The Importance of Reputation for the Evolution of Decentralization

By Craig Calcaterra and Wulf Kaal

Abstract

Chapter 6 underscores the importance of reputation systems for the decentralized economy. Reputation is the proper incentive, instead of money, for motivating the most efficient cooperation and long-term stability in business. Existing Web3 smart contract solutions often incentivize people to devote their energy to taking advantage of their business associates in anonymous environments. Through the promise of future business opportunities, reputation changes the relationship from adversary to partner. Reputation changes the transaction from a single-stage zero-sum game into a repeated positive-sum game. The value that is created in the transaction is that the reputation of both parties is improved in a harmonious profitable transaction for the long-term.

The book can be accessed here:
https://www.amazon.com/Decentralization-Technologies-Organizational-Societal-Structure/dp/3110673924/
and here:
https://www.degruyter.com/view/title/569051

Chapter 6. Reputation

Reputation is the proper incentive, instead of money, for motivating the most efficient cooperation and long-term stability in business.

Markets are a necessarily chaotic environment that must permit an enormous variety of behaviors, where all parties need the freedom to invent new strategies for cooperation. Such freedom also creates limitless opportunities for preying on anyone with less information. Such information asymmetries create endless arbitrage opportunities: renegotiating, leveraging an opponent's sunken costs, pushing the limits of the law or breaking it outright. Markets lose their ability to create value and profit

when the efficiency of cooperation is sapped by opportunistic behavior. When the environment becomes too adversarial, when trust is diminished, collaboration is no longer profitable. The market collapses.

How do you prevent the chain reaction of opportunistic behavior provoking worse behavior until the market collapses? Relying entirely on strict legal enforcement is not practical, since it limits the opportunities for creativity in business arrangements. Strict legal enforcement is not efficient, because all energies devoted to policing are energies that could be used to cooperate productively. Strict legal enforcement is not possible when the market becomes sufficiently complex and dynamic—laws cannot keep up with the creative contracts that arise when leading experts are continually improving business arrangements.

To prevent people from devoting all available energy to taking advantage of their business associates, you need to change the relationship from adversary to partner. Reputation does this with the promise of future business opportunities. This changes the transaction from a single-stage zero-sum game into a repeated positive-sum game. The value that is created in the transaction is that the reputation of both parties is improved in a harmonious profitable transaction.

In this chapter we discuss what reputation does for an organization, how to build a secure reputational system and what to avoid, and the consequences of secure and meaningful decentralized reputation for society and the economy.

The failure of many DAOs, so far, has been their reliance on the good will of the members of the network. A designer will often imagine the members are incentivized to help the network so they can have business in the future. As the network grows, however, the members become more anonymous. Individually they become less important, so cheating is more locally enticing and less noticeable globally. Eventually (or immediately) the system will collapse when it becomes obvious cheating is the best individual strategy.

Many recent DAOs do recognize how important reputation is, and so, there have been many flawed instantiations of reputational tokens. The system most commonly used is called the Web of Trust. After explaining this natural but flawed idea, we introduce a system that uses the power of decentralization to solve the problem of secure reputation by putting the power to police reputation democratically in the hands of the members of the network.

We now have the technological tools to create transparently auditable reputation on the global scale of Bitcoin. Light speed digital internet communication has eliminated the information asymmetries that attended the Maghribi traders. Instead the modern challenge is to foster productive collaboration between anonymous actors from diverse backgrounds in globally large groups.

The tools of P2P technologies upgrade our ability to create valuable reputation. More accurate mechanized accounting is available through smart contracts. A transparent history of past bureaucratic transactions enables decentralized governance and regulation. With the proper design, a cyclic relationship between customers, the DAO member workers, and the platform's protocols and history, gives feedback loops which engender continual evolutionary improvements. The transparency and open governance procedures create a fair environment that enables a DAO to evolve in healthy and productive ways.

The new technology of decentralized consensus with "triple-entry bookkeeping" that Bitcoin introduced allows decentralized networks to collaborate on profit-motivated projects while maintaining individual privacy with zero knowledge proofs. But they must be organized properly, with the proper incentives and governance.

