Librium

Crowdsurance Technical Whitepaper

v.1.0.3

SparkCo, Inc.

1 Abstract

- **Five (5) percent** of people with the greatest health care expenses in the U.S. population spent **forty nine percent** of the overall health care dollar. [14]
- **Fifty (50) percent** of people with the lowest health care expenses in the U.S. population spent **three percent** of the overall health care dollar. [14]
- **Twenty (20) percent** of insurance premium payments are consumed on average by administrative fees and insurance company profit.
- **Thirty-four (34) percent** of US workforce is engaged in the gig economy. [1]

Private health insurance is broken. It has evolved into an ongoing payment schema, similar to a government sponsored social security substitute, which has made it extremely expensive and inefficient. Instead of private insurance providing **a one-time payment for unpredictable occurrences**, private insurance has instead become externally regulated to cover re-occurring costs, which by nature, have diverged from the original purpose of the insurance itself. Risk profiles should be adjusted in real time. Subscribers should be **rewarded for length of time on the system** without accident and frugal insurance claim submission habits. Instead, what occurs today is often the opposite.

Librium Insurance is a decentralized and fully transparent risk pooling system. Funds are collected by the system and then distributed by the system, automatically. The system is hyper cost efficient in that it eliminates the management fees of traditional insurance companies while real-time self adjusting for risk. Most interestingly, thanks to Librium insurance's decentralized nature, low-risk subscribers are not forced by external regulation to financially subsidize miss-matched risk pools, resulting in significant cost savings. Librium refocuses insurance back to what insurance is supposed to be: simple.

[1] http://money.cnn.com/2017/05/24/news/economy/gig-economy-intuit/index.html

Contents

2 Vision

As our global economy shifts away from the traditional "employed" workforce to the "Freelance" or "gig economy" workforce, a valuable social safety net through employee benefits have been lost: health insurance. It is often those freelance workers who are most at risk for not being able to afford health insurance. Uber is an example of a large and growing gig-economy employer who, unintentionally, is one of the largest platforms to have led individuals in the United States into a position of no health insurance [2]. Librium aims to attract the best talent through providing benefits and a social safety net only previously provided by traditional employers.

2.1 Problem

Health insurance is broken. The marketplace for health insurance, once dominated by small and accessible regional players, has become overrun by Goliath institutions, "middleman" brokers, significant administration costs, inefficient government regulations, complicated and intentionally opaque claim payout mechanisms, and black-box risk assessment models built by insurance actuaries who construct tools that by design cannot be reviewed or audited by the public.

2.1.1 For subscribers

Medical insurance subscribers face unprecedented levels of excess premium costs while being faced continuously with confusion-by-design systems around what coverages include. Insurance schemes which were initially designed for rare and infrequent occurrences have evolved into being sources of funds for all things medical, regardless of subscriber history with the insurer or other standing problems, which has the effect of shifting many cost burdens onto the network as a whole. Health insurance results in as much as $833 per month in premium payments on the average user's paycheck, and yet still often subscribers feel constraints in coverage. In response, over 28 million people in the US forgo health insurance, and this number is growing every year. The majority of medical insurance consumers feel increasingly violated, and the consumer's ability to assess the effectiveness of their insurance plans as a function of their premium is diminished.

2.1.2 For medical providers

Subscriber networks block innovative insurance entrants through leveraging their buying power, to pre-negotiate lower rates than nonsubscribers of the

[2] https://www.npr.org/sections/health-shots/2015/10/11/447157698/who-s-responsible-for-your-uber-driver-s-health-coverage

network have access to. Medical service providers are forced to accept pre-negotiated rates to access subscriber networks. When subscriber networks were first introduced, they were praised by service providers for their ability to attract patients to a medical office than that medical office previously had access to. However, since their introduction and subsequent broad scale adoption, these same subscriber networks have been used to block new entrants into the insurance space while forcing service providers to reduce costs endlessly. Traditional medical providers have lost approximately 66% of their revenue per service provided over the past decade, adjusted for inflation. Medical providers face challenges in billings and communication of covered costs to consumers.

2.2 Solution

The solution is a decentralized, transparent health insurance schema, designed for infrequent claims, based on Blockchain, plugged into a global and decentralized work economy: **Librium**.

2.2.1 Librium Insurance Schema

The main issue in insurance product design is obtaining the balance between the cost of the network and the complexity of the risk assessment. Librium will now introduce the Librium Insurance Schema, implementing a decentralized insurance schema. It compensates the subscriber by incentivizing for self-identified risk profiles while allowing the market to determine, in real-time, the appropriate co-pay for a monthly insurance payout based on a subscribers history with the network, size of premium in relation to other subscribers on the network and frequency of insurance payment draws. The Librium Insurance Schema connects subscribers of similar risk profiles while removing social and economic costs associated with existing medical insurance networks, e.g., fraud, privacy violations, administration costs and "middleman" brokers. The Librium Insurance Schema is an insurance system that rewards and protects users of similar risk profiles while giving transparency to all members and significantly reduced health insurance costs to everyone.

2.2.2 Role inside the Librium Ecosystem

The essence of the Librium Insurance Schema is its role within the Librium Ecosystem, an application-driven freelance marketplace. Inside the ecosystem, workers are enhanced by Service Providers and thus have access to a vast set of work opportunities. Enters the magic of the Librium Insurance Schema, providing workers with a safety net, no matter whom they work for and whatever Service Provider they use. A complete work and insurance package for workers who often lack the stability of traditional employment are given access to stability in healthcare. Indeed, we firmly believe that the best results are obtained when workers do not fear for their future, their job or their health.

2.2.3 The future

We see the Librium Insurance Schema and the Librium Ecosystem as a future part of gig-economy labor standards, solving the vital problem of providing global work opportunities and accurate cost insurance access to freelance workers and the world at large.

3 Librium Insurance Schema

The Librium Insurance Schema is the overarching framework of the decentralized health insurance provided to the Librium workers. This schema is composed of two components: the *Librium Insurance Protocol* and the *Librium Insurance Medium*. Both components are further composed of layers which can be visualized as stacking on top of one another, as illustrated in figure 1.

