Token-Curated Registri

Mike Goldin Follow
Sep 14, 2017 · 17 min read

This blog post is also available in paper fo

Token-curated registries are increasingly common cryptosystems apparently applicable to solving problems in a number of domains. In this document we will provide a more formal but less-than-mathematical view of token-curated registries.

This document is versioned 1.0 because the cryptosystem and incentive game described here can almost certainly be improved. Hopefully this document can be used as a starting point for conversations around how to improve token-curated registries. Many token-curated registries being deployed today bear family resemblance but employ substantively different mechanics. We believe there is a "right" way to do token-curated registries and that wholesale reuse of a canonical implementation should be possible.

The utility of token-curated registries

The product or output of a token-curated registry is a list. Humans have a penchant for list-making and lists appear commonly: shopping lists, lists of "good" colleges, lists of America's most wanted criminals, and many more. Most lists can be abstractly classified as either whitelists or blacklists, and in both cases the contents of a list uniformly satisfy some criteria (things I need to cook, colleges whose graduates on average exit debt within 10 years, individuals with FBI bounties over $100,000).

Useful lists are curated. Often by a single individual in the case of a grocery list, and perhaps by a committee in the case of a top-colleges list. A top-colleges list which may be appended by anybody quickly becomes an all-colleges list and ceases to be useful, since any college president obviously would desire for their college to appear on such a list.

A token-curated registry uses an intrinsic token to assign curation rights proportional to the relative token weight of entities hold
would desire to be curated into a given l
rational, self-interested token holders ar
Token-curated registries are decentrally
for token holders to curate the list's cont

User views: consumers, candidates, a

There are three user types in a token-curated registry and each has different interests, incentives, and interaction patterns towards the registry. Consumers desire high-quality lists. Candidates desire to be included in such lists. Token holders desire to increase the price of the tokens they hold.

Consumers desire high-quality information. If a consumer is making decisions about college attendance on the basis of a list purported to only contain colleges whose graduates exit debt on average within 10 years, they will be disappointed if they and all their classmates some day find that attestation about their college to have been inaccurate.

Candidates desire the attention and consideration of consumers. A school on a list of colleges whose graduates exit debt on average within 10 years will likely see greater application volume than it would were it not on the list. It may even be able to raise tuition on that basis. In our terminology, "listees" are candidates which have been admitted to a registry.

Token holders desire to keep demand for the token they hold high, as this increases its price. Token holders may be otherwise disinterested in the contents of the list they are curating: in our example of a top-colleges list, the token holders need be neither consumers nor candidates of/to the registry. To keep demand for their token high, token holders must keep candidates desirous of having listings in the registry *by* maintaining consumer interest in the registry *by* keeping the quality of listings high. Stated in reverse, *if* the quality of listings are high, *then* consumers will be interested in the registry *such that* candidates will desire to be listed in the registry. Token holders realize a direct financial benefit for curating the list in an expert manner, and the degree of their benefit

increases proportionally to the quality of their curation as consumer and candidate interest rise in lockstep.

The incentive system of token-curated

Token holders are the engine of a crypto registry. To make a token-curated registr denominated in the registry's intrinsic to "good" and accepted as a listee they keep should they desire to terminate their listing. If a candidate is "bad" its application may be challenged by token holders and, if rejected, its deposit is forfeited and divvied up as a reward amongst token holders who participated in the challenge process.

