Democracy.Earth

The Social Smart Contract.

An open source white paper.

Version: September 1st, 2017.

The Social Smart Contract.

Democracy Earth Foundation
democracy.earth

Abstract.

In a world that has succeeded in the globalization of financial assets while keeping political rights enclosed to territories, we need to build new models of democratic governance that enable humanity to collaborate and address pressing global issues. Democracy Earth Foundation is building free, open source software for incorruptible blockchain-based voting within institutions of all sizes, from the most local involving two people to the most global involving all of us. Uneven distribution of opportunity around the globe due to the perpetual confrontation between national governments has led to accelerated climate change, rising inequality, terrorism and forced migrations. Democracy Earth Foundation proposes that the technology stack that includes Bitcoin as programmable money without Central Banks, and Ethereum enabling smart contracts without the need of Judiciary Courts, requires a new layer that signals incorruptible votes beyond the territorial boundaries of Nation-States. This transnational network will act in accordance with the personal sovereignty of its members and protect their human rights with encryption. In our Initial Rights Offering we offer a token called *vote* that will grant participation rights to every human with decision making as its main function. We seek nothing less than true democratic governance for the Internet age, one of the foundational building blocks of an achievable global peace and prosperity arising from an arc of technological innovations that will change what it means to be human on Earth.

1. Manifesto.

> *Democracy is always a work in progress, it's never an absolute idea or it would otherwise be a totalitarian ideology just like all the rest of them.*
>
> José Mujica, President of Uruguay (2010–2015).

Current democratic systems governing societies under the territorial domain of Nation-States have grown stagnant in terms of participation and are leading towards increased polarization. Constituencies are provided with tailor-made media that satisfies their own endogamic beliefs, pulling society apart as discourse and factual debate are replaced with a post-truth mindset. This is a consequence of the drastic expansion in communication channels that shrank attention spans rendering thoughtful analysis expendable. Centralized 20th century information distribution created uniform narratives, realities and identities. The Internet has fractured them. Instances of political participation in the so-called modern democracies are not apt for information abundant contexts and have remained without change since their inception.

Engagement through the traditional channels is weaker among younger generations, often not going out to vote and unlikely to engage in party politics. Meanwhile online activism is increasing with social media becoming the dominant arena for political clashes. This includes Facebook and Twitter (where gossip dissemination is predominant with fake news, bots and trolling among other campaign optimizations) and emergent echo chambers like 4chan.org where anonymity led to political incorrectness or gab.ai consolidating the alt-right community in the USA. Needless to say: endogamy only makes polarization stronger, and our tribalized societies have shown a tendency to continue relativizing truth risking the preservation of resources and the survival of future generations.

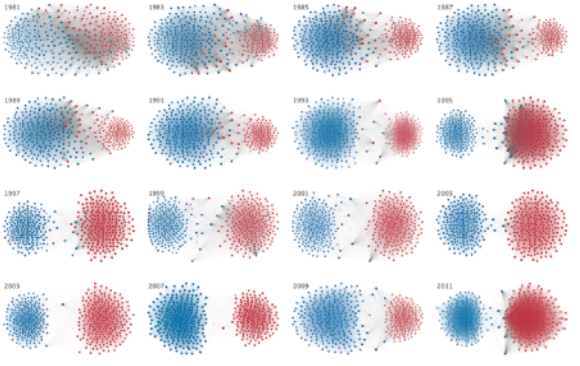
Democratic processes seen during high-stakes elections are often prone to fraudulent behavior with gerrymandering becoming commonplace and a strong link between what the major political parties spend and the percentage of votes they win. In developing nations exploits are literal having ballot boxes burnt by large parties to suffocate the chances of smaller competitors.

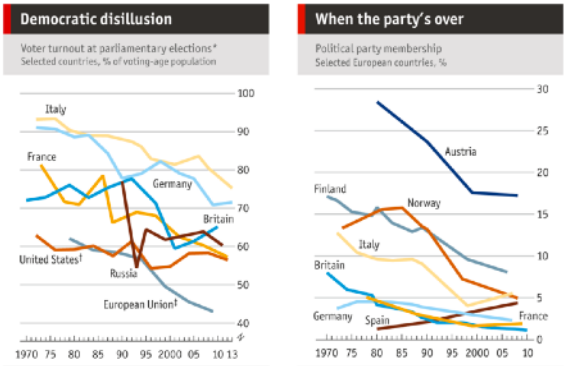
This document proposes a solution that will tackle both the political and technical issues currently weakening the prospects of democracy in the world by offering an alternative that can be adopted directly by citizens and implemented using peer to peer networks. As the internet becomes the dominant force in modern politics we see an indispensable need to develop digital technology for voting that can be securely deployed in any geographical location and for communities of any size.

With internet growth reaching over 3 billion lives (far surpassing major religions and Nation-States) and the development of encrypted networks known as blockchains permitting incorruptible transactions with permissionless audits, there's no reason stopping mankind from building a borderless commons that can help shape the next evolutionary

leap for democratic governance at any scale. Even in regions where internet penetration is below 50%, the digital gap is not based on socio-economic factors but it is rather a generational divide. According to Rick Falkvinge, founder of the Pirate Party: “Politics moves at glacial speeds: nothing seems to happen until suddenly a strenuous noise gets everyone's attention. It is slow because it often takes one generation to die for the next one to take over. And today we live in a world that has the offline generation in charge and the online generation growing up”.

New forms of governance must acknowledge the networked commons connecting humanity and progressively weaken the legacy of national frontiers and its inherent inability to address pressing global issues such as climate change, rising inequality, terrorism, automation and forced migrations. Uneven distribution of opportunity around the globe due to the perpetual confrontation between national governments led to the rise of these issues in the global agenda. We believe the technology stack that includes Bitcoin as programmable money without Central Banks and Ethereum enabling smart contracts





without the need of Judiciary Courts requires a new layer that signals incorruptible votes beyond the boundaries of Nation-States. This transnational network will act in accordance to the personal sovereignty of its members and protect their human rights with encryption.

1.1 Legacy.

We can consider elections implemented by states, provinces and city municipalities as democracies where we are reduced to being passive recipients of a monologue. Citizens are called in-between substantially long periods of time, during elections, to provide a basic input: essentially accept or reject players in the same system. This is the bandwidth of the legacy system that is our so-called modern democracies. Under these systems less than one percent of the population is able to vote on legislation or execute budgets while the rest are legally forced to outsource their full citizenship rights to a representing minority that eventually figures out how to perpetuate itself.

The technology behind representative democracies can be grouped in two sets:

• **Analogue Elections:** Usually paper ballots and ballot boxes with authorities responsible for counting votes and reporting fraudulent behavior. Even though these systems are stable in developed nations, they suffer from severe lack of participation. Barriers are implemented with requirements such as the need to register to vote through an excessively bureaucratic process that ends up blocking a majority of disenfranchised voters. Authorities also gerrymander districts by exploiting survey data in anticipation of electoral outcomes. Even though these systems are easier to audit, this also means that they’re easier to corrupt: in developing nations analogue elections get subverted by mobs representing large parties that burn or 'disappear' ballot boxes, threatening auditors from smaller competitors and letting violence overrun the process in key districts. In our experience with the Partido de la Red running for the City Congress of Buenos Aires in the 2013 elections we found out that no effort mattered more than having sufficient party auditors to cover every district in the city or otherwise votes would get stolen. The larger an election’s te—rritory is, the less likely an analogue system can guarantee a fair process. Further, high implementation costs end up limiting elections to a handful of days per year (if any), rendering democracy an exception rather than the norm regarding how governments actually get elected.

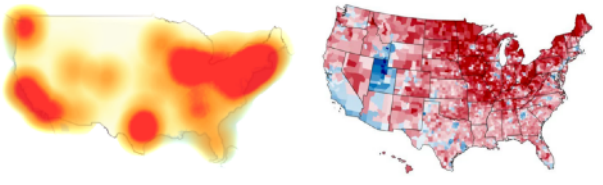
• **Electronic Voting:** Proposals that deliver solutions based on electronic voting machines aim to secure the process through a digital interface yet with the same logic of few elections per year, with the net effect of new technology serving the same purpose of legitimizing professional politicians as old voting technology. Machines can effectively help avoid clientelist techniques used to corrupt an election but open a whole new surface of attack by exposing ballots to the risk of undetected hacks and foreign intervention. Experts on this field (including the Supreme Court of Germany) recommend using electronic voting machines that leave a paper trail or any alternative medium for vote proof. Another approach to secure and transparent voting systems are efforts to make voting machines open source and auditable by the public. Technology can also be introduced directly by citizens using smartphone apps to perform parallel vote tabulation to report partial tallies across different polling stations as a safeguard against official reports. By their very nature, computing systems keep logs and

and cannot guarantee vote secrecy. For this reason any logging of a digital voting system should be public by default and trustless, operating with a distributed ledger syncing the outputs of a shared network. In short: a blockchain.

Traditional analog and electronic elections are strictly for long-term, representative democracies with elective periods ranging from 4 to 6 years. But the underlying dynamic of these systems is that officials are pre-elected from the top-down and presented for citizens to legitimize with their vote. The argument that citizens lack the knowledge and preparation to fulfill political responsibility and don't have enough time in their daily lives to engage in public affairs is weak on merit: more often than not public servants require input from experts on specific fields to draft legislation. As well, thanks to the Internet, mobile phones, social media and satellites, we observably live in a world full of citizens routinely engaging in debate on political issues (albeit lacking any chances of genuine impact.)

