ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed
Computing

Scaleable Proof-of-Personhood: Exploring the Potential of PoP Combinations

Bachelor's Thesis

Jan Boog

jaboog@ethz.ch

Distributed Computing Group
Computer Engineering and Networks Laboratory
ETH Zürich

Supervisors:
Alain Benzikofer, Malik El Bay, Yann Vonlanthen
Prof. Dr. Roger Wattenhofer

September 7, 2025

Acknowledgements

I would like to thank my dedicated supervisors for their support. Yann Vonlanthen, Malik El Bay, and Alain Brenzikofer provided valuable inputs and expertise. During the thesis they advised me using extensive knowledge and experience with me, and our discussions led to many new ideas and conclusions.

I would also like to thank Prof. Dr. Roger Wattenhofer for giving me the opportunity of conducting my bachelor thesis in the Distributed Computing Group.

Abstract

As more aspects of our personal, social, and political lives migrate online, the option of establishing digital uniqueness becomes more important. The rise of AI agents and automated bots has rendered traditional defenses such as CAPTCHAs increasingly ineffective[1]. Proof-of-Personhood offers a promising alternative by ensuring that digital identities represent real, unique individuals. This capability not only curbs mass automated registrations and impersonation, but also creates opportunities for secure and fair consensus.

This thesis explores the potential of combining different Proofs-of-Personhood by focusing on its application to geographic voting. The goal is to create a scalable and secure protocol to be used for voting, using a combination of approaches to leverage their different advantages. This begins with a systematic overview of existing Proof-of-Personhood methods and with a description and evaluation of specific protocols. From this foundation, insights are derived into combinations in general, the different methods of combining approaches, and actual combinations of approaches in practice.

Building on these insights, the thesis presents a protocol that combines the strengths of electronic Passports and Pseudonym Parties. The protocol is tailored for use in geographic voting, and several modifications are proposed to adapt it to specific contexts.

Contents

Chapter 1

Introduction

Proof-of-Personhood (PoP) is a decentralized protocol that ensures each participant in a decentralized system is a unique real human, preventing Sybil attacks, an attack where adversaries try to create multiple pseudonymous identities, in order to gain a disproportionate amount of influence, like obtaining multiple votes. Unlike Proof-of-Work or Proof-of-Stake, PoP allocates influence based purely on human uniqueness, not on computational or financial resources [2].
Proof-of-Personhood protocols use a variety of verification methods. Popular approaches rely on social vouching, physical attendance, biometric verification, or leverage existing tokens, such as government-issued documents.
The importance of PoP has grown as the presence of AI agents and bots online increases. Traditional defenses like CAPTCHAs are increasingly ineffective [1]. PoP offers an alternative by verifying real users while curbing mass automated registrations or impersonation [3].
Given that more aspects of our personal, social, and political lives are moving online, the ability to establish digital uniqueness offers great opportunities. By enabling secure digital voting, PoP can enable online democracy while reducing reliance on centralized institutions [2].

1.1 Proof-of-Personhood Properties

When designing a Proof-of-Personhood protocol, there are a number of properties that can be desirable for such a protocol depending on the applications [4, 5, 2]:

Sybil resistance: This is the foundational property of any PoP protocol. The requirement can be interpreted in different ways, ranging from a relaxed constraint, such as ensuring that no individual can maintain more than 10 accounts (an order of magnitude) to the strict standard of enforcing the principle of ’one person, one account’ without exception.

Decentralization: No authority should have the power to attest to Personhood or strongly affect it. This includes, but is not limited to, governments issuing digital passports or the use of trusted hardware.

Privacy: Users should not need to give up their privacy to obtain Personhood. Additionally, privacy should be preserved while presenting that Personhood and usage in different contexts should be unlikable

Inclusivity: The mechanism should not require assets and should be generally available to anyone, regardless of nationality, race, social status, education, etc. Potentially, multiple methods could be used to ensure accessibility for all.

Scalability: The protocol should be able to easily support millions of users and be extensible to billions, both from a technical and practical perspective.

Accountability: There should be clear and enforceable consequences for misconduct. Fraud, duplicate identities, or abuse should be addressable through measures such as revocation, penalties, or re-verification.
An optional, but potentially beneficial, extension of this is that it should be very hard or impossible to unlinkably change an alias. For instance, it should not be possible to just abandon an account and create a new one.

Verifiability: All Personhood attestations should be verifiable by an outsider.

1.2 Proof-of-Personhood Applications

PoP provides a foundation for linking digital actions to unique human beings, thereby preventing the creation of multiple identities by a single actor. This capability has a broad range of applications, from improving online accountability to ensuring fairness in governance and economic distribution.

1.2.1 Accountability and Fake-Account Resistance

By ensuring that each credential corresponds to a single individual, PoP mitigates Sybil attacks that artificially inflate user numbers, manipulate discussions, or exploit reward systems. This strengthens platform moderation and ensures that penalties or restrictions apply to real people rather than disposable pseudonyms. When implemented with privacy-preserving methods, such as selective disclosure, PoP can maintain anonymity while still enabling trust. In practice, Sybil-resistant identity registries and reputation passports are already used to gate access to online communities, funding programs, and membership-based services, effectively reducing bot participation and fraudulent multi-signups [4].

1.2.2 Voting and Governance

In governance systems, PoP enables 'one person, one vote' models as well as identity-weighted or quadratic voting schemes. These mechanisms offer a possibility of increasing decentralization in protocol upgrade decisions, decentralized autonomous organizations (DAOs), and other community-driven processes, where the integrity of each vote must be safeguarded against duplication [4]. PoP credentials can support deliberative polls, random juries, and other democratic decision-making tools that would otherwise be distorted by multiple pseudonymous accounts. Beyond the blockchain space, PoP has also been proposed for civic digital democracy initiatives, allowing inclusive participation while preserving voter privacy.

1.2.3 Token Distribution

PoP can also enable fair token distribution schemes by ensuring that allocations reach real individuals rather than automated or duplicate accounts. This is relevant for universal basic income (UBI) style distributions, community incentive programs, and airdrops (a one-time token distribution to all users that meet certain criteria). Sybil-resistant registries have already been used to deliver recurring UBI tokens to verified participants, while PoP-linked reputation systems help protocols protect against 'airdrop farming' by coordinated clusters of fake accounts [6]. Given the significant value that has moved through airdrops, hitting an all time high of 4.6 billion USD in 2023[7], robust Sybil defenses are critical to maintain fairness and credibility in these distributions.

1.3 Contributions

The main goal of this thesis is the design of a Proof-of-Personhood protocol for voting in a geographic area. On the path to this goal multiple contributions are made:

- Providing a structured overview of existing Proof-of-Personhood methods.
- Deriving a set of criteria that allow individual evaluation and comparison of PoP protocols
- Creating an overview of existing PoP protocols, analyzing their strengths and weaknesses, and evaluating them along our selected criteria.
- Exploring combinations of PoP methods in general, including some theoretical insights and expierences from the design process of our target protocol.

- A PoP protocol for voting in a geographic area that combines a passport and a Pseudonym Party approach, including various options of modifiying that protocol to different requirements.

Chapter 2

Overview of Different Approaches to Proof-of-Personhood

This chapter explores the various approaches to generating verifiable Proofs of Personhood, grouped by their underlying operational models. We distinguish between synchronous methods, which require participants to verify their uniqueness in real time during coordinated events, and asynchronous methods, which allow verification at any time without global coordination.

2.1 Synchronous Proof-of-Personhood

Synchronous Proof-of-Personhood relies on the principle that one individual cannot physically be in two different places at the same time or participate in multiple activities simultaneously. These systems involve network-wide verification ceremonies during which participants must actively prove their uniqueness and humanity in real time.

2.1.1 Pseudonym Party

Pseudonym parties are in-person gatherings held simultaneously across multiple locations. Participants gather at the same time and anonymously receive a pseudonymous identity such as a token or key, which authorizes one copy of digital credentials per person. The system leverages the ability of humans to recognize other humans as a method of ensuring uniqueness and preventing replay or duplication of credentials [2].

These events partially preserve privacy, allowing participants to conceal their identities while still proving their human status. Tokens granted during such gatherings typically grant temporary digital Personhood that can be renewed at subsequent events.

This approach poses practical challenges: participants must travel to a physical location at a scheduled time, which may exclude those unable to attend. Furthermore, coordinating multiple authentic parties across locations in a federated system without enabling credential inflation is difficult [8].

2.1.2 Virtual Pseudonym Party

A virtual variant of the pseudonym party model could be organized using synchronized online video sessions instead of in-person gatherings. In this setup, users join structured video calls network-wide at the same time. Individuals randomly grouped exchange confirmation that none of them is participating in multiple sessions simultaneously. After mutual verification, each participant is issued a token granting temporary Personhood, similar to the physical model [2]. Such virtual gatherings reduce barriers of entry and improve accessibility, enabling participation from geographically remote individuals or those unable to attend in person. This option also introduces new challenges. Ensuring that meeting participants are genuine becomes more challenging, as video interactions are susceptible to manipulation through impersonation or deepfakes. Exact coordination of times and meeting agenda become critical to prevent users from attending multiple meetings.

2.1.3 Reverse Turing-Style Verification

Another synchronous method is akin to a reverse Turing test, where humans prove their humanity by performing tasks that are easy for humans but hard for AI systems/bots. At regularly scheduled validation ceremonies, participants must solve a suite of cognitive puzzles known as FLIPs (Filter for Live Intelligent People) under time constraints [8, 9].

FLIPs involve interpreting coherent human-generated sequences of images or stories under time pressure, tasks that are currently difficult for automated systems. This limits the possibility of a single person controlling multiple identities by the assumption that users cannot solve two tests at once [9].

This approach also has its own limitations. The same individual may be able to solve multiple tests within a given time limit. Additionally, as AI systems continue to advance, even human-like puzzle challenges such as FLIPs may become susceptible to automation [4].

2.2 Asynchronous Proof-of-Personhood

Asynchronous Proof-of-Personhood allows users to begin the Personhood verification process at any time, without the need for coordination around specific ceremony dates or sessions. Users can register or prove their uniqueness on their own schedule, making these mechanisms flexible and accessible.

2.2.1 Web of Trust

A Web of Trust system operates by creating a decentralized network of trust: users verify one another through mutual attestation, building a social graph that reflects interpersonal trust relationships. Fake identities are then identified either through targeted challenges or by analyzing the graph structure, since fabricated nodes typically exhibit weak connectivity to genuine users [2].

This decentralized approach offers notable advantages. It avoids scheduling conflicts and physical logistics, increasing accessibility. Its reliance on community validation maintains user autonomy. It also scales organically as the network grows, without necessitating centralized orchestration.

A potential issue is that well-coordinated attackers might forge connections with real users, establishing sufficient trust edges to circumvent detection. The effectiveness of Web of Trust also depends heavily on social structures in which newcomers or marginalized individuals may struggle to gain sufficient trust, resulting in exclusion or shift of power to established participants.

2.2.2 Personal Data

These approaches leverage unique personal data to ensure that each real individual can create only a single account. Although zero-knowledge proofs can obscure sensitive information to preserve privacy, inherent risks around misuse or data leakage remain.

Know your Customer

The KYC model is a model that is used in traditional finance. By gathering verifiable personal information, such as names, ages, addresses, and government-issued credentials, a link from users to their accounts is created, introducing clear accountability and enabling mechanisms such as banning, monitoring, or taking legal action when necessary [10].

The main problem with KYC-style systems is that they raise concerns about privacy and accessibility. Requiring individuals to share sensitive documentation can undermine anonymity, deter participation from privacy-conscious users, and exclude those who lack the necessary documents.

Image/Video

Another approach leverages the individuality of human faces, users submit photos or videos of themselves to establish Personhood. Other participants then review and may challenge the authenticity if they suspect duplication or nonhuman presence.
Although this method enables decentralized verification, its reliability has decreased with the rise of deep-fakes and generative AI. Malicious actors can now easily create convincingly authentic video or image content, making it increasingly difficult to distinguish genuinely unique humans from manipulated replicas.

Zero Knowledge Biometrics

Biometric-based methods, including fingerprints, facial scans, or iris recognition, confirm that each account corresponds to a distinct human being, through their unique biometric information. When paired with zero-knowledge proofs or homomorphic encryption, these systems can obscure the raw biometric data while still validating uniqueness [11].
Like all personal data, biometric data is inherently sensitive and irrevocable. If breached, it cannot be replaced like a password could be. Additionally, gathering of biometric data often requires custom hardware, if off the shelf solutions do not provide the required security, leading to a single point of failure and therefore centralization.