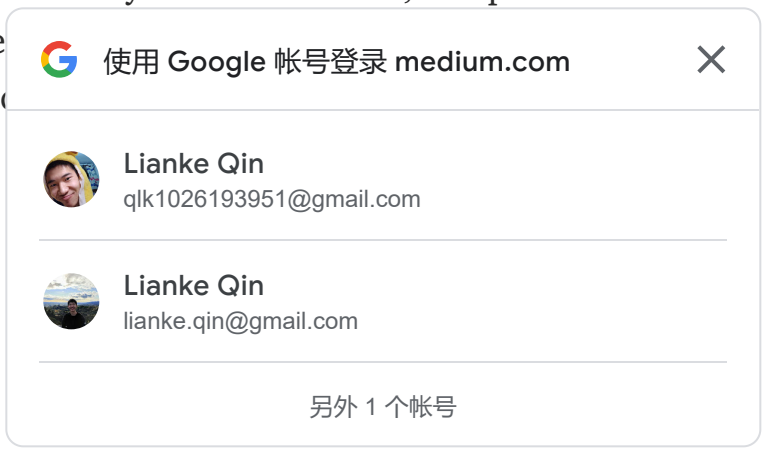
Candidates will not apply to the registry who believe they would obviously be rejected, as this would result in a financial loss for them. A college which only offers majors in bird-watching and charges tuition of $50,000 per year is so unlikely to be admitted to the registry of colleges whose students exit debt on average within 10 years that, rationally, they should not bother to apply. It is candidates on the margin of likely acceptance to the registry from whom token holders stand to increase their holdings, as these candidates have non-zero likelihood of both applying and being successfully challenged.

Token holders have a tactical incentive to challenge and reject every candidate to their registry in the interest of increasing their holdings, but this is at odds with their strategic interest of increasing the *value* of their holdings. An empty list is of no interest to consumers, so candidates would not bother applying to it. Candidates drive fundamental demand for a registry's intrinsic token, and so by behaving tactically rather than strategically, token holders go against their own interests and incur a potentially severe financial loss. Generally, it is in the interest of economically rational token holders to behave strategically and curate a high-quality list.

Parameters of a token-curated registry

This section may be used as a reference, these parameters will be referred to later. Collectively, we may refer to them as "the parameters", particularly as "snapshots" of the parameters, and also as "current canonical" parameters. A snapshot of the parameters

capture the current canonical parameters as they are at some time, and parameters in a snapshot are frozen: they do not change parameters do. If not otherwise specifie the current canonical parameter.



MIN_DEPOSIT

The number of tokens a candidate must the duration of their listing thereafter.

APPLY_STAGE_LEN

The duration, in blocks or epoch time, during which an application can be challenged. If this period passes with no challenge being issued, the candidate becomes a listee.

COMMIT_PERIOD_LEN

The duration, in blocks or epoch time, during which token holders can commit votes for a particular challenge.

REVEAL_PERIOD_LEN

The duration, in blocks or epoch time, during which token holders can reveal committed votes for a particular challenge.

DISPENSATION_PCT

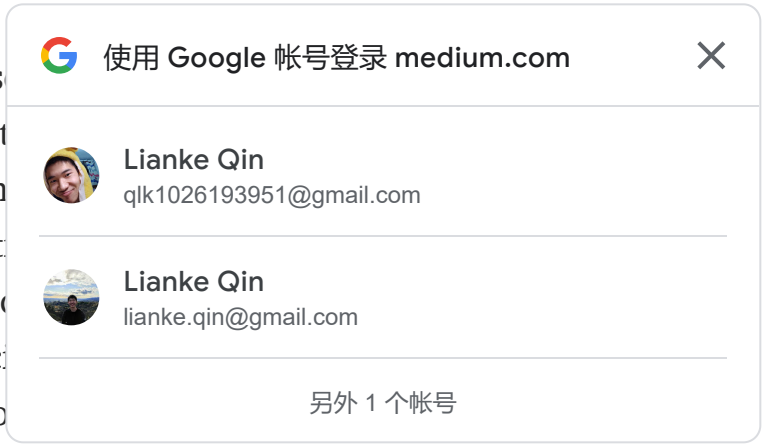
The percentage of the forfeited deposit in a challenge which is awarded to the winning party as a special dispensation compensating for their capital risk.

