PEER TO PEER INSURANCE ON AN ETHEREUM BLOCKCHAIN

General Consideration of the Fundamentals of Peer to Peer Insurance

Joshua Davis
Joshuad31@yahoo.com

ABSTRACT. Ethereum is a blockchain 2.0 technology capable of providing a platform for the operation of smart contracts. Whereas Bitcoin functions as a currency this new technology would function to allow software code to hold, transfer, receive, or spend digital assets. The Ethereum blockchain is a decentralized ledger governed by computer protocols that facilitate, verify and enforce contracts. It is within this blockchain protocol that smart contracts are negotiated. In theory this technology could allow for the creation of DAOs Decentralized Autonomous Organizations which are corporate entities that possess no full-time human employees while still being able to perform all the same functions as traditional corporations. Insurance is an obvious first use case of truly programmable money and provides a great opportunity for smart contracts to demonstrate the extent of their capabilities.

I. INTRODUCTION

The current trend of the sharing economy is seeking to decentralize every type of service into a peer to peer model. We have seen this with companies offering distributed taxi and hotel services such as Uber and Airbnb. Technologies such as the smartphone capable of running apps which connect riders with drivers or renters with home owners have been a powerful platform which has enabled this innovation. These services are now more convenient and are more price competitive than their traditional counterparts while simultaneously providing income opportunities to people that didn’t exist previously.

Can these models for innovation within the transportation and travel industry be applied to revolutionizing financial products such as insurance? Once the initial barrier of finding a way to trust someone you don’t know is overcome these services seem straightforward enough. Offering to drive someone to the airport or to let someone stay overnight in your house doesn’t seem to break any laws or be governed by any regulation. Insurance on the other hand is a very different picture. There are laws preventing someone in your neighborhood from going door to door suggesting that everyone contribute monthly to a single pool of money which would then be used to pay for expenses in the unfortunate event any of the members were involved in an auto accident.

Both the taxi and hotel industry are regulated but not to the same degree as the insurance or banking industry. But this doesn't seem to have stopped people from building a currency around just about anything even the iconic image of a shiba-inu. It is not currently illegal in the US to mine dogecoin without a license and to use it to pay for something other than purchasing national currency (Wikipedia entry for History of Bitcoin, n.d.), although it did become illegal in 2009 to produce and use liberty dollars as a currency (Wikipedia entry for Liberty Dollar, n.d.). So at best cryptocurrencies are allowed to operate in a regulatory grey zone. Can crypto-contracts for insurance also be allowed to operate in the same regulatory grey zone?

The potential power of blockchain 2.0 platforms promises that outsiders with far less capital could potentially build financial instruments. Access to capital would no longer be a major hurdle limiting the ability for people to innovate. Smart contracts can provide just as much utility as financial instruments offered by traditional corporations with millions or billions of dollars in capital. Potentially these platforms could create a level playing field to those people who would like to participate in innovating the space of financial contracts but have very little financial backing or support to create the massive infrastructure of a traditional corporation. If someone was able to demonstrate that their new financial innovation was able to work as a test case among a small community of people that could then serve as a foundation allowing smaller players to enter the field of markets such as insurance.

Just because cryptocurrency is able to operate in a grey zone does not necessarily mean crypto-contracts will be granted this same privilege. Those that wish to innovate in this space need to make a strong argument that new financial services created on a blockchain should be regulated differently than traditional financial services. Is it possible to find a model in place today which might allow us to begin to make the case for crypto-contracts as unique financial products which should enjoy unique privileges?