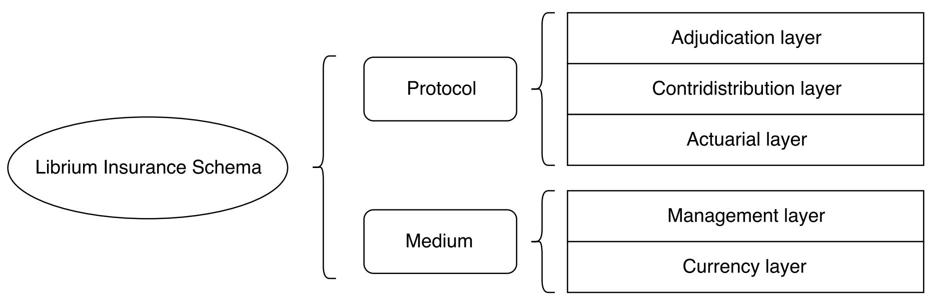

Figure 1: Librium Insurance Schema

3.1 Protocol

The Librium Insurance Protocol represents an abstracted layer which specifies the procedures and interface methods of the insurance schema. In the same way that the HTTP protocol can be implemented across programming languages, and transport layers (cables, fibers), the Librium Insurance Protocol can be implemented across different mediums. The protocol itself conditions the dynamics of the Librium Insurance Schema, including fund movements, incentives, payments, co-pays...

As described in figure 1, the protocol is comprised of three layers, stacking on top of each other:

- **Actuarial layer**: establishes the risk profile of the members of the insurance schema, in order to make sure the system remains fair to everyone.
- **Contridistribution layer**: is a mix between contribution and distribution. It governs how funds are contributed to the insurance schema, and how they are then distributed between the members.
- **Adjudication layer**: ensures that fraud on the insurance schema is reduced to a minimum, to avoid honest members financing malicious players.

3.2 Medium

The Librium Insurance Medium is the means through which the protocol is implemented. It is comprised of a *Management Layer* running on top of a *Currency Layer*. The Management Layer represents the implementation of authority managing the funds and creating the procedures required to implement the protocol. The currency layer represents how the funds are represented. The choice of the management layer and currency layer conditions other characteristics of the Librium Insurance Schema, such as decentralization, risk-adjusted performance, availability...

Note, the Librium Insurance Protocol is medium agnostic and could be implemented by a traditional financial company (*Management Layer*), using US dollars (*Currency Layer*). Of course, such configurations, that do not use the Librium Insurance Medium as described in this document, lose the majority of the advantages of a decentralized schema and are mentioned only to emphasize the robustness of the protocol.

4 Contridistribution layer

The contridistribution layer of the Librium Insurance Protocol is a mix between contribution and distribution. It governs how funds are contributed to the insurance schema, and how they are then distributed between the members.

The contridistribution layer is constructed around the concept of an *Entangled Token*. An Entangled Token is a store of value that once activated transfers its value over a defined period between two locations; a *Private Pool*, and a *Public Pool* at a rate predefined by the protocol. An insured user of the insurance schema would purchase a specified number of tokens per time period, which would activate and be placed into a *Private Pool*. Over the course of a specified period of time, a percentage of that time period's purchased token value, would be transferred from the user's Private Pool to the community owned Public Pool.

In parallel, the same percentage of the remaining value of the previous time period's activated token value would be transferred from that user's private pool to the community owned Public Pool and so forth and so on. With users continually paying in a consistent premium each time period, a user's private pool would approach a steady state value, while the Public Pool would constantly increase in holdings as value is transferred from Private pool to Public pool.

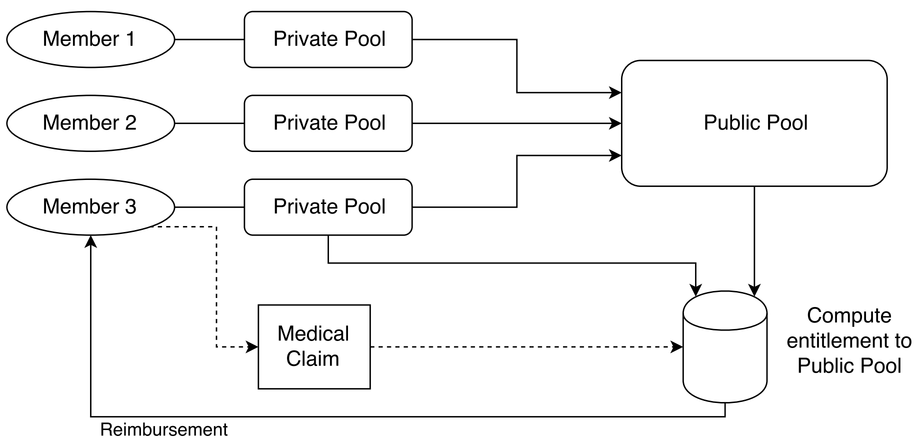

Figure 2: Contridistribution layer

In the event of a qualifying insurance claim event occurring during a time period, whereby the time period is pre-defined by the protocol, the claiming user would be entitled to draw value from the Public Pool at a ratio determined by the size of that user's Private Pool as a function of the average size of the Private Pools of every other party attempting to draw value from the Public Pool during that time period. When more value is drawn from the Public Pool than exists in the Public Pool, the Public Pool is split proportionately as a function of Private Pool Size and any remaining balance from any individual's portion of the pool, if needed, is allocated to the larger bill amount, or if not needed, then rolled over to the next time period. Any time the Public Pool is drawn from, it is mandated that the user's Private wallet is "used first" and diminished to zero.

It is anticipated that during each pre-defined time period, the Public Pool of value would be nearly or entirely diminished leaving any remaining amounts owed to be the responsibility of those individuals who incurred the original bill, or any funds left over to be rolled into the next time frame. In this scenario, the non-covered amounts of the original bill, function as a real-time, market adjusted "co-pay". Users of the insurance schema would have the ability to increase the number of tokens purchased per time period up or down by a specified factor which in turn would affect their steady state private pool balance and their entitlement multiplier for access to the Public Pool. Through this mechanism, individuals who want to self-risk-adjust and decrease their overall exposure to large "co-pays" can increase their monthly premium payment.

4.1 The Entangled Token Defined

Borrowing a term from quantum physics, entanglement represents the shared state of two objects physically separated by distance. Here the entangled Token represents an inversely entangled store of value whereby as the stored value in one location decreases, the stored value of its entangled partner increases. Such transfers occur until the value of a given entangled store of value is entirely depleted, or the value is transferred to a new owner as per the protocol.

The concept of an entangled store of value is one which can be implemented in a variety of ways as, for example, a smart contract based token, a system of wallets or the minting of entangled coins in pairs with incorporated timers. The protocol can support any form of implementation, block-chain based or otherwise.