Zero Knowledge Credentials

Zero-Knowledge Credentials enable a synchronous Proof-of-Personhood by allowing users to prove possession of a trusted document, such as an ePassport, without exposing any personal data. These documents, issued by recognized authorities, store identification and biometric information in an NFC chip with cryptographic signatures that can be verified against public registers [8].
In practice, users scan their credentials and optionally provide a biometric sample (e.g., a face scan), which the system verifies locally. Instead of transmitting personal data, the user generates a zero-knowledge proof that asserts the validity of the credential without revealing the actual content. As a result, data linkage is minimized, and user privacy is better maintained [12].
This approach builds on widely accepted identity infrastructure, 193 member countries follow the specifications provided by the International Civil Aviation Organization (ICAO)[13]. It ensures strong Personhood verification, and upholds privacy by design. Moreover, selective disclosure allows users to prove only what is strictly necessary, such as age or citizenship, without exposing additional personal details.
It also has its own drawbacks. Reliance on official documentation can exclude

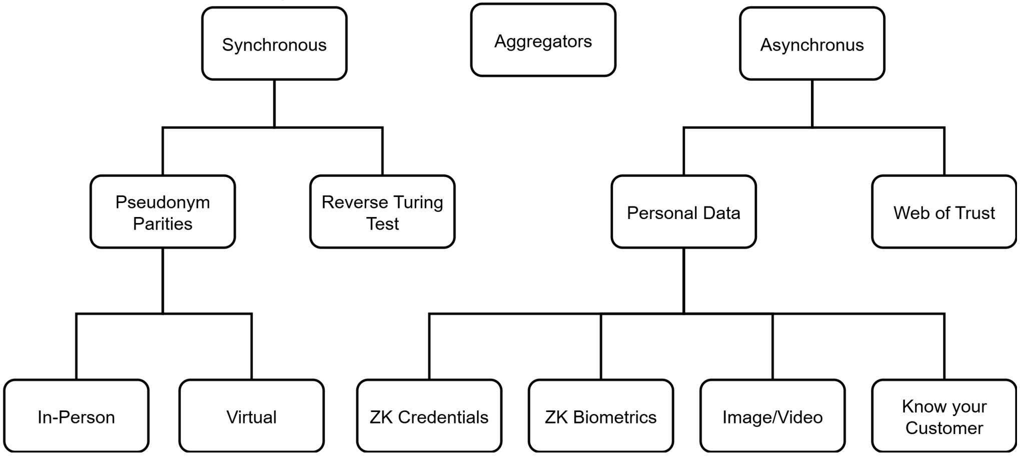
vulnerable or undocumented populations. In addition, absolute trust is placed in the issuing authorities, which could introduce biases or systemic vulnerabilities.

2.3 Proof-of-Personhood Aggreagators

Proof-of-Personhood aggregators let users verify their humanity using the methods they prefer, while platforms only need to integrate with one unified interface. This model enables users to select among various Proof-of-Personhood protocols and simplifies implementation by avoiding separate integrations for each method. Aggregators enhance interoperability, allowing verified users to seamlessly prove their Personhood across multiple blockchains and decentralized applications. Requirements for specific applications can be different, for example, users needing to fulfill multiple Proofs of Personhood from different providers.

This convenience introduces trade-offs. Relying on a central aggregator becomes a single point of failure: If compromised, it could undermine identity verification across all integrated platforms. The selection of supported identity providers may narrow over time, reducing user choice and potentially consolidating power. On the other hand, if one of the many protocols up for selection is compromised, every app will be compromised until that protocol is fixed or removed. Additionally, users can uphold multiple identities using different verification methods for each.

Figure 2.1: Overview of all PoP Methods



Chapter 3

Overview of Proof-of-Personhood Protocols

This chapter describes a broad range of PoP protocols, examining their underlying mechanisms, strengths, and limitations. Following each description, the protocol is graded according to our derived criteria. This allows for a structured comparison between different approaches. The aim is to document existing methods and provide a clear basis for identifying trade-offs and potential combinations.

3.1 Evaluation Criteria

After examining various PoP Protocols and with the properties mentioned in the first chapter in review, we have decided on the following criteria. These criteria create a framework that allows us to evaluate each protocol individually and provides us with a basis for comparison between them.

Security (Sybil resistance): This is the foundational property of any PoP protocol. It prevents a single human from creating multiple valid identities or Personhood tokens, ensuring the principle of 'one person, one account'.

Decentralization: Verification and governance should be distributed across many independent actors. This reduces the risk that any single party can block enrollments, alter outcomes, or become a single point of failure.

Privacy: As little personal data as possible, or none at all should be required and collected, so individuals can prove Personhood without revealing sensitive information that could be exposed or abused.

Pseudonymity: Participation should be possible without linking an account to a real-world identity. It ensures that the 'one-human' proofs remain unlinkable to a specific person unless the user chooses otherwise.

Accessibility: Participation for all, regardless of socioeconomic status, nationality, documentation, language, or disability. This avoids excluding legitimate users through technical, financial, or procedural barriers.

Low effort Enrollment, maintenance, and recovery processes should be simple and infrequent. Clear steps, minimal user actions, and straightforward recovery paths help maintain long-term participation.

Accountability: There should be clear and enforceable consequences for misconduct. Fraud, duplicate identities, or abuse can be addressed through measures such as revocation, penalties, or re-verification.

Technical Scalability: This is the ability to register and serve a large number of users efficiently from a technical perspective. It maintains predictable costs and reliable performance even as adoption grows.

3.2 Encointer

Encointer's PoP relies on Pseudonym Parties, requiring users to attend network-wide verification ceremonies to obtain temporary Personhood. A participant preregisters a one-time public key, then shortly before each ceremony window, the protocol randomly assigns them to a small meetup at a specific location. At the meetup, participants display their app, mutually attest presence, and record the headcount. Once the attestations are submitted on chain and align with the majority count, the account receives a new Personhood 'ticket' and becomes eligible for UBI. Encointer caps the number of first-time users per meetup, uses endorsements to admit newcomers, and runs a reputation mechanism that guarantees assignment only for accounts that attend regularly while penalizing no-shows, which encourages users to keep a single, stable account [14].
This approach offers strong Sybil resistance due to its nature of synchronous in-person meetups, but requires a rather high effort from participants and may be inaccessible to users with disabilities or those living in remote areas.

Evaluation

Security (Sybil resistance): (+ +)
Simultaneous randomly assigned physical gatherings make it extremely difficult for a single person to obtain multiple valid identities.
Decentralization: (+ +)

Ceremony scheduling, participant assignment, and verification are coordinated entirely on-chain, without reliance on a central authority, reducing single points of failure.
Privacy: (+)
No personal data is stored on-chain, and cryptographic proofs maintain anonymity at the protocol level. However, in-person attendance inherently reveals physical appearance to other participants, which can leak identifying information.
Pseudonymity: (+)
On-chain credentials remain pseudonymous, but in person interaction allows other attendees to visually identify participants.
Accessibility: (+)
Open to anyone within a supported area, but the requirement for recurring in-person attendance creates barriers for those with mobility issues or living in remote locations.
Low effort: (− −)
Requires consistent participation in scheduled physical gatherings, which demands time, travel, and planning and leads to significantly higher effort than online-only approaches.
Accountability: (+ −)
Enforcement is limited to the loss of an account and its associated reputation.
Technical Scalability: (+)
Protocol mechanics scale well on-chain, but the limit on new users per gathering limits growth speed. Also, Encointer Pseudonym Parties are local by design, so scaling would include combining multiple local solutions.

3.3 Virtual Pseudonym Party

A hypothetical virtual pseudonym party adapts synchronous verification to an online setting and requires users to attend network-wide ceremonies to obtain temporary Personhood. Shortly before each ceremony window, the protocol randomly assigns users to three short video calls with different peers. During each call the protocol generates liveness prompts (for example, reading a short text aloud or performing a specific gesture), after a brief conversation, each participant issues attests the presence of the others and confirms if they believe they are human. When all three rounds are completed, the protocol aggregates incoming attestations, checks for conflicts, and submits the results on chain. If a threshold of consistent attestations is met, the account receives a new Personhood token.
This approach improves accessibility and the effort required compared to in-person pseudonym parties, but compromises security. Liveness during a video call is weaker than physical presence, and reliability depends on bandwidth and device quality.

Evaluation

Security (Sybil resistance): (+ –)
Simultaneous, randomly assigned video calls with multiple independent peers make it harder for a single person to hold multiple valid identities, but deepfakes, pre-recorded video, or AI agents remain possible and are only getting better. Identity farming (outsourcing the verification procedure to low income workers) could also be a problem.
Decentralization: (+ +)
Scheduling, participant assignment, and verification can be coordinated entirely on-chain, avoiding reliance on any single authority and reducing central points of failure.
Privacy: (+)
No personal data is stored on-chain, but live video inevitably reveals visual and audio cues.
Pseudonymity: (+)
On-chain credentials remain pseudonymous, but during calls, participants can see and hear each other.
Accessibility: (+ +)
Only an internet connection and a device with a camera are required. Participation is possible from anywhere.
Low effort: (–)
Requires regular attendance at scheduled verification ceremonies, but eliminates travel and can be completed from any location.
Accountability: (+ –)
The primary enforcement mechanism is the loss of an account.
Technical Scalability: (+)
There is no inherent technical barrier to scaling the number of participants, but it would require a newbie limit on calls similar to Encointer.

3.4 Idena

Idena's Proof-of-Personhood is based on regular network-wide validation ceremonies in which all participants must solve a set of FLIPs. visual puzzle sequences designed to be easy for humans but difficult for automated systems. A participant begins by registering their account and, at the appointed time, receives a batch of FLIPs to solve under strict time constraints. Successful validation renews the account status and grants continued participation rights. Following the ceremony, validated users are tasked with creating new FLIPs, which will be curated and used in subsequent validation events. Idena incorporates a reputation system that tracks each participant's performance over time, missing or failing a ceremony results in a loss of reputation, and repeated failures can lead

to permanent removal of the account [9].
This approach has high accessibility, only requiring internet access, and it also provides high privacy. However, it is heavily dependent on the continued difficulty of FLIP puzzles for AI systems. It is also possible that certain humans could solve multiple FLIP batches within the allotted time, and solving of FLIPs could easily be outsourced.

Evaluation

Security (Sybil resistance): (+ –)
Synchronous, time-limited FLIP puzzles make it difficult, but not impossible, for a single person to validate multiple accounts simultaneously. However, tasks can potentially be outsourced to low-wage workers, and advances in AI may solve these puzzles reliably.
Decentralization: (+ +)
Ceremony scheduling, FLIP distribution, and result verification are coordinated entirely on-chain, avoiding reliance on any central authority.
Privacy: (+ +)
No personal data is collected or stored, and puzzle solving does not reveal identifiable information.
Pseudonymity: (+ +)
User accounts cannot be linked to real-world identities through protocol-level data, ensuring strong pseudonymity.
Accessibility: (+ +)
Only an internet connection and a compatible device are required, enabling participation from anywhere.
Low effort: (–)
Requires regular attendance at scheduled validation ceremonies, but participation can be completed entirely online.
Accountability: (+ –)
Enforcement is limited to the loss of an account and its accumulated reputation if ceremonies are missed or failed repeatedly.
Technical Scalability: (+ +)
No inherent technical limits to the number of participants, ceremonies, and verification processes can scale with network capacity.

3.5 World

World's PoP relies on biometric verification using proprietary 'Orb' scanning devices, which perform high-resolution iris scans to establish the uniqueness of a user. A participant visits an Orb operator, where the device captures an image

of their iris. The raw image is processed locally to generate a unique iris code, which is then immediately hashed. The original biometric image is then deleted. Using zero-knowledge proofs derived from the hash, the system can confirm that the iris code has not been registered before, thus proving the uniqueness of the user, without revealing the biometric data itself. Successful verification links the participant's public key to a World ID credential, allowing them to prove Personhood in supported applications without rescanning [11].
This approach offers strong Sybil resistance due to the uniqueness and difficulty of forging biometric traits, while allowing repeated proofs without re-disclosing the biometric data. However, it depends on centralized hardware manufacturing and distribution, as well as trust in Orb operators to follow the deletion policy. Deployment is limited by the availability of Orbs, and the use of biometrics raises concerns about long-term data security, potential misuse, and public trust.

Evaluation

Security (Sybil resistance): (+ +)
Iris biometrics are highly distinctive and extremely difficult to forge, providing strong protection against multiple registrations.
Decentralization: (–)
Although verification proofs can be used in decentralized systems, the capture process relies on proprietary Orb devices and centrally coordinated manufacturing and distribution, introducing trust and supply chain dependencies. The Protocol also heavily relies on the trustworthiness of Orb operators
Privacy: (+ –)
The iris is scanned locally, transformed into a unique code, and the raw image is deleted before leaving the device. Zero-knowledge proofs protect the uniqueness check, but the use of biometrics inherently raises concerns about potential data misuse or policy violations.
Pseudonymity: (+ +)
Once registered, users can prove personhood using a World ID without revealing their biometric data or linking to their real-world identity.
Accessibility: (+)
In principle, it is open to anyone, but participants must physically travel to an Orb location. Access may be limited in regions with few or no devices.
Low effort: (+ +)
Only a one-time in-person registration is required and ongoing participation does not require additional ceremonies or repeated biometric scans.
Accountability: (+)
Accounts can be revoked or banned in cases of detected fraud or policy violations and the user will not be able to create a new one since his iris is already registered.
Technical Scalability: (+ –)

Already deployed as one of the largest PoP networks, however scaling requires very large ammount of capital, due to the reliance on Orbs.

3.6 Humanode

Humanode's PoP is based on biometric face recognition. A user begins by installing the Humanode client, During the registration process, the client prompts the user to complete a series of randomized liveness challenges, such as head movements or changes in facial expression, that are captured via their device's camera. The biometric data is processed locally to create a unique template, which is then encrypted and used to verify the uniqueness against existing templates in the network without revealing the raw facial image. If no match is found, the user's public key is registered as a verified Humanode, granting them the ability to participate in governance, consensus and applications based on Sybil resistance [15].
This approach offers a very accessible and low effort PoP to users, but advancements in deepfake technology question the security of the protocol.

Evaluation

Security (Sybil resistance): (+ –)
Facial biometrics with liveness detection provide reasonable resistance to multiple registrations, but verification through consumer-grade phone cameras is potentially more vulnerable to spoofing than dedicated hardware. Advancements in deep-fake technology also raise concerns.
Decentralization: (+)
Verification and identity management can be coordinated without a central authority, but relying on commercial phone hardware and operating systems introduces potential points of influence.
Privacy: (+ –)
A facial scan is processed locally to generate an encrypted template before leaving the device, minimizing exposure of raw biometric data. However, the inherent sensitivity of facial biometrics still poses privacy concerns if encryption or local processing is compromised.
Pseudonymity: (+ +)
On-chain credentials remain unlinkable to real-world identities, and the facial template cannot be reversed into an image.
Accessibility: (+ +)
Registration is open to anyone with an internet connection and a camera-enabled device.
Low effort: (+ +)

Requires only a one-time registration, with no recurring ceremonies or periodic re-verification unless account recovery or dispute resolution is needed.
Accountability: (+)
Accounts can be revoked or banned for violations, and the violator cannot create a new one since his face has already been registered.
Technical Scalability: (++)
There is no inherent technical barrier to scaling participation.

