Retrust: A Vision for Decentralised Reputation

Liam Zebedee
https://liamz.co

With thanks to: Alec WM, Nick Beith, Abram Symons, Ross, Marco, Mick de Graaf, Matthew Carrano, Nathan, Marijn Bent :- for all your discussions and input into these ideas.

Introduction

Trust after blockchains

Trust and reputation are interchangeably used to refer to a fuzzy metric of human social interaction. Trust differs notably from economic resources in that it is infinite in its supply, a right given to every man, and incredibly hard to earn - it is yet a scarce resource.

Blockchains have upended trust through cryptoeconomic incentives that align actors. Like the Internet made the distribution cost of information marginal, the blockchain makes the cost of creating trust marginal. A smart contract can set out the rules of a relationship, own assets as collateral and perform the basic duties of a trusted third party for the marginal cost of paying the miners.

What is the value of reputation when smart contracts can be made? Simply put, there are still opportunities for maliciousness:

- Curated reputation marketplaces do not scale naturally (Circle tokens) or require manual handling when malicious actors cause trouble
- Non-curated protocols are vulnerable to Sybil attacks

The value of reputation

Reputation is an integral part of the new wave of service marketplaces, like **Uber** and **AirBnB.** It has been a core part of goods marketplaces for a while, with **eBay** and the like.

Using reputation as a signal, marketplaces can:

a) **curtail the behaviour of bad actors** - such as a drunk rider, who will be banned from Uber if their rating goes too low.
b) **incentivise good behaviour through market mechanisms** - drivers with higher reputation are matched first over others

Reputation mechanisms scale, so long as the reputation signal reflects reality (see information asymmetry).

So what distinguishes reputation and trust?

- **Trust** - an agent-specific commodity that they create in any amount of supply. It is scarce.
- **Reputation** - a social score that arises from interacting. Interaction is exchange between two agents, wherein it can be any resource, including money and tokenized representations of trust.

The promise of decentralised reputation

Decentralised reputation is thus an interesting challenge: **what if we realised the benefits of decentralization (lower costs, greater accessibility to others) for reputation**?

While it can be said that with decentralised reputation, we could reduce the price of an Uber, and provide more power for drivers/riders in a marketplace, this is **not** the most interesting way to analyse it.

Instead, let's frame it in terms of **what new products/services we could design, given a way to measure the reputation of people?** What mechanisms would we be able to build, what social structures could be enabled? What human behaviour arises when your actions do follow you?

> **Core proposition #1**: Just like how the free market allows everyone to choose between providers, we should be able likewise to choose who we trust and let that worldview be a part of and govern every interaction.

Benefits of decentralisation

For those who are in the blockchain space, they know that decentralisation has benefits. The articulation of these benefits is more often than not, attached to the use case at hand (financial intermediaries and Bitcoin, decentralized assets and cryptokitties).

However, there is still a profound vacuum of users for dApps. The reason for this - we haven't hit the perfect balance of costs and benefits yet, and thus not a user experience that is compelling enough to become a product.

What does the spectrum of blockchain decentralization provide in terms of benefits when implemented correctly?

- **Less trust = Less cost for interacting**
- **Reduced risk** in agreements = more confidence
- **More degrees of freedom in interaction:** thanks to new ways of representing goods (ERC20, ERC721 tokens, DAI stablecoins) and the Turing-complete flexibility smart contracts, we can build styles of interaction that weren't possible before
- **Fewer points of failure**
- **No censorship** and **accessibility for all**
- **Openness**
- **More ownership** - users own what they contribute, which can lead to more meritocratic structures.
- **Worldwide scale** - don't forget that the platform we build upon, is worldwide. So anything that is beneficial, is beneficial for the world.

Read further:
The Benefits of Decentralization - Doug Petkanics
https://medium.com/@petkanics/the-benefits-of-decentralization-88a0b5d0fd39

Keeping these benefits in mind while designing, means our eyes are more open to possibilities of problem-solving. Believing in a real quality, like "openness", "fairness" (DAO voting and the like), "ownership" (through cryptoassets) is essential to realising the tools we have and how we can cut through barriers.

Core proposition #2: the core goal of the decentralisation/web3 movement is not incremental improvement, but transformative change.

The ideal UX of reputation protocols

Organic usage. Reputation should be interaction-based. There should be no need to specify trusted friends/seeds (ex: Circle), nor keep this information updated, as it is automatically derived from interactions.

Application-agnostic. Reputation should not only be portable between dapps, it should interoperate to support a user's identity.

Open and accessible. The ability to generate trust should be free, as in real-life. Not based purely in economic expenditure (stakes).