4.2 Calculating the Private pool

The Private Pool dictates access entitlement to the Public Pool. Private Pools that are above average in size result in more significant access to the Public Pool. The Private Pool is calculated through three components: the user adjusted Premium Paid per Time Period, the Contridistribution Layer defined Decay Rate, and the System Generated Risk Premium.

Paid Premium Each user can adjust their Premium Paid per Time Period. Users are rewarded for increasing the size of their Paid Premium per time period through the increased size of their Private Pool.

Decay Rate The contridistribution layer issues a pre-defined half-life "Decay Rate". Each token purchased as a paid Premium transfers its value at time steps predefined by the protocol and at a percentage predefined by the protocol, to the Public Pool. The lower the decay rate, the more users are rewarded for staying with the system longer. The larger the decay rate, the more value is transferred to the Public Pool per time period.

Risk Premium Each participant of the crowdsurance is given a risk premium score referred to in this paper also as an Actuarial Multiplier. The mechanism for calculating Risk Premium is defined by the Actuarial Layer, discussed in Section 5. The risk premium score is factored into the Contridistribution Layer as a multiplier of the Token Transfer Decay Rate.

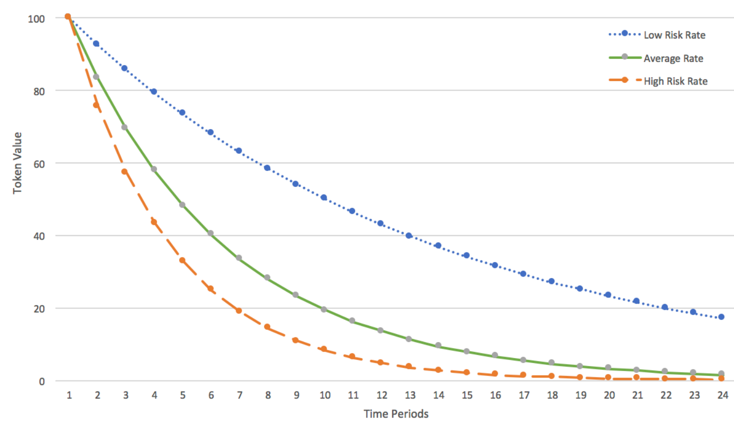

Figure 3: Token Decay Rate of three example Risk Profiles.

As discussed, the inversely ”Entangled Token” transfers its value at time steps predefined by the protocol and at a rate defined by the protocol. When calculating a User’s Private Pool, the protocol defined decay rate and the user’s risk premium are multiplied.

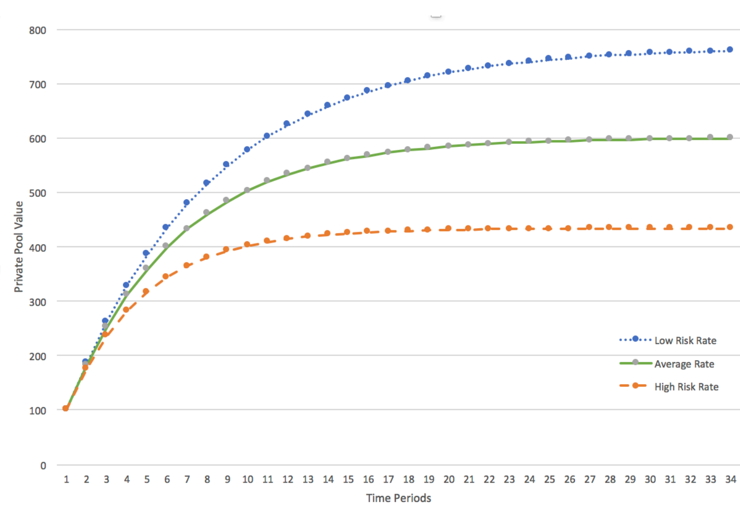

Figure 4: Private Pool across three example Risk Profiles.

This mechanism reduces the accumulation rate of a user’s private pool, which in turn limits the size of the achievable steady-state private pool which limits access to the private pool. To achieve a larger steady-state private pool, required to gain larger access to the public pool, a user could increase monthly premiums.

4.3 Strengths and Weaknesses

The Contridistribution Layer is a risk sharing tool that collects funds from its user-base into a Public Pool and then distributes those funds to individuals of the user-base to help cover the costs of unexpected events. This mechanism significantly reduces premium costs and increases transparency. Figure 5 is a graphical representation of the coverage and source of funds used for coverage.

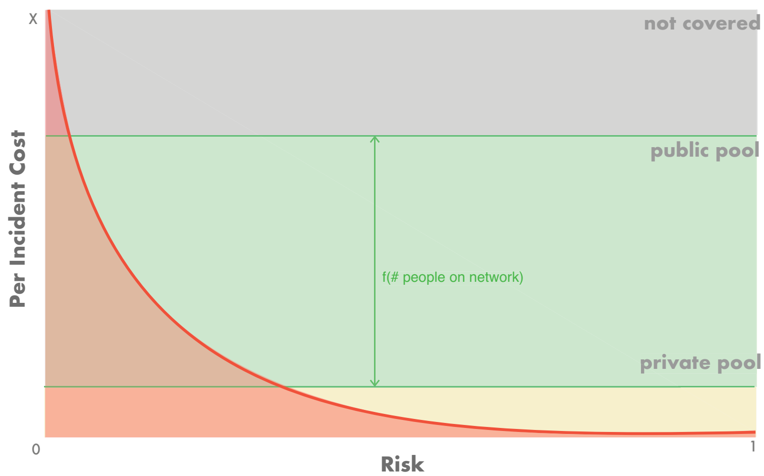

Figure 5: "Cost to Risk Curve", a graphical representation of the sources of funds used for claim coverage.

The cost to risk curve shown in Figure 5 is divided into three segments; the Private Pool, the Public Pool, and the Not Covered segments. Each user's private pool, as described in this paper, determines what percentage of the public pool that user has access to. Whenever a claim is made, the private pool is depleted first, covering the costs of the often occurring, but low in cost claims. The Public Pool is represented by the green section of Figure 5. As with every traditional insurance schema, the maximum payout per period can never exceed the money collected from subscribers. As such, the public pool has a ceiling on the amount of money it can payout per period. This ceiling is a function of the size of the risk pool and the length of the time period of the coverage period. The longer the time period and the larger the number of people on the system, the larger the public pool coverage protection available for "rare large payout" events at the expense of the large time in-between payments.