3.7 BrightID

BrightID's PoP is based on a decentralized social graph, where the strength of a user's identity is determined by their connectivity in the graph in general and the proximity and connectivity to trusted entities known as 'Seeds'. A participant begins by creating a BrightID account and forming connections with existing verified users. Verification can occur through direct meetings, either in person or online, with a Seed, or indirectly by connecting through mutual contacts who already have verified links to Seeds. The protocol analyzes the structure of these connections, and graph algorithms evaluate how closely a user is embedded in the trusted network. Seeds have the authority to report suspicious accounts, and if a reported account lacks sufficient trusted connections, it can be flagged and removed from the system [16].
This approach offers strong decentralization and high privacy, as no sensitive personal information is collected and verification depends solely on social graph relationships. It is highly accessible in regions with active communities of verified users, but onboarding can be more difficult for isolated individuals without existing connections. Although the system is resistant to isolated Sybil attacks, coordinated infiltration of the social graph over time poses a potential challenge.

Evaluation

Security (Sybil resistance): (+)
Relies on social graph connectivity to detect Sybil accounts, with higher trust assigned to users closely connected to Seeds. This provides moderate resistance against isolated fake accounts, but does not offer hard guarantees against coordinated infiltration over time.
Decentralization: (+ +)
Verification and trust building are distributed across a network of independent users and Seeds, with no single central authority controlling access.
Privacy: (+)
No personal information is collected or stored, but the network of connections of a user can indirectly reveal aspects of their identity or social relationships if

analyzed.
Pseudonymity: (+)
Accounts are not inherently tied to real-world identities, but pseudonymity can be compromised because social graph connections are correlated with public or known relationships.
Accessibility: (+)
No formal barriers to entry, anyone can join by connecting to existing verified users or attending a meeting with a Seed. However, onboarding may be slower for people with no previous connections.
Low effort: (+)
The initial setup is relatively simple, but maintaining and expanding trusted connections over time may require periodic interaction with other verified users.
Accountability: (+ −)
Enforcement is limited to the loss of an account, however building a new network of connections could be slower since honest participants will not add the same user twice.
Technical Scalability: (+)
The system can grow with user adoption, but graph analysis could become computationally expensive on a large scale depending on implementation.

3.8 Circles UBI

Circles UBI's PoP mechanism is built on a Web of Trust model that uses economic incentives to encourage honest verification. Each participant mints their own personal currency, which is considered equal in value to the currencies of others only if there is a mutual trust link. To execute transactions, users exchange currencies along chains of trust connections, ensuring that everyone ultimately receives tokens they deem valid. Establishing a trust link with another user is equivalent to accepting their currency at parity, effectively vouching for their authenticity. If a user extends trust to a fake or duplicate account, they risk receiving currency that no one else accepts, creating a built-in disincentive for trusting unverified identities [17].
This approach aligns economic value directly with network trust, offering a market-based method of Sybil resistance without requiring centralized oversight or direct personal data, but the transaction may also be impossible if no trust chain exists.

Evaluation

Security (Sybil resistance): (−)
Relies primarily on economic incentives to discourage trusting fake accounts,

without hard technical guarantees. Collusive groups could still create mutually trusted Sybils, although their value is limited outside the cluster.
Decentralization: (+ +)
Trust relationships and currency exchanges occur entirely on-chain, with no central authority controlling verification or transactions. The integrity of the network emerges from distributed trust links.
Privacy: (+)
No personal information is required at the protocol level. However, trust relationships can reflect real-world associations, which could inadvertently reveal aspects of a user's identity.
Pseudonymity: (+)
Users can remain pseudonymous, but their position in the trust graph and public transaction history may indirectly link them to real-world identities through social network analysis.
Accessibility: (+ +)
Open to anyone with internet access, with no geographical or hardware constraints beyond standard connectivity requirements.
Low effort: (+ –)
Initial registration is simple, but maintaining a functional account requires actively forming and updating trust relationships to ensure smooth transactions.
Accountability: (+ –)
Misconduct is penalized indirectly through social and economic disincentives, with the main enforcement being loss of account utility or trust links.
Technical Scalability: (+ –)
Struggles with unconnected or sparsely connected nodes and transaction paths depend on the density of the trust graph. Large-scale graph analysis can also become computationally intensive.

3.9 ZKPassport

ZKPassport is not a full PoP protocol, but still provides a mechanism that allows users to prove their uniqueness by presenting an official government-issued identity document, such as a passport, while keeping all personal information private through the use of Zero Knowledge Proofs. The user scans the machine-readable chip or the data page of their passport, and the system verifies its authenticity and uniqueness based on the cryptographic signature of the issuing authority. Using a zero-knowledge protocol, verification confirms that the document is genuine and not linked to any other account, without revealing identifying details such as the holder's name, birthdate or passport number. Once validated, the user receives a credential that can be used in online systems to assert Personhood without further exposing the document [18].
This approach offers high security combined with low required effort, but re-

lies heavily on the trustworthiness of issuing authorities and excludes individuals without official documentation.

Evaluation

Security (Sybil resistance): (+ +)
Verification is tied to government-issued cryptographically signed credentials, making it extremely difficult for a single person to obtain multiple valid identities without committing high-risk document fraud.
Decentralization: (– –)
Relies on centralized issuing authorities, such as governments, which hold the power to approve or deny access to credentials and can revoke them at will.
Privacy: (+ –)
Zero Knowledge Proofs can ensure that none of the personal data on the credential is revealed during verification. However, the initial scanning process still carries the risk of information leakage.
Pseudonymity: (+ +)
Credentials can be transformed into anonymous proof tokens, preventing linkage to the holder's real-world identity unless voluntarily disclosed.
Accessibility: (–)
Excludes individuals without compatible government-issued documents, which can disproportionately affect marginalized groups, refugees, or those in countries with poor documentation systems.
Low effort: (+ +)
Requires only one-time registration, with no recurring ceremonies or repeated verifications needed.
Accountability: (+)
Credentials can be blacklisted or revoked, allowing targeted bans without revealing personal identity.
Technical Scalability: (+ +)
Once the verification system is in place, it can easily handle a large number of users without significant additional infrastructure.

3.10 Proof of Humanity

Proof of Humanity's approach to PoP combines video-based identity verification with a Web of Trust endorsement system. To register, a user provides an Ethereum stake and uploads a video of themselves stating a specific phrase, along with metadata such as their name and Ethereum address. This submission is added to a public registry and must be endorsed by existing verified users to become valid. Challenges are also built into the system: anyone can dispute a profile by submitting evidence that the person is not unique, not human, or otherwise violates the rules. Disputes are resolved through Kleros, a decentralized court system that relies on crowd-sourced jurors to make final decisions [19]. The protocol maintains Sybil resistance by making duplicate registrations economically costly and socially detectable, while its public registry creates transparency and supports community-driven verification. The system also introduces privacy trade-offs, as profile videos are permanently stored on a public blockchain, which can deter participation from privacy-conscious individuals.

Evaluation

Security (Sybil resistance): (+)
The combination of staking, video submission, and community-based challenge mechanisms creates strong disincentives against creating multiple valid identities, but none provide concrete one human, one account guarantees.
Decentralization: (+ +)
Verification, staking, and dispute resolution are coordinated through smart contracts and a decentralized governance framework, removing the reliance on any single authority.
Privacy: (– –)
Verification videos are stored on-chain or accessible publicly, making them viewable by anyone and posing a significant privacy risk.
Pseudonymity: (– –)
Because verification videos must show the applicant's face and are publicly available, accounts can be directly linked to real-world identities.
Accessibility: (–)
Open to anyone able to record and upload a video, but requires staking funds, which can create barriers for users with limited financial means.
Low effort: (+)
After the initial registration and staking process, no ongoing participation is required.
Accountability: (+)
Misconduct or false registrations can result in both loss of account and forfeiture of the stake, providing a strong enforcement mechanism.
Technical Scalability: (+)
The protocol has no fundamental scalability barriers, though manual review of challenges could slow onboarding at a very large scale.

3.11 Human Passport

Human Passport, formerly Gitcoin Passport, is a PoP aggregator that collects and verifies multiple independent identity signals to assess the likelihood that a user represents a unique human. It integrates with various PoP providers and trust sources, such as social media accounts, ENS registrations, BrightID, and government-issued ID checks, assigning weighted scores to each credential. Users connect these credentials to their passport, which is stored on-chain or in decentralized storage, and the combined score determines their eligibility for participating in Sybil-sensitive activities like quadratic funding rounds. The system encourages users to accumulate various verification stamps, thereby increasing their trust score and reducing the risk of Sybil attacks [20].
This approach benefits from high flexibility and accessibility, as users can choose from many verification methods and incrementally strengthen their passport without relying on a single PoP protocol. However, its Sybil resistance depends heavily on the strength of the aggregated sources, and weaker credentials can dilute overall security if weighted too leniently. Additionally, while the aggregation model offers decentralization at the data level, the scoring logic and weighting decisions are governed by Human Passport, introducing some centralization.

Evaluation

Security (Sybil resistance): (−)
Relies on aggregating multiple independent verification methods to increase Sybil resistance. Security depends on the quality and diversity of the connected proofs, but no single, hard-to-fake mechanism is enforced by default.
Decentralization: (+ −)
Uses decentralized identity standards and allows multiple independent issuers to contribute attestations, but the aggregation process is coordinated by Gitcoin's infrastructure, introducing some centralization.
Privacy: (+)
Supports privacy-preserving attestations where possible, though certain verification sources may require personal data to be shared with third parties. Privacy ultimately depends on the verification methods chosen.
Pseudonymity: (+)
Can maintain pseudonymity if privacy-friendly verifications are used, but methods that link to real-world accounts or identities reduce pseudonymity.
Accessibility: (+ +)
Highly accessible due to online participation and flexibility in verification sources; users can choose from a range of proofs with varying geographic and technical requirements.
Low effort: (+)
Once set up, maintenance is minimal. Effort depends on the complexity of the

verifications chosen.
Accountability: (–)
Misconduct can be addressed by revoking or invalidating credentials, but enforcement is tied to the chosen proof sources rather than to the aggregator itself.
Technical Scalability: (+ +)
Easily scalable, as verification and credential issuance are distributed among multiple independent providers, with the aggregator simply compiling scores.

3.12 Rarimo

Rarimo functions as a different kind of PoP aggregator, but in contrast to Human Passport, Rarimo does not combine the different proofs, it allows users to verify different PoP methods and later proof their validity to a third party vial Zero Knowledge Proof and selective disclosure. It supports a variety of identity proofs, including document-based methods such as passport verification. Users can link one or more supported proofs to their decentralized identifier, with attestations issued by trusted verifiers. These attestations are stored in a privacy-preserving format, allowing users to selectively disclose the verification status without revealing the underlying personal information. The flexibility of the system allows participants to choose from different verification methods depending on their privacy preferences, technical capabilities, and geographic restrictions [**?**].
This approach benefits from high accessibility and scalability, as it does not rely on a single verification method, and it leverages existing infrastructure for document authentication. However, its Sybil resistance is directly tied to the strength and diversity of the chosen verification sources, and reliance on external issuers introduces some trust dependencies that may limit full decentralization.

Evaluation

Security (Sybil resistance): (+ –)
Sybil resistance depends on the strength and diversity of the external verification sources used (e.g., passport checks, biometric attestations).
Decentralization: (+ –)
The protocol itself is decentralized in how credentials are stored and verified, but trust is partially placed in external issuers such as passport authorities or other identity providers.
Privacy: (+)
Uses selective disclosure via decentralized identity standards and zero-knowledge proofs to confirm verification status without revealing underlying personal information. Some verification sources may still require personal information that could be leaked.

Pseudonymity: (+)
Credentials can be linked to on-chain identities without revealing the real-world identity unless the user chooses to disclose it. Some verification sources may still require personal information that could be leaked.
Accessibility: (+ +)
Highly accessible, as it supports multiple verification methods, allowing users to select the one most suitable to their location, documentation, and connectivity.
Low effort: (+)
One-time verification with no requirement for recurring ceremonies, though users may need to renew credentials periodically depending on the verification method.
Accountability: (−)
Misconduct can be addressed by revoking or invalidating the associated credential, but the strength of the enforcement depends on the underlying verification source.
Technical Scalability: (+ +)
Supports a wide range of verification sources, making it adaptable for large, global user bases. The actual proofs are done by independent PoP providers.