We will explore what is required to build a secure and meaningful reputation system and suggest a basic architecture. First, we discuss a commonly used reputational architecture that is not secure.

Web of Trust

Most every DApp developer becomes aware a reputational system is necessary to keep their DAO together. Ideally a reputational system will run in the background without needing any conscious user input. As long as a member is behaving properly—following the stipulated protocols of the DAO—their reputation should improve automatically. Those who violate the protocols should lose reputation, so they lose power in the network and cannot cause as much harm. Most every developer comes up with a solution to automating reputation based on the Web of Trust. Every implementation we've seen stumbles into some minor variation on this same basic trap, so it's worth dwelling on what goes wrong before explaining an alternative solution.

The Web of Trust was first used in giving decentralized security to email and other internet data transmission technologies in a scheme called PGP (pretty good privacy) encryption, published by Phil Zimmerman in 1992. The idea is to design a system for growing a network of trusted public keys (see Section 2.8 above) specifying the correct owners of addresses. Then message senders can look up the addresses and be sure they are sending the message to the correct owner. The fear is that a malicious user can falsely claim ownership of an address in the directory in order to intercept messages. How does the decentralized network add new members?

A third party, who has previous reputation in the network as trustworthy, verifies that the new member is who they say they are. As more parties verify addresses, eventually within the whole system, the subnetwork of people you trust will include a chain of trust between members indirectly connected to the address you are requesting.

The more people in your trust network who verify an address, the closer the connection, the more trustworthy the information is.

The basic design which incorporates the basic Web-of-Trust scheme in an abstract reputational system is as follows. Imagine a network of people who participate in business transactions. Each transaction is recorded by each member along with a rating for how satisfactory it was. If Alice and Bob have a first transaction, Alice rates Bob and Bob rates Alice. The value of the transaction is multiplied by their rating from -100% to 100% to determine the reputation the transaction generates. The entire history of self-reports can be stored, decentralized in the blockchain, available for anyone to read. Alice's reputation is now calculated by one of many possible schemes for summing up the reputation contained in each transaction. Generally, the reputation generated by a more reputable person has greater effect on the sum than a less reputable person's transactions. And more transactions with higher value will create more reputation.

Unfortunately, the sockpuppet attack will suck all value from the network. Setting up fake accounts, an attacker can build their reputation by making transactions between their own accounts. Once their reputation is sufficiently large to trick a member, they can use it to cheat the system.

In response to the sockpuppet attack, a developer may choose to handicap the system by charging fees to make transactions (similar to DoS defenses) or imposing identity protocols—referred to in banking as KYC, know your customer protocols—to solve the problem. Then it would be too expensive to mount a sockpuppet attack, since you would need to pay for each transaction. This doesn't help. Such defenses push the cost of defending the network onto the users. The cost to defend it is exactly as much as it is worth to break the defense, except it's multiplied on every transaction with every member in the system. If the reputation is worth $1000, and it takes $900 to fake the reputation, the attacker has an incentive to do it.

Further, lessening the anonymity of your members weakens the power of the decentralized network. Personal privacy protects your members, so it's more secure. Members can be more transparent in their business dealings without fear of being victimized, so the decentralized network is more efficient.

These problems with the Web of Trust, incidentally, are part of why it's called "pretty good privacy" instead of "good privacy". It works well for low-value information transmission, but it should not be used for transactions involving larger wealth in the general economy. Those transmissions incorporate stronger cryptographic security.

The proper solution is to give your members more power over their reputation. Give the members themselves the power to police their own reputation. The leading experts, themselves, are the people who are best equipped to invent the regulations

for policing their own industry. They are best incentivized to defend their own reputation and future profits. The best way to encourage continual long-term improvement, is to reward them properly for policing and legislation and development.

Inductive argument for reputation architecture

We want to build a reputational system that is mostly automated, like Bitcoin, or the Web of Trust. So it should maintain decentralized consensus as long as the majority is running the automated program honestly, that is, they haven't hacked the program. However, we need to make a system that is not susceptible to the type of gaming that the Web of Trust is prey to.