Unlike traditional insurance schema, the Contridistribution Layer of the Librium Insurance Schema affords full transparency to the system in how the pool functions and how the pool is paid. Very rarely occurring situations where multiple high in cost incidents occur simultaneously, represented in gray in Figure 5, are not insured by this system. This is the kind of situations that would cause traditional insurance companies to go bankrupt, while the Librium Insurance Schema adds a safety mechanism to maintain its existence. However the larger the number of people on the system, the more robust the system becomes to perturbations from high risk events and the smaller the grey area becomes. If desired, high deductible re-insurance could be purchased from traditional insurance companies to cover those black-swan events.

4.4 Examples

The following section describes three specific examples of the Contridistribution Layer. These examples are all based on the same simplified configuration of the protocol.

Simplified Configuration

Defined by the protocol:

- Decay rate: 1.2 (16% of premiums are transfered per time period)
- Time period: 1 month

Defined by the user:

- Average monthly payment: $100
- Resulting private pool steady state: $600
- Resulting time to reach steady state: 18 months

Global characteristics:

- People in the Insurance pool: 1000
- Public Pool availability per time period: $100,000 (approximately)

Example 1: Three Injury Claims

In a given month, three people (0.3% of population) are injured, leading to medical claims. In this example, all three people have a steady state private pool of $600. Person A, submits a claim for $500, Person B submits a claim for $10,000 and Person C submits a claim for $35,000. With the same balance in their private pools, each person is entitled to the same share of the public pool. Each of the three people is entitled for up to $33,333. Person A's claim of $500 is completely covered by his Private pool, reducing his Private Pool to $100. Person A's claim to the Public Pool is removed and the funds are again made available. Person B's claim of $10,000 is first covered by his Private pool of $600, reducing his Private Pool to $0 with the remaining balance of $9,400 being completely covered by his entitlement share of the Public Pool of $33,333. Person B's claim to the Public Pool is removed and the remaining $23,933 of funds are again made available. Person C's claim of $35,000 is first covered by his Private pool of $600, reducing his Private Pool to $0 with the remaining balance of $34,400 being partially covered by his entitlement share of the Public Pool of $33,333. Of Person C's remaining balance of $1,067, he is now entitled to a second round of Public Pool funding. Because Person C is the only person still drawing from the public pool, he is welcome to draw his outstanding $1,067 from the entire remaining balance of $57,266, completely eliminating Person C's debt Balance and leaving a remaining $56,199 in the public pool balance to be rolled over to the next time period.

Analysis: *In this simplified Example 1, enough money was available in the Public Pool to cover the expenses due. The longer the time period, or the larger the number of people available in the insurance pool, the more risk can be absorbed by the system*

Example 2: Four Injury Claims, money due beyond public pool

In a given month, Four people (0.4% of population) are injured requiring medical claims. In this example, all four people have a steady state private pool of $600. Person A, submits a claim for $500, Person B submits a claim for $10,000, Person C submits a claim for $35,000 and person D for $60,000. With the same balance in their private pools, each person is entitled to the same share of the public pool. Each of the three people is entitled for up to $25,000. As in Example 1, Person A's claim of $500 and Person B's claim of $10,000 are both completely covered by the system returning $40,700 to the Public Pool. Person C's claim of $35,000 is first covered by his Private pool of $600, reducing his Private Pool to $0 with the reaming balance of $34,400 being partially covered by his entitlement share of the Public Pool of $25,000. Person C now has a remaining Balance of $9,400. Person D's claim of $60,000 is first covered by his Private pool of $600, reducing his Private Pool to $0 with the remaining balance of $59,400 being partially covered by his entitlement share of the Public Pool of $25,000. Person D now has a remaining Balance of $34,400. Because Person C and Person D both begin their claim with the same balance in their private pools, entitlement to the remaining Public Pool Value of $40,700 is now evenly split with $20,350 being allocated to each of the two individuals. Person C has his outstanding balance fully covered in the second round of public pool returning the leftover $10,900 of the Public Pool entitlement to the Public Pool. Person D after one additional round of Public Pool entitlement is left owing a co-pay of $3,200.

Analysis: *In this simplified Example 2, more expenses were submitted than were funds available in the Public Pool. The schema distributed the limited Public Pool funds resulting in the largest co-pay being assigned to the largest bill. The majority of the co-payment burden was shouldered by the largest bill payer of the system who wound up being responsible for about 5 percent of his original bill in the form of a co-payment. If another bill was similar in size with all other things being equal, then co-payments would be split. Here again, the longer the time period, or the larger the number of people available in the insurance pool, the less the systemic risk.*

4.5 Risk Factor

The computation of the risk factor is described in Section 5. The risk factor is factored into the Contridistribution Layer as a multiplier of the Token Transfer Decay Rate. The biggest the risk factor of a user, the biggest the decay rate, thus the lower the steady-state of the Private Pool for the same premiums, reducing his entitlement to the Public Pool.

4.6 Advantages

This system has a number of very significant advantages over existing insurance systems;

- This system re-focuses the fundamental purpose of insurance to cover one-time catastrophic events while still allowing for the flexibility of covering recurring smaller events.
- This system incentivises individuals not to draw down their private wallets, so as not to decrease their access to the larger pool, maintaining money in the system
- This system rewards individuals for staying with the plan for a longer period of time and not submitting claims to the system .
- This system essentially eliminates the need for the 20 percent administrative fee common to most insurance companies.
- This system once implemented is completely decentralized and not subject to regulation or forced acceptance of high risk individuals.

5 Actuarial layer

As described earlier, the reason insurance exists is to share the risk of unlikely incidents between multiple individuals. As such, the only way to avoid a race to the bottom is to make sure the system remains fair to everyone. Indeed, no-one wants to pay more for the risks incurred by someone else.

This issue requires insurance systems to analyse the risk profile of individuals, aiming at improving the fairness between all the participants. Someone that incurs more risks to draw from the insurance reserve will pay more in premiums to accommodate for that risk imbalance. The entity responsible for establishing this risk profile is called an actuary.

In the traditional world, insurance companies play the role of actuaries. They establish the risk profile of individuals through complicated and obscure calculations. These inefficient black box systems induce high additional fees for members of the insurance, and raise the question of fairness as it is completely opaque. We believe that there is no place for a central actuarial authority in a decentralized system such as the Librium Insurance Schema. The innovation of this protocol can not afford the costs and inefficiencies of the relics of the past. As such, the Librium Insurance Schema needs to implement a decentralized actuarial system.

