interlock

Interlock Team

2021-7-26

Contents

Abstract

The web requires *trust* between participants to reach its fullest potential. However, we have centralized the trust-rating function to a handful of gatekeepers, who themselves have questionable credibility and competence. We propose a solution that uses blockchain and other technologies to increase security, privacy, and trust and bypasses those gatekeepers.

Introduction

The thing about these kinds of papers — whitepapers — is that they are supposed to be confident, authoritative, and seductive. Why, we hear you ask? Because stringing together words that create an impression of authoritative and seductive confidence is what often convinces people buy whatever it is you are selling. Everybody wants to invest in the impossible-to-miss certain-to-win solution to some problem that the market has. We have gone through a lot of whitepapers written with the confidence and certainty of a devout missionary seeking converts and, of course, donors. We are not going to do that to you.

Make no mistake, we *are* trying to *convince* you of the merits of our vision and idea — we just have no interest in *hypnotizing* you into agreeing with us. If you believe that the Web is not living up to its founding promises — and you want to change this — then please read on.

The Problem

History

The writers of this paper, dear reader, are old enough to remember the following: napster, gnutella, bit-torrent, Usenet, slashdot, RSS Feeds, Tor, Google before it became evil, and Open Source before it became cool. We remember an internet where nobody knew that you were a dog — and, more importantly, nobody cared. We remember when being social on the internet meant that you had a blog, read (and shared files on) USENET, and participated in Slashdot discussions and flame-wars as an 'Anonymous Coward'. We remeber that being informed meant that you used Google Reader — RIP — to read RSS feeds which were absolutely everywhere. And if you *really* wanted to stick it to The Man, you installed Linux on your second-hand beige-box and Firefox on your folks' Windows computer — we still have vivid memories and strong feelings about MSFT, and quite a bit of residual PTSD and mental scar-tissue. But, somewhere along the way, the internet took a turn. Now people use Facebook instead of USENET, Twitter instead of RSS, and Netflix, YouTube, and Spotify instead of BitTorrent. Also USENET, Slashdot, and friends are all ghost-towns — while their nearest equivalents have been overrun by trolls, cat-pictures, memes, advertisers, and cybercriminals. Oh, and Microsoft is an increasingly popular and increasingly open-source company — which is as inconceivable as Ghengis Khan becoming an exemplary Red Cross volunteer.

Clearly, there has been a pendulum swing from a decentralized and democratic internet to one that is significantly more centralized and autocratic. A significant driver of this centralization has been the insight that the majority of people are busy enough that they will give up control for convenience — especially if that convenience has a price-tag approaching *zero*. With the increase in convenience, things like web-pages and blogs could be created by people who did not know how to program or administer computers. And even if you did have this skill-set, chances are you would apply it to a *virtual* computer in the *cloud* rather than a physical one in your closet. This centralization of computing was not sinister or evil — far from it — but it was, rather paradoxically, a leap towards making the web accessible and useful to more people than

ever before. In other words, centralization *did* democratize *participation* in the web, but it came at the expense of freedom, control, and privacy. The web that you see today, is the web that Google wants you to see when you use their search, that Facebook, Twitter, and Instagram want you to see when you scroll through 'your' feed. And what they want you to see, is whatever will make you re-share the content or click on an advertisement. You are, in effect, plugged into The Matrix — the entire cyberpunk oevre is not merely dystopic fiction, it is part prophesy and part warning.

Maybe you are thinking, that does not sound so bad — maybe we *have* to sacrifice freedom, control, and privacy to democratize participation in the web. Maybe. Maybe not. Maybe that is *exactly* what the feudal Serfs were thinking while they were working the fields of their lords — maybe we have to sacrifice control over our bodies, our labor, and the (literal) fruits of that labor to democratize participation in agriculture. After all, what is the alternative? Starvation?

We sympathize, dear reader. We sympathize with you, because it is a perfectly reasonable question to ask. Yes, being excluded and isolated from the means of production of our era, is infinitely worse than having our every action tracked, classified, and monetized. But unlike the quarries, mines, farms, plantations, factories, and refineries of previous eras — which all required capital to establish and maintain and upgrade — the means of production of *our* era is, well, **us**.

Do you post on reddit? *You* are creating the value, *they* are capturing it. Do you make videos for YouTube? *You* are creating the value, *they* are capturing it. Do you create content for OnlyFans? *You* are creating the value, *they* are capturing it.

They conceive of a world where they data-mine — yes, the exploitative nature of their business models is even reflected in their *jargon* — everything we do, turn that data into money, and *we* get (basically imaginary) shares, retweets, mentions, likes, so-called-friends, and so-called-followers. They have even removed negative actions such as dislikes for fear that it will drive users — another revealing bit jargon — away. Their mission is to keep us happy and cheerful while we (happily and cheerfully) make them money. You know who also does this? Farmers. What does that make *us*? Livestock. Are you tired of being milked yet?