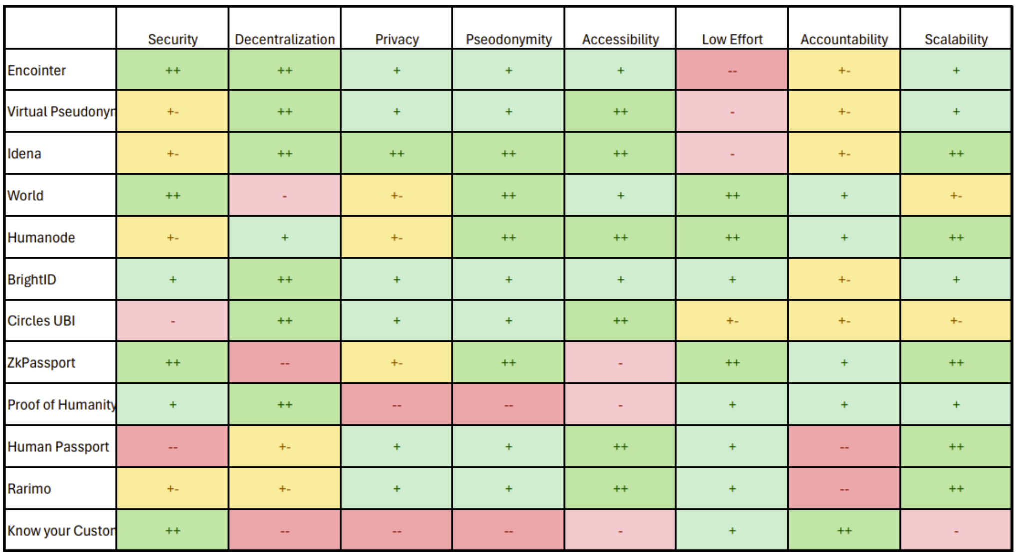
3.13 Know Your Customer

Know Your Customer (KYC) is a process widely used in traditional banking and regulated industries, which, while not designed as a PoP mechanism, can fulfill a similar role in establishing unique, verifiable identities. In a KYC-based system, users submit official identification documents, such as passports, national IDs, or driver's licenses, along with personal information such as name, date of birth, and address. The submitted data is verified against trusted government or institutional databases, and in some cases supplemented with biometric checks such as facial recognition or liveness detection to prevent impersonation. Once verified, the user's account is permanently linked to their real-world identity, ensuring 'one person, one account' through strong legal accountability.
This approach offers high Sybil resistance due to its reliance on government-issued credentials and regulated verification providers. However, it requires the disclosure and storage of sensitive personal information, creating privacy risks if data is mishandled or breached. It also excludes individuals without access to formal identification or those unwilling to reveal their identity, limiting accessibility. Furthermore, KYC introduces centralized points of control and potential censorship, since verification authorities can deny service or revoke credentials.

Evaluation

Security (Sybil resistance): (+ +)
Government-issued identification and regulated verification processes make the large-scale creation of fake identities extremely difficult. Fraud attempts typically require great effort and carry legal consequences.
Decentralization: (– –)
Verification is performed by a single trusted authority (e.g. a bank or KYC provider) and usually stored in centralized databases, creating single points of failure and enabling potential censorship.
Privacy: (– –)
Requires the disclosure of extensive personal data, including legal name, address, and date of birth, often stored by the verifying entity and subject to regulatory retention requirements.
Pseudonymity: (– –)
The goal of KYC is to directly link accounts to real-world identities, eliminating pseudonymity entirely.
Accessibility: (–)
Excludes individuals without access to formal identification or a fixed address and may present additional barriers in regions with limited administrative infrastructure. Registration can be time-consuming and may require in-person verification or physical mail delivery.
Low effort: (+)
Once completed, KYC is typically a one-time process, with no recurring verification required unless documents expire or require updates.
Accountability: (+ +)
The strong link between account and verified identity allows enforcement actions, including legal recourse, watch list enforcement, and permanent bans tied to a person.
Technical Scalability: (–)
Each registration requires manual or semi-manual verification steps, document handling, and regulatory compliance, limiting throughput.

Figure 3.1: Overview of all Evaluations



	Security	Decentralization	Privacy	Pseodonymity	Accessibility	Low Effort	Accountability	Scalability
Encointer	++	++	+	+	+	--	+-	+
Virtual Pseudonyr	+-	++	+	+	++	-	+-	+
Idena	+-	++	++	++	++	-	+-	++
World	++	-	+-	++	+	++	+	+-
Humanode	+-	+	+-	++	++	++	+	++
BrightID	+	++	+	+	+	+	+-	+
Circles UBI	-	++	+	+	++	+-	+-	+-
ZkPassport	++	--	+-	++	-	++	+	++
Proof of Humanity	+	++	--	--	-	+	+	+
Human Passport	--	+-	+	+	++	+	--	++
Rarimo	+-	+-	+	+	++	+	--	++
Know your Custor	++	--	--	--	-	+	++	-

Chapter 4

Concept and Design Goal

In this chapter, we outline the foundations for our work toward designing a Proof of Personhood protocol intended for use in voting within a defined geographic area. To ensure clarity, we first describe our target application clearly and define terms relevant to the discussion. Then we analyze the implications this use case has for its design.

4.1 Target Application

We aim to design a Proof of Personhood-backed voting protocol for a userbase defined by geography, for example, a country, canton, municipality, or ethnic region.

This geographic region can be arbitrarily defined but should ideally be in a convex shape or follow natural borders to simplify implementation. If we want to use a verified credential, like a passport, as part of our solution, it is beneficial if the geographic region is part of a country or confederation that issues this verified credential.

In this thesis, the term residents does not only refer to people with formally registered addresses in a region, but to anyone living in or regularly spending a significant amount of time in the geographic area. This specifically includes: Sans Papiers, Homeless people and commuters with workplaces within the area. We want to allow all residents of that geographic region to vote with equal power. But we specifically do not want to allow owners of a local credential, who are no longer residents of the region, to vote.

4.2 Design Implications

The target application of our protocol, voting within a geographically bounded community, imposes specific design requirements that shape the architecture of

the system.
First and foremost, the protocol must provide high Sybil resistance, enforcing 'one person, one vote' literally. In a voting context, even a small number of additional fraudulent votes could alter the outcome of an election, undermining trust in the process. Ensuring that each participant can only obtain one valid identity is therefore a non-negotiable requirement.
At the same time, the protocol must guarantee high accessibility and inclusivity. Voting is meaningful only if the entire affected population is able to participate. This requires low barriers to entry for all residents of the region.
Closely linked is the requirement of low effort. If participation is too cumbersome, turnout will be low and the resulting user base will be unrepresentative. To achieve both scale and diversity, the process of obtaining and using a valid identity should be simple and require minimal time and resources.
Another critical aspect is geographic eligibility. Unlike global Proof of Personhood protocols, our system must strictly restrict participation to those who reside in or regularly inhabit the designated geographic region, while excluding citizens who have moved away. This requires mechanisms that can reliably tie eligibility to residency without creating undue exclusion.
Finally, the protocol must preserve privacy and anonymity. Although personhood and geographic eligibility must be established at registration, the act of voting itself must remain unlinkable to individual identities.

4.3 Promising existing Approaches

4.3.1 Aggregators

Existing PoP aggregators, such as Rarimo and Human Passport (Gitcoin Passport), do benefit from very high accessibility, illustrating the benefit combinations can have on it. But they are otherwise not well-suited for a geographically scoped voting protocol. They combine a variety of Proof of Personhood methods without strictly enforcing the principle of one person, one ballot. These systems lack safeguards against users who register multiple accounts through different verification methods, which allows small-scale attacks, and do not natively verify geographic eligibility.

4.3.2 Pseudonym Party

Pseudonym Parties present a promising approach, offering strong security and ensuring accessibility by relying on human presence and the innate ability of humans to recognize other humans. Their main drawback is the high effort required from participants, who must attend in person ceremonies at specific times and locations. At the same time, they naturally enable enforcement of geographic eligibility, since participation can be restricted to gatherings held within the defined region.

4.3.3 Passports/Credentials

Passports offer a straightforward mechanism for Proof of Personhood, providing high Sybil resistance through trusted, government-issued credentials. They also require low effort from users, since verification can be performed quickly with existing documents and many residents already have them. However, this approach raises accessibility concerns, as not all individuals in a region hold valid passports, and obtaining one may be costly or bureaucratically difficult. Passports also provide a natural way to enforce geographic eligibility, particularly when the voting region aligns with the jurisdiction of the issuing authority but includes citizens who are no longer residents. In addition, reliance on centralized government infrastructure introduces trust and privacy risks, since sensitive personal data is inherently tied to the credential.

4.3.4 Biometrics

Biometrics, specifically the approach used by World, fills a similar niche to passports by leveraging unique physical characteristics, such as iris scans, to establish strong Sybil resistance. They provide nearly the same level of security as passports and, like passports, require relatively little effort from users after the initial registration. They even provide a small geographic aspect since the one-time registration could only be offered/accepted within the geographic region. However, biometric methods introduce distinct challenges: they often require specialized hardware (e.g., Orbs) that may limit accessibility and introduce centralization risks through control of the devices. Although cryptographic protections can help hide raw biometric data, the privacy implications are significant, since biometric traits are immutable and highly sensitive.

Chapter 5

Combinations of Proof-of-Personhood

Combining different Proof-of-Personhood methods offers a way to address the limitations inherent in any single approach. No single method perfectly balances security, accessibility, privacy, and scalability, but by combining complementary mechanisms, a system could potentially achieve a strong score in all desired aspects.
This chapter explores methods for integrating multiple PoP approaches and examines the benefits and trade-offs of such combinations. A sequential combination, requiring users to pass several PoP verifications, and parallel combination, allowing them to choose from multiple options, each impact the properties of the final protocol in distinct ways.
In addition to theoretical considerations, we also look at attempts to design entirely new PoP protocols by combining existing methods to achieve a protocol suitable to our target application of geographic voting. Studying these efforts provides valuable information on the practical challenges of combinations.

5.1 Combination Types

There are two main ways of combing PoP methods: parallel, where users choose from available methods, and sequential, where users are required to absolve multiple different verifications.

5.1.1 Parallel Combination

In a parallel combination approach, users can choose from multiple PoP methods to complete their verification. Each method is accepted as equally valid, and a successful verification through any one of them grants the user full access or voting rights. This approach maximizes accessibility, as it allows individuals to select the method that is most convenient or feasible for them. However, a parallel combination also carries significant security risks. Without additional safeguards, the same individual could register multiple accounts by completing different verification methods for each. This makes parallel systems unsuitable for scenarios that require strict 'one person, one account' guarantees unless additional cross-checking measures are implemented.

5.1.2 Sequential Combination

In a sequential combination approach, users must complete multiple PoP verification methods before being granted access or voting rights. This layered verification substantially strengthens Sybil resistance, as compromising the system requires defeating all included methods. The primary drawback is reduced accessibility and increased participant effort, as users must navigate multiple verification procedures, each with its own requirements and potential barriers. This can limit adoption, especially in contexts where participation rates are critical.

All Synchronous PoP, like, for example, Pseudoonym Parties, can technically be viewed as sequential combinations of single verification ceremonies. In the case of Pseudonym Parties, a user has to attend multiple meetups to be accredited Personhood.

5.2 Improving Security of Parallel combinations

A naive parallel combination is currently not very suitable for our goal, since it would effectively double the votes a single person could obtain if both methods are accessible to them.

5.2.1 Cost of Improving Security

By definition, the pseudonymity and privacy properties that are desired in a protocol make it very hard to ensure that one person can only obtain one account, since accounts should remain unlinkable to users.
If a user registers via protocol 1 and obtains a PoP c_1 and obatains c_2 from registering through protocol 2, it should not be possible to link c_1 to c_2. Since the only common factor between the two certificates is the user, the only way they could be linked is using information about the user, which would then violate pseudonymity and privacy.
As a consequence, if we want to ensure that each user is only able to obtain one account, we need to compromise on privacy and pseudonymity, meaning protocols would collect and share and compare certain user information. If we want to avoid that, the check needs to be done separately from the actual PoPs, leading to additional steps that potentially require user effort.

5.2.2 Methods of Enforcing One User, One Account

Proof-of-Non-Participation

The idea behind Proof-of-Non-Participation is to require each user, in addition to showing one valid credential, to also demonstrate that they did not register through any other method. In principle, this should be easier than performing a full registration: for example, during a Pseudonym Party, a user might simply present a location proof that shows they are not attending an event, without having to go through the entire verification flow again.
However, designing such proofs is inherently difficult. By nature, a Non-Participation proof must be unique to every PoP method: What counts as 'not attending' a pseudonym party is very different from 'not using' a biometric check or 'not registering' with an ePassport. There is no single generic mechanism that can be applied across all systems.
In some cases, it may even be impossible. For example, a user could prove that they have not used their Passport within the protocol (since credential usage can be tracked), but there seems to be no way to prove that they simply do not own an Passport in the first place. This fundamental limitation means that Proof-of-Non-Participation can only work in a small ammount of cases.

Partial Participation

The Partial Participation approach requires users of one PoP protocol to engage partially in another, without completing the full registration process. The idea is that if users are forced to show up or contribute periodically to a second protocol, it becomes infeasible for them to simultaneously maintain a second full account using that protocol.
For example, a user who relies primarily on a Web-of-Trust-based identity might be required to attend every third Pseudonym Party gathering. This does not give them an additional valid credential from the Pseudonym Party system but enables the combination by preventing them from sustaining a second full account there.
The main challenge is determining how much partial participation is 'enough'. If the burden is too low, malicious actors may still succeed in holding multiple accounts. If it is too high, ordinary users may be discouraged from participating at all. Moreover, depending on the combined protocols, the required level of partial participation may vary significantly, potentially requiring a lot of effort from users.

Impossibility

The Impossibility approach aims to prevent users from enrolling in multiple PoP systems by making it technically or logistically impossible to use both at the same time. A typical strategy is to schedule verification ceremonies of two synchronous protocols at overlapping times, so that an individual cannot physically or virtually participate in both.

This method is highly context-dependent and unique to each pair of PoP protocols. In some cases, it may provide strong protection, especially when both protocols rely on synchronous participation that cannot be automated, such as Encointer Pseudonym Parties [14] or Idena FLIP ceremonies [9]. However, suitable overlaps are often difficult to identify and, for many combinations of protocols, no natural 'impossibility condition' exists at all. For example, synchronous protocols can conflict in time, but asynchronous or document-based, like Web-of-Trust, akin to BrightID [16] or Passports akin to ZKPassport [18], methods do not lend themselves to such coordination.

As a result, while Impossibility can work as a targeted defense, it is not a universal solution to ensure one account per person across all PoP methods.

Incentivization

The Incentivization approach discourages users from creating multiple accounts by attaching tangible costs or opportunity trade-offs to doing so. In practice, this often means requiring participants to stake resources, expend effort, or regularly maintain their accounts in ways that make it economically or practically unappealing to operate more than one identity.