II. LENDING CLUB MODEL

One existing model for regulation of peer to peer insurance may be seen in peer to peer lending clubs known as a ROSCA (Rotating Savings and Credit Associations). Advocates fighting for the rights of poor and minorities have successfully convinced some regulators that exceptions in the law should be applied to peer to peer lending groups. Regulatory exceptions have been provided to lending circles such as tandas and cundinas not merely because they were acknowledged as being beneficial to society but because *fundamentally their nature was shown to be different than traditional commercial lenders*. This example gives us insight which might be applied to peer to peer insurance. How was peer to peer lending shown to be fundamentally different than commercial lending? On what basis was peer to peer lending granted regulatory exceptions for laws which apply to commercial lenders? A clearer understanding of the regulatory environment for existing peer to peer financial instruments will allow us to better make our case for the optimal amount of regulation for this new technology.

Regulatory compliance comes with a cost. Lending clubs typically lack the resources to meet the same regulatory standards as traditional loan origination entities because they are run by the poorest members of society who cannot otherwise find the means to have credit extended to them. Thus lending clubs traditionally operate outside of existing law. The “regulation” which serves to protect consumers in these cases is the strong ties of a local community and the practice of only entering into a lending circle with those whom you are able to trust. The social pressures associated with nonpayment on these types of loans assures a very low default rate.

In the event that defaults do occur the structure of the lending club assumes that the cost of such defaults are shared among all honest participants thus limiting the loss to any one member. The size of the monthly payment each individual is capable of making and the number of people in a group also places a relative cap on the size of losses which are possible. This limitation also restricts the degree to which profit from theft is possible thus placing a limit on the incentives that might exist related to fraud. Costs associated to the loss of social capital within the community would therefore seem to always be greater than the gains one might receive by fraudulent activity.

The system described above differs greatly from commercial lending in the following ways:

1. Commercial borrowers receive loans from organizations not individuals they personally know.
2. Commercial lenders extend loans to individuals on the basis of credit histories not community ties.

3. The degree of risk incurred by commercial lenders is higher because loan amounts are higher.
4. Lenders raise capital to issue loans rather than capital being acquired on an as needed basis.
5. Lenders manage pools of capital large enough to incentivize fraud towards investors with whom they have no social bond.

Thus regulation to protect lenders who are assuming a higher risk from individual borrowers and to protect investors who are subject to the risk of greater losses from lenders seems perfectly reasonable. But when this regulation is applied to lending clubs it doesn't seem to make sense for the following reasons:

1. People who find themselves excluded from the benefits of the traditional lending system are being subject to its governance.
2. People who seek to reconcile disputes within their local communities are told that extralocal rules preclude their ability to settle differences between individuals.
3. Non-profit organizations which hold no capital risk are being subject to the same standards as for-profit organizations which manage large pools of capital.
4. Loans for amounts that typically max out at values 40 times smaller than your average mortgage loan are being given the same scrutiny as larger debts which carry greater risk to its participants.
5. Such regulations fail to consider the low rate of default already operating within the existing system and the degree to which losses are relatively negligible when compared to commercial lending.

Commercial banking regulations when applied to lending clubs seem equivalent to the requirement that a personal loan made between friends require the same documentation necessary to obtain a credit card. Should a loan default for 10 dollars to buy a pizza be given the same scrutiny as the default on one's student loans? Traditional lending laws do not seem to be a good fit for peer to peer lending. This is what the state of California seemed to affirm with its passage of legislation SB-896. The legislation establishes a licensing exemption within the California Finance Lenders Law, which will make it easier for nonprofit organizations to expand their lending (Day, n.d.). This legislation gave greater freedom for lending clubs to operate with fewer regulatory requirements thus fewer costs associated to legal overhead and licensing.

Can the Ethereum community make a credible case that the nature of peer to peer insurance provided by a DAO (Decentralized Autonomous Organization) smart contract is fundamentally different than traditional insurance products managed by traditional insurance companies? If so can the case be made that peer to peer insurance qualifies for a similar reduction in regulatory and legal overhead such as enjoyed by lending clubs? We need to clearly define what unique attributes qualify a smart contract as a peer to peer insurance provider to begin to answer these questions. By considering the fundamentals of how an insurance smart contract would be implemented in Ethereum we can see what distinguishes these financial instruments from traditional insurance providers.