VOTE_QUORUM

The percentage of tokens out of the total tokens revealed in favor of admitting/keeping a challenged candidate necessary for that candidate to get/keep listee status. The VOTE_QUORUM does not count non-voting tokens, and unrevealed tokens are considered non-voting. By way of example, a VOTE_QUORUM of 50 means all challenges are simple majority votes.

Listings

A listing is one member in the uniform s
registry. For a token-curated registry of t
identifying a college by its well-known n
consideration in deciding the form a list
authenticable against the listing. In the c
suffice, as spoofing the physical and soci
consumers requires a significant proof-o



The means of authentication should, to the extent possible, be left to the discretion of the consumer. Consumers of a registry which stores domain names on the basis of some criteria may authenticate their connections to such domains in any number of ways: under the HTTPS certificate regime, web-of-trust, or using hashed secrets stored in listing metadata provided as an attestation from some oracle. It is important that listees and consumers establish at least one de facto means of authentication which both can support, or the registry will not ultimately be useful.

Applications

When a candidate for listing in a token-curated registry decides to take the step of actually applying for a listing, an application process begins. To make an application, a candidate must make a deposit in the registry's intrinsic token of at least MIN_DEPOSIT, where MIN_DEPOSIT is the number of tokens at stake should a challenge arise. Once an application is made, it can be resolved after APPLY_STAGE_LEN if no challenge was raised in that period. An application which resolves with no challenge results in the candidate becoming a listee.

An application which is challenged resolves at the conclusion of the challenge, and the candidate's status is determined then by the result of the challenge.

An application stores a snapshot of the current canonical parameters when it is instantiated, and all actions taken on or against an application reference its snapshotted parameters.

Challenges

Challenges may be initiated against candidates in their application period, or against listees. There may not be more than one
a given time. A challenge is initiated by
against some application or listing whos
“touch-and-remove” for challenges agai
MIN_DEPOSIT).

When a challenge is instantiated, a snap
parameters are stored with the challeng
token holder can participate. At the vote’s conclusion, either the challenger or candidate’s deposit is forfeited. DISPENSATION_PCT percent of the forfeited deposit is awarded to the winning party in the challenge as compensation for that party’s capital risk. The remainder of the forfeited deposit is awarded to voters in the majority voting bloc according to token weight. Token voters in the minority voting bloc neither lose tokens nor receive any reward.

(Note: The DISPENSATION_PCT essentially specifies the necessary certainty of a rational challenger in their ability to win a challenge for them to actually issue that challenge. For example, if the special dispensation is set at 50% a rational challenger must be above 66% confident in their ability to win a token vote to raise a challenge. This is because when there is a 33% chance of -100% deposit and a 66% chance of +50% deposit, $(0.33)(-1) + (0.66)(.5) = 0$.)

If the challenge was made against an application, then at its conclusion the application is deleted and the candidate may or may not become a listee. If the challenge was made against a listing, then at its conclusion the listing may or may not be deleted.

Edge case: “touch-and-remove”

If a challenge is made against a listing whose deposit is less than the current canonical MIN_DEPOSIT, the listing is immediately removed and the deposits of both challenger and listee are returned. This can occur when a candidate becomes a listee having posted some snapshotted deposit amount, and at some point after the snapshot was taken the current canonical MIN_DEPOSIT increases.

Why touch-and-remove? First, accept that deposit amounts in challenges must be of equal value, lest token-voters behave in a
to defeat the party with the larger depos
accepted that, why not specify deposits s
the deposit of the challenged listing? It i
on the basis of the deposited token's mar
opportunity cost the challenger, and par
participating in the challenge. Touch-an
poisoning which could be done by listing
giving strategically-minded, activist token holders discretion to simply remove such listings at a minimal cost.

For honest listings to guard against touch-and-remove griefing should the canonical MIN_DEPOSIT increase, listees can make deposits as large as they like, and any amount over the current canonical MIN_DEPOSIT may be withdrawn at any time. In a challenge, the current canonical MIN_DEPOSIT tokens are snapshotted at challenge instantiation and only that amount are ever at stake.