It Gets Worse

The previous section was a little bleak — we will give you that. But — as you can probably surmise from this section's title — this paper is going to get bleaker before it gets brighter.

If the end of the previous section has you feeling like you have been conned, like you are — sooner or later — the eventual victim of an unsustainable and tenuous pyramid scheme, well, that was our intent. To be clear, we are not trying to scare you with ghost stories. We *wish* these were just ghost stories — the exaggerations of a handful of nerds, hackers, and cypherpunks trying to shock you into listening. But the pyramid is built on a shaky foundation and the dangers are real.

How could it get worse? Well, in addition to being exploited, and metaphorically robbed, by the feudal lords of the internet, you are also being exploited, and *literally* robbed, by the scammers and criminals that have a growing presence on the internet. We have a multitude of delightful statistics that back up this claim. The areas of cybercrime, fraud, and identity-theft are so ripe and pregnant with opportunities that even nation-states are eager to get in on it — and they are not even trying to conceal their involvment. Yes, they give *zero* fucks, because they are confident that the majority of the populace is too distracted and too impoverished to actually — in the words of Morpheus — *wake up*.

The obvious question is, why are there so many scammers and cybercriminals. What is there to steal? Is it worth the risk? What are the risks? Well, the modern cybercriminal is not like a bank-robber or hostage-taker. The bank-robber or hostage-taker uses coercion and intimidation

to steal money. The modern cybercriminal is more like the mythical japanese creature *noppera-bo*. This creature is a faceless ghost that steals the faces of humans. Cybercrime is about stealing people's faces and using them as masks — it is about *deception* more than it is about coercion or violence. The faces in this metaphor are usually authentication-credentials that may lead the criminal to their ultimate goal, currency, crypto or otherwise.

And that is just the most obvious form of theft — material theft. Once business and politics and religion enter the equation, lines and categories start to get blurry very fast. For example, can *truth* be stolen? If so, does that make a flat-earther a criminal? What about the corporate marketing department that uses flawed benchmarking methodologies to convince you that their product is superior to the competition? What about alternative or traditional medicine books? What about the *hundreds* of pseudo-historical, pseudo-scientific, and pseudo-sociological narratives that are weaved every election cycle to convince people that their neighbors and fellow citizens are the cause of their anguish — rather than the massive institutions, corporations, and beaurocracies that have every incentive to profit from and perpetrate anguish and tragedy across continents and across generations (you do not have to look further than McDonalds and Phillip-Morris)?

The point is, the truth is very important, but it can be hard to pin down. Very few things can be considered absolute truths. The web — under its current commercialized and oligarchic stewardship — perpetuates, exacerbates, and profits from, vanity, greed, delusion, ignorance, envy, hatred, and outrage. Instead, it should give users the tools to better understand themselves, human nature, and our connectedness to all things — an ancient idea that is in fact more relevant to the modern world than it ever was to the ancient world.

Criminals and tech corporations both see the internet-user as something to be exploited. The fromer seeks to attack and corrupt the state of your bank account, while the latter seeks to attack and corrupt your state of mind. You will find it easy, even effortless, to be angry with the former, but you may find it difficult to be angry with the latter — you cannot be angry with the tobacco company for selling you exactly what you asked for.

Identity, Trust, Belief

Before 1971, if you held a dollar in your hand and examined what was written on it, you would see 'Exchangeable for Gold'. After 1971, it would only say 'In God We Trust'. We used to believe in the dollar because we used to believe in gold — now we believe in the dollar because we believe in the dollar. This is what some historians would call a revolution, others would call it a *paradigm shift*. Paradigm shifts, and for that matter paradigms themselves, are — and please do not mistake this for belittlement, quite the opposite in fact — entirely *imaginary*. You cannot measure or touch a paradigm. A paradigm does not emit heat or have mass. Yet paradigms have been the organizing principle of society since humanity learned how to speak and write things down. A paradigm is a shared hallucination.

Every paradigm contains the seeds of its own destruction. The bible was the first book that was mass-printed — shortly after that the catholic church lost half of its believers to the various protestant denominations. The feudal and heriditary paradigms of Europe were eroded and overthrown by the steady growth of capitalism. The industrial capitalist paradigm had, after the Great Depression, given birth to both fascism and communism. And the surviving contenders of the Second World War, created the Cold War (i.e. bipolar) paradigm. This paradigm collapsed into one of globalisation and informationalism. New gods for old.