1.2 Geopolitics.

A consequence of the US Presidential Election of 2016 is that the fear of foreign intervention has become a leading threat to the security of electoral processes. But although voting machines are an extremely vulnerable target, (defcon 25 had a large selection of voting machines, all of them were exploited) foreign attacks have a simpler method than hijacking voting machines because directly manipulating votes potentially can be traced, is very expensive, and difficult to execute on a scale large enough to satisfy an attacker. A more efficient approach is instilling public fear by collapsing internet infrastructure days prior to an election in a way that can help push favoritism on a candidate that is perceived stronger than the other one. This kind of cyberattack able to trigger a shift in voter perception is nearly impossible to trace as political subversion and reveals the inherent conflict that a digital commons has with territorial democracies.



This happened two weeks before the US 2016 election when a botnet coordinated through a large number of Internet of Things (IoT) devices executed a Distributed Denial of Service (DDoS) attack that affected Domain Name System (DNS) provider Dyn Inc. bringing down major websites in the US including Amazon, Paypal, New York Times and Wall Street Journal among many others.

1.3 Land vs. Cloud.

In the near future, electrons and light flow freely, and corporate computer networks eclipse the stars. Despite great advances in computerization, countries and race are not yet obsolete...

Ghost in the shell, graphic novel (1995).

The 21st century is witnessing a growing conflict between The Land: governments that monopolize the law on territorial jurisdictions by restricting the free movement of physical goods and bodies; and The Cloud: global corporations that monopolize access to user data able to track and target ideas via personalized advertising. In this world freedom is an illusion: our bodies belong to governments, our minds to corporations. Notorious battles from this conflict include the Apple versus FBI case requesting the jailbreak of an encrypted phone; or the historical dispute between Silicon Valley's cosmopolitanism seeking flexible visas and Washington D. C.'s nationalism raising migration barriers. As this scenario unfolds, encryption plays a role of growing significance to protect the human rights of digital citizens as it can help them break apart from the cloud versus land trap.

The origins of modern cryptography go back to World War II when Alan Turing built the first proto-computers to decrypt Nazi messages. Since then encryption has been legislated in the USA in the same manner kept for traditional weapons: it is included in the Munitions List of the International Traffic in Arms Regulations and related software and hardware must deal with export restrictions. And even though encryption is often considered a right protected under the First Amendment arguing that "code is speech", its defensive nature indicates that it must also be protected under the umbrella of the Second Amendment since it holds the same reasoning behind the "right to bear arms": In an era where whistleblowers are revealing how the Deep State spies on citizens anywhere around the globe, encrypted information is the only realistic guarantee that anyone has to be protected from government abuses (and the corporations that back them).

Secrecy is a fundamental property of free and fair elections as it is a mechanism that helps avoid coercion from those in power and prevents the risk of elections being bought and sold for money. Privacy is the best guarantee a conscious free mind has to think for itself. But on the modern internet: privacy is illusory when using Facebook, Google or any web based service. Even though Internet monopolies pretend being the gatekeepers of online privacy, theoretically Facebook can still impersonate any of its 2 Billion registered users if they ever wanted to. Google and Facebook hold the largest identity

databases in the world surpassing the governments of India and China, while 97% of their reported revenue comes from advertising severely conditioning the kind of experience that users get with their technology. It is in their interest to gather as much information as possible to profile people in order to stay competitive in the attention market and both companies filter information fed to users with algorithms accountable to anyone but their own board. None of their services are really free: personal sovereignty is given away in the same way the natives in the American continent got distracted watching their own selfies in shiny mirrors 500 years ago while the European conquistadors swept their entire way of life at a whim. Uncensored, free and sovereign debates on the future of humanity are being eaten by useless likes that only help perpetuate these corporate entities. Fake news exploits (as they were used during the U.S. elections) or critical content spreading like wildfire (as it happened during the Arab Spring) demonstrates that any effort to stop international influence on national politics is futile as societies spend most of their time online. The Internet is incompatible with Nation-States.

1.4 Intelligence.

I can't let you do that, Dave.

HAL 9000 on 2001: A Space Odyssey (1968).

The best civic tech is tech that gets used every day. Already, Facebook, Twitter and other social media platforms have become by proxy the main interface citizens use to influence everyday politics. But the unseen consequences of giving personal data away through centralized web services can be many and with relevant implications for the future of humanity. The information architecture of how personal data is stored, shared and monetized is fundamental to understand sovereignty in the 21st century.

A looming threat is the use of unrestricted Artificial Intelligence (AI) that gets fueled by user generated content without any kind of public supervision. That was evident in a former Blackwater employee's revelation to us on how data gets weaponized: from an office in Dubai he was able to drive and get the live feed of a drone flying over Syria or Pakistan, but surprisingly the decision whether to kill the target wasn't made by the human operator (or a supervising authority) but by an AI that called the shots over the Internet "at least 90% of the time". This AI was provided by the Silicon Valley company Palantir founded by Peter Thiel (seed investor and Facebook board member). Often described as a Facebook spin-off to provide intelligence services to the CIA, Palantir is credited with having found Osama Bin Laden in 2011.

The issue on AI deciding on the fate of human lives opens up ethical and moral questions. Eventually not even human researchers are able to properly understand how an AI is behaving, becoming a threat if it is a key component of military grade technology. According to author Yuval Noah Harari: "intelligence is breaking apart from living organisms and it won't be monopolized by carbon beings for long." Consciousness is the new political frontier being drawn. A line between machines and humans. In other words: understanding whether we are using the machines or the machines are using us. How we structure human organizations —and govern the code running them— defines who is in charge. As the capacity of silicon intelligence matches Moore's Law growth rates, humanity as a whole must ask itself how it is going to govern the reins of this unprecedented power.

1.5 Decentralization.

Sovereign is he who decides on the exception.

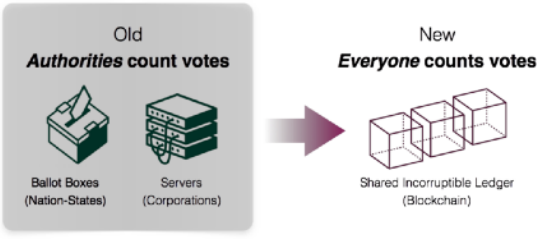
Carl Schmitt, political theorist (1888-1985).

The achilles heel of data hungry, attention farming internet monopolies is their need of a centralized information architecture. They rose as the superhubs in what used to be the promise of a web shaped network by implementing the winning solutions to the leading online use cases. But the consequence has been a privatized ecosystem: closed code, walled gardens and centralization of power in a few hands paving the way for a full surveillance society on what could otherwise be a borderless commons. When Sir Tim Berners-Lee, creator of the world wide web protocols, pointed out the intrinsic risks on today's internet he requested the need to draft a Magna Carta for the Web: "Unless we have an open, neutral internet we can rely on without worrying about what's happening at the back door, we can't have open government, good democracy, connected communities and diversity of culture. It's not naive to think we can have that, but it is naive to think we can just sit back and get it."

Centralization is the single point of failure in elections and is incompatible with democracy. In our experience implementing centralized digital voting for decisions of Partido de la Red, we detected that if an election is high-stakes (all or most members have a biased interest in the outcome), the likelihood of the system being corrupted increases. The biggest risk lies in those who are responsible for controlling servers and database integrity. We have found out on internal elections held in early 2017 discrepancies between information reported by database auditors and the logs voters kept in their local machines: manipulation in vote emission data, aribitrary modification of poll closing date, erased records and sudden ban of registered accounts where proven and denounced leading to a generalized perception of fraud in the whole process. Centralized digital democracies without any consideration for cryptographic security are toys useful for playful purposes but can be

dangerous when implemented in real scenarios under fraudulent hands.

Meanwhile, traditional elections have a technique known as adversarial counting when the outcome is close to a tie. Authorities of all involved parties participate in a manual vote count. But when an election happens within a large population, adversarial counting reduces the cost to subvert it by having an attacker only needing to bribe a few authorities from a competing party to secure a result. Any kind of system that requires trust from participants ultimately runs the risk of having its whole structure collapsing if any authority is fraudulent.

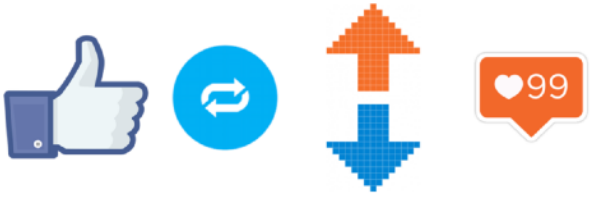


Decentralization is a requirement of democratic elections. Without it there will always be room for corruption. Blockchains enable trustless systems by eroding the need of human authority and increasing the defenses of vote integrity with a shared resource that has scorekeeping as its main function. This permits unprecedented designs for electoral systems. With a blockchain-based democracy votes become censorship resistant and every single voter can audit an election without requiring any kind of access rights to infrastructure. By storing vote data in a blockchain rather than in private servers or ballot boxes, audit costs become abstracted and are turned into a guaranteed right for every participant. Voters are not just mere spectators but also sovereign gatekeepers of the whole process. This kind of transparency cannot be delivered by traditional electoral systems, analog or electronic.

