Universal Union: Decentralizing Democracy

Joshua

joshua.404c@proton.me

https://github.com/A-Universal-Union

Abstract. True democracy lies not in elections or officials but in the shared power of individuals to influence the world they inhabit. The divide between those who shape the future and those who live with its consequences has never felt so vast, demanding a rethinking of how we define democracy. Addressing this divide requires rethinking not just how democracy is practiced, but how individuals can reclaim their rightful influence within it.

This paper outlines a framework to address this divide—one that equips individuals with tools to engage meaningfully in discourse, voting, and organizing within decentralized social structures. Key features include identity protections, robust analysis of election results, and natural language tools that foster understanding and encourage constructive participation. While this document outlines the principles and goals of the platform, it also invites collaboration to refine ideas and develop the technical details necessary to bring this vision to life.

Introduction

Democracy, as a concept and system, has always been defined by its ability to distribute power across society. Born [and evolved] as a response to centralized authority. Its promise was simple: every individual would have a voice, a role, and a stake in the collective future. Yet, in practice, modern democracies increasingly fail to deliver on this promise. Power remains concentrated—not in monarchies, but in the intertwined hands of wealth, influence, and political gatekeeping. The systems intended to amplify individual voices often dilute them instead, leaving most people with little meaningful control over the decisions that shape their lives.

At the same time, society has evolved. Technology now offers tools unimaginable to those who first dreamed of representative governance. The ability to connect, deliberate, and organize is greater than ever, yet these tools remain underutilized in the context of democracy. Instead of empowering individuals, they are often co-opted to reinforce the existing structures of power. This raises a critical question: How can we redesign democracy to fulfill its original purpose in a way that reflects the technological and social realities of the 21st century?

This paper outlines a platform—a framework for modern democracy—that prioritizes participation, trust, and collective agency. It aims to give individuals the ability to engage in discourse, build social structures, analyze outcomes, and vote in ways that are secure, meaningful, and impactful. By leveraging identity protections, natural language tools, and decentralized systems, this platform seeks to return power to where it belongs: with the people.

The intent of any such system should not be to replace physical real world social structures of governance, but to be utilized to engage the public on every issue. Thereby achieving the true purpose of democracy.

Overview

An overview of the purpose of this paper, systems, and features necessary. In this paper we layout a design, a framework, a platform, and an app. This will be an organic document of this new evolution of democracy, to grow as this does. It is our belief that this design as is will provide a very solid foundation to both dig into and build from. As such, the intent is that this design will ultimately be useful, and provide some measure of trust in the context of a decentralized democratic process. This section delves into technical aspects but primarily the intent is on utility.

Collaboration

Collaboration from experts in many areas is out right requested and very welcome. The ability to review and solve problems in domains such as Security & Cryptography, Mathematics, Statistics, Blockchain, Machine Learning, Natural Language Processing, and so on is crucial for developing this as a FOSS platform and app.

Fundamentals

While the reader is not expected to be an expert in any of the fields touched on in this text, it would be very beneficial to have working knowledge of at least graph theory. More in depth areas could include but are not limited to machine learning & statistics, large language models & natural language processing, blockchain, zero knowledge proofs, and cryptography.

Trust

The first challenge we face is defining trust within a decentralized digital context. True trust is an implicit, or explicit, social contract between two or more people whereby the people agree to behave in ways that create stability and provide, in ideal situations, mutual benefit. In democratic processes we need trust to be codified, and in a decentralized context is no different.

> Democracy depends on trust, the trust we have in the process and in ourselves to make the best decisions we're capable of with as little or as much information as we have. Decentralization challenges and undermines our trust in the outcome and each other by giving equal power to anyone and everyone, including those who would do us harm or strip us of our freedom, control, and voices. The success of a decentralized democracy therefore depends on systems that measure trust in order to uphold the integrity of democratic processes.