Musings on economics and capitalism

https://en.wikipedia.org/wiki/Principal%E2%80%93agent_problem

https://en.wikipedia.org/wiki/Moral_hazard

https://medium.com/scalar-capital/an-elegant-relationship-dai-eth-mkr-4e4d5e69590

https://twitter.com/naval/status/1012211955459690496

Recently I've delved into economics. Here are the important concepts I've learnt about:

- **Risk**. Risk is the expected value of an event. The expected value is the probability of such event, multiplied by the payoff function.
- **Firms**. Firms are the structures we use to organise ourselves efficiently. They come to exist because of 1) economies of scale with transaction costs.
    - Due to the wicked problem arising from the uncertainty of incomplete contracts, firms are lowest risk vehicles for contracting.
    - Due to the **hold-up problem** (prisoner's dilemma): firms can effectively acquire other firms, eliminating efficiencies stemming from the game theory of competition. An inefficiency can arise as a result of power, wherein bargaining takes place.
        - In relation to risk, power is determining the certainty of some events. It has its own value independent of $.
        - If you are reliant upon me for materials, I can either be acquired (undergoing a game of discounted future present value of XYZ) or negotiate (wherein I use my information to determine risks)
- **Capitalism**. Incentivises in a decentralised manner, the creation of value through a system of private property. Private property is enforced by the **law**, which is maintained by courts that are financed from taxes.
    - The government is an effective insurer for the law through taxes.
    - Firms and individuals are both incentivised by power: *it is agency that defines agents*. Firms are a more efficient structure for pursuing power and undertaking risks. Firms are designed to create value, owned by the firm, and governed by its shareholders.
- **Information and power**. Information enables power from the core, and extending outwards is the real reason firms exist - so they can have power. Information has an asymmetric payoff.

- **Value**. Value is the parent of money. Values can be *intangible*, wherein they don't have a number attached to them - such as human rights. These values are enforced by law. Values that is tangible is most often so in the form of money. Money is the invention that allows shared co-operation.
    - Progress creates value, and is incentivised for agents by capitalism.
- **Crowdsourced reputation**. Reputation in Uber is crowdsourced - it represents a signal of risk.

What taxonomy thus does EBSL fall under?
EBSL enables a new form of value based on a social consensus.
Governed by the individuals of a community

The problem previously is that of Sybil attacks
We can't have universal decentralised reputation like in Uber

Because the signal of risk can be hacked:

- how can we verify rides?
    - By appointing a person to do so
- How can we track reputation?
    - By allowing users to submit reviews after a ride
- How do we mitigate the ride verifier from corruption?
    - In small groups of 50, it is unlikely as the social ramifications will be terrible
    - But this will not scale due to the capacity of only one person
    - Thus another person must be hired - this is the transactions cost theory of why a firm exists
- With more people, the risk that one will be corrupt and escape liability is high.
    - The ride verify can certify rides that haven't happened, and thus inflate the reputation of some drivers. The risk signal is thus ruined.

This is **collusion** or **bribery**. Some countries in the world are more corrupt regimes than others. The difference is their governance of intangible social value.

Governance is an icky-problem:

- We need to hire more ride verifiers in order to scale
- But how do we decide on who to hire?
    - Decision-making is effectively using information from a diverse set of agents to do something
    - Doing something is with all of the power of the firm, including its property (tangible assets) and intangible assets (social relations, etc)
    - The "survival" of the firm depends on its ability to make "low risk" decisions.
        - "Low risk" relating in this context to the risk of ruin, wherein the payoff is a cost that exceeds the firm's capital assets.

        - It also concerns maintaining the values (intangible value) of the firm itself: chiefly power, but secondly other things...
- How can we build decision-making that rewards low risk decisions?
    - Allowing votes from anyone is an example of a Sybil-vulnerable strategy, since voting networks can effectively be forged by single individuals.
    - In Bitcoin/Ethereum, economic work is used to mitigate Sybil attacks - as there are sunk costs with performing it.
    - But Bitcoin/Ethereum rely on a consensus algorithm that is based on **objective knowledge**. Given a set of block headers as *votes*, the longest-chain rule decides the consensus of the longest chain.
    - But how can we achieve consensus on a value which cannot be verified/named objectively?
        - e.g. “profanity: I know it when I see it”
        - The value of a well-written article
        - The comfort of an Uber ride
- Governance is about value, and making decisions with high reward from risk, even if the reward’s value is intangible.
    - Voting is currently done by shares of a shareholder. Shareholders typically allocate capital in accordance with both a *profit motive* and their *personal values*.
        - Boardroom CEO’s are voted in by shareholders
        - In a startup, investors can influence decisions, founders can as well.
    - Large companies typically do decision making with individual authority.
        - Property ownership includes human labour capital
    - Firms exist because of greater power for change at lower cost - they can be **realised** for the gain of its shareholders
    - Economic-based voting largely works, because of the supply/demand mechanics of a company’s shares
        - new members receive only a small amount of power
        - old members (CEO, founders) usually hold their shares, and thus retain the values of the org.
- Why don’t we allow the government to be run with shares instead of votes?
    - Because of tyranny of the majority
        - This is again a case of intangible rather than tangible values.
        - Ie. black people shouldn’t be able to own property
    - Risk of losing values of “universal property rights” is not quantifiable, hence voting with economic power is not incentive compatible (ie. bribery/collusion is possible)
        - Neither is voting with democratic rights either.

What is EBSL thusly?

- A consensus algorithm for subjective knowledge
    - Subjective beliefs in the form of (Belief, Disbelief, Uncertainty)

    - An algebra that includes operations for discounting one belief by another (transitive flow) and adding beliefs together
    - A consensus algorithm which converges on a matrix of values
- An evidence component which maps to a scalar quantity
    - Quantifying evidence for/against a POV

How does it fit into this problem domain?