Trust, just like a paradigm, is powered by *belief*. You cross the street with minimal anxiety because you trust the drivers to be sober enough to obey the traffic laws (also a good example of a paradigm). You use the same two passwords on every site because you trust that the

programmers that made the site have a minimal level of technical competence and a minimal regard for your security and privacy. Some Runescape-playing twelve-year-old kid drops all their hard-earned loot in front of another player and presses `Alt-F4` because that other player told them it was a glitch that would duplicate all of the items in their inventory — that kid *trusted* someone who was *untrustworthy*, and learned a *painful* but *important* lesson about *trust*. The internet is basically like that Runescape example. The entire system depends on trust to get anything done, but there are too many people and you cannot trust them blindly. What to do? Well, we did what we have always done, we created institutions (i.e. social networks and banks) and placed our *trust* and our *faith* in *them*. It sounds perfectly reasonable, no? Sure. But such institutions are powered by people, and the people — just like criminals and liars — have to respond to market-pressures. We used to *trust* our credit-rating-agencies to tell us which financial entities were *creditworthy* — and then we had an economic *meltdown* in 2008 that destroyed the *trustworthiness* of those institutions themselves. Centralizing trust in a handful of institutions will work in a pinch but it could eventually, and without warning, fail — every paradigm contains the seeds of its own destruction.

The Internet's Paradigm

Status Quo

The internet, and especially the Web, are either the result or cause — hard to tell really — of a paradigm shift. The mass on-lining of humanity has shifted the power (i.e. the value or economic surplus) from the previous power-holders (i.e. the mass media, the industry, the publishers, etc). Think about it, more people watched the Fortnite tournament than actual sporting events. In fact, viewership of the *Olympics* has started declining towards the end of the last decade — after a half century of *growing* viewership. Book stores are no longer mainstream, and the internet's pre-eminent book store has evolved into a titanic giant that sells *everything* and delivers it to your residence within 2 days — and they also collect rents for roughly *one third* of all computation and storage that is provisioned on a Cloud. A ride-sharing company has displaced local taxi-cab companies *in the entire world* — not merely in a city or a state or a nation. Video rental stores probably do not exist, but the internet's pre-eminent video rental store has emerged as a formidable cultural force spending tens of billions of dollars per year producing original and highly regarded, or at least highly viewed, films and television series.

This is how paradigm shifts work. The above companies tried to build modest businesses in not-too-contested corner of the market place. The paradigm starts shifting in their favor and they find themselves capturing more surplus than they know what to do with. They slowly wake up to the realization that they are at the top of the pyramid — not by any strategic brilliance of their own, but rather, because the pyramid shifted and contorted itself and they happened to be at the right coordinates at the right time. Western Europe provides an interesting case study — the place was a backwater far away from any action until some adventerous sailors and navigators found sea routes to Asia (that let them by-pass the Eastern Mediteranean middle-men) and to the Americas (which would eventually house the worlds most successful and likely last ever hegemon — as always, every paradigm contains the seeds of its own destruction,).

New Paradigm

Different people have different ideas about what the next paradigm of the web is. Web2.0 got us half-way to where we want to be. Its pioneers, however, could not resist the incentives to maximize the proportion of the economic surplus that they capture — even though these Web2.0

business are essentially *built by the users*. And Web3.0? Depends on who you ask. Right now the mainstream thinks that Web3.0 is the *semantic web* — a decades-old idea that has always struggled to gain traction. Meanwhile, an increasing number of people believe that Web3.0 will center around *blockchain technologies* — but they call it **web3** (we will call it Web3.0 from now on in this paper).

We believe that the new paradigm for the internet/web is hyper-decentralization. The web is decentralizing the media and the news and the publishing industry. The web is decentralizing geography — two people a million miles away can interact with each other over video-chat or VR. The web is decentralizing finance — even stuffy old banks want to get in on the DeFi bandwagon. The web is decentralizing the nation-state — people often times have more in common with globally dispersed like-minded individuals than their fellow neighbors and citizens. The web is decentralizing employment — the number of people working in the gig-economy and the creator-economy is increasing (unfortunately this is another example of users creating a surplus that is captured by online equivalent of a few feudal lords).