Voting

The critical game-theoretic considerations of voting in token-curated registries are that it be token-weighted and commit-reveal. Beyond that, voting need not be implemented in any particular way strictly speaking, but consideration should be given to the efficiency of the voting mechanism in terms of token liquidity.

Token-weightedness is important to give those with the most at stake the most say in the registry's curation, as these token holders are most incentivized to exercise the greatest diligence. Commit-reveal is important so as not to let the voting process itself influence voters to vote in any other way than that which they feel will be most productive for the registry's curation. Token liquidity should be maximized to the extent possible so as to encourage participation in the voting process.

Partial-lock commit/reveal voting is presently the most efficient known token voting mechanism for token-curated registries.

Parameterization

The parameters of a token-curated registry must be responsive to the market dynamics of the registry's intrinsic token. For exampl
that application volume increases to a p
all of the applications being made, the M
response. How parameterization, which
considered an open question at this time

In AdChain, for the purposes of example
listing applications. A different set of the
MIN_DEPOSIT might be much higher to propose a re-parameterization than it is to apply for a listing. Reparameterization proposals are challengeable, with the tokens deposited being at stake for both proposer and challenger. Token holders can vote to reparameterize the registry parameters, or the parameters of the parameterizer itself.

Interesting properties of token-curated registries

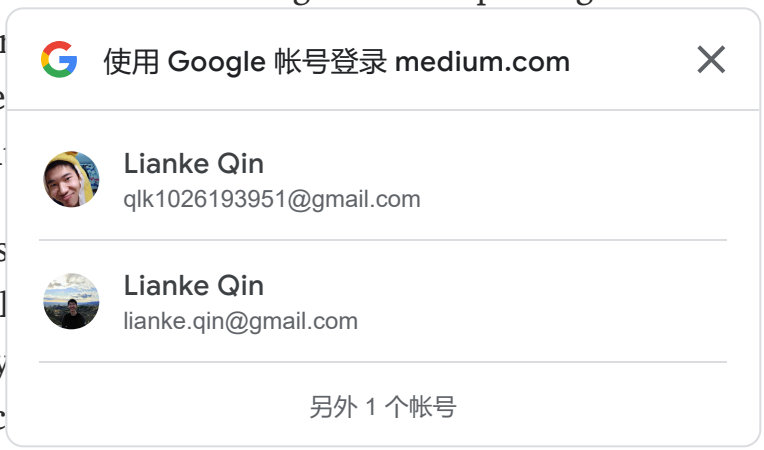
The intrinsic tokens of token-curated registries are necessary elements of self-sustaining systems which are public utilities. Token-curated registries are peak predators of capitalism that perform a useful function at the lowest possible marginal cost.

Token-curated registries satisfy the tenets of Mike's Cryptosystems Manifesto

A token is a necessary element of a system if the use of any other in its place would damage the system's normal functioning. Token-curated registries require intrinsic tokens because token holders must realize both the upside and downside of their good or bad work in order to be motivated to perform their essential curation task. The price of Bitcoin will not be responsive to reduced demand for it in the application of registry listings, meaning token holders' only incentives would be to take all the Bitcoin they could from candidates by issuing spurious challenges and colluding on votes against the interest of the registry's curation criteria. A token whose only fundamental utility is its necessity for making applications to some registry will see its price fluctuate on the basis of demand for those listings, which is determined by the quality of curation done by token holders. Token-curated registries satisfy token-necessity.

A system is self-sustaining if it would continue to function normally in the indefinite absence of its creators. No entity has special privilege in a token-curated registry. All

tokens are equal and only token weight determines the weight of one's privilege in a registry. The creator of a token-curated r
incentive system of the token-curated re
truly decentralized systems. Token-cura



A system is a public utility if it is permiss
Token-curated registries are permissionl
token weight determines privilege. They
are not necessary to incentivize other ac
disincentivize actors from griefing attacks. Token-curated registries produce useful output, which are the curated contents of their lists. Token-curated registries satisfy public utility.