However, applying this method to voting comes with challenges. Incentives must be sustained over time, which can become expensive for the system to maintain. Moreover, the "value" of a single vote is not fixed: in most cases, an additional vote may have negligible influence, but in a high stake, close decision, even a handful of additional votes could change the outcome and thus generate enormous potential 'profit' for an attacker. This asymmetry complicates the calibration of incentives.

One mitigation is to limit the ability of adversaries to create new accounts once a high-stakes vote becomes known. For example, requiring accounts to be registered and active prior to the announcement of a vote reduces the risk of opportunistic sybil attacks. Nevertheless, incentives alone rarely provide a foolproof safeguard against determined adversaries, especially in contexts where the outcome of a vote has substantial consequences.

One Forced PoP

The One Forced PoP approach requires all users to verify exclusively through a single designated protocol. It basically layers one sequential combination on top of any number of parallel-combined PoPs. This guarantees that every account is anchored to the same PoP method, thereby eliminating the possibility of duplicate registrations across multiple systems.
Although this strategy is straightforward and effective at preventing Sybil attacks, it removes many of the benefits of combining multiple PoP methods in the first place. The accessibility and inclusivity advantages that might arise from offering a choice of protocols are mitigated, and the entire system becomes dependent on the strengths and vulnerable to weaknesses of the one enforced protocol. Security should, however, increase, since every user now needs to verify their Personhood through two protocols.

5.3 Combined Protocols

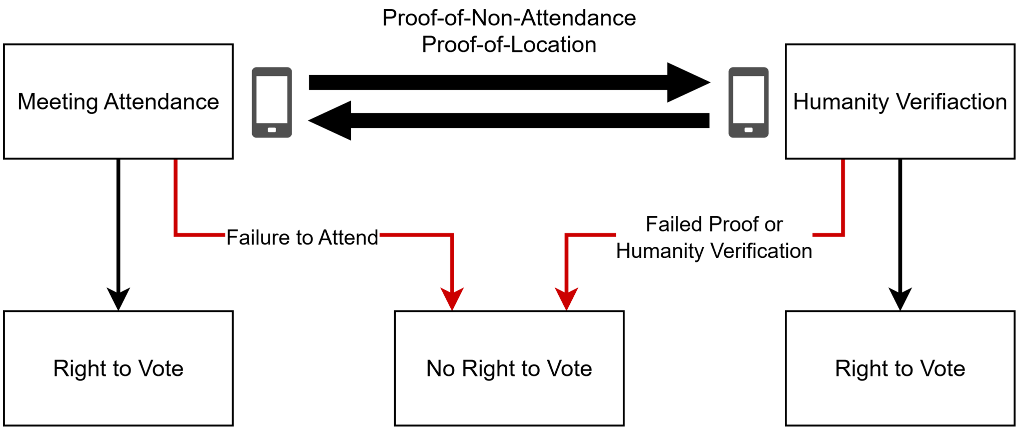
In this section, we explore protocol designs that attempt to combine passport-based verification with Pseudonym Parties for geographically scoped voting. The motivation is to leverage the complementary strengths of these approaches: passports offer a strong, state-backed proof of identity with low effort, while Pseudonym Parties also provide a high Sybil resistance, but while remaining highly accessible, decentralized, and privacy preserving. The goal is to find a solution that remains low effort for users that own a passport and allow Pseudonym Party attendees to preserve their privacy, without excluding anyone, and of course, ensure that everyone can obtain only one vote.
The following sections describe specific combinations, focusing on how the two mechanisms interact, the practicalities of implementation, and the challenges they introduce. We then evaluate limitations such as location accuracy, user effort, security vulnerabilities, and accessibility. A more in depth description of each Protocol can be found in the appendix.

5.3.1 Proof-of-Location Protocol

For this first in-depth attempt, keeping the effort required for passport users was the main goal. It only requires a Proof-of-Location during pseudonym party gatherings, verifying their location within the geographic area and proofing non-attendance of gatherings.
This hybrid protocol combines passports with Pseudonym Parties using smartphones. During party windows, holders of an passport-based credential who are not attending must prove non-attendance by showing proximity absence to party devices (Bluetooth/Wi-Fi beacons) and proving presence in the geographic area

via latency check.

Figure 5.1: Process during one Meeting, Right for Passport, Left for Pseudonym Party users



Proof-of-Location

The Proof-of-Location is separated into two parts. First, a close-range check to attendees' phones via Bluetooth or WIFI ensures that a user is not attending a gathering. Second, a latency test to attendees phones ensures the user is in the eligible geographic area.

Binding Phone to Person

Binding the phone to the user is critical to the effectiveness of the Proof-of-Location. To ensure that the phone accompanies the person during the checks, users are required to re-scan their passport. Additionally, at this point a form of humanity verification could be required, an approach similar to Idena FLIPs comes to mind, but would raise the problem of FLIP generation and arms race against bots.

Limitations

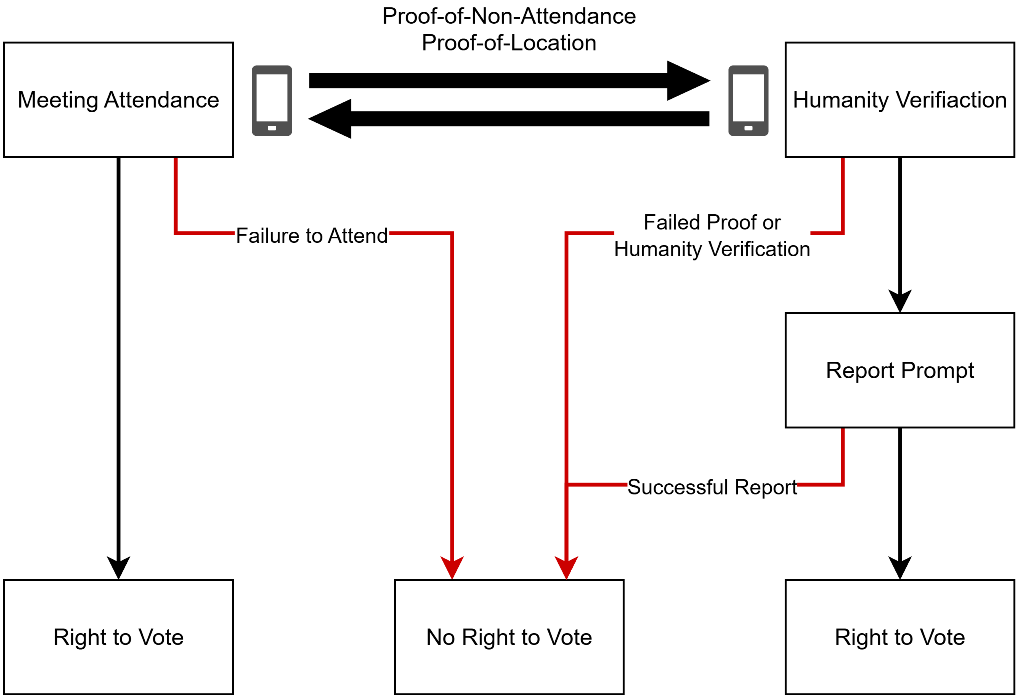
The Proof-of-location is inherently noisy and can be affected by both spoofing attacks and fluctuating network conditions. Similarly, proximity signals, such as Bluetooth or Wi-Fi, offer only limited accuracy and can be unreliable as indicators of physical presence.
Delegation remains a critical vulnerability: for example, someone other than the legitimate user could scan the passport and perform the necessary steps. Even

when additional humanity checks are introduced, reliably binding a person to a single device (e.g., their phone) presents new challenges and may not be sufficient to prevent misuse.
In effect, this approach still requires an additional layer of PoP specifically for passport registered users. During pseudonym party gatherings, the system must ensure that each phone is operated by a real human, and that no single person can complete the humanity verification process for more than one device. The core requirement becomes 'one human, one phone', which is not trivial to enforce and introduces further complexity into the protocol design.

5.3.2 Whistleblower Protocol

This protocol aims to mitigate the risk that a single person verifying multiple accounts by reframing the problem as a question of detection rather than prevention. Instead of making it technically impossible for someone to perform Proof-of-Location or Humanity Verification for multiple identities, the system introduces a social and economic incentive to expose such behavior. During each verification ceremony, anyone who gains access to an account has the opportunity to report that the account holder is not the real user. If the report is valid, the reported account is restricted, and the whistleblower receives a monetary reward.

Figure 5.2: Process during one Meeting, Right for Passport, Left for Pseudonym Party users



Reward Money Source

The success of this system depends on a sustainable mechanism for funding whistleblower rewards. One possible approach is to require users to deposit a stake during registration. This deposit would be forfeited if the account is reported and confirmed to have violated the protocol, and the whistleblower's reward could be paid from this forfeited stake. However, this reduces accessibility by introducing a financial barrier to entry.

Alternatively, the protocol itself could fund the reward payments as an upfront cost and later recover the funds from penalized users. For example, a user whose account has been restricted due to a valid report would need to pay a reactivation fee, allowing the protocol to recover the bounty payout. This model preserves accessibility, but requires careful liquidity management and enforcement mechanisms.

Limitations

This approach has the following problems: First, users may find ways to delegate the verification process to third parties or automate it through restrictive scripts that only allow a minimal form of participation, effectively bypassing the intended checks. Second, the system must protect against misuse of the reward mechanism itself. A malicious user might register fake accounts and immediately report them to claim the bounty, a practice sometimes referred to as bounty farming. Similarly, users who no longer wish to participate in the protocol might self-report their accounts just before leaving, in order to collect the reward, a behavior akin to rage quitting.

These risks can be partially mitigated by requiring a financial stake for registration or whistleblowing, creating a cost for these exploitative behaviors. However, this brings us back to the accessibility trade-off. In addition, funding whistleblower rewards remains a major challenge. The system must either rely on protocol funds or enforce strict cost recovery mechanisms to maintain long-term viability.

Finally, automatization of the Proof-of-Location process still poses a risk, as adoption of the protocol grows an arms race between development of the humanity verification process and bots that sole them will inevitably emerge.

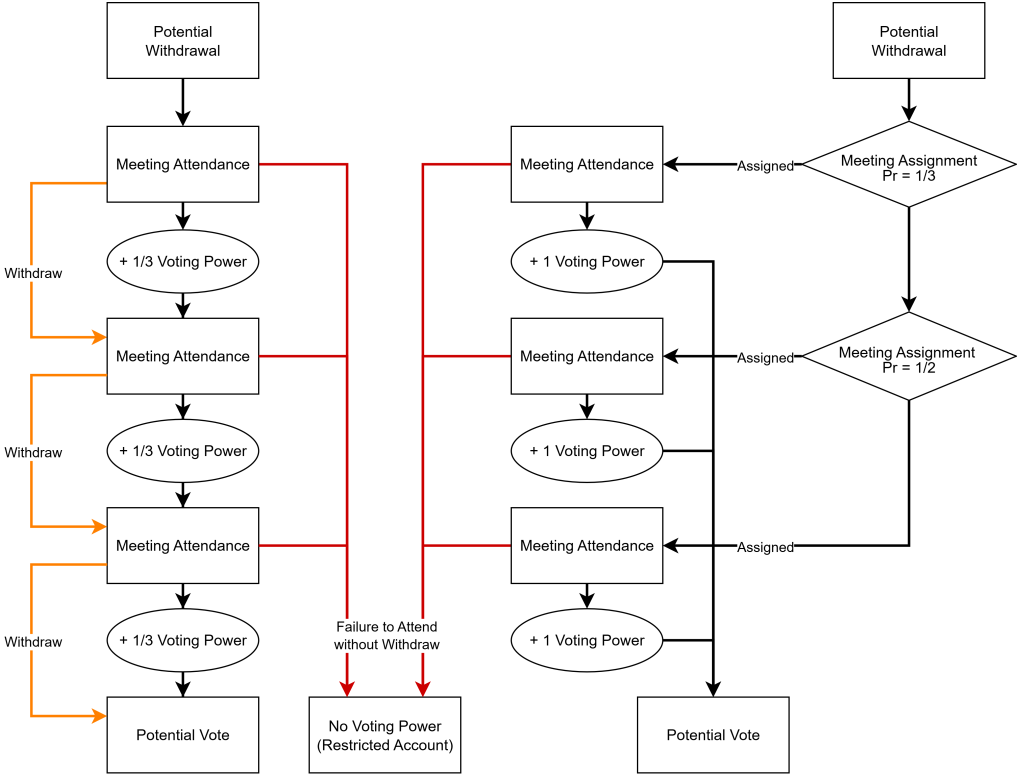
5.3.3 Random Attendance Protocol

The Random Attendance Protocol represents a shift away from Proof-of-Non-Attendance mechanisms by relying instead on a Partial Participation approach. In this system, users registered through passports demonstrate their presence and ongoing engagement by periodically attending randomly assigned Pseudonym Party meetings. Each passport user is individually assigned to exactly one

Pseudonym Party meeting per cycle of three. This design aims to ensure that users remain active and geographically present without requiring close surveillance or highly accurate geolocation.

To promote honest behavior and encourage long-term engagement, the protocol employs a reputation system in which the reputation directly corresponds to the voting power, inspired by the approach used by Encointer [21]. Each user's reputation is evaluated in recurring cycles consisting of three meetings. This structure ensures that passport-registered users must participate in at least one gathering within each cycle in order to maintain their eligibility and influence.

Figure 5.3: Process during a Cycle of three Meetings, Right for Passport, Left for Pseudonym Party users



Withdrawing

To account for real-world constraints, users are allowed to withdraw from meetings at the beginning of each cycle. For users on the Pseudonym Party track, withdrawing carries little or no penalty, whereas missing a meeting without withdrawing leads to the loss of all reputation for that cycle.