III. IMPLEMENTATION IN ETHEREUM

1. **Ownership of a mutual insurance DAO creates a community around the policy.** One possible way to organize an insurance DAO is by treating all the individual policy holders as shareholders**.** DAOs can exist such that the policy and its pool of premiums is not under the control of any one person or select group of people (i.e. board of directors). The DAOs pool of capital belongs to everyone who has a policy and only a majority or super majority can decide to use the capital in the pool for anything other than paying out claims. Any float which is accrued from the investing of premiums would be paid out as rebates to all policy holders. This might give insurance DAOs the basis with which to claim non-profit status unlike traditional insurers which operate on a for-profit basis.

2. **Developers of an insurance DAO don't issue or deny policies**. The first basis for claiming a DAO operates on a peer to peer insurance model is policies are awarded on a peer to peer basis. Unlike traditional insurers it is the policy holders which approve applications for new policies without third party assistance. Not only is such assistance not required, the DAOs programming should expressly forbid such intervention especially by developers or their agents. Peoples initial reaction to this model is one of doubt and reproach because they hold the following fallacies to be true:

   A. Identity verification cannot be easily automated

   Fallacy: Policy holders and DAOs have no way to mitigate a Sybil attack due to the ease of creating false online personas. The arduous task of verifying identities that traditional insurers undergo cannot be automated.

   Reality: Just as identity verification comes at a cost there are also costs required to forge identities. Securing identities is not something evaluated with 100% confidence but with relative degrees of confidence given the opportunities and incentives for people to commit identity fraud. The fallacy people commit when evaluating identity verification is related to matching up the appropriate degree of certainty (greater certainty = greater costs to verify) with the costs associated with fraud. The question that needs to be evaluated is not “can I verify this identity?” but rather “how much does it cost me to verify this identity relative to the asset I am protecting?” and “relative to the payout of a claim and the potential costs associated with fraud how expensive is it for an attacker to forge a credible identity?”

Creating a policy that only insures auto glass is not equivalent to creating a policy that insures every make and model of vehicle up to the full cost of a complete replacement in addition to any harm or injury to the driver, passengers, other individuals and other property. A few interesting facts:

- In 2012, the average auto liability claim for property damage was $3,073; the average auto liability claim for bodily injury was $14,653 (ISO, a Verisk Analytics company).
- In 2012, the average collision claim was $2,950; the average comprehensive claim was $1,585 (ISO, a Verisk Analytics company) (rmiia.org, n.d.)
- Average estimated cost of replacing a windshield is less than 350$ irrelevant of the make and model of the vehicle.

One’s strategy for identity verification for a policy covering auto glass therefore need not be equivalent to a policy for complete auto coverage.

For most early insurance DAOs with humble goals (think auto glass) what is a sensible approach to identity verification? Use established online reputation systems tied to social media. Then have the DAO leverage human intelligence in combination with social media profiles to prevent Sybil attacks. If you think it’s easy to create fake Facebook accounts that seem real to human beings then you probably will not find this argument persuasive. Robots can be created to write convincing profiles and people can be trained to spot robots. It is interesting to think there are evil masterminds out there who employ robots to create hundreds of fake Facebook accounts which dialogue with themselves over the course of several years to create the illusion of real identities. Then presumably such masterminds would create several shell companies for auto glass repair and open hundreds of policies. These fake policy holders would presumably pay a few months of premium payments, then would open up costly claims, receive claim awards and shortly thereafter cancel their policies until fraud completely exhausts the premium pool. All while the real policy holders pay no attention to a possible spike in coverage and do nothing to try to come up with a way to compensate for the attack.