Peak predators of capitalism

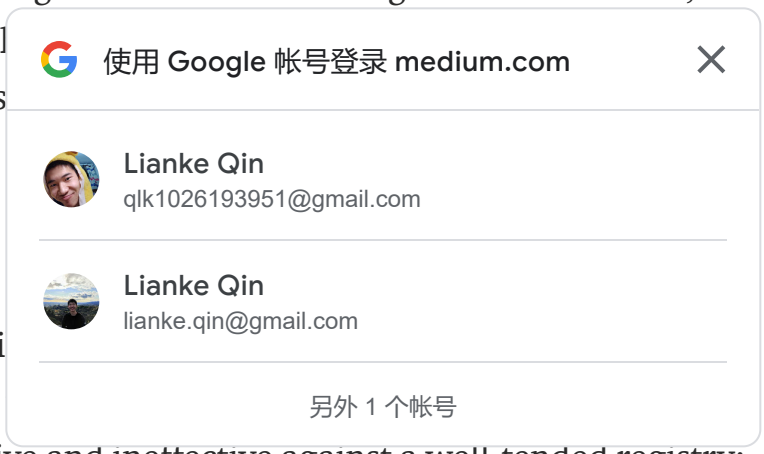
A peak predator of capitalism is a system which produces some useful output at the lowest possible marginal cost. The output of token-curated registries are absolutely free for consumers to make use of: the lists are stored on the blockchain and are totally transparent for any party to read. Rather than paying a vendor to produce a list of some sort, consumers in token-curated registries consume at no cost the product of an entire market of vendors competing against one another to produce the best list a free market can produce.

An entity which believes it can improve a token-curated registry's quality by playing its incentive game better can buy its token at market price, increase candidate demand for the token by increasing consumer interest having bettered the registry's curation, and exit their position having turned a profit to an entity which believes it can do even better than that. Alternatively, a token holder who is good at issuing challenges and voting can realize a perpetual revenue stream just by selling the tokens they win in the incentive game without ever parting with their principal.

In this way, if the market for tokens is efficient, the intrinsic tokens of token-curated registries become optimally dispersed over time to the entities which can use them most productively. In token-curated registries, profitability and productivity are well-aligned.

Attacks against token-curated registries and mitigations

There are a number of theorized attacks against token-curated registries. In addition, there are likely attacks which exist that l
attacks and their mitigations are discuss
severity/complexity/uncertainty order.



Simple trolling

A troll, for any arbitrary reason, might li
satisfy the registry's essential criteria. A
registry. Such attacks should be expensive and ineffective against a well-tended registry: the troll applies with a low-quality listing and loses their deposit when a rational token holder issues a successful challenge. To overcome the rationality of token-voters performing their essential function in the registry, the simple trolling attack must escalate to a madman attack.