5.1 Challenges

However, creating a decentralized actuarial system is not trivial. Multiple questions arise, that need to be answered. The challenges can be separated in three categories:

5.1.1 Source of the data

Traditional insurance companies use forms to gather data about the participants, that will hopefully be relevant in establishing their risk profile. Fraud is not incentivized, by fear of legal repercussions. However, there is no one to begin legal procedures in a decentralized system, no one to enforce legality. Going even further, legislations differ from country to country, and Librium intends to become a global ecosystem. Thus, how to input relevant data in the system in a completely reliable and decentralized fashion?

5.1.2 Storage of the data

Moreover, the storage of this detailed data becomes problematic in the blockchain world of today. First, scalability issues in the Ethereum network would translate in astronomical fees, just to keep the data in decentralized memory. Second, all the data would need to be encrypted for privacy reasons, making it difficult to perform statistical analysis in order to improve the accuracy of risk assessment.

5.1.3 Use of the data

The biggest challenge is to preserve fairness when using the data and establishing risk profiles for participants. Who takes risk assessment decisions? What is their expertise in doing so? Why and how would they be elected as experts?

As explained before, we believe that there is no place for a central actuarial authority in such a decentralized system. These three questions need to be answered by keeping that in mind. Because there is no central authority to control the ecosystem by design, we believe that the actuarial layer must implement trust-less decision-taking and exchange of data. The only way to achieve that is by using game theory and incentivizing people to do their task correctly. This requires to make the following assumption: users are greedy and prefer having more money to having less money, and will thus take actions that are in their best financial interest.

5.2 Conceptual solution

A bit more than twenty years ago, Google began exploring the internet using its web crawler. Unlike other search engines, Larry Page and Sergey Brin decided to convert the backlink data gathered for a given web page into a measure of importance. As such, the more links heading to a certain website, the higher this website would rank in a keyword search result. The algorithm was named PageRank, after one of the founders name. Everyone knows how successful this strategy turned out to be.

The rationale behind this algorithm makes sense: if a lot of high quality people link to a certain page, it is probably of interest. In the same way, if a lot of low quality people link to a certain page, it is probably not of interest. The algorithm basically analyses relationships between multiple entities (websites), and averages an individual quality level based on the rest of its related network.

By extending this concept of averaging individual characteristics based on its interactions with a network, we tend towards what the scientific community calls "social network analysis": investigating social structures through the use of networks and graph theory. Basically, it analyses the effect of networks of people on different issues. For example, some researchers performed a social network analysis to study the impact of social networks on terrorism and political violence [9]. Other researchers studied the social network effects on academic achievements [4].

Social network analysis is also used to study health issues. Interestingly, researchers found correlations between individuals' social networks and their probability to encounter related health issues [8, 5, 2, 3, 7]. Other studies highlighted the effect of social networks on risky behaviors [1, 12, 13, 6]. Even though experts still debate whether the group causes the behavior or if the behavior leads to people gathering together, the conclusion is the same and can be summarized by the age old adage *we are who our friends are*. If a greater percentage of your friends display certain behaviors or higher probabilities toward requiring specific health care, there is a good chance you will display the same traits, statistically. For example, if you are an avid drug user, there is a good chance that you maintain relationships with other drug users in your social network.

With the advent of social media, it is easier than ever to analyze relationships between people and tracing back social networks. These platforms are excellent tools for the purpose of performing social network analysis. By accessing all the data from major social medias (Facebook, Linkedin, Whatsapp,...), one could gain an accurate representation of the social network of most people living in a decently developed country. The bottleneck is of course the available data, thankfully reduced to preserve privacy.

As such, the Librium actuarial layer allows members of its insurance schema to share their social media connexions, in order to benefit from more interesting actuarial multipliers. Then, by merging social networks of insured members and past claims data from the Librium Insurance Schema, the actuarial layer can accurately assess risk profiles and attribute an actuarial multiplier to each individual. This innovative concept is both extremely efficient, removing all the costs associated with traditional actuarial services, and very accurate. Moreover, it is completely transparent, unlike traditional opaque systems, that constitute magical black boxes rather than tools aimed at maintaining fairness between participants.

In effect, the actuarial layer uses members' facebook connexions to assess risk in the exact same way Google uses websites' backlinks to assess page quality. However, the team is still looking for an elegant translation of PageRank into the Librium world...

5.3 Technical implementation

The actuarial layer is made up of three main components: a Facebook application, a Desktop application and a consensus mechanism. The Facebook application will allow access to the member social network to the Desktop client, that will then compute an actuarial multiplier based on certain accepted rules, then report to the consensus mechanism, hosted on the blockchain.

In this section, the example of Facebook is used. However, the concept can be extended to other social media platforms, or other manifestations of someone's social network. Ideally, the system would be based on multiple sources to improve accuracy and reduce exposure to central organizations.

The actuarial layer draws inspiration from the works of Thomas Schelling (Schelling point), Vitalik Buterin (Schelling Coin), the innovative TruthCoin project [11], and its Augur [10] sibling. More information can be found in these papers concerning the consensus mechanism.

Facebook application

The first element of the actuarial layer is the Librium Facebook App. This application lets users give access to their network of connections to the actuarial partners, who are the people bridging the Facebook App with the Ethereum blockchain, in a trustless fashion.

Desktop client

Librium will develop an open-source desktop client for the Librium actuarial layer. This application is responsible for bridging members' social network, from the Facebook App, and the Ethereum blockchain, automatically. As such, it plays a reporting role: it implements the accepted rules of actuarial analysis based on social networks, and submits the results to the smart contracts hosted on the blockchain.

The desktop client has access to the connexions between users (i.e. social network), through the Facebook App, and the Librium claims history, through the Ethereum blockchain. As such, it performs an actuarial analysis based on the history of claims submitted by the network of connexions of an individual. The set of rules used for the actuarial analysis are first suggested by Librium at launch, and define the importance of different characteristics of social networks, as well as how they translate into an actuarial multiplier.

Actuarial partners, running the desktop client, are EQL token holders. The Librium EQL tokens are used as a reputation token in the actuarial layer, in the same way VoteCoins (TruthCoin) or REP tokens (Augur) are used. Not all EQL token holders are actuarial partners. However, they are free to join the Actuarial Group, which will make them actuarial partners and entitle them to financial incentives. Members of the Actuarial Group are obligated to run the desktop client and automatically report to the Librium smart contracts.

Consensus mechanism

The consensus mechanism is the cornerstone of the actuarial layer. It constitutes the guardian against error and fraud, by verifying that the reporting done by actuarial partners is correct. Of course, this has to be done without trusting anyone nor appointing experts.