We believe that this accelerating trend of hyper-decentralization will also decentralize the parts of the web that have to do with *trust*. Right now, the intermediary institutions (i.e. Facebook, Twitter, Reddit, HN, and so on) that ascribe credibility and trustworthiness do so in ways that are *opaque*. We do not know *why* certain tweets appear in our feeds and others do not — and even if we did, there is nothing we can do *customize* our feed (aside from following/unfollowing various accounts). We can see a Reddit user's karma-score as well as the score of their individual posts — which is slightly less opaque than Hacker News's ranking system — but we cannot see *who* up-voted or down-voted that user's posts. In fact, we have no way of knowing if that karma score has not been accidentally inflated by a random bit-flip on Reddit's servers — let alone if it has been manipulated by an insider or inflated by a voting ring. Similar logic applies to Twitter and Hacker News. Hacker News has surprisingly insightful discussions, in spite of its concealment of vote-metadata for posts, but it is still suseptible to insider manipulation and voting rings. Finally, there is the question of whether a single raw integer — whether it represents total karma or total followers or total likes or total retweets — can *actually* capture the trustworthiness, truthfulness, and popularity of an account and the content associated with it. Can you determine if someone is going to be a good and helpful friend or collaborator by the size of their wallet?

Economics

Intro: Three Strains of Economic Thought

Before we continue with our proposed solution, we should probably take a brief detour into economics-land and express how our proposal fits into the main frameworks of economics. From the late 1700s up to the present-day three economic schools of thought have shaped societies around the world — namely, the Neoclassical, the Keynesian, and the Marxian. The Neoclassical school focused on individual freedom and individual incentives, and rejected any form of state-intervention in the economy — in other words they assumed that Utopia was achievable without Leviathan. After the Great Depression set the Neoclassical Utopia aflame, the Keynesian school arose and argued that a Utopia could not be maintained without a Leviathan — they argued that the individual was certainly important, but not nearly as important as the *structure* of the economy. These two views correspond to microeconomics (i.e. reasoning that individuals ruthlessly purseuing their own self-interest will create the most desirable outcomes for all of humanity) and macroeconomics (i.e. reasoning that *tracking* macroeconomic indicators like GDP, unemployment, inflation, and interest-rates and *tuning* those macroeconomic variables

will create the most desirable outcomes for all of humanity). Put differently, one school thinks that individual behavior and actions *cause* the economy, while the other school thinks that the economy *causes* individual actions and behavior. To be clear, we are not taking sides, both points of view are correct they just disagree about the *relative* value of one component in relation to the others. And now onto the Marxian school which requires its own paragraph.

The Marxians are primarily concerned with *the means of production* — specifically, what they are, who is the class that owns them, who is the class that operates them, what are their outputs, what is their economic surplus, and who captures what proportion of that surplus. They marvel at the economic efficiency and dynamism unlocked by the transition from feudalism to capitalism, but they believe that any arrangement in which the class that operates the means of production but does not own or control those means is fundementally unjust, and does not fulfil the (false) promises of Humanism (the philosophy undergirding both Neoclassical and Keynesian social orders). They also believe that individuals and economic-structures are always shaping each-other via a never-ending *dialectics* — in effect, they are *simultaneously* cause *and* effect. And that is pretty much all of the Marxian school *that is relevant to this paper* — there is a lot of other stuff (i.e. central planning as a suitable alternative to the market) that is simply not compatible with a globalized marketplace, nor is it compatible with a trend towards hyper-decentralization.

We basically agree with all of these theories, and want to use the three perspectives to construct a globally decentralized network that will give users freedom, control, privacy, and security.

Reputation and Trust

Trying to eliminate the intermediary institutions that ascribe trust is a little bit like trying to eliminate the police or trying to eliminate schools. Obviously policing and schooling are very important and nobody would ever consider decentralizing them, let alone eliminating them. So should ask ourselves, what kind of a people have no need for the police? What kind of people have no need for schools? The answer, dear reader, is people that are *self-policing* and *self-schooling*. Obviously, such people are very rare, otherwise we would not need schools and police departments. However, a computer that is not under the control of any single individual can in fact be used to implement this kind of flawless self-regulation. If we go back to that earlier Runescape example from Section 4, the game could have been programmed to disallow such acts of deception — whether this makes the game better is another matter entirely.

What we wish to do is to use the decentralized, history preserving, and transactional nature of the blockchain to implement an anonymous trust-network. To be clear, we are **not** trying to replace existing platforms like Reddit or Twitter — this is **not** *XYZ But for The Blockchain*. We do think that blockchain technology will see adoption in content-creation and content-distribution, but we think that those domains are related but separate from the domain of *trust and reputation*.