We propose a rather simple concept for creating trust in a decentralized digital context: social graphs. Specifically seven social connections to serve as the basis of a pseudonyms' trustability. The number seven is arbitrary, but what is important is a hard limit as this will affect trust analysis; having hundreds of connections could easily offset any reduction in trust and undermine accountability.

Each of us knows people, and for each of those people we have varying levels of trust. By having users create social connections to people they trust within the platform we can implicitly define trust. We can then analyze these social graphs (i.e. networks of people) to determine how

much trust another individual or group should have towards a specific identity or subgraph of identities.

By viewing trust in this way we can measure it in many ways. We can look at **social distance** to identify networks of identities that may be the tool of state actors attempting to undermine other states. We can view trust as something to be **staked** for and from our closest social connections. We can consider **historical behaviour** and whether these behaviours align with community values. We can begin to see trust as something to be learned, something subjective where perspective helps to determine trust. It can be viewed as something to be lost within a particular community, and as information to be shared with other communities.

> Several factors play a role in determining trust, but it can often be up to interpretation. A person located in one part of the social graph may view a segment of the graph as untrustworthy for any number of reasons, whereas a person in that segment would naturally see their closest connections as trustable. An identity being very frequently flagged in discussions as inflammatory or distracting may be viewed as untrustworthy due to their actions indicating attempts to undermine and polarize discussion. Highly concentrated connections mostly voting the same way again and again would likely indicate manipulation or fraudulent activity; imagine the citizens of Oceania all attempting to sway an election in Eurasia, according to the whims of Big Brother. As such subgraphs can be flagged as untrustworthy and excluded from the results.

Of course interpersonal connections are not all that matter. We exist within social hierarchies: communities, cities, and so on. These structures play an important role in both the real world, and within the framework (which is addressed again later). They are important for establishing trust at scale and regaining trust and inclusion when things go awry.

Identity

The second challenge is defining what an identity looks like within our system. In the physical world, identity is an inherent trait—we possess it simply by existing. In any system, however, identity must be actively established. To create a fair and open system that supports freedom, it is essential that anyone who can prove their existence has the ability to claim a digital identity.

What we propose is composed of two layers. The first layer is the proof of being human and allows the creation of an identity wallet. The second layer are the pseudonyms that act as identities on the platform, each with customizable authentication protocols.

> Down another path and for the sake of freedom, some identities can be created secretly to fully detach them from a witness or any data that could be perceived as risking their real identity and physical safety. The challenge here will be protecting against bad actors attempting to flood the system with identities. Which they may then of course use to flood political discussion with comments aimed at swaying public opinion or otherwise interfering with good faith discussions.

To create a wallet there are a few hard requirements. The first requirement is of a human "witness" that gets baked into the social graph as the first social connection. This witness must possess a pseudonym and identity wallet. The witness observes the human creating an account as they enroll their biometric data. The second requirement is multi-modal biometric data with liveness checking (i.e. the ability to verify that the biometric input—such as a fingerprint, facial

scan, or voice recognition—is being provided by a live, present individual rather than a static image, recording, or other fraudulent source). After forming an identity wallet (account) the person is free to create pseudonyms. Each pseudonym capable adding social connections through double physical verification (i.e. on each device); helping to prevent against false connections and state level manipulation and interference in other states' affairs. These connections act as stake holders for a pseudonym.

> This means closed social graphs bear a heavy price for fostering bad actors. This is granular down to your isolated hermit and up to world powers with people or ideas to kill. Really any sub set of identities can viably form a community. How that geographic majority decides to govern or organize their region is up to them and those nearest to dissent against, take part in, or guide.

The authentication for the wallet is a relatively straight forward concept involving biometrics, but additional pseudonyms can have their own choices of authentication (e.g. 26+ character passwords, iris scan, voiceprint, etc.). A user may choose to utilize as few or as many authentication steps as they desire, and in whatever order they wish.

This customization would be critical to protecting **secret pseudonyms** and the identities of the people operating them. People operating on a transparent thing like a blockchain, obviously deserve multiple layers of protection to ensure they remain free to conduct themselves as they desire on the blockchain. Accounts formed in this way still represent a human, but they can be seen as having 0 trust and incapable of building trust since building social connections would undermine its function as providing the ultimate anonymity.