The way the consensus mechanism is able to do that is by implementing a coordination game [11] : actors are rewarded when reporting data similar to that of the rest of the group, on average. Actuarial partners trying to game the system would be penalized, as they report different results than the mass. The case of a coordinated "attack" would in fact represent a change of the actuarial framework, and is a feature of the actuarial layer.

To measure coordination, the consensus mechanism uses the first score from a weighted Principal Components Analysis (PCA), which is a statistical technique derived from Singular Value Decomposition(SVD), used to examine a matrix and reveal and sort its effects by influence. This thus represents the degree to which each actuarial partner varied his report with those of a theoretical actuarial partner maximally representative of the covariance across all reports and partners. Outcomes are established by weighted-vote, according to users' ownership of Librium EQL tokens, representing their reputation.

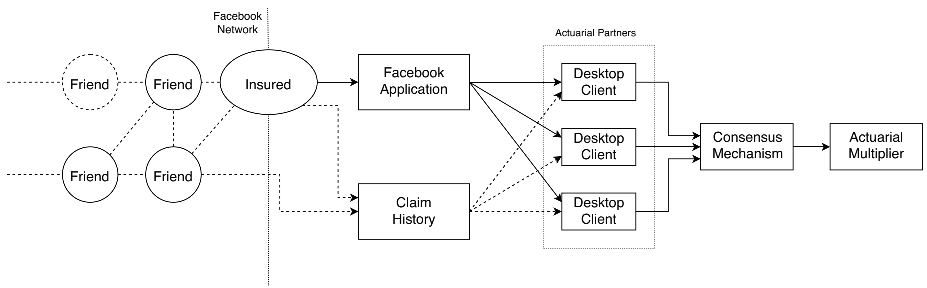

Figure 6: Actuarial layer

After a round of reporting, Librium EQL tokens are redistributed amongst all the members of the Actuarial Group, depending on the correctness of their report and the amount of tokens they hold. Actuarial partners that did not report, or who did not report correctly are penalized, while good actors are rewarded.

Even in the optimal case where all the actuarial partners give the same results, they are still incentivized to continue reporting. Indeed, small fees are collected from the Librium Insurance Protocol, in the form defined by the currency layer, then gradually distributed to actuarial partners. The fact that these incentives are offset and gradually distributed rewards past conformity and provides an incentive to get and keep a high reputation.

5.3.1 Advantages

On top of meeting the challenges described earlier, the solution implemented by the actuarial layer presents a lot of advantages:

- **Trustless**: Every actor is properly incentivized not to cheat the system
- **Decentralized**: No central authority is necessary for the system to function properly
- **Accurate**: Risk assessment is closer to reality than traditional actuaries
- **Efficient**: Removing of costs associated with actuarial services, hence reducing fees to a large extent
- **Expert-less**: The system does not rely on individuals' skills or knowledge
- **No human input**: Librium miners run the desktop application, which interfaces with the Ethereum blockchain automatically.
- **No data storage**: No additional data is stored on the blockchain

5.4 Future

One of the beauty of this technical implementation, is that it is future proof by allowing for a decentralized democracy in the choice of the actuarial system. Indeed, actuarial partners have the liberty to change the software completely, to change the actuarial rules, or choose to use a completely different system to establish risk profiles.

The actuarial layer only sets one thing in stone: the consensus mechanism. Actuarial partners are rewarded when they agree on the outcome of a risk estimation. If enough actuarial partners can come up to agree on a new system or new rules, then the consensus mechanism will continue to do his job while taking innovation into account.

This paper constitutes a proposal of a working actuarial layer and will be first implemented on the Librium Insurance Schema. It is expected to incrementally change with time and new technologies, hopefully increasing its accuracy in assessing risk and increasing its fairness. The software first implemented on the Librium Insurance Schema will be open-sourced, welcoming third-party entities to join the developing community and evolve the system.

Making changes to the actuarial system requires a coordinated decision of a majority of actuarial partners. As such, it can be seen as a democracy, where leaders suggest ideas and other people have the freedom to follow or to discard them. SparkCo will most probably be the first leader or source of influence in this Librium actuarial layer. However, Librium is here to last for a long time, and the consensus mechanism will allow future thought leaders to garner a majority of actuarial partners and change the system.

6 Adjudication layer

In a perfect world, we would not have to verify claims made by users of the ecosystem. We would trust insureds with covered bills and reimburse accordingly. Unfortunately, we are not living in this perfect world.

As such, the Librium Insurance schema needs to reduce fraud on submitted claims, as do every other health insurance company or social system in the world. However, this is not a trivial task. In the same way that a decentralized insurance system would be penalized by requiring a central actuarial authority, it cannot depend on a central authority to reduce fraud.

Two kinds of fraudulent claims are susceptible of happening on any insurance system: completely fake bill and modified bill. The former results in a claim that can not be linked to an actual medical procedure, while the latter is more insidious and merely modifies the assumed cost of an existing procedure.

6.1 Built-in disincentives

Due to how the actuarial layer of the Librium Insurance Schema works, defrauding the system is in fact detrimental to the fraudster's social network. Indeed, every penny stolen from the public pool increases the actuarial multiplier of the people connected to the fraudster. This is true for connexions already on the system, as well as for future members. Moreover, the actuarial multiplier of the fraudster himself will also increase every time, making it less and less financially interesting to take advantage of the system.

Another characteristic of the Librium Insurance Schema is the time it takes to reach the steady state of the private pool. Indeed, the private pool defines the amount of money that can be drawn from the public pool, but that private pool can not be filled in in one go. This effectively rewards users that have been contributing for a longer time, while slowing down remaining fraudsters and forcing them to put more money in the system, making it less interesting to perform a fraudulent stunt, and more interesting to use the platform as an actual insurance system.

6.2 Claim court

When interacting with traditional insurance companies, potential fraudsters are exposed to legal actions in case their detrimental behavior is detected. For a majority of people, this is enough to stop them from taking advantage of the system. In a completely decentralized ecosystem, no central authority exists to go after and sue fraudsters. However, the Librium Insurance Schema implements a protection mechanism in order to discourage harmful behavior.

This protection mechanism is called the claim court. It provides the ecosystem with a decentralized justice system, hopefully detering potential fraudsters. Indeed, if a medical claim is recognized as being fraudulent by the claim court during a claim trial, the insurance member that tried to take advantage of the system will be heavily penalised. The claim court uses the same consensus mechanism presented in section 5.3, and was also inspired by the idea of Vitalik Buterin of a decentralized court[3].