Our network associates users with accounts on the blockchain, similar to how a licence plate is associated with a vehicle — though *unlike* a license plate we do not associate the *identity* of the user with the account. Each account has a certain number of `Inter Tokens` associated with it. These coins are **not** a measure of karma or trustworthiness — rather, they are merely a way to amplify (i.e. upvote) or dampen (i.e. downvote) other accounts. The network does not *score* anything — it merely records the upvotes and downvotes, which account they came from, and how many Vote Tokens (more on this later) have been spent on each upvote or downvote. The idea is that, voting is not free. When a upvotes they are depositing a percentage of those votes into the target account — when downvoting, no votes get deducted from the target account but

the downvote-transaction does get recorded on the blockchain (we do not want users with an overwhelming amount of vote-tokens to be able to bankrupt accounts that they dislike). Users can also *vouch* for other accounts. Vouching is a special kind of upvote — it allows a user to risk a certain amount of their vote-tokens to give another user visibility. If the other user gets upvotes then the upvotes are recorded on the blockchain, but the vote-tokens are shared between the voucher(s) and the vouchee in proportion to how much vote-tokens all of these users have vouched. If the other user gets downvotes then the voucher loses a proportional amount of vote-tokens — so one should not vouch blindly. Vouching can be time-limited, and the vouchee has to explicitly accept the vouch. Lastly users can *share*. Sharing essentially lets a user post an arbitrary byte-string to the blockchain — the network charges a **significant** per-byte fee for sharing. The reasoning is that we want to incentivize users to post *links and URLs* to content on other more mainstream platforms, instead of *actual* content which we consider outside of our scope. This essentially allows accounts to act as *curation feeds*.

As for the actual *scoring*, we decentralize this by pushing it to the *edges* of the network. The idea is that users can run a scoring program that will walk the blockchain and build a graph of accounts as connected by upvotes, downvotes, and vouches — in effect applying a kind of page-rank algorithm to account. The reason we outsource this to the client is that it allows people to build things like feeds in a totally custom way. For example users can play around with *biased* page-ranks (i.e. what would happen if we removed Account XYZ from the blockchain history, or what would happen if we treat these 5 accounts as a single shared account). The possibilities are endless. What would a feed look like if Account X was *my* account? Which accounts have voted for my account(s)? Which accounts have a similar voting pattern to mine?

Each account is associated with a public cryptographic key. Users can sign things that they post on the web (i.e. to reddit or to their own blog), so that users of the Interlock Network can know that the content was posted by somebody that they trust.

If the Interlock Network sees wider adoption, website admins can include a custom HTTP header that includes a signed Interlock Network account number — if a user has installed a Interlock-Network-aware browser-extension they can automatically inspect that account's history and various rankings, interactions, and scores. Years ago, Paul Graham said that he asked applicants to Y Combinator provide their Hacker News account-name as an additional data-point for YC to consider when evaluating the applicants and their proposals — we believe that the Interlock Network can be used in a similar capacity, *but across the entire internet*. Everything from online stores to online gaming communities can make use of the data stored in the Interlock Network to ascertain the trustworthiness of the participants. Even in the domain of startups, companies with a good reputation on the Interlock Network can offer their employees Inter Tokens or upvotes in lieu of stock or shares.

If Web2.0 was about *websites* and *services*, we believe that Web3.0 is about *people* and *content* and their *trustworthiness*.

Quid pro Quo

An interesting application of the Interlock Network would be as a way to implement a *favor exchange*. Think of it this way — you want someone to do you a favor (i.e. you want them to farm potato-cactuses on Runescape) so you give them an NFT Inter Token and they do you a solid favor. Now that the favor is complete, the favor-doer has an NFT token that is directly linked to you that indicates that *you* owe *them* a favor. Once you do them a favor, they will give you a corresponding NFT token that will cancel out your original token. The cool thing about this, is that it encourages the development of long-lived bilateral relationships between accounts and people — whereas the exchange of money generally encourages us to treat other

human beings as vending-machines that do things for us because we we inserted money into them. Clearly it is possible for the two users to never reach an agreement on whether a favor was ever actually completed, in which case the NFT can be reclaimed by the issuer — whether or not this is true is not nearly as important as it being permanently recorded on the blockchain, and the page-rank algorithm can do its magic.

Why Security

Freedom, Choice, and Privacy

Security is a difficult problem — it has *always* been a difficult problem. Throwing blockchain at the problem won't automatically fix it. If websites were signed using a Interlock Network account-signature many phishing attacks — the most common and most successful kind of attack — would be a lot less feasible. However, Interlock Network does not yet exist — and even if it did it would only protect the users that have an account on it from websites that belong to *other* users that have an account on it. So while the Interlock Network concept has enormous potential and could be an extremely powerful security mechanism — if widely used and adopted — it is not a good starting point.