In response policy holders could reasonably petition that the DAOs code be updated to require every claimant include a recorded telephone call with a random policy holder verifying the details of any claim. So now the evil mastermind needs to hire people to lie presuming that the robots of the future still sound like Siri and cannot pass the Turing test. Fraud is not free it comes with a cost. Given the costs of time and money evil masterminds have better things to do than attempting to compromise an insurance DAO for auto glass. Admittedly it is unlikely that anyone would ever purchase a policy that only covers auto glass but one has to pick the low hanging fruit first which means that *the insurance DAO must have its humble beginnings with small value claims.*

It's reasonable to conclude that profiles created on social networks that seem to belong to real people raise the costs of producing a credible online identity beyond the value of small claims. In combination with other verification methods social media profiles can augment the verification of new policies which pay larger claims. Since this model is not used by traditional insurers most people are unaware of how this approach simplifies identity verification with **lower** verification costs and **lower** rates of fraud than traditional more costly verification methods.

B. Policy holders lack the skills to issue new policies

Fallacy: Policy holders are not trained and therefore unqualified to serve as evaluators to determine who is eligible for new policies.

Reality: Two approaches solve this problem. Limitations placed upon the scope of policies and limitations placed upon the type of initial conditions needed to determine eligibility. Issuance of life insurance for instance may be difficult to implement due to its numerous and complex set of initial conditions which determine eligibility. Good insurance DAOs seek to create policies with narrow scopes relying on few initial conditions. Good initial conditions are vastly limited in the ranges of answers that are possible. Good answers should always be reducible to a yes or no or to a value that is a gradient on a scale which can be signified by a number. These types of values can be easily understood by the DAO and by an untrained evaluator to determine eligibility for a policy.

C. Application data verification cannot be easily automated

Fallacy: There is no easy way to automate the verification of all the information that goes into approving a policy due to the complexity of the data or the variety of data sources used for evaluation. Underwriting policies is a skill that cannot be automated.

Reality: Policies with narrow scopes require the verification of a narrow set of initial conditions. Verification requires reliable data sources to confirm an applicant's claims. Sometimes the best "data source" is the applicant's own social network. Finding out how to leverage an applicant's social network to determine the veracity of an applicant's claims is a skill developers need to learn to produce a good insurance decentralized app. There will be the need for decentralized apps to use a variety of creative methods to demonstrate that indeed data verification can be an automated process when human intelligence is leveraged by a DAO.

D. Policy holders won't participate

Fallacy: Policy holders don't have the time or the desire to function as evaluators.

Reality: For insurance with a narrow enough scope the time needed to evaluate new policies can be less than 5 minutes with the aid of technology to simplify the process. Incentives and reassignment strategies similar to Amazon's mechanical Turk can be employed to distribute such micro tasks. Fair rewards for participation and fines for non-participation will assure that the task of new policy evaluation is processed in a timely manner.

E. You cannot trust people will evaluate rationally

Fallacy: Since you cannot rely that a policy holder will act in a rational manner applications will not get consistent treatment.

Reality: This problem is solved by using multiple policy holders to evaluate a single application and taking the majority viewpoint such as a 2 out of 3 or 3 out of 5 opinion.

The computational steps taken to reach an approval or denial are published on the blockchain and new policies are created as entries within the smart contracts ledger. The non-triviality of policy creation is highlighted by the fact that apart from executing the smart contract code which governs the DAOs application process no policies can be created. This code also governs the conditions under which any existing policies would be cancelled. Thus policies exist in a state secured by blockchain technology similar to the degree ones bitcoins are secured by private keys because no one can steal your policy unless they can steal your identity.

3. **Developers do not collect or spend monthly premium payments.** This condition may seem obvious but money is the lifeblood of an organization. Who has access to that money and the rules that govern how it can be spent define an organizations corporate policy. A smart contract DAO uses the blockchain network to collect and spend premium dollars given the rules written in its contract code. Developers write that code but that code should never permit developers access to those funds. This also assumes that modifying smart contract code is a non-trivial task requiring a majority or super majority of policy holders to approve such modifications.