Passport-registered users who withdraw are not assigned a meeting in that cycle, but must attend an additional meeting in the next cycle to compensate. This ensures consistent activity over time while offering flexibility for users who are temporarily unavailable.

Reputation Loss and Gain

The rules for gaining and losing reputation are tailored to each type of user. Passport users earn one reputation point per attended meeting.
In contrast, Pseudonym Party users gain one-third of a reputation point per meeting. If they miss a withdrawn meeting, they may lose a small amount of reputation (such as 0.1), but unexcused absences reset their reputation for the entire cycle and possibly the following one as well.

Limitations

Despite its strengths, the Random Attendance Protocol faces some limitations. One risk is that users might create multiple Pseudonym Party accounts to correspond with different possible passport meeting assignments. This vulnerability could be reduced by extending the reputation lifespan across multiple cycles, making it harder to maintain undetected fraudulent accounts over time.
The main concern, however, is the possibility of saturation attacks. A coordinated group of passport holders might work together to maintain additional accounts on the Pseudonym Party track. Because only one-third of the group is expected to be assigned to a meeting at any given time, the remaining two-thirds could support additional accounts without being detected. The larger the group, the more predictable and exploitable the distribution becomes, allowing attackers to increase their voting power unfairly. One potential mitigation strategy involves unifying the random assignment process across both protocol tracks, thereby reducing the predictability and increasing the difficulty of coordinating such an attack.

Chapter 6

Decentralized Landsgemeinde

The Decentralized Landsgemeinde protocol is the last and most promising effort in combining PoP methods to create a protocol for voting in a geographic area. This protocol combines Passports and Pseudonym Parties similarly to the Random Attendance Protocol introduced in the previous chapter. Passport users are required to attend randomly assigned Pseudonym Party meetings, to ensure they do not additionally have a regular account, and to verify they are still in the geographic area. However, in this protocol, all passport users need to attend the same meetings.

6.1 The Protocol

Pseudonym Party

The Pseudonym Party forms the foundation of this combined protocol and is directly inspired by the approach used in Encointer, though with some important adaptations. Unlike Encointer, gatherings in this protocol are held less frequently, balancing usability with security. Meetings are organized in intervals of three and occur every 27 days. The choice of 27 days, deliberately not divisible by seven, ensures that each meeting falls on a different day of the week, preventing systematic exclusion of participants who may be unavailable on specific weekdays. Increasing the frequency of meetings would improve security but at the cost of greater effort for participants, while reducing it would make the protocol easier to maintain but less resistant to Sybil attacks.

Participants are randomly assigned to meetings with the crucial property that the other attendees in a given session should not be predictable in advance. Each gathering consists of between five and twelve participants. This range has been chosen to strike a balance: smaller groups would create overhead and open the system to small-scale attacks, whereas larger groups would make it more difficult for participants to effectively monitor each other.

In addition, the number of new users at a meeting is limited to less than 1/2 to prevent malicious parties from obtaining a majority at a gathering by registering

a large number of new users.
During each meeting, all attendees verify each other's presence by scanning QR codes displayed on their devices. This mutual attestation provides a lightweight but reliable way of ensuring that every participant is physically present and uniquely accounted for.
Before any account can be used to vote, a user needs to attend all three meetings of an interval to activate their account, in this interval the user is not yet allowed to vote. This is necessary to stop users from creating new accounts to avoid repercussions of missing meetings.

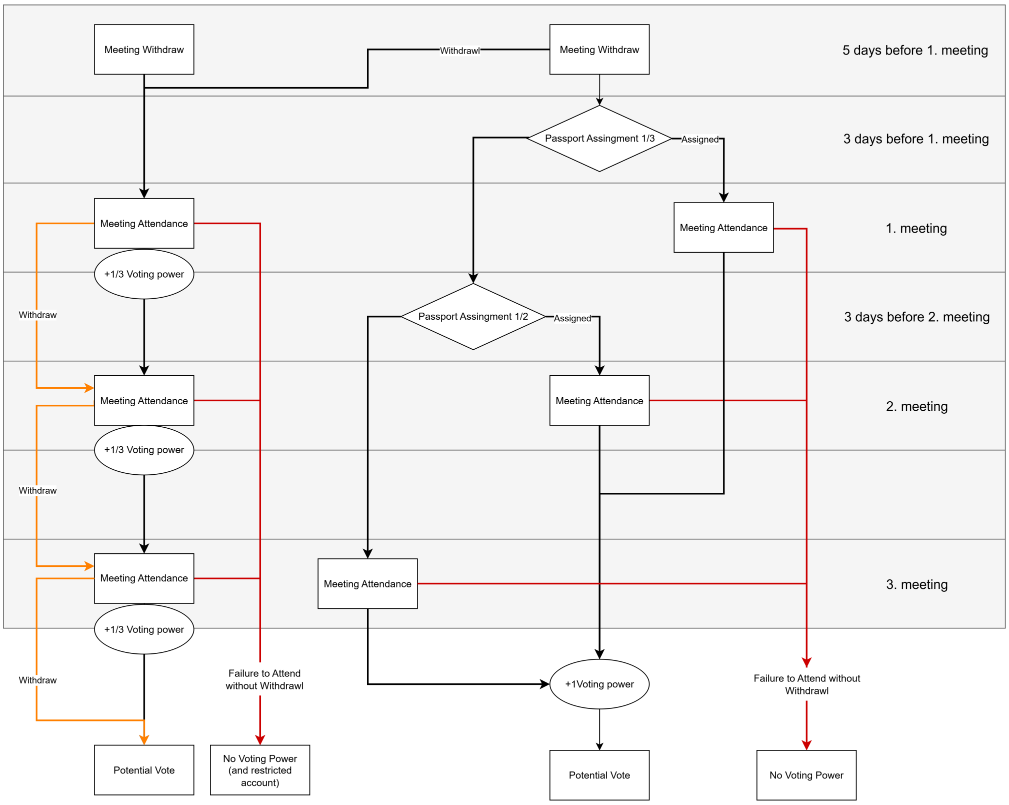
Passport

The Passport part is completely optional for any user. During account creation or at any point later in time, users can verify their Passport using their phone via an approach similar to ZKPassport [18]. This can be done by scanning the passport chip using NFC and the Machine Readable Zone using the phone camera. The Passport is then verified by the phone, and a Zero Knowledge Proof is generated. Finally, a unique hash is generated and saved to ensure each Passport is only used once, providing a strong Personhood for that user.
From this point on, the user will be required to attend exactly one random meeting in an interval of three. This meeting will be the same (at the same time) for all Passport users. If Passport users need to attend a meeting, is announced a few days in advance. Each meeting has the same chance of being chosen.

Attendance and Voting Power

In this protocol, the voting power of a given user is derived from their attendance during the respective interval. In addition, users have the option to withdraw from meetings before the start of an interval to mitigate the repercussions of missing meetings.
For users with a Passport, this means that they will receive 1 voting power (a full vote) if they attend their assigned meeting. If the user cannot attend at a specific gathering, they can withdraw from that meeting before the start of the interval and instead choose to attend the other two meetings to obtain 1/3 voting power each. If the assigned meeting happens to be one of the two, the user will of course receive the full voting power for that interval. Like this, users can be given some leniency while ensuring that the withdrawal system is not abused. So users who do not attend the assigned meeting are then almost equal to users without Passports. If an assigned meeting is missed without withdrawing, the user will not be eligible to vote in this interval.
Users without Passport will receive 1/3 voting power for every attended meeting. Withdrawing from a meeting before the interval will just result in not receiving voting power from that meeting. However, since it makes sense for a malicious

user who has both a Passport account and a regular account to favor the assigned meetings from the Passport account, punishments for missing a meeting without withdrawing need to be more severe. If a user misses a meeting without withdrawing, they will be ineligible to vote in that interval. Additionally, the user will be required to attend all three meetings of an interval to receive voting power again (and will receive full voting power in this interval). This means that they will either miss their assigned meeting to restore the regular account or be unable to restore the regular account.



6.1.1 Security Analysis

In this section we analyze the security of our protocol against various adversaries by calculating the expected gained voting power. Note however, that this does not constitute a security proof, since our adversary is not exhaustive. We look at an adversary that controls both an activated regular account and an activated account with passport (attended all 3 in an interval).
$VP :=$ Voting Power

Prioritize Regular meetings

Here we look at an adversary that withdraws from one or two random meetings in each interval on the regular account, if any of the meetings they have not withdrawn from are assigned for Passport users, they will attend the regular meetings.
Since in this case our adversary never misses a meeting on the regular account, the account never becomes restricted, and all intervals are therefore independent.

1 Withdrawl There are two cases, either there is an overlap between the regular and assigned meetings or not.
Case without overlap: $Pr = \frac{1}{3}$ $VP = 1 + \frac{2}{3} = \frac{5}{3}$
Case with overlap: $Pr = \frac{2}{3}$ $VP = \frac{2}{3}$
This means that the expected value of the obtained Voting Power is $\frac{1}{3} * \frac{5}{3} + \frac{1}{3} * \frac{2}{3} = \frac{5}{9} + \frac{4}{9} = 1$

2 Withdrawls There are again two cases, either there is an overlap between the regular and assigned meetings or not.
Case without overlap: $Pr = \frac{2}{3}$ $VP = 1 + \frac{1}{3} = \frac{4}{3}$
Case with overlap: $Pr = \frac{1}{3}$ $VP = \frac{1}{3}$
This means that the expected value of the obtained Voting Power is $\frac{2}{3} * \frac{4}{3} + \frac{1}{3} * \frac{1}{3} = \frac{8}{9} + \frac{1}{9} = 1$
So, this adversary does not gain a consistent advantage.

Prioritize Passport meetings

Now we look at an adversary that again withdraws from one or two random meetings in a interval on the regular account. However, this adversary prioritizes the assigned Passport meetings over meetings on the regular account. If the regular account is then restricted, the adversary will prioritize reactivating it, since they would otherwise end up with only one account and become a normal user.
Since there is now the possibility of the regular account being restricted different intervals are no longer independent. Therefore we approximate the expected value of voting obtained if the strategy is used forever.

$VP :=$ Voting Power
$X_i := \mathbf{E}[\text{Voting power obtained after i intervals}] - i$

This means X_i is equal to the total advantage of the advarsary over i meeting cycles.

1 Withdrawl We first derive a formula for X_n. If there is a overlap in the first interval, then the adversary cannot obtain extra voting power in the first and second interval, therefore the advantage in this case is equal to the advantage from the third interval onvard. But if there is no overlap the advarsary obtains $\frac{2}{3}$ extra voting power in the current interval, as well as any extra voting power they can obtain from the second interval onward. For $n \leq 0$ X_n is 0.

$$\begin{aligned} X_n &= \frac{2}{3} * X_{n-2} + \frac{1}{3} * (\frac{2}{3} + X_{n-1}) \\ &= \frac{2}{3} * X_{n-2} + \frac{2}{9} + \frac{1}{3} * X_{n-1} \end{aligned} \tag{6.1}$$

Proof. We now prove via strong induction that $\frac{X_n}{n} \leq Y_n$, where $Y_n = \frac{2}{15} + \frac{4}{45n}$

$$\frac{X_n}{n} \leq \frac{2}{15} + \frac{4}{45n} \iff X_n \leq \frac{2}{15}n + \frac{4}{45} \tag{6.2}$$

For our base case we have $X_1 = \frac{2}{9} = \frac{2}{15} + \frac{4}{45} = \frac{10}{45}$ and $X_2 = \frac{8}{27} \leq \frac{4}{15} + \frac{4}{15} = \frac{16}{45}$

Next we prove that $X_n \leq \frac{2}{15}n + \frac{4}{45}$ under the assumption that $X_i \leq \frac{2}{15}(i) + \frac{4}{45}$ for $i \leq n-1$

$$\begin{aligned} X_n &\leq \frac{2}{3} * X_{n-2} + \frac{2}{9} + \frac{1}{3} * X_{n-1} \\ &\leq \frac{2}{3} * (\frac{2}{15}(n-2) + \frac{4}{45}) + \frac{2}{9} + \frac{1}{3} * (\frac{2}{15}(n-1) + \frac{4}{45}) \\ &\leq \frac{2}{45}(n-1) + \frac{4}{45}(n-2) + \frac{4}{135} + \frac{8}{135} + \frac{10}{45} \\ &\leq \frac{2n-2}{45} + \frac{4n-8}{45} + \frac{12}{135} + \frac{10}{45} \\ &\leq \frac{6n}{45} - \frac{10}{45} + \frac{4}{45} + \frac{10}{45} \\ &\leq \frac{2n}{15} + \frac{4}{45} \\ &\leq \frac{2}{15}n + \frac{4}{45} \end{aligned} \tag{6.3}$$

□

So we can conclude that $\lim_{n\to\infty} \frac{X_n}{n} \leq lim_{n\to\infty} Y_n$ so our adversary has an advantage of less than $\lim_{n\to\infty} \frac{2}{15} + \frac{4}{45n} = \frac{2}{15}$

2 Withdrawls This proof is analogous to the proof for 1 withdrawal. We first derive a formula for X_n. If there is a overlap in the first interval, then the adversary cannot obtain extra voting power in the first and second interval, therefore, the advantage in this case is equal to the advantage from the third interval onvard. But if there is no overlap the advarsary obtains $\frac{1}{3}$ extra voting power in the current interval, as well as any extra voting power they can obtain from the second interval onward. For $n \leq 0$ X_n is 0.

$$\begin{aligned} X_n &= \frac{1}{3} * X_{n-2} + \frac{2}{3} * (\frac{1}{3} + X_{n-1}) \\ &= \frac{1}{3} * X_{n-2} + \frac{2}{9} + \frac{2}{3} * X_{n-1} \end{aligned} \tag{6.4}$$

Proof. We now prove via strong induction that $\frac{X_n}{n} \leq Y_n$, where $Y_n = \frac{1}{6} + \frac{1}{18n}$

$$\frac{X_n}{n} \leq \frac{2}{15} + \frac{4}{45n} \iff X_n \leq \frac{1}{6}n + \frac{1}{18} \tag{6.5}$$