- We imagine a fictitious replication of Uber in a decentralised setting, *dUber*
- dUber is founded by a set of participants in a local community
    - They agree on the *intangible values* of the organisation
- Selecting a ride verifier occurs as so:
    - The decision made has a degree of risk attached to it. To enforce that only low-risk decisions are made, we take into two considerations:
        - The tangible cost of the risk - in tokens
        - The intangible cost of the risk - in belief
    - Shareholders post votes on the intangible cost to the organisation's values, based on their own subjective votes
        - A voter might believe that this ride was likely fake, and hence, allocate a strong disbelief of opinion (0.05, 0.9, 0.05)
        - Another might not have enough information to ascertain, and allocate a large portion of uncertainty opinion (0.01, 0.01, 0.98)
    - These opinions are processed according to the consensus algorithm, which arrives at set of points of view (POV)
        - To build a belief network, we have two types of edges.
        - Trust between members, as established by initial incorporation, is an edge
        - The other edge is the opinion on the proposal (of ride verifier, as described above)
    - The POV's are not useful on their own. Finding their EigenVector allows us to determine the weighted consensus of a subjective opinion.
        - This is different to a multi-class PageRank, as we are dealing with subjective logic.
        - Using the uncertainty component, we can estimate a degree of **collateralisation** that would reduce the risk to the organisation (**insuring against what we don't know**)
        - Using the belief/disbelief component, we can 'name' the value (related back to the paragraph in the governance section)
            - What we, the undersigned, **do know** about the suitability of this person as a "rider verifier"
    - The risk undertaken of adding an additional rider verifier increases the firm's capacity for profit.
        - The rider verifier ensures a greater supply/demand, and thus there is more action in the marketplace. Due to economies of scale, this may increase the firm's power. Likewise, due to platform fees, the firm earns rewards from these risks.

        - The fees are generated by users buying the token to transact in the ecosystem.
        - Stakeholders are rewarded according to their risk appraisal.
            - Unlike a traditional firm, where shareholders reap all of the profits of enterprising activities
            - In this system, stakeholders can govern based on their investment into the ecosystem
                - Employees are paid in the token, which they can exchange for shares and for $
                - They can share in the risk and reward of the enterprising, directly related to their decision making
                - By specifying the uncertainty in their beliefs, they ensure the organisation's survival (by neccessity of collateralisation)
                - But they are also rewarded for enterprising through profits they receive on decisions
        - If the rider later becomes a bad rider (low risk), we can liquidate their staked shares to rebalance the value of the collateral token
            - The collateral token is the ecosystem token
            - Used for services, this token is bought from an automatic market maker by users
            - By staking the token, you can govern with it
            - You receive dividends on the staked amounts, as staking decreases supply and increases price
            - The benefit from risk-taking financed by the DAO, will be paid into a bonding curve contract.
    - The reward for risk-taking is profit into the organisation.
        - DAI -> profit -> bank
        - Governance does activity
        - Governance also decides on how to reward activity
        -

The problem with this approach? It doesn't scale.

- Requiring firms to vote on every new member is costly, and at certain points, might detract from the **subsidiarity** of the organisation.
    - If the membership grows to a point where members are more distant from each other, it introduces information asymmetry and risk
- Allowing members to extend the organisation themselves is possible
    - They "self-dilute" their sharepower, wherein they make an endorsement of (1., 0., 0.) - this puts their liability on the line
    - They can invest without significant dilution, wherein they endorse (0.5, 0., 0.5) - this puts 50% liability and 50% liability of the joining party.
- In doing so:
    - Members are rewarded for risk-taking with payoff

    - If the risk results in the user being liable, their assets are liquidated in order to replenish the value of the token
    - If the risk results in a payoff, then the user is rewarded
        - Risks are insured by collateral, wherein the owner of such collateral is a [partial] beneficiary of the rewards
        - Collateral is typically the staking of the governance token
        - The parties taking upon the risk, reap the reward proportional to the capital that was invested to be theirs

    - Members who endorse other members risk-taking can be rewarded too.
    - Rights to profits is allocated such that members are using the power of the organisation
    -

- How do we continue insuring the system against the risk of decisions?
    - Trust flows transitively. Uber continues to trust the credit card companies for up-to-date information security. In the same way, risk is continually liable on those parties that stake their reputation.
    - 100 tokens are created, which are vested between 5 members.
    - The token represents price signal in the ecosystem. Initially member will only have their tokens.
    - Decisions are made and those tokens are vested/staked in the organisation.
    - The token is the network insurance - parties can buy the token from a bonding curve contract. In doing so, they can propose governance solutions.

- The firm exists to combat the hold up problem, which is effectively bargaining/negotiation
- When we are adding a new shareholder, we are bargaining *human capital* for *risk*
    - The human capital is the shareholder, who can bring their investment and thus share a portion of profits from the risk being undertaken
    - The risk is an event where the shareholder brings:
        - 1) intangible value loss
        - 2) tangible value loss
    - The risk liability falls upon the stakeholders, who govern the creation of value. The payoff can be measured by the value of the ecosystem token.
        - In the case of Wikipedia, value is not tokenised necessarily. However, we can still build a reputation network wherein we reward actions, and thus use it for formal governance. There is still a system of governance in place, but relying on informal mechanisms.
        - In this case, the payoff of the risk of onboarding a new member can only be expressed in some degree of consensus.
    - The stakeholders vote on the riskiness of the proposition.
        - How can this scale beyond 150 members? By default, there could be some trust transitivity, but the liability would be personal.