   Peer to peer payments recorded on the blockchain secures and records funds. Payments between policy holders and the DAO are completely auditable thus a higher degree of corporate financial transparency is possible in the world of blockchain insurance. Hopefully this would assist a DAOs participants to make the case that less regulation is needed being that funds are safeguarded from human error or coercion. These claims however don't hold any value without a reliable third party available to audit the contract code. The producing of infrastructure to certify the honest nature of smart contracts may take some time but eventually it is conceivable that DAOs might be capable of receiving a gold seal for financial integrity.

4. **Developers do not approve or deny insurance claims.** A second basis for claiming a DAO operates on a peer to peer insurance model is claims are awarded on a peer to peer basis. Policy holders award or deny claims under the rules written in a smart contract which govern the corporate policy of a DAO. Many of the same requirements, limitations, and fallacies which applied to the issuing of new policies also apply to the awarding of new claims. Typically this elicits similar types of responses. These concerns can be summed up as: can a peer to peer system fairly award honest claims and can a peer to peer system mitigate claim fraud?

   To evaluate these questions we need to boil claims down to their most basic elements. Although many different types of claims exist for various types of policies most claims have three stages:

   - Evaluation for an initial award
   - Payout in either one lump sum or over time
   - Closing out a claim

   To release a claim payment requires the following:

   - Verify if the claim made matches the narrow scope of coverage tied to the initial conditions of the policy.
   - Validate if the assertions of the claimant are true.

   The first concern people have about peer to peer claims has to do with identifying eligibility for an award. The second concern people have about peer to peer claims has to do with the conditions under which payments are made. It is very important to distinguish that awarding a claim is separate from paying a claim. In many cases you wouldn’t want to use the same groups of people to perform these two different tasks. One group is required to consider the claimant’s request under the best possible light and the second group is required to protect the interest of existing policy holders by maintaining the health of the premium pool from fraud. If we can demonstrate that these two groups of people can effectively perform the task assigned to them then we have the basis to make the case that peer to peer insurance is possible.

   If claims are to be fairly awarded it would seem necessary to verify an evaluator’s competency to perform such a task. As with underwriting policies it seems that awarding claims must require some skill or training. The skill level required to award claims is directly proportional to a policy’s complexity. A policy’s complexity is determined by the following three key items:

- A policies scope - number of conditions to be evaluated which impact someone's claim
- Condition complexity - how many different factors are considered to determine if a condition evaluates as true or false
- Factor complexity - how well do factors resolve to numbers.

Using crop insurance as an example we could potentially limit the scope of a policy to one condition, the weather. When evaluating the weather we may choose to take into account rainfall and temperature as factors. Rainfall resolves to measurement in inches and temperature resolves to degrees in Celsius. As mentioned in the Ethereum white paper it is easy enough for a farmer in Iowa to purchase a derivative that pays out inversely based on the precipitation in Iowa, then if there is a drought, the farmer will automatically receive money. But in this case human beings are not required to evaluate a claim and the system is automated.

The above policy would exclude any coverage from locusts devouring a farmer's crop but if such coverage did exist which data feed would you use to determine if a claim is to be awarded? Locust swarms large enough to damage crops would certainly make the news. Perhaps you could have an oracle monitoring several news feeds or a government database to determine if a claim is to be awarded. Determining the extent of the damage thus the size of the claim however becomes a challenge. What data feed can accurately gauge the damage caused by such a condition? Could you potentially pay someone to go out to the farmer's field and measure this damage? What qualifies them to perform this task and can their measurement be trusted? Could other policy holders (who are also farmers) look at real time satellite data to determine this damage?

All of these questions highlight the challenges and potential opportunities facing developers who have creative insights into these particular problems. Developers must be able to accurately evaluate events in the real world to reliable numerical values. The assertion made by designers of peer to peer DAO insurance smart contracts is that there are solutions to these problems which fairly award claims and overcome fraud when paying out claims.