For our base case we have $X_1 = \frac{2}{9} = \frac{1}{6} + \frac{1}{18} = \frac{4}{18}$ and $X_2 = \frac{4}{27} \leq \frac{2}{6} + \frac{1}{18} = \frac{7}{18}$

Next we prove that $X_n \leq \frac{1}{6}n + \frac{1}{18}$ under the assumption that $X_i \leq \frac{1}{6}(i) + \frac{1}{18}$ for $i \leq n-1$

$$\begin{aligned} X_n &\leq \frac{1}{3} * X_{n-2} + \frac{2}{9} + \frac{2}{3} * X_{n-1} \\ &\leq \frac{1}{3} * (\frac{1}{6}(n-2) + \frac{1}{18}) + \frac{2}{9} + \frac{2}{3} * (\frac{1}{6}(n-1) + \frac{1}{18}) \\ &\leq \frac{2}{18}(n-1) + \frac{1}{18}(n-2) + \frac{2}{54} + \frac{1}{54} + \frac{4}{18} \\ &\leq \frac{2n-2}{18} + \frac{n-2}{18} + \frac{3}{54} + \frac{4}{18} \\ &\leq \frac{3n}{18} - \frac{4}{18} + \frac{1}{18} + \frac{4}{18} \\ &\leq \frac{n}{6} + \frac{1}{18} \\ &\leq \frac{1}{6}n + \frac{1}{18} \end{aligned} \tag{6.6}$$

□

So we can conclude that $\lim_{n \to \infty} \frac{X_n}{n} \leq lim_{n \to \infty} Y_n$ so our adversary has an advantage of less than $\lim_{n \to \infty} \frac{1}{6} + \frac{1}{18n} = \frac{1}{6}$

6.1.2 Evaluation

We have created a protocol that satisfies our security requirements and has very high accessibility. Additionally it provides users with pseudonymity and privacy conscious users can choose to use the regular pseudonymity party approach to

avoid the leakage of any personal data.
While the protocol relies on government issued passports, obtaining a passport does not mean obtaining a vote. The required attendance serves as an additional road block. Unfortunately, our protocol requires rather large effort from the user.

6.2 Possible Modifications

Gathering Assignment Announcement

In our current protocol the actual assignment for the passport users gatherings is only announced a few days before the actual gatherings, but it is also possible to announce this assignment at the start of an interval after the withdrawl deadline. The consequence of this would be that it becomes feasible for malicious users to travel long distances in order to attend a gathering in the geographic area.

Interval Size

The size of the gathering intervals can be modified, the consequence of a higher number of gatherings in an interval, is that the consequences of missing a gathering would also linger for longer, it also weakens the geographic element for passport users since they need to attend gatherings less frequently. Having a lower number of gatherings per interval has the opposite effect, increasing the geographic aspect for Passport users and decreasing duration of consequences.
Interestingly, the number of gatherings per interval does not affect the advantage of an adversary that much. If, for example, a user withdraws from half of the gatherings, they has a 50% chance of obtaining half a vote and a 50% chance of being caught, regardless of the number of gatherings.

Meeting Frequency

In addition to the number of meetings in an interval, the frequency of meetings can also be changed. Increasing the frequency increases security at the cost of effort from the user, which possibly has lower attendance as a consequence.

Withdrawl Consequences

One possibility of further decreasing the possible advantage of an adversary is to add consequences for withdrawing. This could be in the form of a small deduction from voting power. For example, each withdrawal could cost $\frac{1}{18}$ voting power. This means that if a user attends 2 meetings and withdraws from a third, they would receive a total of $\frac{11}{18}$ voting power or $\frac{4}{18}$ for 1 attend and 2 withdrawls.

Account Restrictions

Arguably, the most effective way to reduce the possible advantage of an adversary is to increase the restrictions placed on an account when a meeting is missed without withdrawing. This could mean increasing the number of intervals a restriction lasts, so requiring multiple intervals with full attendance, or no longer awarding voting power during the reactivation. After missing a meeting, a user would be required to attend a full interval of gatherings, receiving limited or no voting power at all, before being eligible to vote again.

Increasing these restrictions would also require increasing the requirements of the account activation, otherwise users will just create new accounts to avoid punishment.

While these methods are effective, they also affect users that truly just couldn't make it, be it due to sickness, emergency at work, or something else.

The following two plots show the expected advantage an adversary can gain, when the account restrictions for failing to attend are increased in different ways. Calculations can be found in the Appendix.

Figure 6.1: Plotted Advantage of an Adversary when the duration of the Restriction increases

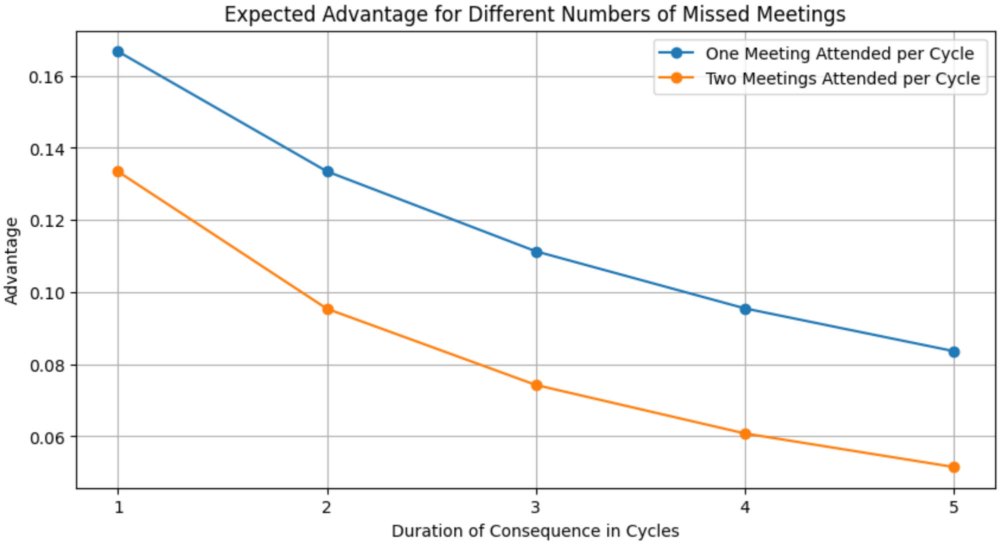
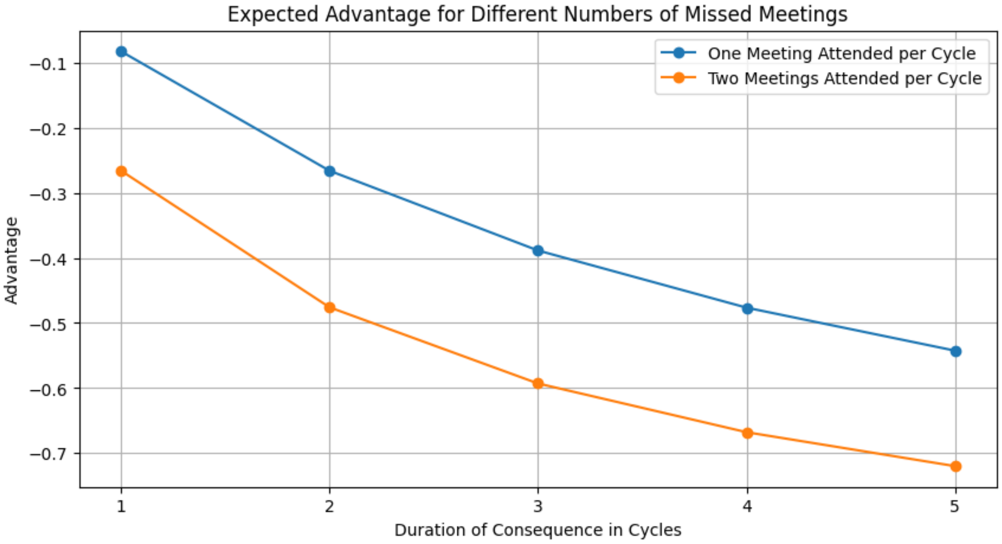


Figure 6.2: Plotted Advantage of an Adversary when Users can't Obtain Voting Power, during the Reactivation Period



Uniform Random Assignment

The current assignment style with one gathering per interval has many convenient properties. However, it requires users to plan far ahead. Potential withdrawal must be made months in advance, which is often simply not possible. By eliminating intervals and assigning passport users to meetings uniformly at random, we can allow users to withdraw up to a few days before the actual meeting.
However, this comes with its own challenges. It requires a new form of restriction for missing meetings since attending 3 meetings in a row is now possible without losing the voting power from the Passport account. Meeting attendance for passport meetings also becomes a lot more volatile, multiple meetings in a row are now possible, as well as no required attendance for potentially years.

Whistleblower Functionality

Finally, there is the option of adding a report function. This would allow users to report others if they beleive that they are using two or more accounts. Such realizations could be made easier, by making it clear during meetings, if a user has an account with a Passport or without. Noticing a user once with and once without a passport would be a clear giveaway. In addition, each user could be assigned an easily recognizable symbol that is shown on their phone during ceremonies, making it easier to report the correct account after the fact.
The interesting thing about this option is that it allows us to reliably punish accounts with linked passports that are not replacable. This is normally not the case, since it is almost always more profitable for a malicious actor to prioritize the account with a passport. Possible punishments include temporary or permanent suspension and could be more severe for repeat offenders.
However, such a feature would need to be more closely researched and planned to avoid abuse and false positives. Malicious users could try to sabotage the protocol through mass reports or something similar.

6.3 Comparison Landsgemeinde

The Landsgemeinde is a traditional form of direct democracy practiced in parts of Switzerland, where eligible citizens gather in an open assembly to vote on local matters. At first glance, this is conceptually close to our protocol: in both cases, individuals must be physically present at gatherings in order to exercise their voting rights. In the Landsgemeinde, the act of showing up is itself the proof of eligibility and participation, while in our protocol, attending meetings grants users voting power that they can later exercise digitally.
Despite these similarities, there are important differences and challenges that make direct replication of the Landsgemeinde impractical in a digital, protocol-

driven setting. The Landsgemeinde is a centuries-old institution that has been deeply integrated into local culture and political practice. Attendance is taken for granted as a civic duty, and the social fabric ensures that those who wish to vote will usually make the effort to participate. In such a context, it is reasonable to assume that absence is primarily due to unavoidable reasons, such as illness or extraordinary events, and that systematic exclusion is rare.

In contrast, our protocol does not benefit from these cultural and historical foundations. It cannot rely on the assumption that all eligible participants will naturally make the effort to attend, particularly in its early stages, when it lacks legitimacy and recognition as part of civic life. Instead, it must explicitly account for barriers such as limited mobility, lack of resources, or scheduling conflicts. For this reason, the protocol introduces mechanisms such as intervals of multiple meetings and the option to withdraw in advance, giving participants flexibility and ensuring that missing a single gathering does not necessarily mean disenfranchisement.

Another difference lies in the question of eligibility. The Landsgemeinde is restricted to formally recognized citizens of a region, typically verified through existing government registries. However, our protocol must independently establish both personhood and geographic presence without relying on such centralized registries. This introduces additional complexity, as we must prevent Sybil attacks, ensure that only residents (and not former residents or outsiders) can participate, and at the same time respect privacy by avoiding unnecessary data disclosure.

Finally, Landsgemeinde is inherently transparent: Attendance and voting are public acts performed in front of one's community. Although this promotes accountability, it also raises challenges for privacy and anonymity. Our protocol must carefully balance the public nature of physical gatherings with the need for private, anonymous digital voting.

In short, while Landsgemeinde serves as an inspiring model of embodied democratic participation, our protocol faces challenges that arise from its lack of cultural embedding, its need for inclusivity across diverse circumstances, its reliance on independent verification mechanisms, and its commitment to preserving both fairness and privacy in a digital setting.

Bibliography

[1] A. Plesner, T. Vontobel, and R. Wattenhofer, "Breaking recaptchav2," in *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, Jul. 2024, p. 1047–1056. [Online]. Available: http://dx.doi.org/10.1109/COMPSAC61105.2024.00142

[2] B. Ford, "Identity and personhood in digital democracy: Evaluating inclusion, equality, security, and privacy in pseudonym parties and other proofs of personhood," *arXiv*, 2020. [Online]. Available: https://arxiv.org/abs/2011.02412

[3] S. Adler *et al.*, "Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online," *arXiv preprint*, 2024.

[4] D. Siddarth, S. Ivliev, S. Siri, and P. Berman, "Who watches the watchmen? a review of subjective approaches for sybil-resistance in proof of personhood protocols," *arXiv preprint*, 2020. [Online]. Available: https://arxiv.org/abs/2008.05300

[5] B. Alain. (2024) A critique of gav's personhood mechanism requirements. Forum post. [Online]. Available: https://forum.polkadot.network/t/a-critique-of-gavs-personhood-mechanism-requirements/10109

[6] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," in *IEEE Security & Privacy on the Blockchain (IEEE S&B)*, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7966966

[7] N. Boey. (2024) 50 biggest crypto airdrops: $26.6b in "free money". CoinGecko Research report. [Online]. Available: https://www.coingecko.com/research/publications/biggest-crypto-airdrops

[8] Wikipedia contributors, "Proof of personhood," https://en.wikipedia.org/wiki/Proof_of_personhood, 2025, accessed: 2025-08-07.

[9] I. Team, "Idena whitepaper," https://docs.idena.io/docs/wp/summary/, accessed: 2025-04.

[10] Humanode Core. (2022, Mar.) Proof of personhood approaches. Accessed: 2025-06. [Online]. Available: https://blog.humanode.io/proof-of-personhood-approaches/

[11] W. Foundation, "Worldcoin: A new identity and financial network," https://docs.idena.io/docs/wp/summary/, 2023, accessed: 2025-04.