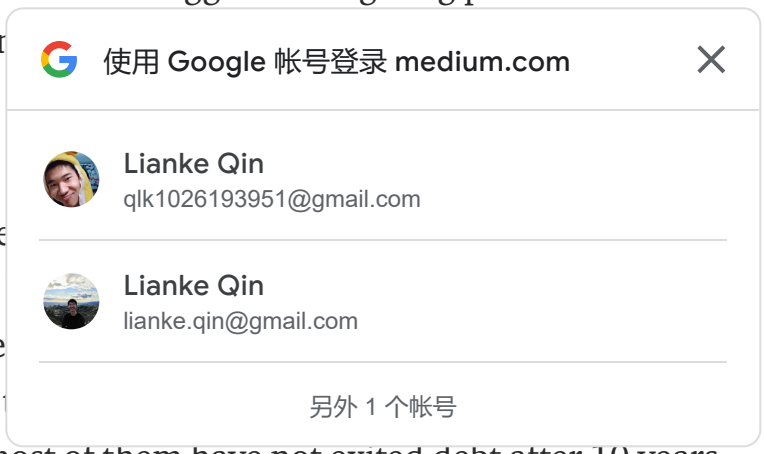
Madman attacks

A well-resourced adversary may have rational incentives to spend a large amount of capital destroying a token-curated registry by purchasing a challenge-proof majority of its active voting tokens and populating the registry with low-quality listings. If a registry performs some useful function at near-zero marginal cost and destroys existing businesses in doing so, it may be in the interest of those businesses to spend money to acquire tokens at market price and then destroy their value by poisoning the registry.

Happily, the security properties of token-curated registries against such majority validator attacks are rather similar to those of Casper. In economic 51% attacks, the attacker's weapon can be destroyed in a hard fork. As per Vitalik, "the intention is to make 51% attacks extremely expensive, so that even a majority of validators working together cannot roll back finalized blocks without undertaking an extremely large economic loss — a loss so large that a successful attack would likely on net increase the price of the underlying cryptocurrency as the market would more strongly react to the reduction in total coin supply than it would to the need for an emergency hard fork to correct the attack." In token-curated registries, the validators are token holders.

A practical concern is that only a minority of tokens are likely to be active participants in voting at any given time (see: Bootstrapping), such that madman attacks may not be as

expensive as the label “majority validator attack” suggests. Mitigating passive token-holding is an important open question ir



Registry poisoning

Registry poisoning is an attack performe
registry poisoning attack, a listed entity
admitted to the registry. A college in the
advantage of its listing status by raising
basis of its listing status find later that most of them have not exited debt after 10 years.

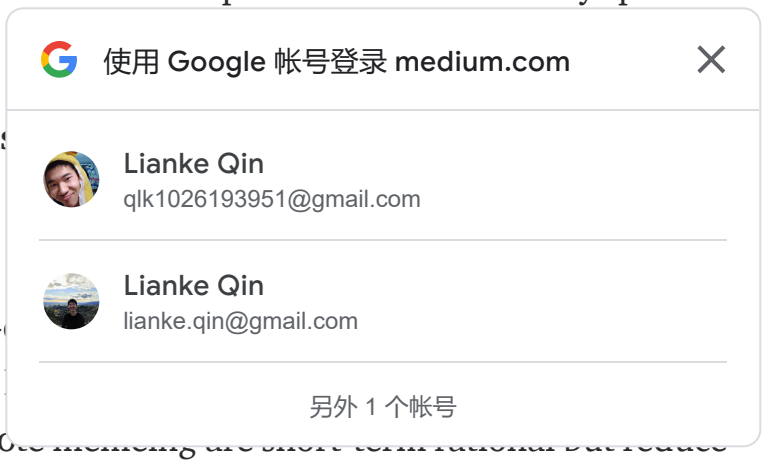
Rational token holders should be active in discovering such behavior and issue challenges against listed entities poisoning the registry. One underexplored concern is that registry poisoning may become relatively cheap if a listing only waits until the MIN_DEPOSIT increases over its canonical value at that listing’s application time such that it would be touch-and-removed upon discovery of its malfeasance. The listing then would not actually forfeit its original deposit. Still, the entity would have lost the opportunity for re-listing by damaging its reputation as such.

Coin flipping and vote memeing

Because there are no direct penalties for making bad decisions in voting, token holders may find it is more profitable to “flip coins” on their votes than spend the time making sober assessments of the issues at stake. This is an example of an attack which is only mitigated by the long-term strategic interests of token-voters to maximize demand for their token, but it is not known the extent to which such concerns will weigh on the necessary critical mass of token-voters to prevent such behavior. Coin flipping is not a very damaging attack: assuming an even distribution of votes between choices from coin-flippers, a minority of activist token holders can tip the scale towards rationality in any challenge.