6.2.1 How it works

When a member of the Librium Insurance Schema submits a medical claim, the protocol computes what he is entitled to draw from the public pool. However, the funds will be held by the system for a thirty days period, allowing for the potential verification of the claim. During that period of time, anyone can open a claim trial, thus becoming a prosecutor. The aim of this trial is to adjudicate on the validity of a certain medical claim.

[3]https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/

The insurance member whose claim has been challenged is called a fraud suspect in this trial setup. The fraud suspect has to build a defense file with proofs and evidence that his claim is legitimate. The following section describes examples of elements that can be accumulated during the medical process and would constitute strong evidence of a legitimate claim. In the mean time, the prosecutor also has the opportunity to amass evidence proving that the claim is fraudulent, if he has access to such information.

In parallel to the prosecutor and fraud suspect building their dossier, a decentralized jury is selected. The jury is the entity responsible for deciding whether the claim was fraudulent or not. This is where cryptoeconomics come into play, allowing for a similar consensus mechanism as the actuarial layer (see section 5.3 for more details) and decentralized prediction market oracles, using Librium EQL as a reputation token. As such, the jury as a whole will tend to accurately determine whether the claim was fraudulent or not, maintaining justice on Librium.

6.2.2 Examples of proofs

When trying to convince a jury that a specific medical procedure took place, multiple elements could constitute very strong evidence. The more elements in a defense file, the more chances there are that the jury will recognize the claim as legit. The following list presents ideas, but is in no way exhaustive. If you think about other elements that could constitute potential proofs that a medical procedure indeed took place, please contact us.

- **Document the procedure**: having someone take pictures and videos of the operation or treatment, admission into hospital, or every other element related to the claim, along with proof of time.
- **Picture with doctor and bill**: take a picture of the claim suspect with the doctor, his name, the bill and a proof of time.

When taking pictures or videos aimed at constituing evidence, it is stronly recommended to use a ”proof of time”, as introduced in the concept of ”proof of life” used by Julian Assange and Vitalik Buterin to prove they were alive. Essentially, including the number of the last block on a specific blockchain (Bitcoin, Ethereum...) and its corresponding block hash allows the jury to validate that a specific picture or video was taken at a specific time.

6.2.3 Financial incentives

In a cryptoeconomic setup, it is important that every participant is incentivized to trustlessly act as required. As such, every actor of the claim court is incentivized to play its role, and to do it in complete honesty.

Prosecutor

Everyone can become a prosecutor, when in doubt about the veracity of a medical claim. However, the prosecutor has to advance the costs associated with the consensus mechanism, used to pay the members of the jury for their work. This will limit the amount of people challenging a claim to those having access to specific information about a claim, which in turn are incentivized to become a prosecutor. Indeed, when a claim is challenged then recognized as fraudulent by the jury, the prosecutor gets the entirety of the fraudster's private pool.

Claim suspect

Of course, people submitting a medical claim are highly incentivized to gather evidence of their medical procedure, as there is a chance it might be required for them to receive their funds and pay their medical bill. In the same way, as described in 6.3, they are also incentivized not to fraud.

Jury

The members of the jury are holders of Librium EQL tokens. As described in section 5.3, the coordination game implemented by the consensus mechanism rewards funds to actors that vote with the mass. As such, people are paid to be part of the jury if they can agree on the decision. However, people trying to vote dishonestly, or differently from the average vote, will loose a part of their funds.

6.2.4 Implementation

The claim court system is similar in implementation to the actuarial layer. Once the consensus mechanism is successfully implemented for the actuarial layer, it can be used with few modifications for the claim court. However, an additional client application would need to be developed.

Other projects, such as Kleros, are currently working on decentralized autonomous justice organizations. Librium will be investigating how such projects can be used inside the Librium Ecosystem, in order to benefit from their expertise.

6.3 Advantages

Thanks to social, temporal and financial disincentives built into the protocol, as well as a decentralized justice organization, the claim court, the Librium Insurance Schema will hopefully be able to alleviate fraud on its platform. Moreover, the claim court also presents two additional benefits:

- **Scalability**: A claim trial is equivalent to a full validation as fallback to be used if an alarm has been raised. However, only a small subset of medical claims go through a claim trial, improving the global bandwidth of the systme.
- **Privacy**: As only few medical claims end up in a claim trial, privacy is completely maintained in the vast majority of cases.

The adjudication layer is well equipped to reduce fraud. Here are the barriers a fraudster would have to go through in order to take advantage of the system:

1. Exploit the trust of his friends, making it more expensive for them to use the Librium Insurance Schema
2. Spend multiple months and a consequent amount of money as premiums to build up his private pool
3. Build a fake medical claim and submit it
4. Wait for a month, praying for the fraud to stay undiscovered
5. If a prosecutor challenges the claim, wait for the investigation period
6. If/When the jury concludes that it was a fraud, loose all his private pool

The risk of loosing funds is important when trying to take advantage of the system, and the long time required to prepare for such a stunt makes it impractical for most. As such, we think that the Librium Insurance Schema is as protected against fraud as traditional insurance companies, if not more.

7 Librium Insurance Medium

The Librium Insurance Protocol is implemented through the Librium Insurance Medium. The Insurance Medium is composed of two layers: a *Management Layer* for managing claims and a *Currency Layer* for paying them out. The following sections describe these two components in more detail, define requirements for the Librium Ecosystem, and at last explore different possible implementations.

7.1 Management layer

The management layer represents the authority implementing the procedures of the protocol. In a traditional insurance company, the management layer would be the company itself, i.e. a central authority. For the implementation described in this paper, we believe that the management layer should embody one fundamental characteristic: **decentralization**. Indeed, a decentralized governing body acting as the management layer of the Librium Insurance Schema would allow for greatly reduced: administrative costs, conflicts of interest, black box policies, inefficient mixing of risk pools through regulation, etc.

7.2 Currency layer

The currency layer represents in what form the funds collected by the insurance schema are collected and stored. For a traditional insurance company, the currency layer would be collected in fiat and stored through various investment vehicles. The currency layer dictates the risk-adjusted returns and availability of the insurance funds. For example, the US dollar has been extremely stable for years, at the expense of significant growth of its intrinsic value leaving traditional insurance companies to store funds in outsourced investment vehicles which cost upwards of 20 percent of investment returns. The currency layer of the Librium Insurance Medium should be constrained by the challenges of fiat while encompassing two aspects;

- **Record of investment returns**: Ideally, the currency layer used by the Librium Insurance Schema should be positioned to increase in value, allowing insurers to leverage their insurance as an investment. In reality, the system should optimize the currency layer around risk-adjusted investment performance, compromising between stability and growth potential.
- **Robustness to perturbations**: Insurance claims need to be paid rapidly. As such, the currency layer must operate through a currency that maintains a transaction volume, or transaction scheme sufficient to absorb large claim payout onto the system. The currency must be trade able for it to be converted for use off line.