Our company, Interlock, has developed an extension — a fork of uBlock — that, in addition to the usual ad-blocking functions, can also detect whether a website is fraudulent based on very effective, widely tested, heuristics. When a user opens a webpage that the extension thinks is fraudulent or untrustworthy, the extension will prevent any user input to the page and issue a warning in the form of a large red banner. The extension has already seen use in some large companies that you have definitely heard of — and for most of its life it has been out of the reach of non-corporate users. Our plan is to make this extension available to *everyone* but to modify it to work with Interlock Network. When the user installs the extension they can open an account on the Interlock Network, link it to the extension, and we will deposite some amount of Inter Tokens into their account. As they use the extension they will get a variable-time and variable-quantity reward for using it. They can also get additional Inter Tokens if they verify that a link dangerous — though this is opt-in as it would require us to request that verification from a random subset of users that are not too tightly connected on the Interlock Network. The extension will also be extended to allow sharing of links from the browser on the Interlock Network. Users can also flag webpages as either being malicious or *containing* malicious content (i.e. a comment on reddit or a video on youtube). And finally the extension can also be used to explore the data stored in the Interlock Network.

Naturally, we encourage the community to create alternative extensions. For example an extension that mimics the old StumbleUpon extension would be very cool to see. Also an extension that mimics the functionality of Google Reader, but for Interlock Network shares rather than actual RSS feeds.

KYC

The **Know Your Customer** laws are an interesting example of laws that require establishing the trustworthiness of a customer. In principle it is much the same concept as checking whether a website is legitimate or fraudulent or whether an account on the Interlock Network is highly regarded or shunned. Obviously, if all transactions happened on the Interlock Network — or on *any* blockchain — KYC laws would be trivial to implement. That is one of the nice side effects of complete transparency. We can combine the data on the Interlock Network with data —

anonymized of course — that we gather from the extension to help the relevant Web3.0 financial institutions (i.e. namely crypto-exchanges and banks that want jump onto the DeFi train) stay in compliance with the KYC regulations.

Cryptonomics

Interlock Token

To back our smart-contracts and our token we have chosen the **Solana** blockchain technology as our transaction-processing platform-component and **Ethereum** as the platform-component on which we mint the actual tokens. Solana has addressed many of the outstanding problems found in similar popular blockchains like Ethereum (i.e. transaction-speed energy-efficiency infinite-smart-contract-loops etc). In fact, the Interlock Network is simply not feasible on any blockchain that does not have cheap transactions. We had hoped that we would be able to use Ethereum since it has an enormous ecosystem and is very popular, but its transactions are thousands of times more expensive then Solana's. We do however recognize the value of Ethereum's ERC-20 standard and the ability to use existing wallets and to transact with other people on Ethereum — so we are minting the coins on Ethereum but connecting them to Solana using the Wormhole bridge between these two blockchains. Ideally, we would use a single popular blockchain like Ethereum but the physics and economics of these technologies makes that impossible, presently. However, if the newer versions of Ethereum increase the TPS and decrease their transaction-costs we could see ourselves porting our code over to these future version of Ethereum — assuming that Solana does not supplant Ethereum in the meantime.

To be honest, we are still not 100 percent certain that our Solana-Ethereum hybrid is going to be able to implement all of the features that we desire for the Interlock Network to have. Worst case, we will have to implement our own blockchain from scratch — we are still evaluating options. At minimum we will use Solana-Ethereum as a test-bed for the basic idea and move on from there.

Economics Redux

Just wanted to circle back to the three economic paradigms mentioned earlier. The Interlock Network satifies both the neoclassical-individualist and keynesian-structuralist perspectives because we can infer a very precise *structure* from the recorded transaction-history between *individuals* — in fact if the Interlock Network gains wide adoption it would probably be of significant interest to all kinds of economists and sociologists. Furthermore we have tried to the design the incentives encourage pro-social use of the blockchain — but of course if any economists (or non-economists) want to chime in then please go ahead. As for the marxians, they can take pleasure in the fact that (a) the user's privacy, relationships, and attention (i.e. the means of production for the information age) are owned by the collective and not by people whose names rhyme with Stark Truckerberg or Track Horsey and (b) the user has the final say over which accounts are more attention-worthy than others.

Interlock Token Solana-Ethereum Architecture

We have given you a short overview and justification of which blockchains will be used as a test-bed for the Interlock Network, now we will give some concrete details about how this will be implemented on top of Solana-Ethereum. So far, we have spoken of the Interlock Network as if it was a proper stand-alone blockchain, so that we can get the *idea* of a P2P reputation network

across to you. However, there are some significant implementation details that diverge from our *idealized description* of the Interlock Network, in the previous sections.

Pretty much all software that runs on a blockchain is going to be much slower — and more expensive — than traditional software that runs on raw silicon (or even in a VM). We should start with the good news — transactions in Solana are extremely cheap, costing only about 10-USD to execute a *million* transactions. The *bad* news is that per-account storage is severely limited and severely expensive. On Solana each account can only store a maximum 10MB of data — which is not enough for our history-based reputation scoring — and each MB costs 3.56 SOL to store per year — which comes out to 10MB-years costing 1200-USD at the current SOL-USD exchange ratio (1 SOL is worth 33 to 34 USD). Storing data directly on the Solana blockchain is not feasible. Other blockchains do allow storing of *more* data than Solana but storing this data still has pretty steep costs (i.e. writing 1MB of data to Ethereum costs a staggering 76-USD one-time-fee).