In order to make a secure and meaningful reputational system, in a decentralized network, several requirements need to be met. Once these are articulated, the most basic elements of the architecture are revealed. This justifies the elementary design described in Chapter 4. We assume the most successful DAOs will be open to any anonymous applicant in the world for its members. Open membership and anonymity are not necessary to build a secure and meaningful reputational system, however, and so are not included amongst the following necessities:

Necessity #1: Forum. To remain decentralized, all members are assumed to be relatively equal. Therefore, evidence of all bureaucratic work needs to be posted in a universally accessible location for eternal review. Similar to blockchain digital currency creation, without a central verifying authority, every reputation token in a DAO needs an openly verifiable history. (Transparency)

Necessity #2: Validation pool. In a decentralized environment, consisting of potentially anonymous actors, the only fair way to assign reputational power is to allow all members to judge the value of contributions, democratically. To avoid the Tragedy of the Commons (the nothing-at-stake problem, "skin in the game"), reputation must be staked and risked with votes on work evidence. This ensures all experts are motivated to police every reputation-staked action, to protect the value of their investment.

Members who fail to participate (liveness fault) will be stably punished because reputation tokens are deflationary: if they don't participate they will not gain any portion of the newly minted reputation tokens, so their own unused reputation holdings will represent a smaller percentage of the total, so they will receive a smaller percentage of future reputational salaries.

To avoid sockpuppet attacks and tyranny of the majority each user is capable of staking any portion of their reputation token holdings, creating a proportional democratic governance process.

The vast majority of validations pools should be completed automatically, by running the reputation program, with no conscious decision necessary from any user. When things are running well, the only exceptions should be when the members are debating new rules, as we discuss below in Chapter 7 on governance. All other votes should resolve unanimously, with the only dissention due to people who are not running the consensus program, or otherwise not following the rules. This is seemingly enormous redundant calculation overhead. But compare it to the calculations Bitcoin or Ethereum use to maintain consensus. It is the price to pay for decentralized consensus. It wasn't possible before the recent advances in information technology. (Democratic investment)

Necessity #3: All the new reputation tokens are minted in proportion to fees. Whenever a new reputation token is minted, to be meaningful it must be grounded in something real. In any DAO devoted to profit, the foundational object is money. So all reputation tokens need to be tied to the fees the DAO earns. (Foundational meaning)

Necessity #4: All new reputation tokens are initially staked 50/50 in a validation pool, for and against the post which brought the fees into the DAO. For security, when a reputation token enters the system, it should be neutral, so that one faction is not favored over another. Validation pools should begin fairly. Newly minted reputation tokens should be staked half in favor, half against. This insures that all actions can be fairly judged by existing token holders, who will not be swayed by an unbalanced validation pool from a new large fee. (Fairness)

Necessity #5: Reputational salary. All fees should be shared with the entire network of reputation holders relative to their holdings. This is the key to making reputation tokens valuable and future-oriented. The importance of reputation is its ability to motivate members to cooperate, to harness their own selfish interests in service to future well-being of the group. The incentive that makes this possible is the promise of future rewards. Delayed gratification is the key to group harmony and long-term stability.

The active member who performed the work which attracted the customer fee is not paid directly; instead the fee is split in the reputational salary. The direct reward for the worker is that 50% of the newly minted tokens are staked as an upvote in the validation pool in their name, so they can win these new reputation tokens if they performed the work properly, according to the protocols of the DAO. This prevents many short-term arbitrage opportunities.

Further, the salary needs to be reputation-weighted, i.e., people with more reputation get more money for two reasons. First, to satisfy individual selfish interests. Second, to prevent sockpuppet attacks. If salary is distributed more equitably, say equally to all members, then the obvious strategy for gaming the system is to create multiple accounts and distribute your work between the accounts. (Meritocracy and future orientation)

Necessity #6: Review through references. Finally, each new post has the opportunity to reference older posts. If the new post is validated, their value can affect the value of past posts positively or negatively. Old posts can have their reputational value change, depending on how important users perceive the precedent for the system. This further stabilizes the system by magnifying the power of reputation for motivating people to behave in ways that help the group in the long term. It also encourages innovation.

