to stake a larger amount of tokens (at a risk to them).

CLAIM WAITING PERIOD

Brand new accounts without a good standing history or the minimum staking balance requirements are subject to a claim waiting period and are not eligible to file a claim immediately.

PROOF OF LOSS

Any claim should provide a proof of loss, that will not be recorded on chain, for privacy reasons. This can be done via Zero Knowledge Proof.

A zero knowledge proof is a mathematical construct that does not reveal any additional information to any party when proving a claim. This is recorded as a data hash signed by the appointed assessor.

The proof of loss must be confirmed by the assessor and then by determined to be within the scope or outside the scope of the policy, whereupon the claim is approved or denied.

Thus the approval or denial of the claim must be contained within the zero knowledge proof. This ensures we have a non-repudiation claim either way without carrying any private information on chain.

It is critical that the proof of loss must be provided in a format where the zero knowledge proof can be easily verified, meaning care must be taken to ensure an idiomatic deterministic mechanism to provide and verify proof of loss.

We will define a protocol to establish this, as any variation will result in different hashes being created, negating the validity of a zero knowledge proof..

SECURITY

It's notable that the system is resistant to certain attacks for instance the dreaded Sybil attack. Attackers have nothing to gain from multiple identities because being passive in the ecosystem does not reward one, and being malicious actually costs money. Following the rules is the most profitable in this instance.

4. DISPUTES

CLAIM ASSESSMENT TRIBUNAL

Claims will be assessed via a tribunal system of 3 parties. If the decision is unimous the decision to pay or withhold paying is upheld and uncontestable. If however there is a split vote, the decision is contestable.

If there was a denial of claim, only the policy holder can contest the decision by staking an additional amount of tokens.

If there was an approval of a claim, any other staking member can contesting it's validity. We will include a mechanism for assessors to use this as a type of peer review.

If the vote was wrong, the assessor's stake is burned to make recompense to either the fund or the policy holder.

This ensurs that both false positives and false negatives carry risk. A false positive is any claim that was paid that should have been denied, and a false negative is any claim that was denied that should have been paid.

USE CASES

The following model illustrates how it is more profitable to the policy holder to hold on to the SRX tokens to realise their growth potential, such as to underwrite profits or as investment income.

DOES IT THOUGH? AM I GETTING IT RIGHT?

1. REQUEST FOR COVER

INPUTS:

target savings amount (min: $500, max: $5000)
period in months (min: 12, max: 36, inc: 6)
initial deposit (< target)

OUTPUTS:

Policy Overview (target, period, deposit, premium)

SUPPORT FUNCTIONS:

Risk Free Return (to calculate savings interest)
Calculate Risk (risk factor for particular requesting address, age, stake, history, etc)
Calculate Premium (risk amortization function that amortizes risk vs savings growth over period and determines fixed policy payments)

2. ACTIVATE POLICY

INPUTS:

target savings amount (min: $500, max: $5000)
period in months (min: 12, max: 36, inc: 6)
initial deposit (< target)

OUTPUTS:

success: active policy
failure: error (e.g. insufficient funds for deposit, declined, etc)

SUPPORT FUNCTIONS:

Risk Free Return (to calculate savings interest)
Calculate Risk (risk factor for particular requesting address, age, stake, history, etc)
Calculate Premium (risk amortization function that amortizes risk vs savings growth over period and determines fixed policy payments)

3. POLICY PAYMENT

INPUTS:

payment authorization

OUTPUTS:

success: active policy (update status)
failure: adjust policy (update status, adjust contributions)

SUPPORT FUNCTIONS:

4. REGISTER CLAIM

INPUTS:

claim amount (< target)
stake authorization (authorized stake is taken from savings, if savings balance < stake authorize from wallet)

OUTPUTS:

success: claim registered and assessor assigned (claim status: awaiting proof of loss)
failure: claim registration error (e.g. invalid claim amount, insufficient stake, etc)

SUPPORT FUNCTIONS:

Select Assessor (e.g. from FIFO queue based on staked amounts)

5. SUBSTANTIATE CLAIM

INPUTS:

hash of proof of loss (by claimant, proof of loss provided to assessor through off chain features in product front end)

OUTPUTS:

claim status update: awaiting approval

SUPPORT FUNCTIONS:

6. VERIFY CLAIM

INPUTS:

hash of claim details signed by assessor (ZKP-HMAC, must match hash provided by claimant)
assessment outcome (approve / decline)

OUTPUTS:

approve: claim stake released, claim amount payout
declined: claim stake consumed, claim closed
both: portion of assessor stake locked for period (e.g. 30 days)

SUPPORT FUNCTIONS:

SUREX TOKEN ECONOMICS

1. WHAT DOES THE SRX TOKEN REPRESSENT?

The SureX Token (SRX) repressents share benefit from the profits derived from both policy premiums and investments. Does it though?

The SRX Token is a Continuous Utility token.

2. WHAT MAKES SRX A UTILITY TOKEN?

The main characteristic of a utility token is when the token has functionality within the ecosystem which adds more value to it, than it would have had if the user were just HODLing the token and not using it.