As a result of these economic realities, we will use Solana as a P2P transaction processor — but not as a storage engine. Instead, we will use Solana's WebSocket API to listen for transaction-notifications that involve our Interlock Network smart-contracts. These notifications — which are basically transaction logs — will be stored in the Postgres-based timeseries database called TimescaleDB. We will make this DB publically readable — but rate-limited, for economic reasons. Full archives of the DB will be made available weekly via BitTorrent (or something with similar or better properties — we are keeping an eye on Storj and related technologies) so that users of Interlock Network can query this data locally, with minimal latency, and with minimal API fees. It is our goal to make this data — these transaction logs — the property of the *entire internet* and not just a single company. We should also note that *anybody* can snoop on the JSON RPC API that Solana exposes and build their own data-base — so there is no danger of Interlock drawing up the bridge and charging exorbitant fees on a whim. The reason that we offer an API and a BitTorrent archive is that the Solana API has a limited retention period. Our understanding is that retention can be configured on a per-validator basis — so some validators might have more or less transanction-history than others. The only way for Interlock to have the full history is to run our own validator — which certainly sounds like fun — but that would be overkill because we only care about a tiny subset of the millions of transactions that happen on the Solana blockchain. By providing a public API and distributing an archive we are making it possible for people to see, and verify, the complete Interlock Network history.

As for the smart-contracts themselves, our plan is to implement a single smart-contract *per verb*. As discussed previously, there are only a handful of verbs — *upvote*, *downvote*, *vouch*, *share*, and *quid-pro-quo*. Each verb is basically its own smart-contract and takes an account number as an argument. The account invoking the verb pays for the cost of the transaction — which is measured in thousandths of a SOL — as well as a tiny and negligible percentage to an interlock-owned account — this is to help fund the development of the Interlock Network and other related interlock products. The verbs upvote, downvote, and vouch are pretty straight forward to implement since they just manipulate balances and store no data. Implementing *share* however, is a bit more of a challenge because of the high storage-fees on Solana. When the share-program is invoked, it is done via a transaction, which contains opaque 8-bit instruction-data. This instruction data is *thrown away* by the share-program as soon as it gets it — however, WebSocket listeners will *snatch* all the metadata about the transaction including the 8-bit instruction-data, *so it is not lost*. If the data is longer than *560 bytes* our *share program* will emit an error and our listeners will *ignore* the transaction — 560 bytes is enough to encode meaningful meta-data about content (i.e. a link along with perhaps a checksum of some kind). The *share* smart-contract will charge a one-time per-byte fee to incentivize users to keep their shared content as short as possible — and to disincentivize the spamming of our database.

The *quit-pro-quo program* is very similar to the *upvote* program, except it mints and deposits an account-specific NFT that cannot be withdrawn or spent by the receiving account — see the previous section, *quid pro quo*, for more details.

Tokenomics

Voting and Sharing

Since we are already talking about Solana and architecture, it seems natural to segue into the tokenomics of our Inter Token currency. Most tokens and cryptocurrencies like to make guarantees about the maximum supply of their tokens. We feel that having to choose between inflation and deflation is a false dichotamy. We clearly want to make use of the century of brainpower that went into monetary theory and the more-than-half-century of brain-power that went into game-theory (specifically the subfield of mechanism design) to create both long-term and short-term incentives that will encourage pro-social behaviour and participation on the interlock network.

We want people to vote, but we also want them to vote thoughtfully — to that end votes are emphatically **not** free. They cost Inter Token. We also do not want people to hoard Inter Tokens, because that means that they are not voting. This is why we actually have different *flavors* of Inter Token. The vanilla Inter Token is like any other token that can be bought and traded. But we also air-drop a vote-only flavor of Inter Token these coins are only good for voting — except for the occaisional token-swap in which an account can exchange their vote-only tokens for the actual Inter Token. A vote-token is either spent or unspent — if unspent it is not exchangable. In other words, when a user votes they transfer their unspent token to the account that they voted for, but their *own* account receives a *spent* token that cannot be used for anything — except buying Inter Token. This is very much like Japan's policy of *Window Guidance* — except we are guiding voting behaviour, instead corporate behaviour.