        - Ie. endorsing a new member brings liability to your stake in tokens, at a minimum collateralisation of 100%.
    - How does the feedback loop work?
        - Stakeholders pool their investments to take upon risk
        - They are weighted according to how much they've invested
        - They are rewarded by the ecosystem token
            - The mechanism of distributing this is up to the domain
            - In a for-profit context, it will be used to provision goods/services
            - In a not-for-profit context (ie. wikipedia), it will be governed and rewarded according to processes. Ie. reputation, voting, gift economies
    - What is the mechanism of the feedback loop?
        - Objective: minimise risk, maximise payoff
        - Can the payoff be negative? What allows **ruin** to happen?
        - Can we distribute liability across shareholders according to their risk appraisals?
        -

Exploring a new mode of co-operative enterprise

- Same as starting a co-op **company**.
    - Shareholders invest assets for equity in *shares*
    - Governance linked to sharepower
    - Limited liability of shareholders
    - Organisation typically pursues *social goal*
- But differently:
    - Sharepower is allocated according to enterprising ability
    - Governance is based on voluntary association
        - Rewards are distributed proportionally
    - Shared value (token) is the intangible value
    - Shared reward (external value like DAI/payments) is

1. Govern new organisation
    a. Create shares from capital
2. Propose enterprising
    a. Vote on the risk
    b. Enact based on member's capital **or** a sharepower majority
3. Enact enterprising
    a. Returns are owned by the organisation
    b. If members-capital:
        i. Bargain a transaction of capital to shares.
    c. If collective endeavor:

i. Distribute shares according to bonding curve.

How do you kill off shareholders who take bad risks?

- Their sharepower is directly staked in their ability to perform risk-taking
- Their risk-taking is a SHORT on their shares. They get the capital by locking up their shares.
    - But then how do people vote?
- I think it should be forward-facing:
    - Rules are decided upfront

How does this relate to reputation?

Reviewing article on value:

https://en.wikipedia.org/wiki/The_Social_Contract

- the Kantian categorical imperative: human beings should always be treated as ends and not as means.
- The ambiguity of “value” vs “values
    - What is the most common form of unpaid labor in our society? Surely, housework. And what is the principle way in which values are invoked by pundits and politicians? “Family values.”
    - The value of “values” in contrast lies precisely in their lack of equivalence; they are seen as unique, crystallized forms.
- The tokenisation/quantification
    - These tokens can be more or less formalized. In our own society, the realization of unpaid domestic labor, for instance, is not especially formalized: it is imagined largely as love, or perhaps, in more concrete terms as the future ability to play with one’s grandchildren.
- On social structures (governance)
    - social structures of this kind didn’t really exist in any material sense at all; they were imaginative constructs that were only realized during ritual moments
    - “society” is made to appear in its total form. But Turner’s formulation also offers a much more compelling explanation of why it must be made to appear: in order to provide an arena for the realization of social value.
- On universes:
    - there is an internal game, where members of a certain status group are vying over their own peculiar notion of esteem;
    - on the other hand, there is a larger struggle within the society as a whole to establish that particular notion of esteem, and the style of life with which it is associated, as the highest or most legitimate value
    - **Politics**. this is what politics is always ultimately about: not just to accumulate value, but to define what value is, and how different values (forms of “honor,” “capital,” etc.) dominate, encompass, or otherwise relate to one another; and thus at the same time, between those imaginary arenas in which they are realized.
    - . It’s only then, when universes collide, that it occurs to anyone to cement one universe’s status by insisting that it is somehow more real than any of the others,
- On recursion of value systems:
    - If value systems create a potentially endless series of little worlds—“a thousand totalities”—and if the ultimate **stakes** of **politics** are negotiating how these come into relation with one another, then the obvious question is how?
    - Infravalues
        - the tacit, interior values that inform how ones goes about pursuing value within certain fields (in the case of truth claims, logical consistency, verifiability, etc.) and

reassembling them as an explicit value in themselves. We can refer to such tacit interior values as infravalues. Rather than being seen as ends in themselves, they are thought of as necessary prerequisites for, or means to, being able to pursue those forms of value that are socially realized in the kinds of arenas I have been describing.

- Metavalues
  - This notion of “efficiency” is a perfect example of an infravalue translated into a metavalue.

Governance, risk and enterprise

These are some ideas I’ve been brewing around a consensus algorithm I’ve been passionate about for many months. It introduces a couple new concepts, namely the idea of belief-uncertainty model of knowledge.

With blockchain, we have effectively achieved marginal cost for trust. We can make contracts, agreements, with other people in a way that is as efficient as distributing movies over the Internet.

But still, we are searching for the secret of how tokens reinvent the system. Not yet have we seen a blockchain “business” - DAO’s are the most interesting experiment of current, yet all of the major innovation has been in decentralized finance.

Fundamentally, the law exists to enforce two things in my opinion:

1. The mechanisms to achieve capitalism - private property, systems of liability (corporations), fiat money
2. The mechanisms to achieve intangible value - human rights

What a blockchain does is provide a completely different jurisdiction with which to implement law. And with this comes some interesting facets -

1. Limited liability was originally invented to increase investment without increasing risk of ruin for the investor.

Decisions are taken by organisations.