5. **Developers do not pay out insurance claims.** Although this fact is obvious to most of us it cannot be overstated enough that developers have no control of funds. Once policy holders evaluate a claim as true and a payment as valid the smart contract DAO uses the Ethereum network to pay out claims and all such payments are publicly auditable on the blockchain.

6. **Trusting the DAO is not equivalent to trusting the developers**. This technology is unique in that it will allow you to predict with a greater degree of reliability how your

claims will be awarded than you could with a traditional insurance company. This is because the insurance DAOs corporate policy is based upon software which is more predictable than insurance corporate policy based upon human decisions. The smart contract must obey its code. A board of directors need not always obey their own corporate charter nor must a single employee always do things according to corporate policy. If a node running smart contract instructions somehow malfunctioned the result would be published for anyone to evaluate and audit. If other nodes in the network detect this malfunction the result is rejected. If human beings malfunction since the result of their malfeasance is not immediately published and auditable it could potentially be weeks, months or years before anyone finds out and by that time the damage may be irreversible.

There is still the need for new applicants to determine if any potentially malicious code exists within the smart contract policy which would lead to their own financial loss, but once that determination has been made unless or until the code is changed an underlying assurance of predictability exists which is more solid than promises made by human run insurance organizations.

7. **The DAO smart contract is an autonomous agent over which developers have no control.** Once activated the smart contract DAO is a corporation where no fulltime employees are responsible for its operation. If it is found to be in violation of the law it would be solely responsible for its own actions. Developers who program a smart contract in doing so may not be violating any known laws. This same grey area exists with Uber who disputes with regulators that their cars are required to meet the same safety and insurance requirements imposed on taxis and follow the same laws imposed to restrict the number of cabs within a city. Whether or not developers have any responsibilities being that they do not run any aspects of the day to day operations of the insurance organization is an interesting question.

   If modifying smart contracts depends on a consensus mechanism centered around policy holders making proposals and voting on changes this puts the responsibility associated with meeting changing legal requirements on the policy holders themselves. Perhaps initially an insurance DAO may operate within the scope of all existing legal requirements but if these requirements change over time the DAOs operations may fall outside of legality. If no consensus can be reached among policy holders to bring the DAO up to the new legal standard this creates an interesting problem. Who then becomes responsible for the operation of the DAO outside of the law? Who would be arrested? Would you attempt to stop the DAOs function by arresting individual policy holders? Wouldn’t this be a futile effort given that the DAO will continue to function so long as some policy holders remain active? Payments are the lifeblood of the DAO and on a peer to peer payment network there is no third party payment police that exists to restrict such transactions. Problems like these highlight how our legal framework needs to be reconsidered given that this this new technology is not well regulated within the scope of existing insurance law.

8. **The developers do not own or control the hardware on which the DAO runs.** This is a unique consequence of smart contracts running on decentralized blockchain technology. If the DAO has a flaw the developers cannot fix it by unplugging the DAO or accessing hardware in which the DAO resides because it doesn't reside on any single piece of hardware.

IV. CONCLUSION

DAO smart contracts have the potential to decentralize financial products such as insurance. Corporations decentralized to the degree envisioned by the Ethereum community have never been possible before in human history due to the reliance on trusted third parties to broker financial transactions. With peer to peer payments and now potentially peer to peer contracts being made possible by blockchain technology many opportunities exist for the creation of financial products and services which have never existed before. Given the low barrier to entry for participation in this new space this should revolutionize what we believe to be possible in the world of financial contracts. If such decentralization proves to be technically possible the regulatory framework which governs participation in these entities becomes the only remaining barrier to entry into this new financial system.

GLOSSARY OF TERMS

Ethereum: A decentralized publishing platform featuring stateful user-created digital contracts. Ethereum uses ether as payment to execute smart contracts allowing contracts or other agents to lease out computational cycles of hardware operating on the network by paying a fee. This results in decentralized smart contract code on a public ledger maintained and ran on decentralized hardware.