This gives members the ability to review past actions, allowing a more careful analysis of patterns of behavior, encouraging actions which make lasting contributions (such as protocol development) and punishing actions which are judged to harm the long-term health of the platform. (Valuing the past)

Necessity #7: Multiplicity of token types Reputation tokens need to have power limited to their proper domain, meaning that for each different expertise, there is a separate type of non-interchangeable reputation token. Each type of reputation token is only powerful within the DAO containing the members with a skill specific to that token. So there may be different reputation tokens for developing smart contracts, or for advertising products, or for making governance decisions in each DAO. Each user will likely own several different types of tokens related to their individual expertises. (Domain-specific expertise)

Consequences of the architecture

Many types of DAOs with diverse reward structures can be created to address the variety of business needs.

The meritocratic incentive structure of the architecture ensures stability and security by motivating self-policing of a DAO.

Fair reward structures introduce proper incentive to ensure continual improvements instead of degeneration from rent-seeking.

Adopting the seven principles creates a balanced, meritocratic, incentive-driven positive feedback loop. The elements of the system that cyclically drive and change each other are

The outside customers (analogous to information transmission)

the members inside the DAO, i.e., the workers (information processing)

the forum (information storage)

The feedback loop is as follows: The customers' fees encourage the members to work and to develop improved protocols for work. The members post to the forum their evidence of work, the results of validation pools, and new protocols for how they

do business. The forum makes the DAOs history available for customers to evaluate which services seem useful and which smart contracts they should engage.

The feedback loop exists within the rigorous code-is-law system of smart contracts that allows efficient self-execution and self-regulation. But its dynamic nature gives the system the slack needed to redress failings with appeals (as smart contracts improve to include the logic that enables them) and with reviews through references.

This feedback loop creates an evolutionary platform which continually improves the DAO. New posts reinforce or reverse precedent. Code-is-law smart contracts are continually improved for usability and to better reflect the authors' intentions.

The word "evolutionary" is key. DAOs have the freedom to organize any way they choose. If they fail to find the right incentives for productive behavior, they will certainly go extinct. The feedback loop that includes customers outside the DAO naturally punishes any unproductive DAOs, by loss of fees.

The impossibility of creating eternally perfect protocols, as illustrated by Arrow's Impossibility Theorem and the Folk Theorems of Game Theory, is addressed by a system which continually improves protocols and smart contracts to react to changes in the market. This way the system is more stable and better reflects the spirit of the law as it evolves in the long run.

The 6th necessary structure, review through references, is crucial for moving the members' motivation to the future. First, references that decrease old posts' values allow us to punish behaviors that are later found to harm the platform. This discourages gaming the system, and helps address the problem posed by the Folk Theorems, of not being able to create a perfect static system. We can create a system that improves in time by reviewing its past. Second, references that increase the value of an old post enable a DAO to create an incentive system which encourages a culture of development. But the DAO must actively create the culture which encourages development, using protocols with substantial rewards for productive development. This requires effective governance (which will be discussed in the next chapter) to ensure the DAO participates in following a protocol which regularly recognizes the value of old posts with references.

This helps create a decentralized history for the DAO, which gives us momentum. History gives clarity on where we are and where we are going. History is the basis for making governance (which etymologically means "steering") more effective. History allows members to judge whether they are properly promoting their unifying transcendental values. History brings stability. (See Chapter 9.)

Reputation dilates time. It allows us to slow down immediate transfers of wealth, allowing us to consider the future and the past. Future-oriented incentives come from reputation-based salaries. Past-oriented incentives come from the editability of reputation. We can slash reputation, through references, based on actions from any time

in the past that are later seen to be harmful. Or we can augment reputation for actions later seen to be helpful to the network.