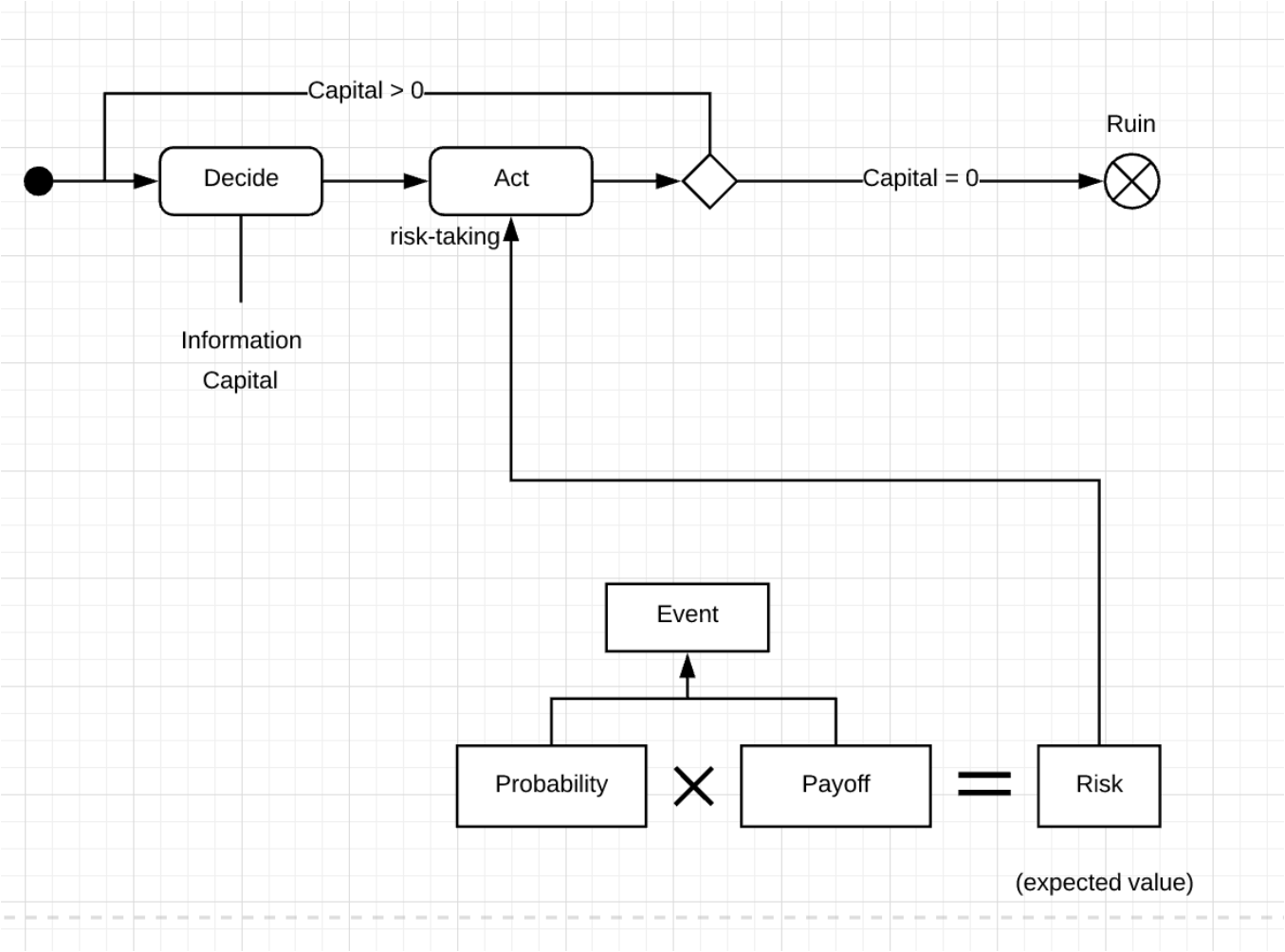
Capitalism involves rewarding entrepreneurs much more than the individual actors involved.
But is this necessarily the best idea?
What about individual leverage?