The following aspects assures it as a utility token, when users can:

- stake into MCR pools to underwrite risk of others
- buy policies
- make investment decisions with regards to the underlying value token
- stake their tokens to make claims assessments

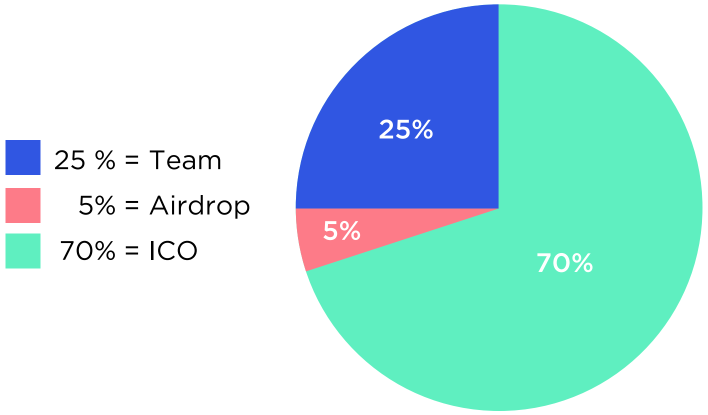
SRX is therefore a **Continuous Utility Token** whereby users can lock value into our ecosystem in order to participate in our available products and services.

3. TOKEN ALLOCATION

We will launch an ICO (or BCO) to serve as a kickstarter for our risk pool. Additionally the funds will be used for business development, operations, legal, technical, administration and marketing.

The breakdown of what the capital will be allocated to is as follows:

70 %	Sold in the ICO
25%	Reserved for the Team
5%	Released via Airdrop to the community



4. BONDED CURVES

Bonded curve tokens are smart contracts with a custom-tailored formula with mint and burn functions. Once launched, users can buy and sell into the curve. Buying pushes the price up along the curve whereas selling pushes the price down along the curve. The SureX Token will be bonded to a simple 10% buy/sell curve in linear progression. This is usefull for things like our capital pool.

Therefore we don't have a fixed token supply.

PROPERTIES OF BONDED CURVE TOKENS

- Limitless supply. There is no limit to the number of tokens that can be minted.
- Deterministic price calculation. The buy and sell prices of tokens increase and decrease with the number of tokens minted.
- Continuous price. The price of token n is less than token n+1 and more than token n-1.
- Immediate liquidity. Tokens can be bought or sold instantaneously at any time, the bonding curve acting as an automated market maker.

The adaptive supply of a Continuous Token (recall that it is newly issued when purchased and removed from circulation when sold) is a unique and enabling feature which allows for supply to adjust to demand and for Continuous Tokens to be continuously available for purchase at predictable prices. IS THIS TRUE FOR SRX?

HOW DOES A BONDED CURVE TOKEN MAINTAIN VALUE?

We may have ample supply in our capital pools but it may still lack value. Good liquidity protocols should be designed to ensure both supply and value.

Bonded curve tokens leverage seigniorage shares and provide incentive for not dumping the tokens or engage in pump-and-dump schemes.

5. RISKS: FRONT RUNNING ATTACKS

Front-running attacks occur when the one makes profit out of performing a transaction before another participant while knowing about such a transaction in advance.

SOLUTIONS

Transaction Counter Method

An attacker's aim is commonly to send their own transaction before the victim's transaction is executed. We can empoy a transaction counter in our smart contract to prevent this from happening.

Whenever a state-modifying transaction occurs in a smart contract, we can increment a universal transaction counter by one. So when sending a transaction that we believe could be front-run, we will also send a **transactionCount** value (which dictates what the transaction counter's value should be when the transaction is initiated).

If the transaction counter's value is NOT equal to the value we've specified, the transaction reverts.

The downside of this method is that if any other transactions increment the counter before ours, ours may revert, frustrating our users since their transactions could revert.

Gas price limiting

Another solution would be to limit gas prices, so nobody can create a front-running advantage.

This requires very little overhead (which saves users on gas-fees). In Solidity, making a modifier called

gasThrottle is a solution, this would check that the gas cost for the transaction (with the function call **tx.gasPrice**) is less than or equal to an amount we will call MAX_GAS_PRICE.

That would prevent people from seeking preferential treatment from miners to a certain degree, by ensuring a higher gas fee. It still allows them to jump ahead in the queue, but limits how much they can push to do that.

The problem with this strategy is that it needs to be supervised in perpetuity. Gas costs on Ethereum are highly variable. What might be a reasonably “high” gas cost today may be far too low/high a month from now. If your MAX_GAS_PRICE limiter is too low, your dApp may be frozen, as no transactions with such a gas price will be accepted by miners on the network.

Malicious miners can still choose not to order transactions by gas price, so they themselves can do front-running of their own.

CONCLUSION

Still need to write something here.

SUREX INSURANCE

A peer-to-peer insurance offering on the Binance Smart Chain ?

BILLA COETSEE, CAPTAIN ZIKA, ANDY KIBZ, MARCELLE LABUSCHAGNE

COVER ART HERE

SURE**X**

17 April 2021

TABLE OF CONTENTS