In any market, as technology improves, services improve, and the service providers themselves are best capable of assessing the service. In this case, regulations should be created by service providers. In a hierarchical structure, where members are siloed and have few formal connections with those immediately above and below their tier in the hierarchy, this leads to the moral hazard problem that the service provider has an incentive to weaken the standards and regulations. In centralized systems, this means the regulators and service providers need to be separated. In a decentralized system the whole group are equal-powered service providers, and they have an incentive to regulate each other, to protect their own reputation.

A variety of values can be effectively encouraged by manipulating parameters in the reward and punishment structure of reputation distribution, as will be analyzed later in Chapter 7 when we discuss decentralized governance.

Security

The seven requirements listed above are borne out of the necessities of security.

Sockpuppet attacks are inevitable if you want the membership to be open and to allow anonymous members. These properties are essential for fostering the individual autonomy that makes a global decentralized organization efficient and powerful. Therefore, every time reputation is used, it must be weighted, so that 10 accounts with 1 token each have the same power as 1 account with 10 tokens.

Second, most reputational systems fail from the sockpuppet attack on the Web of Trust model. As mentioned above, the idea is that an attacker will set up sockpuppet accounts to follow the reputational system faithfully, but only add reputation to their own sockpuppet accounts, building their own power, until they can exploit the network with false reputation.1 This is prevented by committing to a reputation sys-

[1] This is the flaw in every single reputational implementation we've audited in the blockchain DAO space. For example, an active project we particularly respect, SingularityNet, also falls into this trap. Their reputation system essentially boils down to tracking and accounting for the self-reported quality of transaction (our #6), the quantity of value of the transaction (our #3), the length of time of satisfaction (our #6), and the weight of the previous reputations of those involved in the transaction (our #2). Without implementing the other necessities, the sockpuppet attack will eventually erode their value, once it becomes valuable enough to merit the attack. See the details of their system, which implement

tem which follows Necessity #3, that all the new reputation tokens are minted in proportion to fees, working in concert with Necessity #5 that all fees are shared proportionally with the entire group. Then the cost of corrupting the system with the sockpuppet attack becomes impractical. Without stipulating Necessity #5, the sockpuppet accounts can pay themselves, so the attacker doesn't lose much money (just DoS prevention fees, like Ethereum gas). With #4 and #5 implemented, the cost of faking your reputation is (at an absolute minimum) double the value of the reputation.2 This is the essence of how you make reputation more valuable than money and focus the group on the goal of improving the reputation for its future value. With a dynamic governance model (next chapter), such attacks can be monitored and policed in a profitable manner that completely eliminates the threat.

Concentration of power is the greatest threat to any decentralized organization. Especially one which is devoted to profit, which is inherently competitive. This is known in distributed computing and blockchain as the 51% attack. The idea is that if a single member, or even a sub-coalition, gains 51% of the power in an inherently democratic organization, they will eventually control it, no matter what the safeguards are. A stable 51% power becomes a dictator, and the organization is no longer decentralized.

Improved information technology, itself, promotes decentralization. When everyone has access to the same technology for broadcasting and processing information, monopolies on communication are harder to form. One person cannot take all of the jobs and exponentially accumulate concentrated reputation.

Fair accounting and transparency in reputation promotes decentralization. When customers can reliably compare reputation, they are able to harness the available talent, instead of waiting for the most talented to become available. The differences in reputation do not accumulate as much when weaker members are given the opportunity to exercise their talent.

Anonymity promotes decentralization. The cult of personality is less likely to develop around one member who has comparable talent to others.

The nonfungibility of reputation tokens naturally promotes decentralization. Each reputation token has a separate history that can be slashed or augmented in the fu-

⍰⍰
some of the necessities, in "A Reputation System for Artificial Societies" by Anton Kolonin, Ben Goertzel, Deborah Duong, Matt Ikle Available online at https://arxiv.org/ftp/arxiv/papers/1806/1806.07342.pdf (Retrieved 8/8/20).