1.6 Sovereignty.

On today's internet, voting has still emerged as the main interaction. Every time users like, upvote, heart, link, or retweet content they are signaling a preference that serves a feedback loop generating better recommendations for them. But the action won't go any further: it's a fake vote that lacks institutional implications. Likes in social media operate as worthless tokens that can be inflated with a single click even though they set the price of advertising dollars. Network effects turned this interaction into a metric that highlights the influence of a specific idea within a crowd, often being a tool for those in power to survey society's needs. But the financial and political benefits of these transactions are entirely kept by the network owners.

Sovereign technology able to operate in peer to peer networks, validating identity, preserving anonymity, encrypting data, decentralizing infrastructure, with free (as in freedom) open source code can completely disrupt the described landscape.



Throughout history only three kinds of sovereigns prevailed: the sovereign tribe where a crowd follows a leader; the sovereign king loyal only to God; and the sovereign republic with continental lands governed under one law. Blockchains operating in cyberspace are giving rise to a fourth kind: the networked individual. It's not a far fetched possibility: conquering personal sovereignty is already a reality for those who run their finances with bitcoin and other crypto holdings. As investor Naval Ravikant puts it: "You can cross an international border carrying a billion dollars in bitcoin entirely in your head." This kind of sovereign act is unprecedented even for contemporaneous Heads of State.

The widespread adoption of blockchains is giving rise to a model that initially grew under the shadows of established institutions but eventually will render them obsolete. Blockchains are automated bureaucracies that offer significant financial benefits in terms of transaction costs while abstracting the need of intermediaries. They enable systems of free association that help break the political and financial coercion that governments and banks impose by restricting the right to vote or limiting access to capital. A technologically advanced society can flourish beyond territorial domains anywhere there is an internet connection with digital citizens becoming part of a new kind of diaspora.

2. Paper.

> *It is the technology that we do not control the one that is used to control us.*
>
> Emiliano Kargieman, space hacker (1975).

A foundational principle of democracy is the right to be heard. Today most of the world's population is not heard: having a voice is an accident of birth. Individual and collective voices are politically and economically silenced by 'illiquidity' - the marginalized are given no instruments to broadcast or amplify their voice. Modern democracies are the birthchilds of the Printing Press Era: printed constitutional systems dependent on wet ink contracts and the speed of the postal service. Representative democracies are an accident of the information technologies of the 18th century.

A liquid democracy is based on a dynamic representation model that works with a bottom-up approach: citizens are able to freely elect within their social graph (friends, colleagues, family) who they want to have as representatives on a specific set of topics. It is the most flexible form of democratic governance that can be constructed with digital technology,

governance that can be constructed with digital technology, operating as a hybrid that enables direct or delegated voting at any time. There are few precedents of trustworthy bottom-up environments that led to authoritative content, Wikipedia being a pioneering case. But if history is any guide, the last time civilization faced a paradigm shift regarding encyclopedic enlightment it was precisely on the epoch preceding the rise of modern democracies.

This paper details the implementation of a liquid democracy using Sovereign, our democratic governance application that operates with blockchain tokens using a basic set of smart contracts. Simplicity in the design and language used to express this design matters for the purpose of a genuinely democratic device. No technology will ever be able to satisfy democratic aspirations if it can only be understood by an elite. As cryptographer Ralph Merkle stated:

> *We do not call upon ordinary untrained citizens to perform surgery, fly airplanes, design computers, or carry out the other myriad tasks needed to keep society functioning, what makes governance different? The problem is readily understood: if we give governance to "experts" they will make decisions in their own best interests, not in the best interests of us all.*

2.1 Token.

An ideal voting system must be able to satisfy in the greatest possible extent these conditions:

- **Secrecy:** voter must be able to cast vote in secret.
- **Verifiability:** voter must be able to verify tallied vote.
- **Integrity:** system must be able to verify correct vote tally.

Additionally, due to the risk that coercion through physical violence or threats in contexts prone to political violence, an option able to protect coerced voters must be introduced:

- **Resistance:** voter must be able to override own vote if necessary.

In the work led by researchers Hosp & Vora, an Information Theory approach was taken to model voting systemsleading to the conclusion that a natural tension exists with a system aiming for perfect integrity, perfect ballot secrecy and perfect tally verifiability. All three cannot be simultaneously achieved when an adversary is computationally unbounded, able to brute force a system if unlimited time or memory are available. For this reason we consider indispensable to implement digital democracies using blockchains. With network effects already in place, blockchains are able to verify transaction integrity and prevent token double-spending. Bitcoin's proof of workmodel achieves this by rewarding computational capacity verifying transaction blocks (what is often referred as mining), leading to a network "300 times more powerful than Google's resources" according to pioneer Balaji Srinivasan. For this reason, our design is based on tokens within a blockchain network operating as political cryptocurrency.

What differentiates a vote from money (or in broader terms: a political economy from a financial economy) is that political currency is designed to guarantee participating rights under fair conditions to all members within an organization. Rights aim to satisfy overall legitimacy in the governance of an institution. While money is the language of self-interest, votes express the shared views of a community. Political currency is not strictly meant for trade but for social choice.

Feature	Coins	Votes
Utility	Trade.	Governance.
Mining	Computation	Attention
Liquidity	Scarce.	Guaranteed.
Signal	Self interest.	Social choice.
Value	Matter.	Information.

2.1.1 Implementation.

Considering that value can be driven by memetic capacity, the Democracy Earth token granting voting rights will be branded with the single most important message any democracy can convey: *vote*.

The *vote* token can be implemented using smart contract code across a variety of blockchains that permit Turing Complete scripts, including Bitcoin. Our design is blockchain agnostic in recognition of a computer science field still in its infancy where significant innovations remain to be invented. Nonetheless we are working on implementing the *vote* token under these smart contract environments:

- **Ethereum**: Using a set of solidity smart contracts under the Ethereum ERC20 token standard.
    - **Rootstock**: We are taking the necessary steps to make solidity code compatible with Rootstock's smart contract interpreter for the Bitcoin blockchain.
- **Lightning**: With the activation of segregated witness in the Bitcoin protocol that enables routing of payment channels with the Lightning Network protocol, liquid democracy delegations can be mapped using satoshi-level transactions carrying an attached *vote* identifier. Blockchain settlement cost must be covered by the implementing organization.

Also, multi-chain implementations are encouraged in the spirit of seeking greater experimentation and collaboration regarding these technologies.

2.2 Voting.

The *vote* token aims to be a standard for digital democracy able to interoperate with other tokens, setting a common language for the governance of blockchain based organizations. Within the context of liquid democracies, a range of voting transactions is permitted with *votes*:

- **Direct Vote**: Selfish voter Alice is allowed to use her tokens to vote directly on issues as in a direct democracy.
- **Basic Delegation**: Alice may delegate *votes* to Bob. As long as Bob has access to those tokens he can use them to vote on Alice's behalf.

- **Tag Limited Delegation**: Alice may delegate *votes* to Charlie under the specified condition that he can only use these tokens on issues carrying a specific tag. If the delegation specifies that delegated *votes* can only be used on decisions with the *#environment* tag, then Charlie won't be able to use these anywhere else but on those specific issues. This leads to a representation model not based on territory but on knowledge.
- **Transitive Delegation**: If Bob received *votes* from Alice, he can then delegate these to Frank. This generates a chain of delegations that helps empower specific players within a community. If Alice does not desire to have third parties receiving the votes she delegated to Bob, she can turn off the transitive setting on the delegation contract. Circular delegations (e.g. Alice receiving the tokens she sent Bob from Frank) are prohibited since the original allocation of *votes* from an organization to its members carries a signature indicating who is the sovereign owner of the *votes*.
- **Overriding Vote**: If Bob already used the delegated *votes* he received from Alice but she has a different opinion on a given issue, as the sovereign owner of her votes Alice can always override Bob's decision. Voters always have the final word on any given decision with their original *votes*.
- **Public Vote**: Often referred as the *golden rule* of liquid democracies, all delegators have the right to know how their delegate has voted on any given issue with their *votes*. In the same way congressmen votes are public, on liquid democracies competing delegates on any given tag have an incentive to build a public reputation based on their voting record in order to attract more delegations.
- **Secret Vote**: A method that can make *vote* transactions untraceable to the voter. This is indispensable in contexts of public elections held within large populations that have a high risk of coercion. Even if perfect secrecy on *vote* transaction is achieved, user's can still be fingerprinted with exposed meta-data. For this reason, research on integration with blockchains designed for anonymous transactions with a proven track record is encouraged. This might include a mining fee to settle the *vote* transaction that can be either subsidized by the implementing organization or directly paid by voters. We recommend research and integration of secret *votes* with these blockchains:
    - ZCash: implements shielded transactions using zero-knowledge proofs
    - Monero: uses ring signatures with stealth addresses.