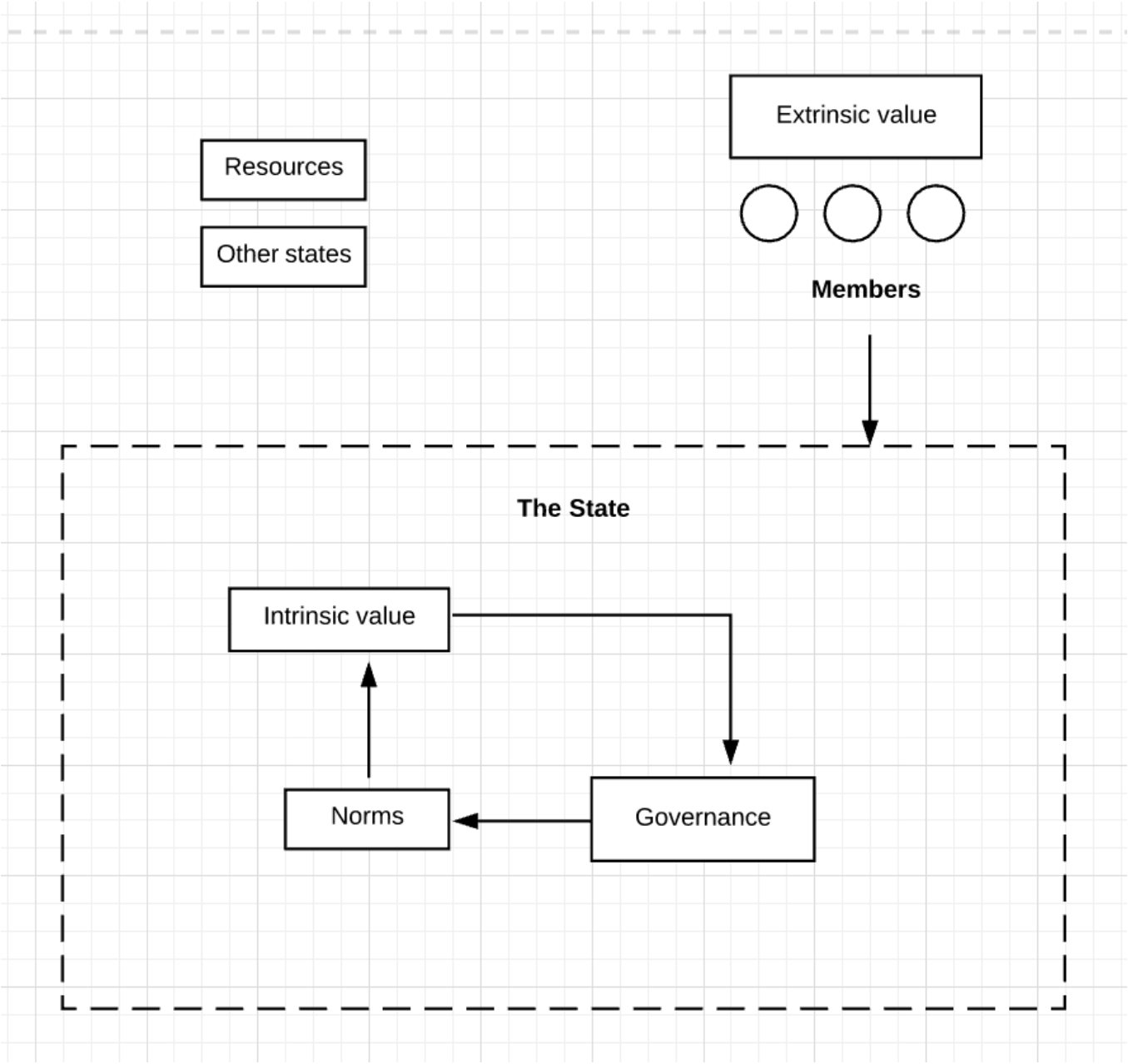
Let’s imagine a completely different type of governance based on crowdsourced risk appraisal.
Token economies are about orienting value within the community.

So imagine our ridesharing example:

- We begin our organisation by investing $10K between a collective of 10 members. Each member commits to the purpose of the organisation, as building a local ridesharing network for members.
- We imagine governance to follow in any style of startup, involving everyone doing everything at once. For the purposes of our framework, it doesn't matter. The votes may be different but the mechanisms are the same.
- Stakeholders must vote on how to spend the capital of the organisation, lest they only have access to their personal capital.
- Voting is a process where the stakeholders come to a consensus on one belief - whether a decision will ruin the organisation.
    - This is an implicit belief. Organisation converts capital into more capital through enterprise, which is the activity of risk taking. The risk is the expected value of the probability of an event multiplied by its payoff.
    - Typically, we will be realising the possibility of a *positive* payoff through the financing of capital.
    - But if the payoff is negative, it will also incur a loss.
    - If there are too may losses, the organisation will be unable to finance future enteprising, and thus become *ruin*ed.
- This model of governance is decentralized, rather than centralized-
    - Every user is entitled to license their risk to another enterpriser, and share in the rewards if that risk pays off.
    - The shared capital pool is allocated such that users can agree in whole to sharing in a venture's liability
        - The incentive - more capital the higher the success rate
    - The organisation governs its value through the share
        - The share is a token.
        - The governance process enables risk-appraised investment from its members
        - In return, the organisation can receive its revenues back in
            - The token itself
            - Other forms of value (DAI)
            - Intangible benefits
    - When users reappraise their risk, they commit capital to invest. And when revenue comes in, they are able to govern how the reward is distributed.
- The key insight is this -
    - Where value equals the token
    - Organisations can govern mechanics of power and value generation
    - So an 'employee' could get paid in DUBER token
    - And this token could be according to a bonding curve, which allows them to share in the risks through governance, *and* take their share of the profits (through some automatic market making)

    - Every stakeholder is allowed to dilute their share of the organisation's equity. This is analogous to a share. However other stakeholders will not have any liability unless they endorse such a member.
    - The organisational liability is based alone in the token, which is a token bonding curve. Any member can exit at any time, thus selling their shares.
- So how does the incentive structure work? How are **rewards** shared? How is **risk** distributed?