DAO or decentralized autonomous organization: A smart contract which operates as an autonomous agent on the blockchain capable of managing digital assets to execute corporate policy as determined by the smart contract software programming.

Smart contract: Software code which is capable of holding, transferring, receiving, or spending digital assets. Uses the blockchain publishing platform to run computations which determine how financial assets are managed. Also understood as software subject to computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that obviate the need for a contractual clause.

Blockchain: A decentralized public ledger (database) of transactions shared by all nodes participating in a system based on the Bitcoin protocol. Such an identical ledger allows nodes on the network to achieve consensus. A full copy of a blockchain contains every transaction ever executed in the ledger. With this information, one can find out how much value (or other assets) belonged to each address at any point in history.

ROSCA or Lending club: A group of individuals who agree to meet for a defined period in order to save and borrow together, a form of combined peer-to-peer banking and peer-to-peer lending. Each member contributes the same amount at each meeting, and one member takes the whole sum once. As a result members will at some point be given access to a substantial pool of funds during the life of the ROSCA which they may use for whatever purposes they wish. This method of saving is a popular alternative to the risks of saving at home, where family and relatives may demand access to savings. Other names for these types of organizations include: tandas (Latin America), cundinas (Mexico), susu (West Africa and the Caribbean), hui (Asia), or pandeiros (Brazil).

Transparent: The clear explanation of the computational basis for how a smart contract reached a specific result which includes:

1. Publishing of the smart contract code
2. Publication of the computational steps taken to reach the result when the smart contract code was ran.
3. The publication of the result with its relevant timestamp
4. If the result determines a transfer of funds occurs the publication of any financial transactions associated with the result.

Auditable: The ability to determine accurately the complete history of a smart contracts financial accounts encompassing all spends and payments made to or from the DAO. This is possible because all transactions are recorded by all nodes which operate to maintain the blockchain.

Non-malleability: The inability for contract code to be changed by developers or other 3rd parties. The inability for contract code to be arbitrarily changed by policy holders who have the ability to vote on changes. This quality protects the integrity of the contract code from changes by malicious parties.

Payment friction: The difficulty for payments to move between different monetary networks when passing through centralized 3rd party financial institutions subject to government regulation. Payment friction results in the inability for software to autonomously manage financial resources due to changing financial regulations and changing technological constraints placed on funds as they move between networks.

Sybil attack: An attack wherein a reputation system is subverted by forging identities in peer-to-peer networks in order to gain a disproportional representation within the system. Defending against Sybil attacks is to prevent a single off-line identity from creating or controlling multiple on-line identities.

Claims verification: The determination by a peer if a claim is within a policies scope. Peers (other policy holders) evaluate if a claim is eligible and if so a claim award is granted. This is not always the same as a claim payment which may require further assessment to determine the extent of loss of value a covered asset has incurred.

Claims validation: The process by which a currently open claim is validated as satisfying the conditions of a claim award. This process assesses the loss of value an insured asset has incurred and results in the payment of a claim to cover this loss. In many cases this task is performed in coordination with a specialized oracle that interfaces with smart contract code via an API.

REFERENCES

Day, P. (n.d.). *The Importance of SB 896*. Retrieved from The Inclusive Economy: http://cfed.org/blog/inclusiveeconomy/the_importance_of_sb_896/

rmiia.org. (n.d.). *Cost of Auto Crashes & Statistics*. Retrieved from rmiia.org: http://www.rmiia.org/auto/traffic_safety/Cost_of_crashes.asp

Wikipedia entry for History of Bitcoin. (n.d.). Retrieved from http://en.wikipedia.org/wiki/History_of_Bitcoin#Regulatory_issues

Wikipedia entry for Liberty Dollar. (n.d.). Retrieved from en.wikipedia.org/wiki/Liberty_Dollar