2.3 User Experience.

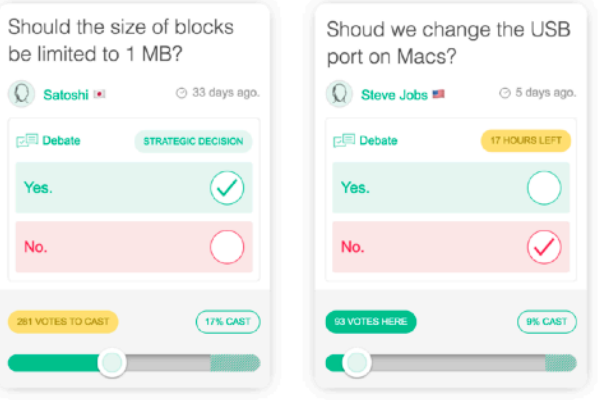
User Experience (UX) is a critical aspect of a decentralized architecture and becomes even more important as the redundant layers of centralized architectures condense to the user. In a centralized internet architecture, the user does not own the interface or experience. In a decentralized internet architecture, the user interface (UI) should be based on the user's perspective. In this sense, transactions get done under three distinct views:

- **Self**: Using a public identity related to an individual.
- **Organization**: In representation of an organization that extended representation rights to individuals (e.g. workplace, club, political party, etc).
- **Anonymous**: Without any connection to a public identity.

This understanding of *SELF / ORG / ANON* shape-shifting requirement highly influenced our interface and token design. At any given time a Sovereign user can adopt any of this modes to interact with decentralized organizations.

2.3.1 Liquid.

Sovereign aims to make liquid voting immediate and simple. Any friction in the process must be avoided and the delegation widget should be constantly exposed on the interface while browsing issues or looking at member profiles. For this purpose, Sovereign uses a *liquid bar* that permits transacting *votes* with a single gesture either on mobile and desktop devices.



The *liquid bar* allows these actions:

- **See available *votes***: Since in a liquid democracy a user can have 1 or more delegated *votes*, having a constant reminder of the balance helps the user understand his or her current power within the system. If some of the *votes* were delegated with strict conditions (e.g. a *Tag Limited Delegation*), this means that a user won't have the same amount of *votes* available to spend on every issue.
- **See cast *votes***: A percentage value with the amount of *votes* currently cast on other decisions or delegated to other members of the community is shown. The user can tap or click at any time on that value to view a complete list of the issues where he or she is currently having a *vote* and decide whether to keep them there or make a strategic change.
- **Slide to *vote***: The user can use his thumb (or mouse click) to slide the *liquid bar* handle and upon the release of it he or she will be prompted a confirmation request whether to *vote* or not.
- **Tap to *vote***: If the user does not want to allocate more than 1 vote, he or she can simply tap on the *liquid bar*handle once and will be prompted to confirm a single *vote* transaction.
- **Remove *votes***: At any time, as long as the poll is still

open, the user may remove his or her *votes* from a decision by simply sliding the *liquid bar* handle back to the initial position.

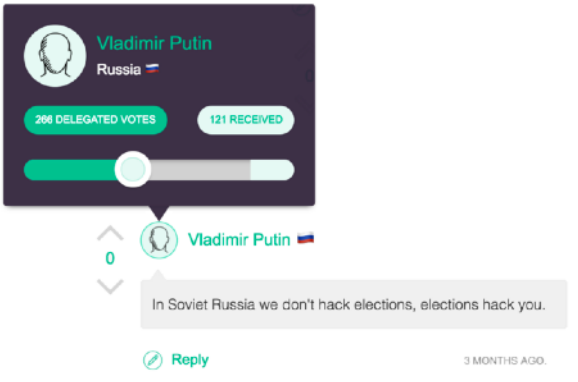
We see this interaction as a step forward from the *like* pattern found in social media. *Likes* limits voting to mindless clicks and can be inflated at will. Since *votes* operate as a scarce resource in the system, they cannot be generated at will and always require a minimum of tactical thinking regarding how a user's interaction will influence a specific decision. *votes* have real implications to the user as a stakeholder of a decentralized organization while *Likes* only serve their controlling corporations.

2.3.2 Delegations.

A *liquid bar* also displays the *vote* delegation relation a user has with any other member of an organization. Delegations go both ways:

- **Sent**: A user must be able to delegate any of his available *votes* while checking the current delegated amount (if any).
- **Received**: A user must be able to understand how many *votes* were received from someone else.

Every time a member profile is displayed on Sovereign, the current delegation status between the user and the member is shown.



2.3.3 Agora.

Sovereign also has a debating component codenamed *Agora*. Debating is likely as important as voting on any democracy. Agoras display *threaded conversations*, a successful design pioneered by Reddit and Hacker News. We consider this UX pattern as the best way to engage in thoughtful conversations online as they have the most valued comments bubble up, helping sort the information for a debate using the collective intelligence of the community.

But unlike web based applications, Sovereign does not allow testimonial interactions: instead of permitting infinite *upvotes* or *downvotes*, if the user agrees with a comment from someone else in the platform, it will trigger an instantaneous delegation of a single *vote*. Hence Agoras permit:

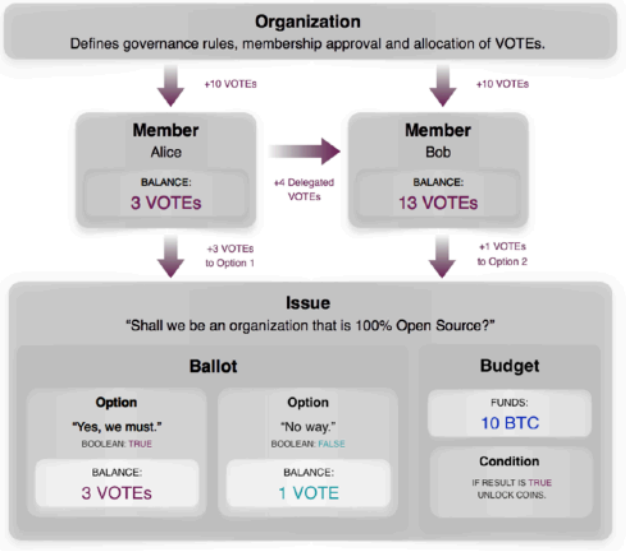
- **Upvote**: Send a single *vote* delegation from the user to the commenter.
- **Downvote**: If a user disagrees with someone's comment, a *downvote* can either retrieve a *vote* from the commenter back to the user if there was a previous delegation. Or if no `delegation relation exists among them, then` a *downvote* will act as a penalty sending a *vote* from the commenter back to the funds of the organization implementing the Sovereign instance. The criteria for this kind of penalty can be set in the *constitutional smart contract* of the implementing organization.

This will make delegations more frequent across the platform. Debates constantly exposed to the risk of *vote* transactions means that they are subject to real political impact. This mechanism can help reward good arguments and punish the influence of trolling without requiring the need to develop moderating authorities in the system.

2.4 Smart Contracts.

When Claude Shannon wrote his foundational 1948 paper on Information Theory, he was able to demonstrate how circuits can perform logic functions by expressing a binary state of `1` and `0` (`true` or `false` states). Since then, digital technology shaped the dynamics of all kinds of information systems. With this in mind we focused on building an efficient design for a governance machine able to operate with blockchains that keeps its human operators as sovereign rulers by means of the vote. In the same way bits move in computers signaling a `true` or `false` state, *votes* signal a boolean value for institutional decisions to be recorded under smart contracts.

vote tokens operate within the institutional boundaries created by this set of contracts: `Organizations`, `Members`, `Issues`, `Ballots` and `Budgets`. These are the building blocks that help create a governance circuit that can scale to operate liquid democracies within communities of any size.



2.4.1 `Organizations`

The entity or institution implementing a Sovereign instance is referred as an `Organization`. This entity acts as a governing authority defininig who are the Members allowed to participate in its decisions and granting them *vote* tokens. Since `Organizations` can live in a decentralized network, the

2.4.1.1 `Constitution`

The *constitutional smart contract* determines how *votes* will be allocated to members among other governance decisions. Allocation conditions are a prerogative of the organization depending on its goals: in some cases it can be aligned with financial rights (e.g. the shareholders of a corporation getting one *vote* per share); in other cases can be assigned based on an egalitarian distribution to all members (e.g. tax payers within a jurisdiction each getting a same amount of *votes*).

The basic settings to be found on a constitution are:

- **Decentralized ID** (or URL): An identifier that helps refer to the `Organization` anywhere on the network and that it is connected to its `Domain`.
- **Bio**: A basic description of the organization including its name, website, address, jurisdiction (if applicable).
- **Funding**: The amount of *vote* tokens this organization will manage and how these will be allocated to every member and grant access to `Budgets`.
- **Membership**: Requirements to become a valid member within organization. This criteria defines the voter registry that guarantees a fair electoral process of a democracy and can be scrutinized by its members.
    - **Open**: Anyone can freely join an organization.
    - **Voted**: Existing members must vote on applicant members. A percentage criteria must be set for approval.
    - **Fee**: The organization requires a payment for membership approval.
- **Content**: Defines who is allowed to post `Issues` on the organization.
    - **Open**: Anyone (whether its a member or not) can post. Only members get the right to vote.
    - **Members**: Only approved members have the right to post.
    - **Special Members**: Members that meet certain criteria (e.g. a minimum of delegated *votes* or *votes* received under a specific tag) have the right to post.
    - **Anonymous**: Defines whether anonymous content is allowed to be posted.
- **Moderation**: Describes the rules that help define a code of conduct among members of an organization.
    - **Ban**: An amount of *downvotes* required to ban a member from participating in the organization and the penalty attached to it (e.g. a period of time)
    - **Expulsion**: If an organization is based on *Voted Membership Approval*, a member can receive negative votes from other members signalling that such identity has been corrupted or is no longer part of the organization. This criteria can be established as a minimum percentage required.
- **Voting**: The allowed `Ballots` to be used for the decisions to be made by the organization and specific settings such as *quadratic voting*.
- **Reform**: The requirements to change any of the rules set on a *Constitution* (e.g. a special majority).