7.3 Possible implementations

We believe that the Blockchain technologies of today will evolve in immeasurable ways in the short-term to near future. Here we describe three possible implementations of the Librium Insurance Medium, using technologies available today. In the following sections, potential technologies under development will be investigated to prevent any uncovered shortcomings when releasing the Librium Insurance Schema into the Librium Ecosystem.

Proposition 1: Using EQL tokens as currency layer, and Ethereum smart contracts as a management layer. This solution has multiple advantages: completely decentralized, workers can use their Librium pay directly, high growth potential. However, until Librium reaches large scale and proves itself, EQL

[3] http://www.pionline.com/article/20170516/ONLINE/170519892/outsourced-insurance-assets-grow-10-globally-in-2016-8212-report

might not provide the same stability and high trading volumes as larger cryptocurrencies. Moreover, until their platform improves scalability, Ethereum smart contracts are still expensive and slow to use.

Proposition 2: Using Ethereum as currency layer, and Ethereum smart contracts as a management layer. This solution has multiple advantages: completely decentralized, existing record of past performance and growth, high trading volumes. However, the risk is still significant as all the eggs are placed in the same basket, in a single cryptocurrency, which might decay in a distant future. Moreover, until their platform improves scalability, Ethereum smart contracts are still expensive and slow to use.

Proposition 3: Issuing a new asset-backed ERC20 token as currency layer, pegged to an index of the most prominent cryptocurrencies (BTC, ETH, BCH, XRP, LTC...) by market cap. A central authority would be responsible for issuing and burning tokens in exchange for these cryptocurrencies, thus pegging the token value. Ethereum smart contracts would be used as a management layer. This solution has multiple advantages: decentralized insurance schema, existing record of past performance and growth, high trading volumes, diversification, future-proof (the index only keeps the biggest cryptocurrencies by market cap, adding new ones and removing decaying ones). However, this solution relies on a central authority for maintaining this pegged ERC20 token. Moreover, until their platform improves scalability, Ethereum smart contracts are still expensive and slow to use.

7.4 Investigated technologies:

Many of the shortcomings presented above will become solvable in the near future. Multiple technologies are being investigated, on top of following the progress made on Ethereum scalability:

- **TrueBit**: Scalable verification solution, making smart contracts off chain and efficient.
- **Rootstock / Counterpary**: Bringing smart contract technology to the Bitcoin blockchain, possibly allowing for a decentralized index of BTC and ETH, using
- **BTCrelay**: Bridge between the Bitcoin and Ethereum blockchains, expanding on Rootstock to make it work both ways.
- **Commit.network**: Cross-Blockchain interoperability, possibly allowing for a decentralized index of BTC and ETH.
- **0x**: Decentralized exchange, allowing automatic transfers between EQL tokens and the currency defined by the currency layer.

8 Conclusion

This paper introduced a truly decentralized insurance schema. Different layers have been presented in order to abstract the functions of the system from each other. All the components of traditional insurance companies have successfully been replaced by their more efficient, decentralized counterparty, leading to a completely innovative and disruptive system.

We see the Librium Insurance Schema and the Librium Ecosystem as a future part of gig-economy labor standards, solving the vital problem of providing global work opportunities and accurate cost insurance access to freelance workers and the world at large.

References

[1] J. D. Allen et al. “The relationship between social network characteristics and breast cancer screening practices among employed women”. eng. In: *Annals of Behavioral Medicine: A Publication of the Society of Behavioral Medicine* 21.3 (1999), pp. 193–200.

[2] L. F. Berkman. “Assessing the physical health effects of social networks and social support”. eng. In: *Annual Review of Public Health* 5 (1984), pp. 413–432. ISSN: 0163-7525. DOI: 10.1146/annurev.pu.05.050184.002213.

[3] S. H. Bland et al. “Social network and blood pressure: a population study.” In: *Psychosomatic Medicine* 53.6 (Dec. 1991), p. 598.

[4] Robert M. Bond, Volha Chykina, and Jason J. Jones. “Social network effects on academic achievement”. In: *The Social Science Journal* 54.4 (Dec. 2017).

[5] R. M. Christley et al. “Infection in social networks: using network analysis to identify high-risk individuals”. eng. In: *American Journal of Epidemiology* 162.10 (Nov. 2005), pp. 1024–1031.

[6] S. T. Ennett and K. E. Bauman. “The contribution of influence and selection to adolescent peer group homogeneity: the case of adolescent cigarette smoking”. eng. In: *Journal of Personality and Social Psychology* 67.4 (Oct. 1994), pp. 653–663.

[7] R. C. Kessler, R. H. Price, and C. B. Wortman. “Social factors in psychopathology: stress, social support, and coping processes”. eng. In: *Annual Review of Psychology* 36 (1985), pp. 531–572.

[8] Douglas A. Luke and Jenine K. Harris. “Network analysis in public health: history, methods, and applications”. eng. In: *Annual Review of Public Health* 28 (2007), pp. 69–93.

[9] Arie Perliger and Ami Pedahzur. “Social Network Analysis in the Study of Terrorism and Political Violence”. In: *PS: Political Science & Politics* 44.1 (Jan. 2011).

[10] Jack Peterson and Joseph Krug. *Augur: a Decentralized, Open-Source Platform for Prediction Markets*. Tech. rep. URL: https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf.

[11] Paul Sztorc. *TruthCoin: Peer-to-Peer Oracle System and Prediction Marketplace*. Tech. rep. Dec. 2015. URL: http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf.

[12] Kathryn A. Urberg, Serdar M. Degirmencioglu, and Jerry M. Tolson. "Adolescent Friendship Selection and Termination: The Role of Similarity". en. In: *Journal of Social and Personal Relationships* 15.5 (Oct. 1998), pp. 703–710.

[13] Thomas W. Valente, Peggy Gallaher, and Michele Mouttapa. "Using social networks to understand and prevent substance use: a transdisciplinary perspective". eng. In: *Substance Use & Misuse* 39.10-12 (2004).

[14] Mark W. Stanton and MK Rutherford. "The High Concentration of U.S. Health Care Expenditures". In: *Agency for Healthcare Research and Quality* (2005).