Voting activity is obviously done via its own tokens, but what about sharing? We feel that sharing should be billed directly in Inter Token. Unlike voting, where we do not wish people to hoard their votes, sharing is a little different. We certainly want people to share, but we do not want them to *spam* our DB with *noise*. For example, at 560 bytes and 200 billion — the number of yearly tweets processed by twitter at time of writing — shares per year, the Interlock Network accounts would be generating 101 TB of data per year. That is a *lot* of data to store, index, mirror, and distribute — we want to make every byte count, specifically so that ordinary users can feasibly do their own mirroring and querying. This state of affairs does give users with more Inter Tokens (i.e. because of more received upvotes or because they purchased more) a bit of a social edge. We are not entirely sure if that is a good thing or bad thing. We have considered various policies, such as distributing the share-costs across the entire network as a *percentage*, or at least doubling the per-byte fee *with each new share* — on a per account-basis — so that accounts can share cheaply at least once a day, but they cannot firehose every random brainwave onto the network. The former policy might incentivize account-owners to engage in complex behaviors akin to tax-evasion and capital-flight. The latter policy seems more sensible and equitable, but this is one those things that will probably require extensive experimentation, before we can accept it as a *good idea*. We suspect that the economics of sharing will motivate people to post a handful of links to things like their blogs, personal-websites, twitter-accounts, github-accounts, and aggregators using those specialized platforms for sharing, in order to avoid paying for something that the Web can provide for free. This possible outcome suits us just fine, as it creates a high signal-to-noise ratio — which is exactly what we are after.

Investing and Governance

To facilitate investment in the project we are going to pursue a DAICO model. The idea behind the model is that investors can invest a specific amount of SOL or ETH (they can choose to invest on either Ethereum or Solana) into an investment-fund account for the Interlock project. This account has a monthly limit on withdrawals and any withdrawals beyond that limit would have to be voted on by the investors. A fixed number of SOL/ETH can be invested (i.e. the target number) and investors cannot exceed a maximum-proportion (which is **five percent** of the target number). Investors have voting-power which is proportional to the amount that they have invested. Each new round of investment will be a new DAICO involving a different investment-account and the same — or slightly tweaked — smart-contract to manage those funds. The presence of multiple and unlimited rounds is to give new investors an opportunity to participate fairly and equitably in the project. The presence of proportion-limits is to ensure (a) a minimum number of investors (i.e. 20) and (b) that no single investor has unilateral veto power during a vote. Investors will also receive ownership over accounts with a proportional amount of Voting Inter Tokens as well a normal Inter Tokens. Each investor will also receive upvotes from upvotes from the Interlock Team as a form of symbolic thanks.

For this to work correctly, we will have to break away from our theme of privacy and anonymity — allowing anonymous investors would be the same as allowing any investor to invest a proportion larger than 5 percent, which defeats the purpose. Additionally, allowing anonymous investors might interfere with KYC laws. Though, we can probably experiment with fully anonymous rounds for smaller investment targets (i.e. a few dozen thousand dollars).

We are also interested in trying to raise fund on Solstarter when that platform is ready — but until they launch, we will have to go with the DAICO model. **We will update this section with details for how the inaugural DAICO round will be run soon**.

Technical Contributions

Regarding technical contribution we will follow an RFD/RFC model where project design documents are proposed and discussed on various community channels (i.e. github, discord, and others). If the project and community get large enough we will likely adopt a governance model akin to Rust's. We diverge from the traditional RFC process in that we (a) adopt proposals by voting via smart-contract and (b) developers can show their support and affinity for each-other and their ideas by using the upvote/downvote mechanism that is already in place. We do not require separete personal and developer accounts, but we also do not require the same account. Keeping with the theme of privacy and anonymity a developer can have as many accounts as they want and the project/community would have no way of knowing — which is *already* the situation in the real world (i.e. one can make as many github accounts as they want). Voting is consensus-driven — proposals require unanimous approval. Unanimous consensus is meant to eliminate the competitive nature of voting — all disagreements should be resolved at the *discussion* phase before a proposal comes to a vote. We believe that there are very few *true* and *unresolvable* contradictions in engineering. Proposals can be resubmitted for voting.

Each technical contributor is given an NFT that allows them to vote. Each technical contributor must explicitly refresh their NFT every 30 days otherwise it gets burned. The idea is that if a contributor drops off the grid, their absence will not cause the system to lock-up. The Interlock Team can always issue new NFT's to contributors returning from a hiatus. The Interlock Team can also burn the NFT's of anybody who has not contributed any code in the previous 300 days — we have not found a way to enforce this via smart-contract so the process is, at the moment, manual.

What's Next

security industry and interlock

We are currently migrating this content from the original whitepaper, check back later.

ecosystem and frictions

We are currently migrating this content from the original whitepaper, check back later.

phishing statistics

We are currently migrating this content from the original whitepaper, check back later.