> For example a military leader serving in a dictatorship who wishes to engage in discussions of dissent would want to further obscure their identity, and would never want to associate a statement of dissent with their more public interactions on the blockchain ones which may very well be associated to their real world identity.

Social Structures

Social structures are the foundation of human interaction, and democratic systems must anchor themselves within this foundation in order to be successful. These structures—groups such as communities, organizations, and nations—are not just extensions of individual connections but vital mechanisms for collective action and decision-making. For any democratic tool to be practical, it must facilitate the creation, maintenance, and interaction of these groups. Without this, any framework would risk being disconnected from the very systems it seeks to support and improve.

This framework posits that **forming and joining organizations** to mirror real world social structures is necessary for success. Necessary not only for providing useful features and interactions, but this is absolutely critical simply for the adoption of the framework in the first place. It can nearly be guaranteed that any existing government would want the ability to clearly define requirements for members of their organization.

> It is easy to imagine some forms this could take, for example joining the organization under two witnesses who are staked in your joining of the organization along with specific details such as your name, date of birth, and government identification numbers. **[note: government adoption/integration likely looks like... pseudonyms being staked in**

a centralizing fashion under strict observable guidelines inside of organizations]

Security and Recovery

The wallet, of course, needs multi-modal biometrics both to create and access it. With liveness checks—designed to ensure that a live, present individual, rather than a static image, recording, or other fraudulent source, is providing the biometrics—it is hoped that this will prevent most, if not all, fraudulent access from sophisticated actors. However, where there is a will, there is often a way. As such, we believe measures should be designed to expect breaches if weakly protected, while ensuring they are only temporary when the pseudonym is connected to real humans that you can otherwise communicate with and trust. These real-world connections, requiring a majority (e.g., four out of seven), provide the mechanism of recovery needed to change the authentication method for a pseudonym.

Any pseudonym, unless secret (and meaning it is potentially untrusted and unrecoverable), can be created requiring none to many methods of authentication with defined steps for authentication. So if the wallet is breached, the pseudonyms are not necessarily breached as well. These layers of security chosen on a pseudonym may even be used to inform trust metrics potentially.

The goal here is to provide as much security as an individual wants or requires to successfully engage in the democratic process. In order to effectively achieve this goal we need to rely on social authentication, device binding, and customizable authentication protocols.

> It is possible, especially as technologies evolve, for bad actors to steal a person's biometric data and immitate them in some manner that fools the system and grants them access to the wallet. Further, it is feasible that over a long enough timespan that a human may be born who is exactly identical to a person alive today – however unlikely. It is for these reasons that pseudonyms also require authentication. This means an individual is ultimately responsible for a breach of their pseudonym.

Changing the authentication protocol on a pseudonym requires two things 1) having the current authentication credentials necessary to access the pseudonym and 2) social authentication from a set of seven pseudonyms (seven is an arbitrary odd number, the important thing is there is a hard limit as this affects trust analysis). This means that upon breach, a pseudonym will have two users, until such a time that one of them is able to use the social connections to secure it from the other.

Device binding is the last layer of protection we'll describe. As it represents **a number of complex problems** to which a solution is not yet devised. Suppose you create a wallet tied to your biometric data, this wallet is bound to the device you create it on until transferred. Next you lose this device. You now have lost access to the wallet, permanently unless a recovery method can be designed for the wallet. Suppose now that in 20,000 years an entirely identical human to you is born, they also do not have access to that device and thus the wallet cannot be re-used and they are now excluded from the blockchain. Device binding via Trusted Platform Modules (TPMs) is a useful layer of protection, and so it is our hope a solution is found.

Using The Platform & App

Now that we've got all these humans vouching for one another, they can vote amongst themselves and each observe statistics aggregating to see what they say about the results and different segments shown in the trust analysis. They can of course also engage in discussion about votes, people, anything – discussions about discussing. This open space to communicate to any other living person is critical for harmonizing opinions, but will also enable polarization to happen much quicker.