Uber drivers organise into a union
They share the same infrastructure, the brand, the app
The Uber reputation is based perhaps on a star rating
But is backed up actually by insurance/collateral
Every member has their risk appraised by a complex trust network of other members
Value being created is twofold:

- Tangible - cost of a ride
- Intangible - not being raped?

The intangible is represented by the token
What the token represents is always intangible value
It cannot represent anything else
The intangible value is equivalent to power

Reputation = reliability = repeat liabilityT

A user might give you a good rating for a ride
And that rating might be part of a framework of endorsements
Whereby the user can sell that rating token
And it translates into the native share token

Reputation is just risk
At the end of the day, we just care about liability
If a user is riding with you, their endorsement of your account - that is part of the equation
They come out clean (0 cost)
But they still have to stake something

The rider however earns an endorsement (0.8,0,0.2) for 4 stars
And the network is able to determine their effective insurance rate/backing
Depending on the collective risk appraisal
Which stems from the decentralised risk setup based on governance
Ie.

- The directors/main management decides on who will verify rides:
    - Ride verifier verifies rides
        - It might be FOAM-based location points
        - It might be community members

We can calculate the degree of liability simply from that of its members
If it is the DAO, then it is the whole organisation's assets
But if it is an individual line of risk, then it is just the collateral locked up here

Let's imagine there's a complaint
And the driver has done something bad (idk)
There is a cost C which is maybe 20DAI
This cost is incurred first by the person who endorsed the user, and then leading up the chain
We can govern this:

- The risk of corruption is tied with the risk of the token's value
- The token represents the value of the community's word

Users perhaps stake an amount to make a dispute?
And based on the linear power (the eigenvector of reputation) of users
We can enable decision-making

We are always dealing with risk
And when we aren't dealing with risk, we are dealing with intangibles or risk buildup (black swan)

Imagine that the rider gets paid in the token
The organisation must transact in its legal tender
Otherwise there will be no incentive since the value capture doesn't return to shareholders?

A typical organisation issues shares, which bring dividends
So a token might have dividends/a right to dividends
The dividends are the benefit of the risk being taken
But the organisation can vote on the degree of risk

At any one time, the shares represent power
The incentive is - as long as a user can maintain his stake, they can maintain their power/influence
And they can vote on the degree of dividends distributed

There is 100% of share power
Created upon vesting
And then afterwards users can dilute their own personal equity?
At a risk to them

Subjective consensus - the algorithm which allows a group of users

Decision-making effectively takes human capital, which converts crowd information into a risk signal
Subjective logic allow us to model this quite well
But how do we orient the growth of the value as a feedback loop in the system?

Ie. why don't firms award employees voting rights? Because they are not undertaking the same degree of risk
But they are - they are awarded equity, which permits some degree of power (albeit very small)

How do we scale the shareholders?
How do we incentivise them?

Risk is probability (over time) and a payoff.
If the payoff is negative, then there will be fewer dividends paid out
Because the payoff should always be tangible, no?
Payoff can be tangible in the token itself
But where does the token get value?
In the case of using the network.

How do members join? They all agree to mint and divest shares from a pool of collateral they create
Ie. a normal company with starting capital
How do we scale the values?
Individual members endorse other members
And their reputation is scaled according to their vesting period

- Start dUber
- Have 20 tokens
- To use the network, users exchange tokens on Uniswap
    - Tokens are put up at a price by members
- Users pay in the tokens, the shareholders receives a fee of 1%
- Shareholders can burn their power to withdraw tokens
- How do new shareholders get created?
    - They govern a set of rules on how this works.
    - **Vesting mechanism**: insure against risk of shareholder malfeasance by group voting as to the uncertainty of adding a shareholder.
        - The uncertainty thus represents the number of tokens that must be bought
        - The tokens are thereby vested for that period, ensuring an economic stake over time.
        - The tokens are investment into the organisation. They are an investment into the intangible value by means of scarcity (locking tokens up).
        - The agreement is carried out between the stakeholders and the new stakeholder. They agree to the additional investment as a risk, insured by the token stake.
        - They use the consensus mechanism to vote and achieve consensus upon the risk being undertaken by their body.

    - Alternatively, the stakeholder who is inviting the user takes upon the risk themselves.
    - But the invited stakeholder is only entitled to their weighted portion of the profits/shares
    - That stakeholder does however change the share price when they transact.
        - If they dispose of shares to the bonding curve, they get $.
        - If they convert

The problem, is of building that belief network. How do governments protect against corruption is maybe a problem of social cost - where societies are less socially integrated, there is higher risk of corruption, as the value of the social fabric is worth less in the collective.

- Making an organisation have a non-fungible reputation token.
    - This is a tokenisation of the intangible values of the organisation.
- Building this reputation token atop a sustainable media:
    - GoTverning actions that represent the values of this system
    - Issuing bonds

The idea is that the organisation is initially pure with respect to its value.
Its members allocate trust freely among each other.
When there are profits, they are paid in proportion to the members trust base

- Members with higher weight receive more income.
- The profits are priced in the org's native token.

The token represents the economic tie - if the organisation differs in value, the token can be forked/split in two.