Templates defining common practices for specific kinds of organizations are encouraged to simplify the setup. Sovereign will include templates for corporations, political parties, trade unions, clubs and coops among others.

2.4.2 `Members`

Every Organization has members that get the right to vote on the decisions of the organization. Membership criteria is defined in the *constitutional smart contract* and is key for the trust on any democratic environment. Among the most common ways to subvert an election is the manipulation of voter registry. Securing this aspect with cryptographic means as well as an approval protocol is critical. Once a member is approved within an organization, he or she gets a specific amount of *votes* to be used for its governance.

All `Organizations` who take the responsibility to approve or disapprove `Members`, contribute with this task to the *Proof of Identity* process described on Section 3.3.

Compatibility with decentralized identity protocols is encouraged for the purpose of guaranteeing decentralized governance. The specification of DIDs (decentralized identifiers analogous to the web's URIs), proposed by the W3Cenabling self-sovereign verifiable digital identity is recommended.

2.4.3 `Issues`

An organization consists of a collection of *issues* each describing a decision to be made by the members. Membership properties described in the *constitutional smart contract* define member's voting and posting rights. An issue in its most basic form has these properties:

- **`Description`**: Text of the decision to be made.
- **`Tags`**: Categories that describe the decision within the organization. This helps members navigate across issues, define areas or teams within an organization and limit the scope of a delegation of *votes*. If the implementation is done with blockchain environments that are used to manage a fixed taxonomy (like Blockstack), a common distributed language for tags based on decentralized domains helps making the democratic environment more fair as it avoids members trying to control naming conventions for their own benefit. For this reason, within an open network `Tags` that describe `Issues` or are used to constraint delegations, are pointers to other `Organizations`. This is detailed in the *Proof of Identity* process.
- **`Signatures`**: Members that are authoring the proposal. It can remain anonymous if an organization's governance rules allows it.
- **`Ballot`**: The presented options for voters to participate on this decision.
- **`Budget`**: An optional element that may include locked funds in a cryptocurrency address that can trigger an action if a decision is voted in support.
- **`Timespan`**: For the final tally, an open poll must also set its scope in time and define the kind of decision being made. There are two types of decisions:
    - **`Tactical`** (limited in time): These are contracts that receive *votes* until a closing date is met, where a given block height within the blockchain

implementing the *vote* smart contracts can be set as the end line for the electoral process. Once all transactions have been tallied and a final result is recorded, all tokens get returned to the corresponding voters and can be used again on future decisions.

- `Strategical` (unlimited in time): Never-ending open polls that are perpetually registering the consensus of a decision state. *votes* can be retrieved by voters at any given time if they feel the need to discontinue their voice in support or rejection of a decision. But as long as the token is assigned to signal a preference on a contract ballot without closing date, it is part of the strategical decision. A common use for strategical decisions can be the members voting for approval of other members within the community of an organization.

2.4.4 `Ballot`

An issue can be implemented with any possible ballot design according to the specifications defined in the *constitutional smart contract* of the organization. The building blocks for a ballot are its `Interface`, `Options` and `Criteria`.

2.4.4.1 `Interface`

By default Sovereign provides the most commonly used choice mechanisms for ballot interaction. Further innovation on ballot interfaces is encouraged.

- **`SingleChoice`**: One selectable option.
- **`MultipleChoice`**: One or more selectable options.
- **`Cardinal`**: A given score per option with a pre-defined range of value.
- **`Ranked`**: Sortable options as ranked preferences. Arrow's impossibility theorem must be taken into consideration for any innovation regarding ranked ballots. This theorem states that rank-based electoral systems are not able to satisfy fairness on three key aspects at the same time:
  - **Unrestricted domain**: all preferences of all voters are allowed.
  - **Non-dictatorship**: no single voter possesses the power to always determine social preference.
  - **Pareto Efficiency**: if every voter prefers an option to another, then so must the resulting societal preference order.

2.4.4.2 `Options`

In order to enable the information processing of *votes*, ballots carry boolean values expressed in their options. This lets *vote* transactions signal a *decision state* that will act as a force modeling the institutional choices for the implementing organization. This makes all decentralized organizations also into programmable institutions. Options can then be:

- **`True`**: It will signal a `true` boolean value if selected (often described with 'Yes' or 'Positive' label strings).
- **`False`**: Signals a `false` state (e.g. can display 'No' or 'Negative' labels).
- **`Linked`**: The option is connected to another decision within the organization.
- **`Candidate`**: A member or list of `Members` from the organization. This helps elect authorities within the organization or it can be used for membership approvals.

2.4.4.3 `Criteria`

Finally, counting methods for the final or ongoing result of a decision within an organization.

- **`Plurality`**: Simple majority wins decision.
- **`Majority`** A minimum percentage is required for winning decision.
- **`DHont`**: Widely used by Nation-State elections based on member lists.
- **`Schulze`**: Commonly used by open source communities and Pirate Parties using ranked choice ballots.
- **`PageRank`**: Created by Larry Page and Sergey Brin, counts votes weighting voter reputation in a graph.

2.4.5 `Budget`

Every `Organization` can have 1 or more cryptocurrency addresses to fund its efforts. Sovereign permits to fund an `Organization` with Bitcoin and in its `Constitution` define a criteria on how these assets get distributed among `Members`:

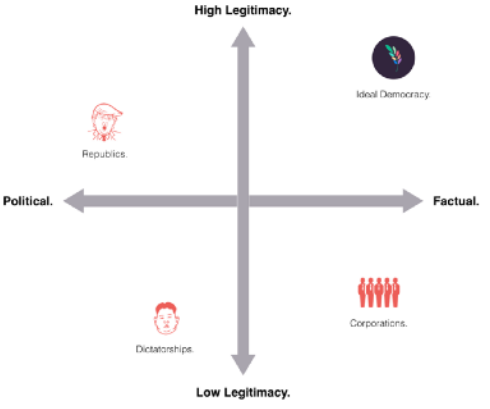
- **Percentage for *Proof of Identity***: Applicant `Members` can submit their *Proof of Identity* evidence to get membership approval to an `Organization`. If *votes* approve the new member, it strengthens the reputation of a self-sovereign identity in the open network by rewarding him or her a fixed amount of Bitcoin to permit hashing the *Proof of Identity* on a blockchain. Some `Organizations` may allow a bigger reward than others, effectively creating a Reputation score that can protect the network against *Sybils* or false identities. This process is detailed on Section 3.
- **Percentage for `Issues`**: `Members` seeking to use resources from the `Organization` can request them by attaching a `Budget` to an `Issue`. A `Member` can request to used funds from a pool specifically reserved for this. If the final tally of a decision reaches a certain value (`true` or `false`), it can then enforce the final decision by unlocking coins or triggering a transaction sending the requested assets to a specific address.

2.5 Security.

With Sovereign we are aiming to provide a lightweight governance framework that permits all stakeholders of an organization to participate and enforce decisions through the use of cryptography. But it is important to state that we are not aiming for a democratic system based on mob-rule or *majoritarism*. History offers sufficient examples on how a blind majority can end up failing the aspirations of a republic often putting demagogues in power.

Our main goal is to deliver a system able to guarantee the greatest amount of legitimacy while empowering the most

knowledgeable voices in any community. The difference between fact and promise is simple: while the art of politics consists in sustaining the fiction that breeds trust on established institutions (e.g. politicians during campaigns), cryptographic proof of events delivers a more reliable method for trusted governance. The incorruptible nature of blockchain transactions provides an incentive for people not to lie, hence organizations storing votes and decisions in them get driven by facts rather than promises. Corruption can be fought at its root as we develop a new sense of citizenship based on digital networks.



Still, liquid democracies can be gamed in different ways with outcomes dominated by the unintended consequences of two dynamics representing extreme ends of the participation spectrum:

- **Lack of delegations** leading to a *polyopoly*: extreme fragmentation of voting power.
- **Abundance of delegations** leading to a *monopoly*: extreme concentration of voting power.

Each outcome impacts one of the two axes measuring the quality of democratic governance. The incentives on the *vote* political economy are designed to keep a stable equilibrium aiming to guarantee the highest level of legitimacy and fact-based decision making.

To become a trusted environment for decentralized governance under large communities (cities, nations or global scale), Sovereign must be protected against different kinds of attackers: *Mobs*, *Corporations*, *Sybils*, *Fakes* and *Big Brother*.

2.5.1 Polyopoly.

a.k.a. *Mobs*

Among the most notable research projects on the field is Google Votes. This was an internal implementation made for Google employees led by engineer Steve Hardt where he created a liquid democracy plug-in to be used on the internal version of Google+. The project had the following numbers in terms of impact:

- 15,000 participants.
- 371 decisions.
- **3.6% of delegated votes** in total.