[2] This calculation is performed in Craig Calcaterra, Wulf A. Kaal, Vlad Andrei, "Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems", U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-11, February 18, 2018.

ture. So, every different token has a different value. While every token may theoretically be sold at auction, it will be more difficult to sell a token for full value at auction, because of the devaluation due to risk. A reputation token is inherently more valuable for a person who deserves it, than for someone who merely bought it, because of its secondary use in making future earnings. Compared with cash coinage, reputation is more difficult to accumulate. So, economies of scale are weakened. Reputation tokens are earned (not bought) when they are created, and so they are not as transferrable between enterprises. For all these reasons, the market for reputation will be much less liquid than for truly fungible tokens.

The economy of reputation tokens is inflationary, since they are constantly being created. Therefore, reputation naturally promotes decentralization of power. People earn new reputation with every productive act. Therefore, the total quantity of reputation grows continually, so the value of a single token decreases (assuming steady state, and not, e.g., exponential growth of customers). This also makes reputation tokens more difficult to trade, because their variable inflation makes it difficult to value precisely. If one member happens to have a very high reputation, they need to do proportionally more work to maintain the disparity, making reputation less likely to concentrate when people have comparable talent. This promotes equality and decentralization of power as a natural counterbalance to the accumulation of individual power. As we will discuss in the section on governance, below, an organization may choose to manipulate the parameters determining how inflationary the token is, thereby promoting different values.

Decisions made by weighted reputational power also protect the tokens' value from tyranny of the majority. Under a one-person-one-vote system, half of the members have less than average expertise, but equal power. This incentivizes experts to gain power by catering to less expert prejudices instead of following the most effective decisions. Under reputation-weighted voting, the incentive changes to follow the majority of expertise, which changes weight, based on the success of actions.

Decisions made by weighted reputational power also protect the tokens' value from various Tragedy of the Commons problems. Tragedy of the Commons occurs when members are not properly incentivized to police the evolution of the organization. For example, if complicated technical smart contract improvements are put to a vote by a large organization, very few people will have the ability or interest to participate in the debate. When they vote, they will not have the expertise to make a sound judgment and so experts are again incentivized to manipulate non-experts with sophistry. Therefore, many different types of reputation tokens are needed for the many types of expertise. Then, the validation pools which oversee every action in the DAO incentivize experts to participate or else they risk losing the opportunity to gain more reputation tokens and maintain or increase their relative power. Sharing the newly

minted tokens with those who police the action inhibits this free-rider problem of non-participation.

Dynamic design example

We repeat the basic process of generating reputation, generalizing from the example of the Software Review DAO given in Chapter 4. Imagine a generic DAO consisting of worker/members devoted to a task and customers willing to pay a fee to engage a worker and pay a preassigned fee for that task:

A customer uses the DAO smart contract (SC) to engage a worker by encumbering the fee in the SC and specifying the task.

The SC randomly picks a worker/member from those members available. (The only other smart contract in use will be an availability smart contract which members engage by encumbering their reputation tokens.)

The worker completes the task according to the principles the DAO has previously collectively agreed upon.

The worker posts evidence of their work.

The work evidence post (with customer comments) triggers the SC to open a validation pool—a voting pool where any member can stake their reputation by voting to approve the work or disapprove.

The SC mints new reputation tokens in proportion to the size of the fee.

The new reputation tokens are staked half in favor of the work evidence in the worker's name (this is the worker's reward); half are staked against and left unassigned (they are burned if opposition wins, so there is no bias in policing).

Majority wins and the reputation tokens are split amongst the winners. Ties favor the worker.

Finalized results are posted for review.

The fee is split amongst the entire DAO in proportion to their reputation holdings (reputation-weighted salary).

A slightly more complicated scheme could borrow from the dynamic design of U.S. Constitution, to create a cyclic system of checks and balances. The Workers, the Judges, and the Customers could each have three separate types of reputation tokens. The Customers would use their reputation tokens (along with a fee) to request work from the Judges. The Judges assign jobs to Workers with contracts, encumbering the fees. The Workers actively complete the jobs for the Customers according to the contract to release the fees.

