**Cryptinsure**

Situation

* Pending transaction – has anyone ever felt the fear of a pending transaction – the sheer terror of your money being in between one wallet and another
  + During this time, you don’t know whether your money will reach your destination or not
    - You check through the transaction address letter by letter, ensuring that you have copied it in correctly
    - The fear you feel is real – it is very easy to leave a letter our, or incorrectly write a 0 as O
* Blockchain public addresses are long strings of numbers that are difficult to write out
* Cryptocurrency is still in it’s infancy – the UX is low down on the priority list of things to improve upon
* Many potential users – such as retail users or small businesses are not confident with technology and want reassurance when using a new technology that their money will be safe
* Current best practice with cryptocurrency payments is to send a small transaction first, then the larger one, in order to ensure it is being sent to the correct location

Problem

* Copying an address, or using a QR code can lead to mistakes being made
  + A character can be left out of an address or changed
  + A QR code may have a blemish on it due to a dirty screen or wear and tear in real life
  + A mistyped address for a wallet with an ENS name could also mean that ether would be lost
* Other issues include putting in an address for another cryptocurrency (such as may happen with an exchange e.g. Shapeshift
* Fraud is also endemic in the cryptocurrency community – fake address for ICOs or payments may be given, people may change the QR code on a website etc **(find Sandeep’s article)**

Solution

* By implementing a smart contract in which an insurance fee will be taken, users can pool their risk when making important transactions – in our example, we will be looking at the use of a mis-typed address.
* A user can choose to insure their transaction for a certain fee, e.g. 1% of the transaction
* When the cryptocurrency is transferred to the wallet address, another transaction is also made to a smart contract with the 1% transaction fee and the ID of the transaction just made that it refers to
* If the user subsequently realises that they have put in an incorrect address (in this case, an address with 1 incorrect character), they can then make a claim
* In this claim, they will put in the transaction ID for the mistaken address, and the address that they meant to send the money to
* The smart contract will then compare the addresses against each other – if there is a difference of 1-5 characters, then the smart contract will pay back the claimant

Evaluation – why does this help?

* It means one of the big problems of cryptocurrency – that of mistaken payments can begin to be solved
* For small businesses beginning to use cryptocurrency, it can ensure that their payments have a reduced risk of sending to the wrong place

**Fraud** – How do you prevent people from just sending money to their friend or themselves, and then pretending that they meant to send to another address?

* Rather than sending money back to the original sender, the claim would be sent to the intended recipient. This way, it would prevent one from committing fraud – the likelihood of someone creating two wallets with public addresses which are quite similar is extremely small and would be economically unviable
* The number of transactions, the period of time over which these transactions appeared and number of claims made etc, could be fed in and determine how much the premiums will cost, or how much the smart contract will pay out
* As Identity uses on the blockchain become more prevalent, people’s reputation as blockchain users will become a bigger part of how they interact with others – a wallet with an identification could have a ‘trusted user’ token that is given to the insurer each time they make a claim and helps to define the credit level.

What is the need for the insurance industry here?

* At the basic level, the smart contracts would run themselves.
* Insurance companies would still be needed in order to underwrite the risks and determine premiums needed per transaction or how much of a payout would be required.
* As more complex scenarios develop – e.g. customers being defrauded, customers with low reputation making large claims, real people could be brought in to make judgements that computers are unable to.
* How to build in profitability?
  1. Once Ethereum moves to Proof of Stake – Pooled Ether in smart contracts could be used to stake Ether (risks include staked Ether being locked into the staking contract when needed for a claim)

Future use cases

* Long term – this kind of smart contract could be used for other use cases as well
  1. E.g. a trusted customer, ie someone who has made over 100 payments to the insurance contract, has been defrauded – they sent their payment to an address but have realised that it was a fraudster’s account details
     + Due to their high reputation, they are able to make a claim for this fraudulent activity and receive back a portion of the payment
     + At this stage it may require claims analysts and others in order to ensure that the claims being made are credible

How often does this happen?

General usage is that you do a small transaction

What’s insurance’s role in this?

Underwriting and risk

Payment?

Other possible use-cases

Applicability to fraud