The small percentage in delegations means that Google Votes operated more as a direct democracy than a liquid democracy. Delegations occurred mostly among those users who actively campaigned to attract them (e.g. vegans in a team hoping to gather power to choose office snacks). The risk of few delegations is that it opens the democracy to the known risks of mob rule. Although this might keep legitimacy high, the quality of the decisions being made by an organization becomes more political than factual. Knowledgeable voices able to address specific problems within a community become disempowered.

This is the leading reason we have put most of our efforts in the development of a reliable UX that can turn delegations into a common habit reducing as much friction as possible in the interaction. Also since the *vote* token operates in a blockchain, delegations don't need to necessarily happen within the Sovereign application. Messaging applications, tweets and e-mails can be sent with *vote* addresses or QR codes attached to them making the *vote* token broadcastable across multiple networks.

2.5.2 Monopoly.

a.k.a. *Corporations*

When the German Pirate Party implemented Liquid Feedback, a pioneering liquid democracy software developed in 2009, it reached a participation level of ~550 affiliates that led to a linguist professor becoming the most influential member of the party. Martin Haase was in charge of translating all uploaded propositions in the system to a neutral language in order to avoid any ideological bias, making him grasp 167 delegations from other members.

The consequences of having a monopolizing leader in a liquid democracy environment goes against the spirit of an ecosystem that aims to incentivize more participation. In liquid democracies *celebrities* can become extremely influential being able to attract most of the delegated votes. An attacker willing to subvert an election can promote a TV star wearing a QR code to get a sudden influx of delegations from fans and viewers, instantly becoming a monopolizing force. Monopolies are a threat to liquid democracies since they can disincentive less fortunate voters to participate, hijacking the legitimacy of the decisions being made.

2.5.2.1. Quadratic Voting.

A key setting of a liquid democracy system is to permit quadratic voting for delegations. The cost for Alice to delegate votes to Bob increases exponentially the more votes get delegated. With quadratic delegations Alice can only delegate Bob 1, 2, 4, 8, 16 or even 128 or 512 *votes* but no value in between. This makes any delegation tax the delegator by reducing the opportunity cost of delegating to another member. This method prevents the rise of monopolies within the market dynamics of liquid democracies, always making the participation of all members relevant. If some organizations desire a more vertical chain of command (e.g. corporations), quadratic voting can still be disabled in the *constitutional smart contract* of a Sovereign implementation.

2.5.5 Sybil Attack.

a.k.a. *Identity Theft*

Whoever has the ability to control the registry of voters of any given election can directly influence the end result. A classical example is registering defunct members of society to vote in an election. On decentralized networks this is commonly referred

as a sybil attack (a name taken from an homonymous 1976 film based on a character that suffers a multiple personality syndrome). Sybil nodes are those that identify themselves as independent actors in the network while they all are under the control of a single operator. In decentralized environments sybil attacks are the most common threat and for this reason we consider indispensable that for *votes* to be granted they must get validated through a protocol (social and algorithmic) that works as *Proof of Identity*.

2.5.6 Fake news.

a.k.a. *Gossip*

It is no coincidence that the battlefield of modern democracies is disputed in the media. News organizations have unprecedented capacity to shape voter perception. Across different jurisdictions worldwide, governments wage an internal war between the State and the largest local media conglomerate. This is the playbook behind Donald Trump and his fight against the CNN & New York Times tandem; or the reason Vladimir Putin invested significant resources to create Russia Today in order to have a way of presenting alternative facts. Controlling the message tends to matter more than truth itself. Free media and independent journalism are a fundamental requirement for stable democracies. But if evidence of institutional facts are hard to prove, the room for manipulation is greater than the room for truth to prevail. Traditional institutions are secretive and lack transparency even if they are public offices. Blockchains enable a way of storing institutional facts that guarantees transparency in organizations. In this sense, *fake news* can be fought with a new institutional model able to store *Hard Promises*.

2.5.4 Squatting.

a.k.a. *Big brother*

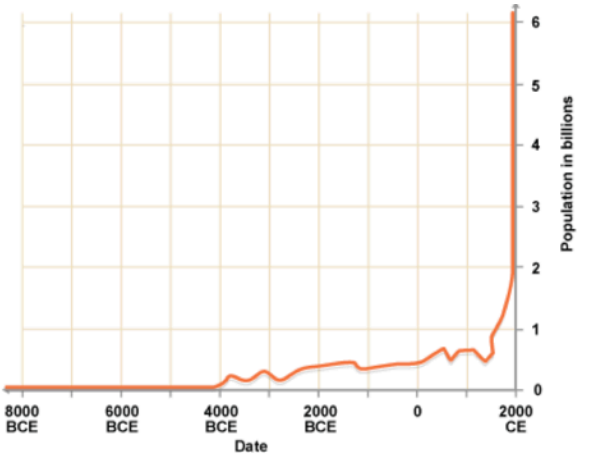
A liquid democracy operates across domains. Setting up an `Organization` within a network of delegatable *votes* is analogous to spinning up a server on the web. Domain squatting is the practice of occupying abandoned or unused web addresses in expectation of a profit. This has led to a billion dollar market having the most commonly used words (identifiers) as the best kind of digital real estate, e.g. Sex.com being the highest price paid domain.

Under a large scale, liquid democracy's game eventually grows around the `Tags` being used to describe delegations and issues. In a closed system, the most used `Tags` lead to a reduced universe of relevant voters. Reduced voter participation increases the prediction ability of a democracy, rendering moments open up for collective decision-making useless. Democracy thrives as long as participation is incentivized. To prevent this exploit, financial and political interests must be aligned. *Tag squatting* can be prevented if the taxonomy used to make liquid delegations and issue descriptions, operates in an open network: `Tags` refer to `Organizations` that are registered under a decentralized domain name system. After all, every `Organization` needs a domain name. [Blockstack.org] specializes on decentralized domain names currently managing over 70,000 Decentralized IDs (DIDs). These are obtained via a *Proof of Burn* process where users burn Bitcoin in exchange for Blockstack tokens that permit registering a new namespace.

A liquid democracy operating across a decentralized network has delegations done in representation of multiple `Organizations` that a `Member` belongs too. Besides helping describe an issue being voted within the network, `Members` have an incentive to belong in organizations: they provide **reputation**. For this reason, a *Proof of Identity* process has among those starting up `Organizations` a relevant role validating decentralized identities.

Words define political ideas. The social narrative built by the art of politics consists of deciding semantic intention. Power defines the theatrical impressions that imprint our memories each time we say *left*, *right*, *free*, *equal*. Language is a legacy code that enables large scale human collaboration and its virtues cannot be denied.

3. Execution.



A pressing fact that goes to the core of what is behind the political and economical challenges of the 21st century is the rise in population growth: United Nations estimates that by the year 2100 the world will surpass 10,000,000,000 sapiens. In other words: the planet's carrying capacity will be reached by the end of this century.

Clues on the risks of running out of resources can be found in the cultural legacy of islands. A far away land such as Easter Island was during most of its history a closed system lacking any contact with the rest of the world. Its population had no means for survival other than its own resources, constantly facing the dangers of famine, epidemics and civil war. Even though these menaces seem far under a globalized economy, the sudden rise in human population during the past century is the driving force behind increasing CO_2 levels in the atmosphere and the collapse of public infrastructure unable to deal with massive migrations. Refugees are escaping wars that seek to secure energy resources for a future that is coming at us fast as the pace of technological innovation accelerates. Though some have already put escape plans into place, including private efforts to reach Mars in the upcoming decades (resembling the biblical story of Noah's Ark), the urgent call to safeguard humanity as a whole must be both amplified and answered.

Distribution of opportunity and intelligent collaboration accross the globe cannot be achieved peacefully unless every voice gets heard, without exceptions. Global governance is the

next logical step in a world already connected over the Internet. Blockchains lead towards the possibility of liquid governance laying out the foundations for a democracy of peers. Permission from established Nation-States is not required: citizens anywhere in the world can embrace this change using sovereign networks.

3.1 Rights vs. Debt.

> *"What is justice?" the philosopher asked. "Pay your debts and don't lie" Kefalos (capital), a wealthy arms manufacturer, replied.*
>
> Plato, *Republic*. Philosopher (428-348 BC).

Although politics and economics are often perceived as different realms, history teaches that money means power and power means votes. In order to effectively promote democracy it is essential to adress both.

The association of debt, morality and wars remains at the root of the economic mental models of society. Coins were first created by the great empires to finance wars by enabling the purchase of provisions for soldiers in distant regions and rewarding them for victory. Soldiers could loot silver and gold from conquered cities and then exchange it afterwards as the emperors minted coins with the precious metals in order to create markets. Eventually empires would also ask for a share of those coins to be given back as a tax that was directed at the maintenance of the army. The moral narrative was that citizens were *indebted* to the emperor for their security, for being alive. Debt evolved to justify any form of coercion sustaining the power hierarchies in countries anywhere. Lack of liquidity is the most tangible and immediate barrier to freedom under which the majority of humanity finds themselves.