The separate Judge DAO, Worker DAO, and Customer DAO would each separately maintain their own forum for storing their history and protocols, including standards for work and fees they've negotiated to accept. The Judges would mediate between

the smart contracts the Workers and Customers found acceptable and handle appeals when Customers or Workers are not satisfied with the completion of a contract. Presumably, the best Judges would be Workers, who would know best how to regulate their industry; the best Workers would be Customers, who would know best what is desired; the best Customers would be Judges who would best understand the most effective work to engage.

The checks and balances feedback loop is:
Customers motivate Judges with fees
Judges motivate workers with contracts
Workers motivate Customers with work.
**Insert cartoon diagram:
Customer →fee and ←review of Workers
Judge →smart contract for work and salary ←review of customer ←appeals→
Workers → work and review of customers ←availability for sc work
**

How will the fees and work standards be determined? The market. This is not a cop out. It is well understood that the market provides the most effective mechanism for price discovery. (See Chapter 8.) Secondarily the market determines how many members the DAO can support in its network, and how much work they should do. The market's answers find the right equilibrium between all the industries and companies to determine how much of each service and commodity is required to keep civilization running efficiently.

Will the market find the right levels for these rewards? It hasn't been perfect in the past. Monopolies and centralized companies are built to prevent the market from discovering the right price. Liquidity is how a market achieves price discovery. Liquidity is given by decentralization, so decentralized markets will perform more efficiently, once the overhead institutions are deployed providing the proper catalysts for business.

Criticisms

The P2P architectures that have been most successful, so far, in organizing large and valuable networks have been blockchains, such as Bitcoin. The Ethereum blockchain has the ability to organize DAOs with reputation tokens and smart contracts that can poll their members. Unfortunately, the technology today is too slow and expensive to poll its members on every transaction that a member takes. The number of messages required to make sure all nodes are aware of all votes by all members on each action a member takes, quickly multiplies into an unmanageable number, even for light-speed computers, partly because of deliberately added latency required for

decentralized consensus in redundant distributed computing. Voting is not efficient on contemporary blockchains.

This is another chicken and egg problem. Voting will be more efficient with valuable reputation. Reputation can't be valuable without meaningful voting. Part of the reason you need a large number of nodes is because we shouldn't trust individuals, so we decentralize control by making it redundant. But if we had a meaningful reputational system with the potential for review, we could rely on fewer nodes. This mechanism is one reason proof of stake is more efficient than proof of work. We could randomly select fewer nodes who are staking their reputation to do the work of polling the group. Then we can review their work in the future. As discussed above, the consensus necessary to build reputation is expected to be near unanimous nearly all of the time, as you build reputation by following the pre-approved protocols. So, it will be easy to detect any Byzantine behavior from the randomly selected nodes, and punish them appropriately. We discuss how the efficiency improvement of randomly delegated consensus can be implemented securely later, in Chapter 8, when we explore banking and ZKRollups.

As will be discussed in the section on governance, below, when a DAO is developing their protocols, the votes to poll consensus will not be near unanimous. Such contentious debate should not use strict validation pools anyway. You should not stake your reputation tokens in order to register your opinion on a contentious topic. Only once the debate has settled, should members risk their reputation to verify consensus with validation pools. So, debates should be held on platforms hosted by DAOs which use more efficient P2P technology than blockchains, such as distributed hash tables.

Summary

Reputation has lost much of its meaning during the disruption that we are experiencing as the global society is emerging. As old institutions fall, there is a fire sale mentality amongst people in dying fields where they cash in on the reputations that were built over previous generations. As our political systems fail, politicians behave avariciously, playing any dirty trick available for short-term gain that in previous stable times would have been unthinkable. As print newspapers fail, they publish false and libelous stories in order to gain popularity or clicks. Everywhere, standards of behavior that protected reputation in the past are eroding. Reputation itself is becoming a suspect concept as people use it and value it less and less.