Discussing

To counter act polarization we should seek to make the polarization more transparent and more easily classified. To do this we propose a radical change to the typical classification users engage with on social medias. Instead of like and dislike, we need to expand from 2 to many more classifications that offer strong insights for machine learning algorithms to cluster comments by.

Classifications

- I like / dislike this
- I agree / disagree with this
- I don't fully agree with this
- This challenged / inspired my opinion

Clustering

With our user input (classifications, a sort of rating system for comments), we can look to machine learning algorithms and natural language processing to create bins in which comments will be catergorized for users according to their historical behaviour and trends regarding how they previously categorized similar comments.

Any specific discourse the user explores will be filtered through this lens by way of these bins within which the user finds and explores comments and their threads of discussion. This will help define the borders of the echo chambers many of us find ourselves shouting inside. A person's active categorization of content helps identify the shape of their perspective and perception and improves machine learning algorithms intended to provide predictive categorizations.

Exploration

Of course we must consider how people will find particular discussions to engage in. In the search for interesting topics of discussion Natural Language Processing (NLP) and Large Language Models (LLMs) will be routinely utilized to narrow the search space for the user. Grouping discussions based on topics, keywords, ideology, polarization, and anything else that may seem useful during a layer 3 app's creation.

Voting

Voting operates in two distinct ways: **proof-required** voting, which guarantees voter eligibility; and **proof-free** voting, which facilitates broad participation without strict identity checks. Both of which can operate inside or outside of organizations.

Proof-required voting aims to ensure that only eligible pseudonyms participate to support the integrity of elections. This type of voting would presumably be most relevant for high-stakes decisions and formal elections, where trust in the process is paramount. Possible means to achieve this:

- **Smart Contracts**: Handle the verification of Zero-Knowledge Proofs (ZKPs) and manage token systems to mark participation.
- **Zero-Knowledge Proofs (ZKPs)**: Allow users to prove their eligibility while keeping personal data private.
- **Biometric Verification**: Ensures each vote comes from a unique identity tied to a biometric signature.
- **Geospatial Verification**: Confirms eligibility based on geographic restrictions where relevant.

Proof-free voting, in contrast, allows any pseudonym to be involved. Possibly useful any time there is no need for detailed personal verification. This can still be useful, because of key features such as:

- **Data Analysis**: Trends, anomalies, and behavior patterns are analyzed to detect manipulation.
- **Visualization Tools**: Relationships between pseudonyms are displayed, providing insights into voting patterns.
- **Filtering Options**: Subgraphs or groups can be excluded to simulate the impact of trust-based participation.
- **Trust Aggregation**: Users' trust scores influence how their votes are perceived or weighted in analyses.

Polling

Polling expands democratic engagement by allowing users to collect opinions on topics of interest, either formally or informally. Pollers can decide whether to require proof of identity, allowing them to adjust inclusivity versus trust concerns. In either scenario access to tools to filter responses based on trust metrics or subgraphs within the social network, providing nuanced insights.

Polls that **require proof** of identity ensure verified participation and accurate geographic or demographic representation. Mechanisms mirror those of proof-required voting, including biometric checks and ZKPs.

Polls requiring **no proof** of identity ensure open participation and rely on systems of analytics to offset the risks of bad faith participation.

Organizations & Hierarchies

One integral feature, especially for adoption of this technology, is the ability to define organizations and internal hierarchies. Groups and communities form the backbone of democratic engagement. Users need to establish such collectives around shared goals or interests.

> Membership would be achieved in a customizable myriad of ways. Perhaps before the illuminati send you an invite token, you have to be witnessed sacrificing a goat. The point is, you must be allowed inside.. like a vampire. From that point your pseudonym just needs to be able to pass the vibe check. Or perhaps a community creates an organization that requires a trust score of 0.9 or greater and within the perimeter of the physical community with a public QR code for an invite.