The *vote* token will be distributed as a **Right** opposing the historical association of **Debt** and morals, generating a new breeding ground for transactions that are not based on the possibility of coercion. It aims to bring equivalence to transacting entities, restoring balance and fairness as the new moral standard. Democracy Earth's core motivation is enabling freedom and personal sovereignty, a possibility that can only be reached if individuals are able to say 'no' and go for an alternative order uncoerced and free. This cannot be achieved with induced scarcity as it is often found on most crypto assets, but rather through a guaranteed access to *votes* to every member of society turning governance rights into a liquid instrument.

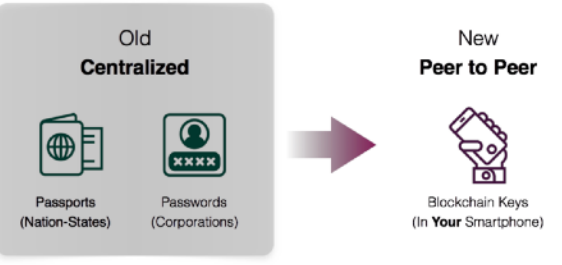
3.2 Initial Rights Offering.

Democracy Earth Foundation will constitute itself as a Sovereign organization and will issue an *Initial Rights Offering* of *vote* tokens designed to reach everyone on Earth. This process will offer two mechanisms:

- **Political Access**: A native way of getting *vote* tokens where anyone can *mine* his or her corresponding share of *votes* through a *Proof of Identity* process.
- **Financial Access**: For those who want to allocate resources to strengthen the development of a global democracy with the *vote* token.

3.2.1 Political Access.

Identity is foundational to personal sovereignty and the kernel of voting systems. Votes (on any system) are valid if and only if membership is verified within an organization, no democracy can run on corrupted identities. Today's standard identity systems are based on central authorities forcing users to share private information risking identity theft if they get hacked. Precedents include United Kingdom's Gov.UK and India's Aadhaar, both which have been plagued by reports of improper security practices including leaks that compromised the privacy of millions. For identities to be self-sovereign, they cannot be owned or controlled by governments, organizations or corporations that ultimately have as a priority the extraction of value from their users. Our approach with Sovereign is that it is organization-centric as a technology, but an organization can become decentralized if its identity verification process lacks the need of authority. Therefore, the key to sustain the value of the *vote* token as a means for a borderless democracy is to effectively validate all participating identities through a decentralized process that can create, update or revoke keys. This is how Democracy Earth Foundation will grant access to *votes* as a right.



Votes can be obtained at no financial cost by anyone able to demonstrate his or her own identity under a decentralized protocol referred as *Proof of Identity* (POI). *votes* obtained under this mechansim will trigger an allocation throughout time in the claimed public address of the identity. This process requires a self-hosted wallet that is connected to the content and data used for a *Proof of Identity*. The wallet contains a private key known only to its user that is related to a public key able to receive *votes*. If sufficient *votes* validate the evidence used for the *Proof of Identity*, the wallet will unfreeze a corresponding amount of *votes* following the rules of a *Universal Basic Income*dynamic that allocates tokens throughout time.

3.2.2 Financial Access.

Vote tokens can be obtained at a financial cost based on its current market value in exchange for Bitcoin and Ether. Founding members of Democracy Earth Foundation will put a share of their corresponding *votes* to fund efforts that strengthen the reach and impact of the *vote* democracy by committing the use of funds in the following way:

- **70% for Development**: For all contributors of Democracy Earth's open source git repositories and infrastructure costs. We will use Sovereign for the governance of all projects, deciding with *votes* how to reward each merged pull request and contribution.

- **15% for Community**: Customer service, marketing and outreach efforts, social media, communication, events and meetups.
- **12% for Operations**: Legal and accounting, travel expenses, office and co-working spaces.
- **3% for Identities**: A fixed pool will be used to subsidize the cost of hashing *Proof of Identity* transactions.

Those who accessed the *vote* token through a financial mechanism can use *votes* as an asset among their crypto holdings and for custom implementations of liquid democracies of any kind. Value of the *vote* token can be measured by the size of the network it can establish as an alternative to closed systems. A benchmark can be found on the Facebook network currently valuing 2 Billion users with a market capitalization of ~ $500 Billion averaging an estimate of $250 per user.

Unlike *Likes*, *votes* directly empower its holders with the right to participate on any financial benefit that can be connected to their use. With the creation of Sovereign as an interface for blockchain-based liquid democracies operating with *vote* tokens, Democracy Earth Foundation's aim is to deliver a *Linux moment* to Facebook: analogous to the rise of open source operating systems in the early 1990's, Linux became an alternative to the monopolizing force of Microsoft's Windows that dominated the market of personal computers back then. A free and open Internet must pursue the creation of a social network where no single entity can exercise algorithmical control of the shared ideas in exchange for the private information of its users. As we acknowledge the political influence social media already has in the world, the urgency to laying out this kind of open network is even more pressing.

3.3 Proof of Identity.

A self-sovereign identity must be voluntarily generated by the user claiming it. For this purpose the user must broadcast a proof of his or her identity that strictly satisfies a criteria that can be met by human judgment in order to avoid AIs interfering with the process. Hence, the proof shall be in a format that requires a large amount of cerebral bandwidth: video. The proof shall satisfy three key aspects:

- **Incorruptible**: The video file must be protected against any modifications once it has been used as a source for proof.
- **Truthful**: The contents expressed in the proof must be proven by other parties as valid or invalid.
- **Singular**: The proof shall validate a single identity and forbid having a same identity connected to other proofs.

Even though any digital governance system can benefit from the trust already present in existing networks that validate identities (i.e. Facebook or Nation-States), for the political purposes of authentic personal sovereignty is that a decentralized protocol for validating self-sovereigns must be put in place. The benefits of this public record in the networked commons can eventually be used by governments or private organizations in different ways (e.g. verifying age or nationality). Here we propose a new method for validating identites without the need of a *Big Brother*.

In order to limit Sybil Attacks and ensure that only alive users are participating in the network, the system will continuously and randomly require users to re-state their self-sovereign identity through the making of a new Proof of Identity video. In the same way that physical identities are constantly checked by comparing picture to person, users will need to constantly re-create their Proof of Identity and submit it to Attention Mining (see sections 3.3.4 and 3.3.5) in order to authenticate their legitimacy. The randomized challenge will be time-limited, and failure to fulfill requirements within the given time will incur in the account getting frozen.

3.3.1 Demo.

There is a precedent that helps to illustrate this. According to NYU professor David Yermack, newborn Roma Siri became the first baby to have a blockchain valid birth certificate on November 7, 2015. The process, even though symbolic at the time, consisted of a video showing baby Roma that described her vital signs and included witnesses of her birth. Once the video was filmed, a cryptographic hash of the digital file was generated and encoded into a Bitcoin transaction. This means that regardless where the video is stored, the permanent record of its hash on the Bitcoin blockchain can verify that the file's data was not corrupted and that it existed at the time the proof was generated. With this incorruptible evidence, Roma became a blockchain-certified citizen.

This demo serves as an example for the steps that need to be followed for a decentralized *Proof of Identity*:

1. **Film proof** using any smartphone camera.
2. **Hash proof** on a blockchain to guarantee incorruptibility of evidence.
3. **Validate proof** through a voting process among peers (*Attention Mining*).

3.3.2 Proof Video.

A proof can be done with any recording application as long as it satisfies the requirements of the protocol. An extension no longer than 2 minutes is recommended for the video. In it the user must follow a series of scripted steps in order to help validators judge:

1. **Face**: Film frontal expression (as when taking a *selfie*) and each side of the head without wearing eyeglasses, hats, makeup or masks of any kind.
2. **Names**: Say out loud the following indicators:
   i. Full given name (language-based identity).
   ii. Full surname (blood-based identity, additionally it can state information regarding mother and father).
   iii. Nationality (territorial-based identity, it can include place of residence or tax paying jurisdiction).
   iv. Alternatively the user can use a nickname if avoiding connection to other identities is desired.
3. **Biometrics**: Say out loud or demonstrate in a reliable way any of these indicators.
   i. Birthday (day, month and year). This is mandatory since allocation of *votes* will be based on age.
   ii. Height (inches or centimeters).
   iii. Weight (pounds or kilograms).
   iv. Gender (male, female, etc).
4. **Public Key**: An address where *votes* will be sent if identity is validated. This will be the Decentralized Identifier (DID) pointing to this user. If this identity eventually is voted as corrupted or the user (or any listed

witness) revoke it, then the allocated *votes* will get invalidated for future use.

2. **Witnesses** (Optional but recommended):

   i. List of other previously validated identities that shall act as witnesses for this identity. The listed DIDs can get granted the rights to revoke, update or cancel this proof (e.g. in case loss of private keys or biological death).

   ii. Other identities physically on location might appear in the video stating their full names and public keys, endorsing this identity.

   iii. Certifications. Even though this would be falling back to central authority, legacy reputation from state-issued documents can help make a video proof easier to trust. This might include a birth certificate, driver's license or a national ID as long as it doesn't hold any sensitive information (e.g. social security numbers in the US). In the publication *Digital Identity Issue Analysis* (Consult Hyperion 2016) it is noted that centralized organizations currently serving as identity providers will evolve to become "identity proofers" - someone still needs to carry out the checks that an individual is who they say they are as they bridge the digital and physical worlds.