Long-term thinking is necessary to guarantee cooperation. Reputation is the mechanism for incentivizing long-term thinking in business and government. Fungible cash rewards are short-term, immediate rewards. Reputation rewards people in the

future. Designing the incentive structure of your organization with a focus on reputation is necessary for stability.

Reputation is not just an option for any DAO that has power or value. It is absolutely essential. For a DAO that is devoted to an altruistic ideal—a religious organization like the Quakers, or an educational organization like Wikipedia—the unifying force is the ideology. Members won't squabble and jockey for power if the organization is not devoted to power. For DAOs that are built to make money, ideology is important to maintain the long-term stability of the organization, but ideology is not enough.

The ideal DAO relies on the power of decentralization. It needs to give its members maximum autonomy. This means the DAO must be open. The members are free to participate or not, they can come or go as they please without being excluded. For privacy they need anonymity.[3] The members of the DAO may come from any location or culture on the planet, and hide their true location behind VPNs. How do you maintain integrity and cohesion for the group with such extreme decentralization?

1000 years ago, the Maghribi traders solved a similarly difficult problem with far less tools than we have. Using only handwritten letters, the Jewish merchants set up a reputational system in a decentralized network that spanned the Silk Road. A reputational system that built trust in contracts that would take months to execute. With complete control of the assets, there would be nothing to prevent agents from vanishing or skimming or burying the profits and claiming bandits stole the merchandise. Nothing incentivized the agents from cheating except the promise of building better reputation.

Reputation was the key to maintaining the internalized firm efficiencies of free trade of information and free business contracts between members, despite enormous technical challenges including extremely limited communication (latency on the order of months) that created strong information asymmetries and the attendant adverse selection and moral hazards in the principal-agent problem.

When reputation in your DAO credibly promises future business, your members are incentivized to go above and beyond the stipulations of the smart contract. Without the promise of improving your reputation, a zero-sum mentality dominates the arrangement. Both parties' best strategy becomes exerting the absolute minimum of effort while still technically fulfilling the stipulations of the contract. That degenerate system will destroy the business atmosphere. Self-executing, self-regulating smart contracts between anonymous parties in an open system, create a near perfect zero-sum situation—unless your DAO also includes reputation.

[3] Or pseudo-anonymity where they have an invented code name—or many invented code names—since the system must track them somehow.

With a meaningful and secure reputational system, the situation becomes a positive-sum game. When there is a chance for each party to build reputation at the conclusion of a smart contract, they are incentivized to fulfill the stipulations to the best of their ability. In fact, they should go above and beyond the stipulations to satisfy the other party. This is amplified with the modern tools of information technology. When the record of your behavior can be eternally stored for review, when anyone on the planet may scrutinize the details of how the transparent bureaucratic details of the contract were fulfilled, when the accounting process for reputation tokens is publicly auditable and digitally secure, reputation's value is magnified.

How do we incorporate reputation into a decentralized organization? If there is no ultimate centralized leader to be the arbiter of what is right or wrong, how do we know what is a good or bad reputation? Democratic systems can solve this problem without a centralized dictator. With the new advances in information technology we can efficiently keep track of much more complicated reputation-building behaviors with digital tokens. With advances in cryptography and distributed computing algorithms we can keep our reputations private and decentralized and secure against subversion by those who would game the system.

By giving all people more power, we create a system where leaders are continually rediscovered immediately where and when they are needed—we create a liquid meritocracy. With secure and meaningful reputation, our liquid meritocracy has momentum and history.

To make the system effective in the long run, we need decentralized mechanisms for guiding the group. To make it efficient, it needs stability, so these steering mechanisms need to be subtle. Before any of this Web3 vision of the future has a chance of success, we need a revolutionary new system of decentralized governance.

Bibliography

Formating example:

Evans, Dave (Apr. 2011). The Internet of Things: How the Next Evolution of the Internet is Changing Everything. CISCO White Paper, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed June 1, 2020).

Wikipedia. Last Universal Common Ancestor, https://en.wikipedia.org/wiki/Last_universal_common_ancestor (accessed June 1, 2020).