[12] "Rarimo docs: What is rarimo?" https://docs.rarimo.com/, Rarimo, 2025, accessed: 2025-06. [Online]. Available: https://docs.rarimo.com/

[13] International Civil Aviation Organization, *Doc 9303: Machine Readable Travel Documents. Part 8: Emergency Travel Documents*, 8th ed., 2021, emergency Travel Documents specification. [Online]. Available: https://www.icao.int/sites/default/files/publications/DocSeries/9303_p8_cons_en.pdf

[14] A. Brenzikofer, "encointer – local community cryptocurrencies with universal basic income," 2020. [Online]. Available: https://arxiv.org/abs/1912.12141

[15] D. Kavazi, V. Smirnov, S. Shilina, MOZGIII, D. Lavrenov, and the Humanode Core, "Humanode whitepaper, v. 0.9.7: "instrumentality of mankind"," Humanode, Tech. Rep., 2025, last updated May 15, 2025. [Online]. Available: https://whitepaper.humanode.io/

[16] B. Team, "Brightid whitepaper," https://www.brightid.org/whitepaper, accessed: 2025-04.

[17] C. Team, "Circles protocol whitepaper," https://github.com/CirclesUBI/whitepaper, accessed: 2025-04.

[18] ZKPassport, "Zkpassport documentation," https://docs.zkpassport.id/, 2025, accessed: 2025-08-09.

[19] Kleros Documentation Team, "Proof of humanity," accessed: 2025-08. [Online]. Available: https://docs.kleros.io/products/proof-of-humanity

[20] H. P. Team. (2025) Human passport developer documentation. Developer documentation. [Online]. Available: https://docs.passport.xyz/

[21] Encointer Documentation Team. (2025, aug) The encointer book. Primary documentation resource for the Encointer protocol. [Online]. Available: https://book.encointer.org/

[22] BleuIO Blog. (2022) Measuring distance with bluetooth in indoor environment using python. Blog post. [Online]. Available: https://www.bleuio.com/blog/measuring-distance-with-bluetooth-in-indoor-environment-using-python/

[23] E. Katz-Bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards IP geolocation using delay and topology measurements," in *Proceedings of the 6th ACM SIGCOMM Internet Measurement Conference (IMC)*. Rio de Janeiro, Brazil: ACM, 2006,

pp. 71–84, conference paper. [Online]. Available: https://dl.acm.org/doi/10.1145/1177080.1177090

[24] P. Sheng, V. Sevani, R. Rana, H. Tyagi, and P. Viswanath, “Bft-poloc: A byzantine fortified trigonometric proof of location protocol using internet delays,” *arXiv preprint arXiv:2403.13230*, 2024, preprint. [Online]. Available: https://arxiv.org/abs/2403.13230

[25] Self Protocol Documentation Team. (2025) Self protocol: Overview. Technical documentation (Overview). [Online]. Available: https://docs.self.xyz/technical-docs/overview

Appendix A
Further Protocols

A.1 Proof of Location Protocol

For this first in-depth attempt keeping the effort required for passport users was the main goal, only requiring a Proof of Location during pseudonym party gatherings, verifying their location within the geographic area and proofing non-attendance of gatherings.
This hybrid protocol combines ePassports with Pseudonym Parties using smartphones. During party windows, holders of an ePassport-based credential who are not attending must prove non-attendance by showing proximity absence to party devices (Bluetooth/Wi-Fi beacons) and proving presence in the geographic area via latency check.

A.1.1 Pseudonym Party

Meetings are organized every 27 days, striking a balance between effort and security, shorter intervals would increase the burden on participants, while longer intervals would weaken protection against Sybil attacks. Attendees are assigned to groups in a way that makes the composition of each meeting unpredictable, preventing collusion or manipulation. Each gathering consists of five to twelve participants, a size chosen to maintain effective oversight while avoiding excessive overhead or vulnerability to small-scale attacks. During the meeting, participants mutually verify each other's presence by scanning QR codes displayed on their devices. At the same time, their phones also scan for nearby devices belonging to ePassport registered users via Bluetooth or Wi-Fi hotspots, with the possibility of including distance estimation. [22] and set up latency tests.

A.1.2 ePassport

Registration begins with scanning the passport and generating a Zero-Knowledge Proof, following an approach similar to Self or ZKPassport. This step may optionally include an additional biometric check, such as a face scan, to further strengthen verification. From that point onward, during some or all Pseudonym Party gatherings, users are required to re-verify their passport to confirm that the legitimate owner is actively using the device. At the same time, the phone checks its proximity to the devices of other attendees, thereby providing both a Proof of Location and a Proof of Non-Attendance for those not present at the gathering.

A.1.3 Proof of Location

Location methods based on network latency vary widely in accuracy. In the best test sets, median error rates were around 67 km, though significantly lower deviations were observed for very short delays: with latencies under 4 ms, the median deviation dropped to about 15 km [23]. This approach however turns the problem in to an Approximation problem, making it computationally unfeasible for a our protocol. By contrast, other Proof of Location approaches report inaccuracies of up to 1000 km, which substantially limits their reliability.[24] It is also worth noting that most studies have been conducted in the United States, where network density is relatively low and distances between nodes are large, potentially skewing results compared to denser regions.

A.1.4 Bind Phone to Person/Passport verification

To ensure that users keep their phones with them during the Proof of Location and Proof of Non-Attendance process, they are required to rescan their passport at those verification points. This involves reading the RFID chip via the phone's NFC scanner, combined with the Machine Readable Zone (MRZ), and in some cases scanning a QR code in a browser depending on the exact protocol implementation. A key challenge is the potential cloning of passports. This risk is partially mitigated by the encryption of the chip data, which can only be decrypted using a key derived from the MRZ. Some passports also include active authentication features to further reduce the risk of cloning, though it remains unclear how easily such mechanisms can be implemented on mobile devices. The Self protocol, for example, has stated plans to integrate this in the future. [25]

Other Approaches

An alternative to repeated passport scanning would be the use of biometrics. In this model, the same biometric sample—for example, a fingerprint or face

scan—would be required at every login. Granting access to another person would mean permanently losing control of the account, as the biometric could not be changed. These checks could also be compared to the biometric data already stored on the passport to strengthen verification. However, current mobile devices often provide limited access to their biometric hardware and data, restricting the feasibility of this approach.
Another option would be to integrate lightweight humanity verification tests designed to prove that there is a human actively using the device. However, these checks are insufficient in practice, as a single person could easily complete such tests on multiple devices, undermining the principle of 'one person, one account'.

A.2 Whistleblower Protocol

This protocol aims to mitigate the risk that a single person verifying multiple accounts by reframing the problem as a question of detection rather than prevention. Instead of making it technically impossible for someone to perform Proof of Location or Humanity Verification for multiple identities, the system introduces a social and economic incentive to expose such behavior. During each verification ceremony, anyone who gains access to an account has the opportunity to report that the account holder is not the real user. If the report is valid, the reported account is restricted, and the whistleblower receives a monetary reward.

A.2.1 Pseudonym Party

Meetings are organized every 27 days, striking a balance between effort and security, shorter intervals would increase the burden on participants, while longer intervals would weaken protection against Sybil attacks. Attendees are assigned to groups in a way that makes the composition of each meeting unpredictable, preventing collusion or manipulation. Each gathering consists of five to twelve participants, a size chosen to maintain effective oversight while avoiding excessive overhead or vulnerability to small-scale attacks. During the meeting, participants mutually verify each other's presence by scanning QR codes displayed on their devices. At the same time, their phones also scan for nearby devices belonging to ePassport registered users via Bluetooth or Wi-Fi hotspots, with the possibility of including distance estimation. [22] and set up latency tests.

A.2.2 ePassport

Registration begins with scanning the passport and generating a Zero-Knowledge Proof, following an approach similar to Self or ZKPassport. This step may optionally include an additional biometric check, such as a face scan, to further strengthen verification. From that point onward, during some or all Pseudonym Party gatherings, users are required to re-verify their passport to confirm that the legitimate owner is actively using the device. At the same time, the phone checks its proximity to the devices of other attendees, thereby providing both a Proof of Location and a Proof of Non-Attendance for those not present at the gathering.

A.3 Random attendance Protocol

The Random Attendance Protocol represents a shift away from Proof of Location and Proof of Non-Attendance mechanisms by relying instead on a Partial Participation approach. In this system, users registered through ePassports demonstrate their presence and ongoing engagement by periodically attending randomly assigned Pseudonym Party meetings. This design aims to ensure that users remain active and geographically present without requiring constant surveillance or highly accurate geolocation.
To promote honest behavior and encourage long-term engagement, the protocol employs a reputation system in which the reputation directly corresponds to the voting power. Each user's reputation is evaluated in recurring cycles consisting of three meetings. This structure ensures that passport-registered users must participate in at least one gathering within each cycle in order to maintain their eligibility and influence.

A.3.1 Voting Power/Reputation

Reputation can be used to further incentivize honest behavior within the protocol. In this design, reputation is directly tied to voting power, making it a critical factor in ensuring fairness. To maintain reliability, the reputation is linked to cycles of three meetings, which guarantees that users registered through passports must attend at least one gathering within the lifespan of their reputation. This mechanism not only enforces regular participation, but also prevents users from passively maintaining influence without active engagement.

A.3.2 Passport

Registration begins with scanning the RFID chip on the passport and the machine-readable zone (MRZ), after which a Zero-Knowledge Proof is generated using a protocol similar to Self or ZKPassport. Once registered, passport users are required to attend exactly one randomly assigned meeting within each interval of x meetings. This requirement ensures that a single individual cannot easily maintain more than x accounts simultaneously, while still allowing for the possibility of limited overlaps. Failure to attend an assigned meeting results in penalties, such as the loss of voting power or temporary suspension from the protocol. The scheme can also be reinforced with whistleblowing mechanisms, where participants may report users who attempt to delegate their attendance to others, further discouraging dishonest behavior.

Withdrawing

At the beginning of each cycle, users have the option to withdraw from any number of meetings they are unable to attend. This provides flexibility while ensuring accountability. For Pseudonym Party participants, missing a meeting without prior withdrawal results in a significantly larger reputation loss than if they had withdrawn in advance. For passport users, withdrawing means that the respective meeting will not be assigned to them, but they must compensate by attending one additional meeting in the following cycle. This mechanism balances leniency for unavoidable absences with incentives to plan responsibly, discouraging misuse of the withdrawal system.

Reputation loss/gain

For passport users, each meeting attended grants one unit of reputation. If a user is assigned multiple meetings within a single cycle, this reputation is divided across them. However, failing to attend a meeting without withdrawing in advance carries a penalty: the user must attend all three meetings in the following cycle to restore their reputation.

For Pseudonym Party users, attending a gathering contributes one third of a reputation point, reflecting the three-meeting cycle. Withdrawing from a meeting in advance results in only a minor penalty, such as a deduction of one-tenth of reputation (or, depending on implementation, no penalty at all). By contrast, missing a meeting without withdrawing resets the user's reputation to zero for the entire cycle. In some variations, this penalty may even extend into the next cycle, requiring renewed attendance before reputation can be regained.

Appendix B

Calculations

B.1 Account Reactivation/Restriction

B.1.1 Longer Period

To start, we recall the formulas we derived for the simple case with a reactivation period of 1 triple. Namely, $X_n = \frac{2}{3} * X_{n-2} + \frac{2}{9} + \frac{1}{3} * X_{n-1}$ for 2 attended meetings per cycle and $X_n = \frac{1}{3} * X_{n-2} + \frac{2}{9} + \frac{2}{3} * X_{n-1}$ for 1 attended meeting per cycle.

In these formulas, the first summand corresponds to the case where there is an overlap in a cycle. In our original derivation the duration of the restriction was one cycle, so the next meeting where the adversary could obtain an advantage was 2 meetings later. Now the restriction remains for b cycles, this means that if there is an overlap, an adversary can only obtain Voting Power again after b + 1 cycles. Therefore, we replace X_{n-2} in our formulas with X_{n-1-b} giving us $X_n = \frac{2}{3} * X_{n-1-b} + \frac{2}{9} + \frac{1}{3} * X_{n-1}$ for two attended meetings per cycle and $X_n = \frac{1}{3} * X_{n-1-b} + \frac{2}{9} + \frac{2}{3} * X_{n-1}$ for o

For each $b \in \{1, 2, 3, 4, 5\}$, these series can again be proven to be descending for any n larger than some constant c. We can therefore approximate the adversary advantage in each case by calculating X_{500}.

B.1.2 No Voting Power

We first recall the formulas for longer restriction periods with $X_n = \frac{2}{3} * X_{n-1-b} + \frac{2}{9} + \frac{1}{3} * X_{n-1}$ for 2 attended meetings per cycle and $X_n = \frac{1}{3} * X_{n-1-b} + \frac{2}{9} + \frac{2}{3} * X_{n-1}$ for one attended meetings per cycle.

And we are again concerned with the first summand representing the case where there is an overlap, and therefore a restriction is triggered. With this modification, can no longer obtain voting power when a restriction is active. This means that during a restriction, the adversary actually loses out on 1 voting power per cycle the restriction is active. We therefore need to replace X_{n-1-b} in both formulas with $(X_{n-1-b} - b)$ giving us $X_n = \frac{2}{3} * (X_{n-1-b} - b) + \frac{2}{9} + \frac{1}{3} * X_{n-1}$ for two attended meetings per cycle and $X_n = \frac{1}{3} * (X_{n-1-b} - b) + \frac{2}{9} + \frac{2}{3} * X_{n-1}$ for one.

Again, for each $b \in \{1, 2, 3, 4, 5\}$, these series can again be proven to be descending for any n larger than some constant c. We can therefore approximate the adversary advantage in each case by calculating X_{500}.