3. **Declaration**: To guarantee that the person generating his or her identity proof is not being coerced by an unseen attacker, it is mandatory to make a declaration of self-sovereignty (any language is admitted) that also includes an oath regarding the stated facts:I, (Personal Name), declare that I'm making this video as a self-sovereign act. I will be the sole user of all the *votes* given to me as a birth right and act according to my free will and certify that all the information expressed in this video is true.

4. **Timestamp**: Current block height of the blockchain used for hashing at the time this video is being shot. A manual timestamp can simply film the screen of a blockchain explorer application displaying the last block number and the hash corresponding to it. Since this might be complex for most users, apps designed to generate this proof can automatically add this content to the video. This information once the proof is hashed with a blockchain transaction will certify the video was not modified in any possible way by a third party after it was broadcasted to the network.

Even though this process can be more complex than the average sign-up form found on most applications, it is important to state that it is also a political act declaring independency from central authority of any kind. This video is the personal manifesto anyone can make to break free from coercion and a step taken towards a borderless democracy.

3.3.3 Hashing.

Once the digital file with the self-sovereign proof has been generated, a cryptographic hash function applied to it is calculated. Following the steps of the implementation made by Manuel Araoz and Esteban Ordano with ProofofExistence.com, a standard SHA-256 digest is recommended. Once the hash has been generated, it can be encoded in a Bitcoin transaction using an OP_RETURN script that also includes a marker that helps track identity-related proofs. We suggest using 'IDPROOF' (0x494450524f4f46) for this particular use case.

Considering that an average bitcoin transaction consists of 226 bytes with a mining fee as of August 2017 at 27,120 satoshis, the cost for hashing a proof directly on the blockchain is at ~1 US dollar per proof. This can be relatively expensive for a majority of people, hence we recommend scaling this process by also enabling a Chainpointimplementation able to store up to 10,000 proofs per transaction by putting the hashed data on a Merkle Tree and encoding the Merkle root in the OP_RETURN script instead. This will also significantly reduce the memory requirements of the Bitcoin blockchain, being a public resource that must not be abused. Alternatively, virtualchains that run on top of the Bitcoin blockchain that have a focus on identity and namespaces such as Blockstack can be used to satisfy this use case.

Any proof that goes through this process in a digital context is guaranteed to not be corrupted in any way. The digital files being used as proof can be stored anywhere, copied without restrictions and even kept in secret without sharing it with anyone. As long as there is a transaction in the blockchain that can validate the encoded hash with the structure of the digital file, then the evidence is valid. The Bitcoin blockchain offers the strongest resistance to corruption since it has the largest amount of hashing power in the world. With this mechanism in place, the Bitcoin blockchain will function as a decentralized index of self-sovereign identities. Leveraging this capacity will only make the bureaucracy of a borderless democracy stronger than any other government on Earth under any objective metric.

3.3.4 Attention Mining.

In the blockchain nobody knows you are an AI.

Satoshi Nakamoto.

In computer-space identities are nothing but pointers: algorithms lack any awareness about the patterns they are trained to recognize. Identities strictly belong to the human realm (i.e. only a person can recognize another person). So rather than harnessing *distributed computing power* to verify transactions as it happens with most cryptocurrencies *votes* use *distributed attention power* to verify self-generated identity proofs.

A well known precedent of attention mining are CAPTCHA tests often found in the login of high-traffic websites. CAPTCHA is an acronym for *Completely Automated Public Turing test to tell Computers and Humans Apart*. These consist of simple vision exercises that can be completed by a human more easily than by a computer. A field pioneered by researcher Louis Von Ahn, he used this technique to help build datasets able to train machine learning algorithms to read physically printed words. As a Google engineer Von Ahn created a simple test distributed across all login pages that displayed two words obtained from scanned pictures. A user would write both words in a text input field to prove he is human and not a machine. The system already knew the meaning of the first word (hence validating the user is human) but it got trained with the second input as it uses this information to further optimize its character recognition algorithms. This simple exercise has been extended to train all kinds of pattern recognition systems and it contributed to the security of websites preventing bots (and botnets) from intruding.

Attention can also validate human identities on a decentralized network, analogous to Bitcoin's Proof of Work algorithm (POW) used by mining nodes to timestamp peer to peer transactions. In Bitcoin, each miner generates its own

blockchain-compatible proof hash for a new block of transactions and broadcasts it to the network. If 51% of the nodes in the network accept the verified block, it gets chained to the blockchain and the miner starts working on the next transaction block using the accepted block as the previous hash. This technique permits monetary transactions without central banks. A democracy without central governments works the same way but instead of verifying encrypted blocks, human attention serves the purpose to vote on self-generated identities in order to grant them *votes* which can eventually be used for new verifications.

3.3.5 Little Brothers.

Who watches the watchmen?

Watchmen, graphic novel (1987).

The interest to validate a *Proof of Identity* is among `Organization` that approve applicant identities as `Members`. Those who within an `Organization` have the rights to approve new memberships replace the historical function of a *Big Brother*, the Orwellian metaphor often used to refer to a monopolizing entity that enforces its legitimacy on a system, as it is the case with Facebook or Nation-States. By harnessing distributed attention instead of an all-observing central power, validators are in effect an army of *little brothers*. They contribute with their attention to verify proofs by using *votes* signaling `true` or `false` states on:

- **Biometrics**: Evaluating any objective data used in proof (e.g. age matches facial look, properly filming face, etc).
- **Singularity**: Avoiding duplicate identities from participating within an `Organization`.
- **Proof of Life**: Asserting that an identity is alive or dead.

If approved: *votes* cannot be inherited so if an identity is marked as dead by the verifiers, those *votes* will be nullified.

To certify an identity is valid, verifiers cast a *vote* including a `Ballot` with a `true` checked `Option` on it. Otherwise they must cast a *vote* in rejection with a `false` checked `Option`.

All POI related decisions are `Strategical`: without a closing date where allocated *votes* impact in real time. At any time a verifier can switch the *vote* value if it has found evidence that modifies previous judgement. Also, *votes* validating an identity can be removed if the identity already has input from sufficient validators which makes allocation of additional *votes* redundant.

To prevent any kind of centralization regarding the identity verification process and police against dishonest participants, the *votes* used for verification operate the same way as liquid delegations: *votes* get exponentially more expensive to allocate (as in quadratic voting) and, if the identity is approved, a delegation is established with the verifier's *votes*. This helps bootstrap a liquid democracy while also enabling rapid coordinated action against dishonest verifiers.

Little brothers can outperform centralized identity providers in terms of accuracy as they are constantly incentivized to maintain legitimacy within the network. The interest to contribute in the proper validation of identities is directly tied to the value of the *vote* token itself. The legitimacy of any democracy is based on the maintenance of a proper voter registry. By being backed with a decentralized identity index using an incorruptible blockchain that gets maintained with distributed attention, the *vote* token becomes a trusted device for a digital democracy to emerge. Distributed attention power not only brings consciousness to a system once blind to Artificial Intelligences, but also allows participants to own their identities without being coerced to share it with any centralized validator that could monetize from it without consent.

3.4 Universal Basic Income.

The ability to develop a reliable self-sovereign identity validation process, not only guarantees the legitimate value for *votes* to express social choice but it also opens a path able to establish a *Universal Basic Income* (UBI) mechanism that can reach everyone on Earth. Therefore in order to bring the political and economical logic full circle, once an identity gets approved by its peers to participate in the network, the corresponding share of *votes* for each identity on the system is allocated throughout time.

Time is a valuable and limited asset, therefore tradable. Tokenizing time and utilizing that as the fuel for *votes*, liquidates a possession that every member of a global democracy possesses equally while ensuring their rights over decision making processes. Liquidity is a requirement for any democracy that aims to avoid the coercion of its members. As in free markets, voices must be able to be heard in order to count and by granting *votes* via UBI we are tapping on delivering a human right that can effectively empower individuals facing the coming challenges of automation and Artificial Intelligence. This is a natural evolutionary leap on human organization that avoids the *tragedy of the commons* and aims to deliver a new mental model for governance that goes beyond debt and Nation-states. An achievement only thinkable until the emergence of the Internet and blockchain-based networks in modern civilization.

3.4.1 Time.

The rate at which 1 *vote* will be dripped to a verified identity will be synchronized with the Bitcoin blockchain. This means that 1 *vote* equals 1 block (or 10 minutes worth of transactions in the blockchain). Consensus on an ideal Basic Income averages around 10% of earnings. Considering global 'earnable' time is 8 hours per day, 5 days per week, 50 weeks per year - or 2,000 hours per year. Therefore, an Annual Basic Income should be the equivalent of 200 hours or 1,200 blocks per year. This means that any organization deciding to adopt this currency has a 10% discount on the compensation it pays for its collaborators.

Adoption of the token is also incentivized as a political position: the era of mass market communications where companies avoided taking political stances is coming to an end. Increasingly consumption is becoming a political act, with products being articulators of one's identity and worldview. Consumers are becoming community members, and companies are being requested to be transparent about it's internal practices on the aquarium of the internet and social media. As the concept of currencies undergoes a massive disruption caused by distributed ledger technology, we offer a coin that is an articulator of human rights and democracy. What it means is that by utilizing our token organizations will be able to embody and promote those values. So on the great endeavor of building a true democracy, anyone trading on this network, or purchasing products from it, will be a contributor. An act of consumption will become as powerful as a vote.