Collectives are orthogonal to each other, and that fact means you can represent any hierarchy you want using them. The ways individual pseudonyms engage with collectives provide the example by which collectives should be able to engage with other collectives. A particularly cooperative collective could conduct internal polls and later vote as a bloc in larger/external elections or polls. Discussions within collectives can thereby help shape broader public discourse by refining and testing ideas in smaller, trusted circles.

Representation

Collectives provide an easy vehicle through which to offer people representation, and the freedom to choose their level of engagement in their governments' functions. Just as easily a more general form of representation could be utilized in addition or instead of collectives. A more general form such as choosing a limited number of representatives, or proxies. The function is no different, this representative would act as a proxy for you in some sense.

With representation as a feature user engagement is not required but encouraged. Users can choose, and later change, a limited number of representatives to push their beliefs and ideologies in public spheres. Not everyone is a voter, as such many people may in fact prefer to have representation through a proxy. For people who do not wish to regularly engage with the democratic process, but wish their opinions and interests be represented nonetheless, representation makes an attractive option.

[A representative is effectively just a person or collective identity which represents the values, opinions, beliefs, and general ideology of another person or group.]

Choosing Engagement

Alongside representation a secondary need can be seen for granular engagement. Not everyone will want to see every vote ever, and so these people need a way to select their level of engagement as a way of filtering the noise.

Technical Details?

Implementation details such as these are hardly a matter of fact.

Research

The development of this paper and platform will necessitate research in several key areas:

- **Blockchain**
- **Privacy and Security**
- **Zero-Knowledge Proofs (ZKPs)**
- **Statistical Analysis**
- **Graph Theory & Social Graphs**
- **Natural Language Processing (NLP)**
- **Machine Learning**

How the Blockchain Layers might address Use Cases

Discussions

Layer 1: Logs discussions and links them to pseudonyms.

Layer 2: Uses trust and social graph data to filter and propagate messages effectively.

Layer 3: Provides user interfaces and discussion categorization tools.

Voting

Layer 1: Records votes immutably and runs smart contracts to enforce election rules.

Layer 2: Enables ZKP-based proof of eligibility and real-time trust analysis.

Layer 3: Provides user-friendly voting interfaces and results visualizations.

Polling

Layer 1: Logs polling data and ensures anonymity where needed.

Layer 2: Offers subgraph filtering and anomaly detection for proof-free polling.

Layer 3: Allows poll creation, participation, and analysis through the app.

Creating Organizations

Layer 1: Stores group membership and governance rules securely.

Layer 2: Facilitates trust-weighted group interactions and voting.

Layer 3: Provides tools for managing organizations, including hierarchical structures.

Representation

Layer 1: Logs proxy relationships immutably.

Layer 2: Validates proxies and ensures proper trust delegation.

Layer 3: Allows users to set, update, and manage their representation preferences.

Granular Engagement

Layer 1: Tracks user participation and data points for analysis.

Layer 2: Processes social distance metrics to define participation levels.

Layer 3: Offers intuitive controls for adjusting engagement.

Understanding the System as a Whole

Identity System

The foundation of the platform lies in creating and managing pseudonymous identities. The identity system must:

- Allow creation of wallets and pseudonyms with varying levels of anonymity.
- Support identity recovery mechanisms via social authentication.
- Enable pseudonyms to interact within the blockchain while maintaining privacy.

Blockchain Platform

The blockchain platform serves as the infrastructure for all democratic functions. It must:

- Securely store and manage voting, polling, and discussion data.
- Support trust-based analysis for proof-free systems.
- Enable smart contracts to enforce eligibility criteria and execute decisions.
- Scale to support granular engagement across billions of users.

End-Goal App

The app built on this blockchain will:

- Facilitate open discussions, voting, polling, and collective organization.
- Integrate natural language processing (NLP) and machine learning for discourse categorization and prediction.
- Empower users to filter content (i.e. discourse and voting) based on trust, social distance, and interest.
- Support identification and flagging of fraudulent or bad faith activity.