As it grows, it develops mechanisms to award and recognise trust amongst its members

But first, maintenance:

- If a ride verifier destroys value for the organisation?
    - The liability is distributed upon the shareholders who voted most strongly
-

- Uncertainty and risk
    - Using the uncertainty to collateralise, facilitates the organisation to grow and take risks. Without this, members vote with less information than they truly have.
-

- How are belief networks registered?
    - This is left as an exercise to the reader - it depends on the organisation's view on risk.
        - An organisation that requires massive amounts of investment would be open to taking upon risk
        - An organisation could design mechanisms such in a way that rewards value contributed by members (ie. Web 2.0 reputation systems)

State of research

Retrust's core algorithm for reputation and holocratic quorums are implemented experimentally here: https://github.com/liamzebedee/retrust

The key algorithms that are used are:

- Evidence-Based Subjective Logic (EBSL) - for computing reputation
- Modified PageRank / eigenvector analysis - for computing quorums

In early November, I corresponded with the team who designed EBSL, and they gave me their code. In December, I had reimplemented it in Numpy, providing numerous benefits, among them speed and flexibility of analysis.

As I've now finished my last contract, I started drafting this grant proposal.

Concepts of reputation and quorums

Reputation is implemented using EBSL. In EBSL it is implemented as a generic quality of (belief, disbelief, uncertainty), which sum to 1 to form an **opinion**. This can be used to model many things, among them, reputable behaviour, but also subjective qualities such as the "accuracy" of a news article.

Holocratic quorum is how I would describe a voting algorithm I've assembled in Retrust. It provides the weighted influence of a node in a network of interactions, accounting for their reputation in that network too.

Reputation is computed by transforming a matrix of interactions into a matrix of subjective logic opinions, and running an algorithm (EBSL) to converge on a reputation matrix. The reputation matrix itself, is N x N, wherein each row is one node's perspective of the reputation of every other node in the network.

Because of the way EBSL works, these subjective opinions, which exist on a relative scale, can be converted back into their absolute form of total interaction value. Using these new opinions, moderated by how much each node is trusted by any other node, you can apply PageRank to converge an absolute rank of a node's interactions, i.e. a representation of influence.

Attacks and issues in reputation protocols

Considered and still to be written.

Sybil networks

Bribery

Zero-sum risks

Disputes and arbitration

Bootstrapping trust relations

Proposal

Project objectives

- Communicate and socialise the algorithms and ideas of decentralised reputation and holocratic quorums
- Explore and research use cases of decentralised reputation and holocratic quorums
- Develop use cases and experiment with real users to build understanding and guide design of the protocol
- Design and implement the open-source protocol software, which can be consumed/used by other dApps in an **interoperable** manner

Project methodology

Being part R&D, part product development as a protocol, I advocate a design thinking based process to the product development.

Design thinking is about **developing knowledge and understanding around people and problems and proceeding to test those assumptions via developing prototypes**. This 'design thinking' process is characterised by five distinct stages: empathise, define, ideate, prototype, test, implement.

Use cases

Case	**Context**
Amazon's fake reviews problem	Based on a discussion with a fellow developer in the blockchain space, **Marko Baricevic**, Amazon has a huge problem with fake reviews. This is a great starter use case to flesh out the protocol semantics: ● Based in a real-world problem ● Integrates issues stemming from networked trust (Sybil networks) ● Small investment to test hypothesis (open-source goods marketplaces are plentiful)
Decentralised credit network	Extensive discussions with **Abram Symons** (of IdealMoney, EtherBank and BrightID) about designing a decentralised credit network.

Mitigating fake news	Fake news is already an issue, but with the developments from Nvidia in the space of photorealistic generation/modification of images and videos using AI - it's more pertinent than ever to approach this problem.
Education/accreditation platform	Based on another conversation with a colleague, **Mick de Graaf**, there are two problems: ● **Accreditation is lagging**: experience is still the best measurement of knowledge, but we should be able to provide better measurements of knowledge without economic output involved. ● **Education is poor:** if you want to get well-educated in blockchain development, the best resource is often going at it yourself. But, there is hard evidence that mentors will accelerate a student's learning. Why can't we have our cake and eat it too?
Package security	

Areas to explore

Area	**Relevance**
DAO's, governance	Sybil-resistant reputation and voting mechanisms are a key property that EBSL provides.
Scalable P2P agents	Something like Scihub, which relies on Live Proxies to route requests for papers it has not cached, could be made much more resilient by decentralization. Multiple aspects of its infrastructure can be decentralised, such as the frontend (IPFS), search index (token curated registry), file hosting (IPFS/BitTorrent), and DNS (ENS). However, the provision of papers by the live proxies remains as a potential vector of abuse. Integrating a decentralised reputation mechanism, this could be curtailed, and Scihub could have a true Napster moment in its antifragility.
New forms of funding for digital agents	Related to the Scihub example, if live proxies have a reputation that follows them based on how users rate them, perhaps this could be designed as an exchange. Much like how ZRX tokens are used in 0x for both paying the relayer fee, and as a governance token, the counterparty **necessitating a**

	vouch of trust for services could more easily incorporate payment into existing models. This is more related to design of a standard than a technical innovation.
Identity	Identity is a fuzzy concept grounded in interactions and linked to reputation.

Project milestones and timeline

TBA - need to investigate grants/funding options further to determine best path.

Funding requirements

Personal:
6mo work.
Rent + Food + Travel to confs.