“Vote memeing” is a group behavior where it becomes a meme to always vote one way or another in the interest of always being in the majority voting bloc, and is a similar attack to coin-flipping in terms of what motivates it, but with worse effects since a minority of activist token holders cannot tip the scale in favor of rationality.

Coin-flipping and vote memeing are considered a complex attack because they speak to the limits of rationality of token holders



Open questions in token-curated regis

Limits of rationality

In general, there are strategies in token-
pursue in the short-term, but which are
itself is undesirable, coin-flipping and vo
the registry's quality over time. What optimal strategies will participants pursue? Might some participants play the tactical and others the strategic game such that the lists which result are of middling quality, worse than those which can be centrally curated?

Bootstrapping

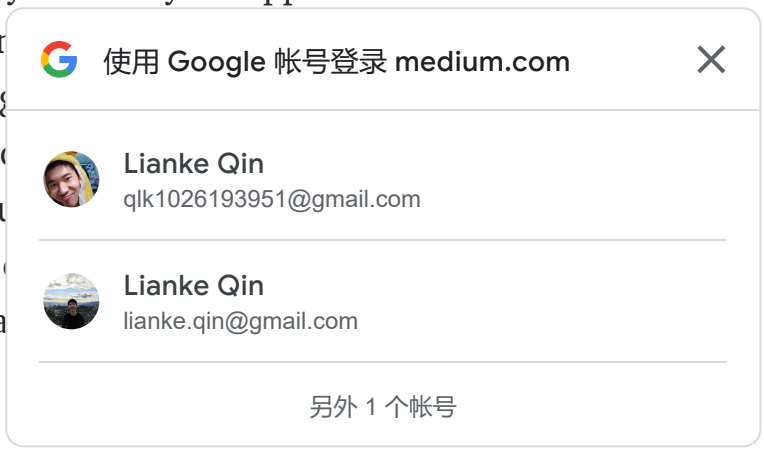
Token-curated registries have a chicken-and-egg problem. Consumers will have no interest in an empty list, nor will candidates desire to apply to a registry consumers have no interest in. In general it will be difficult for a registry to gain sufficient interest and traction from any of the necessary participants in order to instantiate a token-curated registry's virtuous and self-sustaining steady-state. There are a diverse set of opinions on the optimal approach to instantiating a token-curated registry and no single approach has proven to be the clear pattern to follow.

One approach is to collaborate with relevant "legacy" governing bodies for a candidate group (industry lobbies, advisory boards, et cetera) and offering them the responsibility of curating an initial set of registrants. The motivation behind this approach is to leverage the industry expertise of the vetted curators in order to produce a compelling base set of registry listings.

Another approach might be to initially distribute registry tokens to potential consumers and candidates of a registry. This gives otherwise disinterested parties tangible upside in seeding the system themselves.

Minimum economy size

What is the minimum size of an economy necessary to support the decentralized curation of a list in this way? Is it econor
it be rational for the producers of packag
a registry of things which should be purc
token-voters be able to curate a list usefu
whether or not the shopper already has
consumer interest necessary to decentra



Parameterization

Parameterization of registries is not considered well-solved at this time. It is possible that the AdChain parameterizer, for example, could be put into a permanently untenable state. For example, the parameterizer's MIN_DEPOSIT could be set to zero. This would create a very cheap opportunity for trolls to keep the MIN_DEPOSIT set to zero in perpetuity, since a large number of proposals could be created following the success of the initial attack, which could then be processed and activated at any later date. The AdChain parameterizer depends on token holders exercising diligence to prevent such an initial attack from succeeding. Registries can recover from lapses in token holder diligence and poisoning by means of the challenge mechanism, but parameterizers can be permanently damaged if successfully attacked once.

Blockchain Ethereum Consensys Cryptocurrency Game Theory

About Help Legal